

**NO SALE A  
DOMICILIO**

**UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA**

**FACULTAD DE INGENIERÍA  
DE SISTEMAS E INFORMÁTICA**



**“ANÁLISIS DE RIESGOS Y PLAN DE CONTINGENCIA PARA LA INTRANET  
Y PORTAL WEB DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA  
PERUANA”**

**INFORME PRÁCTICO DE SUFICIENCIA**

PARA OPTAR EL TÍTULO PROFESIONAL DE:

**INGENIERO DE SISTEMAS E INFORMÁTICA**

Presentado por el Bachiller:

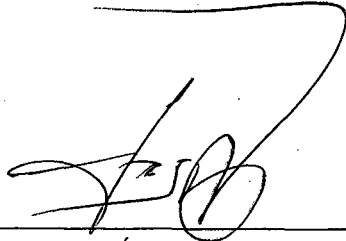
**Ytala Milagros Guadalupe Pizango**

Asesor: Ing. Luis Honorato Pita Astengo

**DONADO POR:**  
*Guadalupe Pizango Ytala M.*  
*Iquitos, 9 de 06 de 2011*

**IQUITOS – PERÚ 2010**

**INFORME TÉCNICO DEL EXAMEN DE SUFICIENCIA PREVIA  
ACTUALIZACIÓN ACADÉMICA APROBADO EN SUSTENTACIÓN PÚBLICA,  
POR EL JURADO EXAMINADOR, DESIGNADO POR EL PRESIDENTE DE LA  
COMISIÓN DE GOBIERNO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS  
E INFORMÁTICA DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA  
PERUANA.**



---

**ING. JOSÉ EDGAR GARCÍA DÍAZ**  
Presidente



---

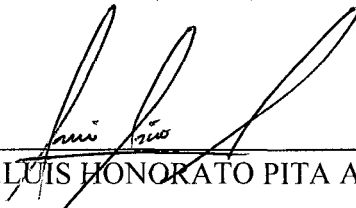
**ING. CARLOS IVÁN GARCÍA GÓMEZ**  
Miembro



---

**ING. MOISÉS HO VASQUEZ**  
Miembro

**Asesor:**



---

**ING. LUIS HONORATO PITA ASTENGO**

---

---

**DEDICO este trabajo a mis padres, por su constante y gran amor, comprensión y apoyo**

---

---

---

---

**AGRADEZCO a quienes me ayudaron en la elaboración de este trabajo, así como en la culminación de mi carrera profesional**

---

---

## RESUMEN

### ANÁLISIS DE RIESGO Y EL PLAN DE CONTINGENCIA PARA LA INTRANET Y PORTAL WEB DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

Por: Bach. Ytala Milagros Guadalupe Pizango.

La Intranet y el Portal web de la Universidad Nacional de la Amazonía Peruana, son un medio a través de la cual se publica información exclusiva de las actividades académicas y administrativas de la UNAP; por esta razón, poseen tecnologías de información y sistemas de información que están propensos a sufrir deterioros naturales o provocados; por este motivo, justifica realizar un análisis de riesgo y mediante su aplicación se obtiene información sobre los activos, sus dependencias y valoración así mismo la identificación de las amenazas a las que están expuestos dichos activos.

Para realizar el Análisis de Riesgo en la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana, se utilizó la metodología Magerit versión 2 junto con la herramienta Pilar versión 4.3. Como punto de partida para la realización del análisis se efectuó una encuesta con el responsable de la Intranet y Portal web de la UNAP, mediante la información recogida se identificó 4 grupos de activos directamente relacionados con la intranet y portal web de la UNAP, de estos 4 grupos de activos se identificaron 1018 amenazas, además se identificó que los controles existentes son pocos efectivos para la seguridad de dichos activos. El Plan de Contingencia para la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana permitirá tomar las medidas preventivas ante la posible pérdida, destrucción, robo y otras amenazas a la que están expuestas los activos, así como las medidas correctivas para garantizar la continuidad del servicio que brinda la UNAP. En conclusión el Análisis de Riesgo y Plan de Contingencia permitirá evaluar qué tan protegidos están nuestros activos y cómo recobrar rápidamente el control y restablecer la marcha normal de la institución.

Palabras claves: Análisis de riesgos, Plan de contingencia, UNAP, Amazonía, Magerit.

## ABSTRACT

### RISK ANALYSIS AND CONTINGENCY PLAN FOR THE INTRANET AND WEB PORTAL OF THE NATIONAL UNIVERSITY OF THE PERUVIAN AMAZON

By: Bach. Milagros Guadalupe Ytala Pizango.

Intranet and Web Portal of the National University of the Peruvian Amazon are a means where the information of the academic and administrative activities of the UNAP is published. For this reason, they have information technologies and information systems but they are exposed to natural disasters or induced damage. For that, it is necessary a risk analysis to get by applying information on assets, their dependencies and the same valuation and identification of threats to exposed assets.

The methodology used to perform risk analysis of the Intranet and Web Portal of the National University of the Peruvian Amazon was Magerit version 2 and Pilar tool version 4.3. The first stage of a risk analysis was to make a survey with the head of the Intranet and Web Portal UNAP, through information collection were identified 4 group of assets directly related to the intranet and web portal UNAP. Of these 4 groups of assets were identified 1018 threats also identified that existing controls are few troops for the security of those assets. The Contingency Plan for the Intranet and Web Portal of the National University of the Peruvian Amazon will take preventive measures in the face of loss, destruction, stealing and other threats that are exposed assets and corrective measures to ensure continuity of service offered by the UNAP.

In conclusion Risk Analysis and Contingency Plan will assess how our assets are protected and how quickly regain control and restore the normal functioning of the institution.

Keywords: Risk, Analysis, Contingency Plan, UNAP, Amazon, Magerit.

## ÍNDICE GENERAL

Dedicatoria	
Agradecimientos	
Resumen .....	i
Abstract .....	ii
Índice General .....	iii
Índice de Tablas y Cuadros .....	v
Índice de Figuras .....	vi
Sección I: Datos generales	
1. Título .....	01
2. Área de desarrollo .....	01
3. Generalidades de la Institución .....	01
3.1. Razón Social .....	01
3.2. Ubicación de la empresa .....	01
3.3. Organigrama funcional .....	01
3.4. Funciones Generales de la Oficina o Área .....	02
4. Bachiller .....	04
5. Asesor .....	04
6. Colaboradores .....	04
7. Duración estimada de ejecución del proyecto .....	04
8. Presupuesto estimado .....	04
Sección II: Visión General de la Solución Propuesta.	
Capítulo I: Introducción	
1.1. Contexto .....	05
1.2. Problemática objeto de la aplicación .....	05
1.3. Objetivos del proyecto .....	05
1.3.1. Objetivo general .....	05
1.3.2. Objetivos específicos .....	06
Capítulo II: Descripción del diseño de la solución (Producto)	
2.1. Técnicas de recolección de datos .....	07
2.2. Metodología y herramientas a emplear .....	07
2.2.1. Metodología .....	07
2.2.2. Herramientas .....	07
2.3. Descripción del desarrollo de la solución .....	07
2.4. Indicadores de evaluación de la solución .....	07
2.5. Relación de Entregables .....	07
2.6. Planificación y cronograma del proyecto .....	08
Capítulo III: Desarrollo de la Solución Propuesta	
3.1. Planificación proyecto .....	09
3.1.1. Determinación del dominio y límite .....	09
3.1.2. Estimación de las dimensiones .....	10

3.2. Análisis de riesgos .....	11
3.2.1. Caracterización de los activos .....	11
3.2.1.1. Identificación de activos .....	11
3.2.1.2. Dependencia de activos .....	12
3.2.1.3. Valoración de activos .....	16
3.2.2. Caracterización de las amenazas .....	20
3.2.2.1. Identificación de amenazas .....	20
3.2.2.2. Valoración de amenazas .....	38
3.2.3. Caracterización de las salvaguardas .....	60
3.2.3.1. Identificación de salvaguardas .....	60
3.2.3.2. Valoración de salvaguardas .....	62
3.2.4. Caracterización del impacto.....	71
3.2.4.1. Impacto acumulado .....	71
3.2.4.2. Impacto repercutido .....	79
3.2.5. Caracterización del riesgo .....	85
3.2.5.1. Riesgo acumulado .....	85
3.2.5.2. Riesgo repercutido .....	93
3.3. Gestión de Riesgos .....	99
3.3.1. Plan de contingencia .....	99
3.3.1.1. Servicios internos .....	99
3.3.1.2. Equipamiento .....	100
3.3.1.2.1. Aplicaciones.....	100
3.3.1.2.2. Equipos .....	101
3.3.1.2.3. Comunicaciones .....	111
3.3.1.2.4. Elementos auxiliares .....	113
3.3.1.3. Personal .....	115
3.3.1.4. Instalación.....	116
Capítulo IV: Resultados y su discusión.....	119
Capítulo V: Conclusiones .....	120
Capítulo VI: Recomendaciones .....	121
Bibliografía .....	122
Anexos .....	125
Anexo 01: Estimación del costo del proyecto .....	125
Anexo 02: Cuestionario .....	127
Anexo 03: Observación directa .....	129
Anexo 04: Descripción de la metodología.....	130
Anexo 05: Glosario.....	133
Anexo 06: Formatos.....	136

## ÍNDICE DE TABLAS Y CUADROS

Cuadro 01: Presupuesto estimado .....	04
Cuadro 02: Valoración de activos - Servicios internos. ....	16
Cuadro 03: Valoración de activos - Equipamiento. ....	17
Cuadro 04: Valoración de activos - Personal. ....	19
Cuadro 05. Valoración de amenazas - Correo electrónico de docentes. ....	39
Cuadro 06. Valoración de amenazas - Intranet de docentes. ....	40
Cuadro 07. Valoración de amenazas - Sistema de gestión académica. ....	41
Cuadro 08. Valoración de amenazas - Windows Server 2003. ....	42
Cuadro 09. Valoración de amenazas - FreeBSD. ....	43
Cuadro 10. Valoración de amenazas - UNIX. ....	44
Cuadro 11. Valoración de amenazas - Apache. ....	45
Cuadro 12. Valoración de amenazas - Servidor de aplicaciones y Base de datos. ....	46
Cuadro 13. Valoración de amenazas - Servidor de Correo. ....	47
Cuadro 14. Valoración de amenazas – Firewall. ....	48
Cuadro 15. Valoración de amenazas – Servidor DMZ. ....	49
Cuadro 16. Valoración de amenazas – Switch core. ....	50
Cuadro 17. Valoración de amenazas – Punto de acceso wireless. ....	51
Cuadro 18. Valoración de amenazas – Switch 3 com. ....	52
Cuadro 19. Valoración de amenazas – Servidor de Backup. ....	53
Cuadro 20. Valoración de amenazas – Red inalámbrica. ....	54
Cuadro 21. Valoración de amenazas – Red Lan. ....	55
Cuadro 22. Valoración de amenazas – Sistema de alimentación ininterrumpida. ....	56
Cuadro 23. Valoración de amenazas – Cable UTP. ....	56
Cuadro 24. Valoración de amenazas – Fibra óptica. ....	57
Cuadro 25. Valoración de amenazas – Transformador de aislamiento. ....	57
Cuadro 26. Valoración de amenazas – Administrador de sistemas y Base de datos. ....	58
Cuadro 27. Valoración de amenazas – Administrador de comunicaciones. ....	58
Cuadro 28. Valoración de amenazas – Operadores. ....	59
Cuadro 29. Valoración de amenazas – Edificio Herbario. ....	59
Cuadro 30. Valoración de las salvaguardas – Protecciones generales. ....	63
Cuadro 31. Valoración de las salvaguardas – Protección de los servicios. ....	64
Cuadro 32. Valoración de las salvaguardas – Protección de la información. ....	64
Cuadro 33. Valoración de las salvaguardas – Protección de las aplicaciones informáticas..	65
Cuadro 34. Valoración de las salvaguardas – Protección de los equipos informáticos.....	66
Cuadro 35. Valoración de las salvaguardas – Protección de las comunicaciones. ....	67
Cuadro 36. Valoración de las salvaguardas – Elementos auxiliares. ....	68
Cuadro 37. Valoración de las salvaguardas – Protección de las instalaciones.. ....	68
Cuadro 38. Valoración de las salvaguardas – Gestión del Personal.....	69
Cuadro 39. Valoración de las salvaguardas – Organización. ....	69
Cuadro 40. Valoración de las salvaguardas – Relaciones externas.. ....	70
Cuadro 41. Impacto acumulado – disponibilidad - Servicios internos.. ....	71
Cuadro 42. Impacto acumulado - disponibilidad – Equipamiento ....	72
Cuadro 43. Impacto acumulado - disponibilidad - Personal ....	72
Cuadro 44. Impacto acumulado - disponibilidad - Instalaciones ....	72
Cuadro 45. Impacto acumulado - integridad de los datos - Servicios ....	73
Cuadro 46. Impacto acumulado - integridad de los datos - Equipamiento.....	73
Cuadro 47. Impacto acumulado - integridad de los datos - Personal ....	74



Cuadro 48. Impacto acumulado - integridad de los datos - Instalaciones.....	74
Cuadro 49. Impacto acumulado - confidencialidad de los datos - Servicios internos. ....	74
Cuadro 50. Impacto acumulado - confidencialidad de los datos – Equipamiento .....	75
Cuadro 51. Impacto acumulado - confidencialidad de los datos – Personal .....	75
Cuadro 52. Impacto acumulado - confidencialidad de los datos – Instalaciones . ....	75
Cuadro 53. Impacto acumulado - autenticidad de los usuarios - Servicios . ....	76
Cuadro 54. Impacto acumulado - autenticidad de los usuarios - Equipamiento . ....	76
Cuadro 55. Impacto acumulado - autenticidad de los usuarios - Personal . ....	77
Cuadro 56. Impacto acumulado - autenticidad de los usuarios - Instalaciones .....	77
Cuadro 57. Impacto acumulado - trazabilidad del servicio - Servicios internos .....	77
Cuadro 58. Impacto acumulado - trazabilidad del servicio – Equipamiento .....	78
Cuadro 59. Impacto acumulado - trazabilidad del servicio – Personal .....	78
Cuadro 60. Impacto acumulado - trazabilidad del servicio – Instalaciones .....	78
Cuadro 61. Impacto repercutido - disponibilidad - Servicios internos .....	79
Cuadro 62. Impacto repercutido - disponibilidad – Equipamiento .....	80
Cuadro 63. Impacto repercutido - disponibilidad – Personal .....	80
Cuadro 64. Impacto repercutido - integridad de los datos - Servicios internos .....	81
Cuadro 65. Impacto repercutido - integridad de los datos – Equipamiento .....	81
Cuadro 66. Impacto repercutido - integridad de los datos – Personal .....	81
Cuadro 67. Impacto repercutido - confidencialidad de los datos - Servicios internos. ....	82
Cuadro 68. Impacto repercutido - confidencialidad de los datos - Equipamiento .....	82
Cuadro 69. Impacto repercutido - confidencialidad de los datos – Personal .....	83
Cuadro 70. Impacto repercutido - autenticidad de los usuarios - Servicios internos .....	83
Cuadro 71. Impacto repercutido - autenticidad de los usuarios – Equipamiento .....	83
Cuadro 72. Impacto repercutido - autenticidad de los usuarios- Personal .....	84
Cuadro 73. Impacto repercutido - trazabilidad del servicio - Servicios internos .....	84
Cuadro 74. Impacto repercutido - trazabilidad del servicio – Equipamiento .....	84
Cuadro75. Impacto repercutido - trazabilidad del servicio – Personal .....	85
Cuadro76. Riesgo acumulado - disponibilidad - Servicios internos .....	86
Cuadro77. Riesgo acumulado - disponibilidad – Equipamiento .....	86
Cuadro78. Riesgo acumulado - disponibilidad - Personal .....	86
Cuadro79. Riesgo acumulado - disponibilidad – Instalación .....	87
Cuadro80. Riesgo acumulado - integridad de los datos - Servicios internos .....	87
Cuadro81. Riesgo acumulado - integridad de los datos – Equipamiento .....	87
Cuadro82. Riesgo acumulado - integridad de los datos – Personal .....	88
Cuadro83. Riesgo acumulado - integridad de los datos – Instalación .....	88
Cuadro84. Riesgo acumulado - confidencialidad de los datos - Servicios internos .....	88
Cuadro85. Riesgo acumulado - confidencialidad de los datos – Equipamiento .....	89
Cuadro86. Riesgo acumulado - confidencialidad de los datos – Personal .....	89
Cuadro87. Riesgo acumulado - confidencialidad de los datos – Instalación .....	89
Cuadro88. Riesgo acumulado - autenticidad de los usuarios - Servicios internos .....	90
Cuadro89. Riesgo acumulado - autenticidad de los usuarios – Equipamiento .....	90
Cuadro90. Riesgo acumulado - autenticidad de los usuarios- Personal .....	91
Cuadro91. Riesgo acumulado - autenticidad de los usuarios – Instalación .....	91
Cuadro92. Riesgo acumulado - trazabilidad del servicio - Servicios internos .....	91
Cuadro93. Riesgo acumulado - trazabilidad del servicio – Equipamiento .....	92
Cuadro94. Riesgo acumulado - trazabilidad del servicio – Personal .....	92
Cuadro95. Riesgo acumulado - trazabilidad del servicio – Instalaciones .....	92
Cuadro96. Riesgo repercutido - disponibilidad - Servicios internos .....	93
Cuadro97. Riesgo repercutido - disponibilidad – Equipamiento .....	94

Cuadro98. Riesgo repercutido - disponibilidad - Personal .....	94
Cuadro99. Riesgo repercutido - integridad de los datos - Servicios internos .....	95
Cuadro100. Riesgo repercutido - integridad de los datos – Equipamiento .....	95
Cuadro101. Riesgo repercutido - integridad de los datos – Personal .....	95
Cuadro102. Riesgo repercutido - confidencialidad de los datos - Servicios internos .....	96
Cuadro103. Riesgo repercutido - confidencialidad de los datos - Equipamiento .....	96
Cuadro104. Riesgo repercutido - confidencialidad de los datos – Personal .....	96
Cuadro105. Riesgo repercutido - autenticidad de los usuarios - Servicios internos .....	97
Cuadro106. Riesgo repercutido - autenticidad de los usuarios – Equipamiento .....	97
Cuadro107. Riesgo repercutido - autenticidad de los usuarios – Personal .....	97
Cuadro108. Riesgo repercutido - trazabilidad del servicio - Servicios internos .....	98
Cuadro109. Riesgo repercutido - trazabilidad del servicio – Equipamiento .....	98
Cuadro110. Riesgo repercutido - trazabilidad del servicio - Personal .....	98
Cuadro111. Estimación de costos en recursos humanos .....	125
Cuadro112. Estimación de costos en software .....	125
Cuadro113. Estimación de costos en hardware.....	125
Cuadro114. Estimación de costos varios .....	125

## ÍNDICE DE FIGURAS

Figura 01: Organigrama funcional .....	01
Figura 02: Cronograma de actividades .....	08
Figura 03: Dominio y límite .....	09
Figura 04: Servicios internos y su dependencia de activos. ....	12
Figura 05: Aplicaciones y su dependencia de activos. ....	12
Figura 06: Equipos y su dependencia de activos. ....	13
Figura 07: Equipos y su dependencia de activos(continuación). ....	14
Figura 08: Comunicaciones y su dependencia de activos. ....	15
Figura 09: Identificación de amenazas - Servicios interno - Correo electrónico. ....	20
Figura 10: Identificación de amenazas - Servicios interno - Intranet de docentes. ....	21
Figura 11: Identificación de amenazas - Servicios interno - Sistemas gestión académica. ..	21
Figura 12: Identificación de amenazas - Aplicaciones - Windows Server 2003 .....	22
Figura 13: Identificación de amenazas - Aplicaciones - FreeBSD. ....	23
Figura 14: Identificación de amenazas - Aplicaciones - Unix. ....	24
Figura 15: Identificación de amenazas - Aplicaciones - Apache. ....	24
Figura 16: Identificación de amenazas - Equipos -Servidor de aplicaiones y Base de datos	25
Figura 17: Identificación de amenazas - Equipos - Servidor de correo. ....	26
Figura 18: Identificación de amenazas - Equipos - Firewall. ....	27
Figura 19: Identificación de amenazas - Equipos – Servidor DMZ. ....	28
Figura 20: Identificación de amenazas - Equipos – Switch core. ....	28
Figura 21. Identificación de amenazas - Equipos – Punto de acceso wireless. ....	29
Figura 22. Identificación de amenazas - Equipos – Switch 3 com .....	30
Figura 23. Identificación de amenazas - Equipos – Servidor de Backup. ....	31
Figura 24. Identificación de amenazas - Comunicaciones - Red inalámbrica .....	32
Figura 25. Identificación de amenazas - Comunicaciones - Red Lan .....	33
Figura 26. Identificación de amenazas - Elementos auxiliares – UPS. ....	34
Figura 27. Identificación de amenazas - Elementos auxiliares Cable UTP .....	34
Figura 28. Identificación de amenazas - Elementos auxiliares - Fibra óptica. ....	35
Figura 29. Identificación de amenazas - Elementos auxiliares - Transformador. ....	35
Figura 30. Identificación de amenazas- Personal- Administrador de sistemas y BD.....	36
Figura 31. Identificación de amenazas- Personal- Administrador de comunicaciones. ....	36
Figura 32. Identificación de amenazas- Personal- Operadores de comunicaciones. ....	36
Figura 33. Identificación de amenazas- Instalaciones. ....	37

## SECCIÓN I: DATOS GENERALES

### 1. Título:

Análisis de Riesgos y Plan de Contingencia para la Intranet y Portal Web de la UNAP – Iquitos, Perú – 2009.

### 2. Área de desarrollo:

- Seguridad de las Tecnologías de Información y Comunicaciones.

### 3. Generalidades de la Institución:

#### 3.1. Razón Social:

Universidad Nacional de la Amazonía Peruana – Facultad de Ingeniería de Sistemas e Informática.

#### 3.2. Ubicación de la empresa:

- o Dirección Fiscal de la Institución:
  - Av. Grau # 1072 – Iquitos.
- o Dirección de la Jefatura responsable:
  - Jr. Tacna # 173 – Iquitos.
- o Dirección del Área donde se desarrolló el trabajo práctico:” Oficina de Comunicaciones de la UNAP”
  - Calle Nanay con Pevas

#### 3.3. Organigrama funcional:

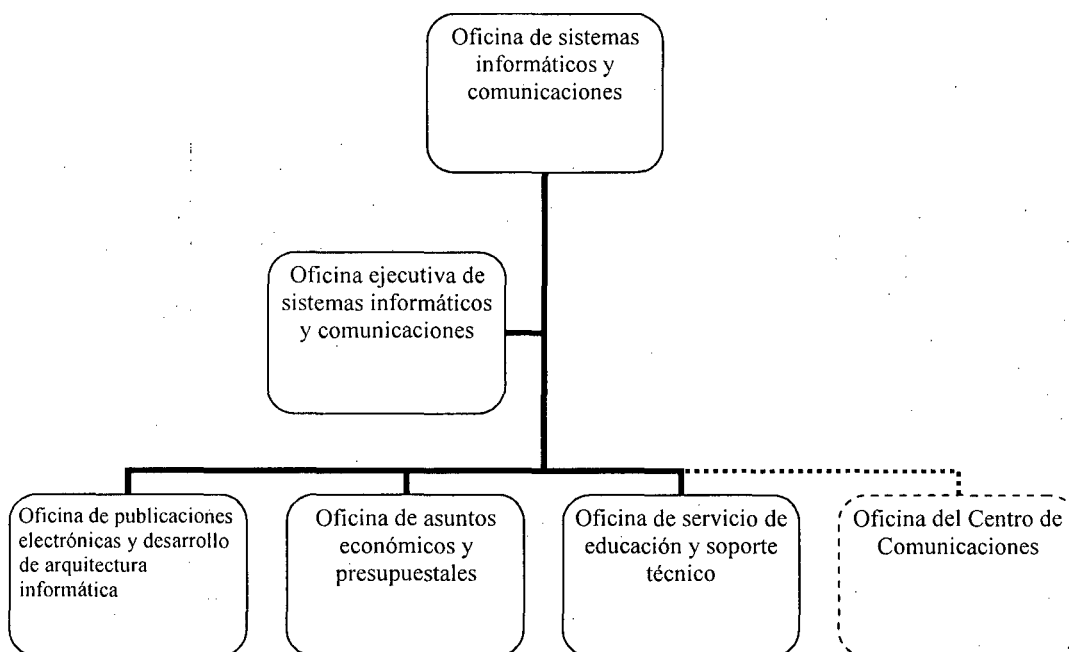


Figura 01. Organigrama funcional

Fuente. Elaboración propia

### **3.4. Funciones Generales de la Oficina o Área:**

#### **Oficina de Sistemas Informáticos y Comunicaciones:**

- Establecer y ejecutar el Plan operativo informático de la Institución.
- Formular y desarrollar el plan de sistemas de información y tecnologías de la información de conformidad con el plan operativo informático.
- Coordinar, supervisar y evaluar el Plan anual de mantenimiento de recursos informáticos.
- Autorizar los gastos y fiscalizar la ejecución del presupuesto de la OSIC en concordancia con el Plan operativo.
- Coordinar con las instancias correspondientes la cantidad y monto de las adquisiciones de hardware y software e insumos informáticos que requiera la institución.
- Informar mensualmente al Rectorado y las instancias que lo requieran la cantidad y calidad/rapidez de los servicios prestados a través de la OSIC.
- Asesorar a la alta dirección y áreas de la UNAP en temas informáticos.
- Cumplir con las normas y procedimientos establecidos en el EGUNAP, MOF Y ROF institucional.
- Evaluar y atender solicitudes de servicios informáticos con carácter de urgencia y temporales a las facultades y áreas administrativas de la institución.
- Exponer y justificar la distribución y/o redistribución de los recursos informáticos ante las instancias que así lo requieran.
- Proponer, evaluar y establecer convenios con instituciones de prestigio local, nacional y/o internacional.
- Cautelar la adecuada conservación y renovación de los bienes informáticos de la institución.
- Coordinar el envío y recepción de información externa e interna de la OSIC.
- Coordinar pruebas para recuperación de desastres, robos y otros.
- Formular soluciones integrales a problemas permanentes y temporales.

#### **Oficina Ejecutiva de Sistemas Informáticos y Comunicaciones:**

- Asesorar al jefe de la OSIC en la formulación de presupuestos de proyectos informáticos de las distintas áreas de la OSIC.
- Planificar y ejecutar el inventario de bienes e inmuebles de la OSIC en coordinación con la oficina de control patrimonial de la OGA.
- Planificar y ejecutar el inventario informático en coordinación con las áreas de la OSIC.
- Brindar la orientación a todo el personal que ingresa a la OSIC.

**Oficina de Publicaciones Electrónicas y Desarrollo de Arquitectura Informática:**

- Identificar, analizar y seleccionar la información requerida para un proyecto de desarrollo de una página Web.
- Desarrollar y administrar proyectos en base a recursos y tiempos.
- Verificar que la información publicada sigue los procedimientos estándares y políticas de control de unidad organizacional.
- Trabajar con el webmaster para asegurar disponibilidad apropiada, control de acceso y copias de seguridad de los archivos.
- Identificar y administrar los ciclos de validación de la información necesaria.

**Oficina de Asuntos Económicos y Presupuestales:**

- Formular y ejecutar el presupuesto anual de la oficina de sistemas informáticos y comunicaciones en coordinación con la jefatura y demás oficinas de la OSIC.
- Elaborar el manual de procedimientos administrativos y directivas internas de la OSIC.
- Llevar el control de los ingresos y gastos de la OSIC.
- Procesar y elaborar los documentos de gestión de la OSIC, que requieren la oficinas generales de planificación y presupuesto, administración OGA, personal OGPER y vicerrectorado.
- Preparar y elaborar los compromisos de la OSIC mensualmente, para ser tramitados ante la OGA.

**Oficina de Servicio de Educación y Soporte Técnico:**

- Organizar, dirigir y controlar el funcionamiento de los laboratorios de la OSIC.
- Coordinar con las facultades la disposición y programación del uso de los laboratorios de la OSIC.
- Planificar, determinar los costos de mantenimientos y uso de los laboratorios que las facultades aportarán para el mantenimiento de los mismos.
- Planificar y ejecutar un cronograma de capacitación mensual, semestral y anual de acuerdo a las necesidades de la institución y el avance de las tecnologías de la información.
- Dirigir, organizar y supervisar la emisión de los cursos y carreras de educación a distancia vía Internet en coordinación con las facultades.
- Programar cursos de capacitación en temas específicos de informática.
- Establecer un cronograma de actividades respecto al servicio de soporte técnico.
- Realizar el seguimiento de las tareas encomendadas al personal de soporte técnico.
- Registrar y controlar el servicio de soporte técnico atendido para realizar la estadística de atenciones previa presentación del reporte de intervención técnica.
- Revisar y realizar mantenimiento correctivo permanente a los equipos informáticos de los laboratorios de la OSIC.

**4. Bachiller:**

- Guadalupe Pizango, Ytala Milagros. Bachiller de la Facultad de Ingeniería de Sistemas e Informática.

**5. Asesor:**

- Ing. Pita Astengo, Luis Honorato. Docente de la Facultad de Ingeniería de Sistemas e Informática.

**6. Colaboradores:**

- Ing. Perdiz Dávila, José. Jefe de la Oficina de Sistemas Informáticos y Comunicaciones.
- Ing. Díaz Montenegro, Marvin. Asistente de la Oficina de Sistemas Informáticos y Comunicaciones.
- Ing. Tenazoa Rivera Mary, Roylith. Responsable de las actualizaciones en el Portal de la UNAP.

**7. Duración estimada de ejecución del proyecto:**

La duración del Proyecto a desarrollarse será de 16 semanas, las fechas de inicio de las actividades será el 1 de octubre del 2009.

**8. Presupuesto estimado:**

Estimación del presupuesto general para el desarrollo del análisis de riesgos. Ver presupuesto detallado en anexo #1.

Descripción	Cantidad	Costo (Unidad)	Costo Total (Soles)
<b>Bienes</b>			
Equipos de cómputo			
Pc de escritorio*	1	2,300.00	2,300.00
Impresora			
Inyección de Tinta *	1	200.00	200.00
<b>Insumos</b>			
Material procesamiento automático de datos			
Memoria USB 2 Gb	1	80.00	80.00
Material de escritorio			
Papel Bond 80 gramos / millar	2	35.00	70.00
Materiales de impresión			
Cartuchos tinta B/N	1	50.00	50.00
Cartucho tinta color	1	100.00	100.00
<b>Software</b>			
Software: Pilar versión 4.3*	1	1,614.84	1,614.84
<b>Otros</b>			
Asesor	1	300.00	300.00
<b>TOTAL</b>			<b>4714,84</b>

Cuadro 01. Presupuesto estimado

Fuente. Elaboración propia

\* Los bienes son de propiedad del desarrollador del trabajo práctico.

\* La licencia del software ha sido proporcionado por el creador del software como una licencia educativa.

## SECCIÓN II: DESARROLLO DEL TEMA

### Capítulo I: Introducción.

El presente informe final titulado “ANÁLISIS DE RIESGOS Y PLAN DE CONTINGENCIA PARA LA INTRANET Y PORTAL WEB DE LA UNAP”, es de gran importancia porque permite cumplir con la segunda etapa del Programa de Titulación por Examen de Suficiencia (PESPC II) previa Actualización Académica para obtener el título profesional de Ingeniero de Sistemas e Informática, mediante la realización del análisis arriba mencionado. Este informe fue desarrollado por la Bach. YTALA MILAGROS GUADALUPE PIZANGO.

El desarrollo del trabajo práctico se realizó entre el 01 de octubre de 2009 al 20 de enero de 2010, este informe final se concluyó el 29 de enero de 2010, en el distrito de Iquitos, provincia de Maynas, departamento de Loreto.

La importancia del desarrollo de este análisis está en que permitirá identificar los activos, las amenazas y las salvaguardas, y por consiguiente, desarrollar un Plan de contingencia para la Intranet y el Portal web de la UNAP, actualmente no existe un Plan de Contingencia y esto ocasiona que los activos se encuentren propensos a sufrir daños. Es por tal motivo e importancia que se realizó el ANALISIS DE RIESGOS Y PLAN DE CONTINGENCIA PARA LA INTRANET Y PORTAL WEB DE LA UNAP para dar solución a la identificación de riesgos. El análisis de riesgos permitirá los siguientes aspectos: la identificación, dependencia y valoración de activos, la identificación de amenazas, la valoración de amenazas, la identificación de salvaguardas, la valoración de salvaguardas, la estimación del impacto y la estimación del riesgo.

El plan de contingencia permitirá los siguientes aspectos: medidas preventivas y correctivas de los activos mencionados en el análisis. El problema queda planteado de la siguiente manera: ¿Es necesario el análisis de riesgo y plan de contingencia para la intranet y el portal web de la Unap?. Para el análisis de riesgo y plan de contingencia se utilizó la metodología Magerit, por ser un método formal para investigar los riesgos que soportan los sistemas de información.

#### 1.1. Contexto:

La Intranet y el Portal Web de Universidad Nacional de la Amazonía Peruana, se encuentra situado dentro del Centro de Comunicaciones de la UNAP, el mismo que se encuentra en la



segunda planta del edificio Herbario, el cual se ubica en la intercepción de las calles Pevas con Nanay.

Esta área se encarga de mantener informado a la comunidad universitaria sobre las actividades académico-administrativas de la UNAP, brindando los servicios de Correo de docentes, Intranet de docentes y el Sistema de gestión académica.

Además, esta área tiene la responsabilidad de la continua comunicación entre las sedes y la seguridad de la misma.

## **1.2. Problemática objeto de la aplicación:**

La Intranet y el Portal Web de la Universidad Nacional de la Amazonía Peruana cuenta con activos; y como todo activo, están propensos a sufrir daños; por tal motivo, se hace necesario realizar un análisis de riesgos, para saber a qué amenazas están expuestos dichos activos, y por consiguiente, desarrollar un plan de contingencia que pretenda reducir la posibilidad de ocurrencia de las amenazas encontradas. Actualmente en la intranet y portal web de la UNAP existen normas y procedimientos que cubren distintos aspectos de la seguridad de los activos pero se carece en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y determinación de controles para aminorar los mismos.

## **1.3. Objetivos del proyecto:**

### **1.3.1. Objetivo General:**

Con la elaboración del Análisis de Riesgo para la intranet y portal web de la Universidad Nacional de la Amazonía Peruana, se podrán identificar los activos, amenazas y salvaguardas con los que cuenta el área y a través del Plan de Contingencia, reducir o eliminar los riesgos a que son propensos dichos activos.

### **1.3.2. Objetivos Específicos:**

- Identificar los activos y su valoración para la intranet y portal web de la UNAP.
- Determinar a qué amenazas están expuestos dichos activos y estimar su valor.
- Determinar qué salvaguardas hay dispuestas y cuan eficaces son frente al riesgo y estimar su valor.
- Plantear las salvaguardas apropiadas que pretenda impedir la ocurrencia de las amenazas, o en su defecto, minimizar el impacto de dicha ocurrencias.
- Elaborar un plan de contingencia para la recuperación de los servicios en caso de que se materialice las amenazas.

## **Capítulo II: Descripción del diseño de la solución (Producto):**

### **2.1. Técnicas de recolección de datos:**

Para el levantamiento inicial de información se utilizó las técnicas de:

- Encuesta(ver anexo #2)
- Observación directa(ver anexo #3)

### **2.2. Metodología y herramientas a emplear:**

#### **2.2.1. Metodología / Estándar / Normatividad:**

MAGERIT - versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

#### **2.2.2. Herramientas:**

Pilar versión 4.3, herramienta automatizada de análisis de riesgo.

- o Ver características de la metodología y herramienta en el anexo #4

### **2.3. Descripción del desarrollo de la solución:**

Al contar el área con un Plan de Contingencia le permitirá reducir la posibilidad de ocurrencia de las amenazas a sus activos y desarrollar los procedimientos de recuperación a seguir en caso de que dichas amenazas se materialicen.

Además con el análisis de riesgo se identificarán los activos relevantes para el área, su interrelación y su valor, las amenazas a que están expuestos los activos y las salvaguardas que existen y cuan eficaces son frente al riesgo.

### **2.4. Indicadores de evaluación de la solución:**

Debido a que no existe ningún Análisis de riesgos y Plan de contingencia actual, no es posible comparar entre antes y después de la aplicación del Trabajo Práctico, pero una vez que se tenga desarrollado, la Intranet y el Portal web de la UNAP tendrá a su disposición los siguientes documentos técnicos:

- Lista de activos
- Lista de amenazas
- Lista de salvaguardas
- Lista de impacto por grupo de activos



### Capítulo III: Desarrollo de la Solución Propuesta.

#### 3.1. Planificación

##### 3.1.1. Determinación del dominio y límites

El Análisis de Riesgo y Plan de Contingencia englobará:

- Los equipos de hardware (servidores, firewall y switches), software (sistema de backup y servidores), de red (punto de acceso wireless y firewall) y comunicaciones (conexión inalámbrica, red Lan) que intervienen para el correcto funcionamiento de la Intranet y Portal Web de la Universidad Nacional de la Amazonía Peruana, los mismos que se encuentran ubicados dentro del Centro de Comunicaciones de la UNAP.
- Todos los activos que no se encuentran dentro del dominio especificado estará exonerado del estudio.

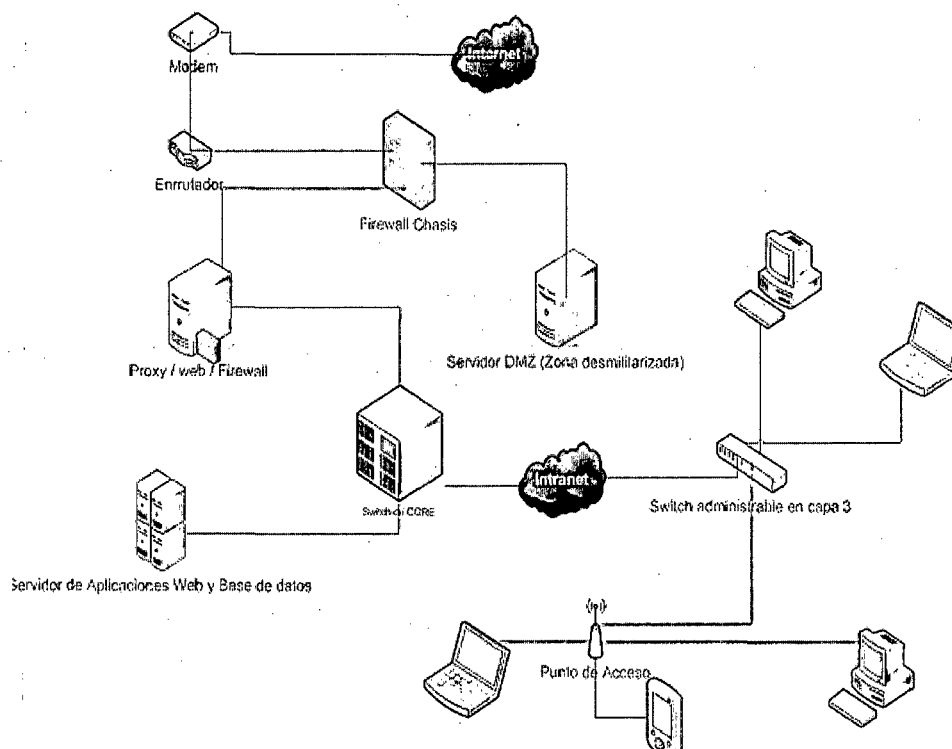


Figura 03. Dominio y Límite  
Fuente. Elaboración propia

### 3.1.2. Estimación de las dimensiones

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

Un activo puede estimar diferentes dimensiones:

- [D] disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- [I] integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
- [C] confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
- [A] autenticidad de los usuarios y la información: ¿qué perjuicio causaría no saber exactamente quién hace o ha hecho cada cosa?
- [T] trazabilidad del servicio y de los datos: ¿qué daño causaría no saber a quién se le presta tal servicio? ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

## 3.2. Análisis de riesgos

### 3.2.1. Caracterización de los activos

#### 3.2.1.1. Identificación de los activos

Los activos se agrupan según:

##### **[IS] Servicios internos**

- [email] Correo electrónico de docentes
- [intd] Intranet de docentes
- [sga] Sistema de gestión académica

##### **[E] Equipamiento**

###### **[SW] Aplicaciones**

- [WS] Windows Server 2003
- [FB] FreeBSD
- [SBA] UNIX
- [AS] Apache

###### **[HW] Equipos**

- [SA] Servidor de aplicaciones y Base de Datos
- [SC] Servidor de correo
- [FR] Firewall
- [SDM] Servidor DMZ
- [SWC] Switch Core
- [WA] Punto de acceso wireless
- [SW3] Switch 3 Com
- [SBC] Servidor de Backup

###### **[COM] Comunicaciones**

- [RADIO] Red inalámbrica
- [LAN] Red Lan

###### **[AUX] Elementos auxiliares**

- [UPS] Sistema de alimentación ininterrumpida
- [WIRE] Cable UTP
- [FIBER] Fibra óptica
- [TRA] Transformador de aislamiento

###### **[P] Personal**

- [ADSD] Administrador de sistemas y Base de datos
- [ADCO] Administrador de comunicaciones
- [OP] Operadores

###### **[IN] Instalación**

- [EH] Edificio Herbario
- [AC] Almacén Central
- [FQ] Facultad Química
- [FD] Facultad Derecho
- [ZA] Zungarococha- Facultad Agronomía

### 3.2.1.2. Dependencia de activos

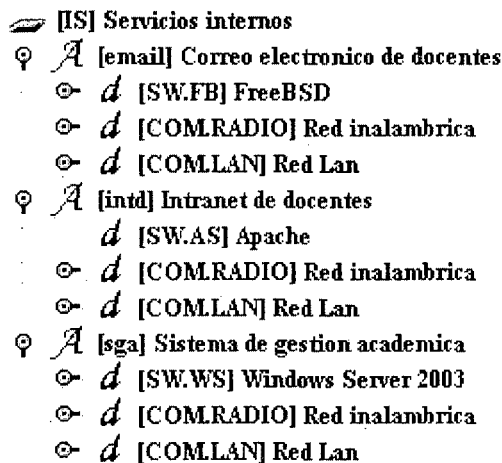


Figura 04. Servicios internos y su dependencia de activos  
Fuente. Elaboración propia

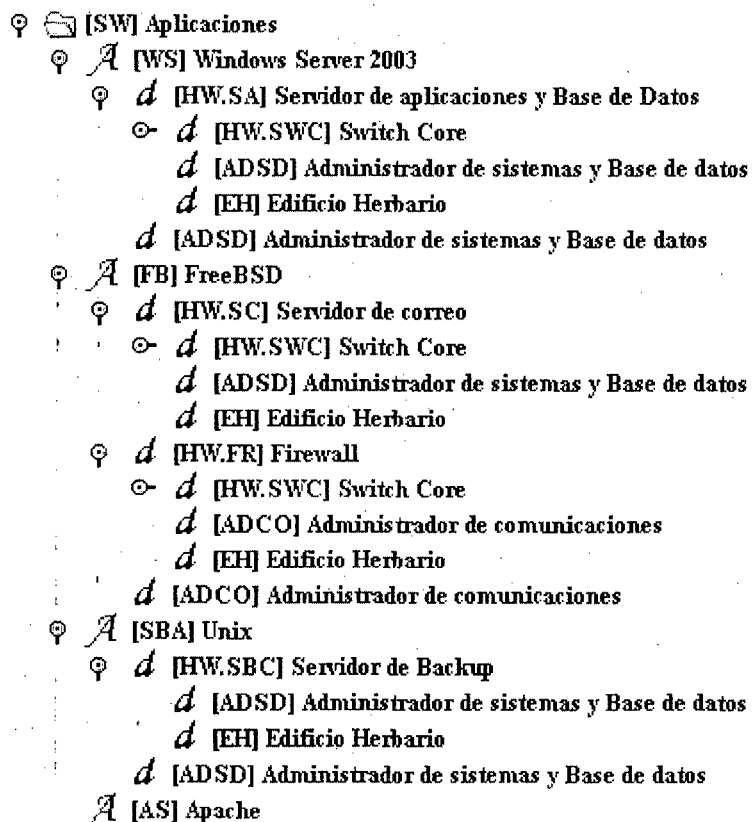


Figura 05. Aplicaciones y su dependencia de activos  
Fuente. Elaboración propia

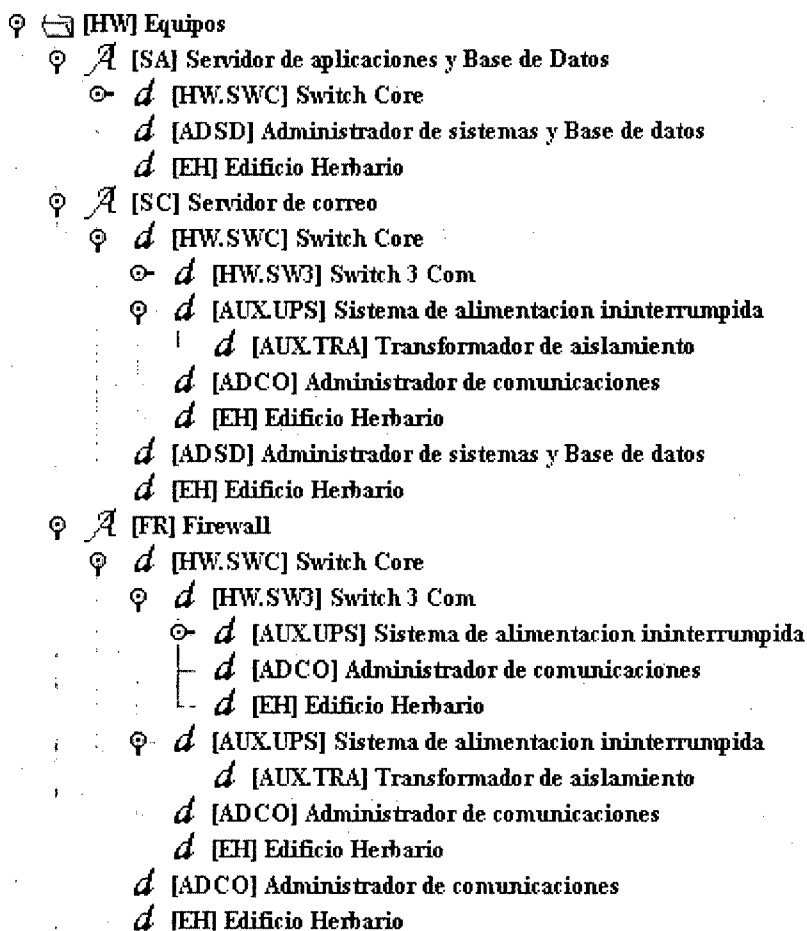


Figura 06. Equipos y su dependencia de activos  
Fuente. Elaboración propia



- ⊙ *A* [SDM] Servidor DMZ
  - ⊙ *d* [HW.FR] Firewall
    - ⊙ *d* [HW.SWC] Switch Core
      - ⊙ *d* [HW.SW3] Switch 3 Com
    - ⊙ *d* [AUX.UPS] Sistema de alimentacion ininterrumpida
      - d* [AUX.TRA] Transformador de aislamiento
      - d* [ADCO] Administrador de comunicaciones
      - d* [EH] Edificio Herbario
    - d* [ADCO] Administrador de comunicaciones
    - d* [EH] Edificio Herbario
- ⊙ *A* [SWC] Switch Core
  - ⊙ *d* [HW.SW3] Switch 3 Com
  - ⊙ *d* [AUX.UPS] Sistema de alimentacion ininterrumpida
    - d* [AUX.TRA] Transformador de aislamiento
    - d* [ADCO] Administrador de comunicaciones
    - d* [EH] Edificio Herbario
  - ⊙ *d* [AUX.UPS] Sistema de alimentacion ininterrumpida
    - d* [AUX.TRA] Transformador de aislamiento
    - d* [ADCO] Administrador de comunicaciones
    - d* [EH] Edificio Herbario
- ⊙ *A* [WA] Punto de acceso wireless
  - d* [ADCO] Administrador de comunicaciones
  - d* [EH] Edificio Herbario
  - d* [ZA] Zungarococha-Facultad Agronomia
- ⊙ *A* [SW3] Switch 3 Com
  - ⊙ *d* [AUX.UPS] Sistema de alimentacion ininterrumpida
  - d* [ADCO] Administrador de comunicaciones
  - d* [EH] Edificio Herbario

Figura 07. Equipos y su dependencia de activos (continuación)  
Fuente. Elaboración propia

- ☐ [COM] Comunicaciones
  - ☐ *A* [RADIO] Red inalámbrica
    - ☐ *d* [HW.SWC] Switch Core
      - ☐ *d* [HW.SW3] Switch 3 Com
        - ☐ *d* [AUX.UPS] Sistema de alimentación ininterrumpida
          - d* [AUX.TRA] Transformador de aislamiento
          - d* [ADCO] Administrador de comunicaciones
          - d* [EH] Edificio Herbario
      - ☐ *d* [AUX.UPS] Sistema de alimentación ininterrumpida
        - d* [AUX.TRA] Transformador de aislamiento
        - d* [ADCO] Administrador de comunicaciones
        - d* [EH] Edificio Herbario
    - ☐ *d* [HW.WA] Punto de acceso wireless
      - d* [ADCO] Administrador de comunicaciones
      - d* [EH] Edificio Herbario
      - d* [ZA] Zungarococha-Facultad Agronomía
      - d* [ADCO] Administrador de comunicaciones
      - d* [OP] Operadores
      - d* [EH] Edificio Herbario
      - d* [ZA] Zungarococha-Facultad Agronomía
      - d* [AC] Almacén Central
      - d* [FQ] Facultad Química
      - d* [FD] Facultad Derecho
- ☐ *A* [LAN] Red Lan
  - d* [AUX.WIRE] Cable UTP
  - d* [ADCO] Administrador de comunicaciones
  - d* [OP] Operadores

Figura 08. Comunicaciones y su dependencia de activos  
Fuente. Elaboración propia

### 3.2.1.3. Valoración de activos

Para valorar los activos se tienen en cuenta el siguiente criterio de valoración:

*Valoración:*

- 10 – muy alto – daño muy grave a la organización
- 7-9 – alto – daño grave a la organización
- 4-6 – medio – daño importante a la organización
- 1-3 – bajo – daño menor a la organización
- 0 – despreciable – irrelevantes a efectos prácticos

Los activos son evaluados según:

#### [IS] Servicios internos

<i>activo</i>	[D]	[I]	[C]	[A]	[T]
[email] Correo electrónico de docentes	[5] <sup>(1)</sup>	[7] <sup>(2)</sup>	[4] <sup>(3)</sup>	[6] <sup>(4)</sup>	[6] <sup>(5)</sup>
[intd] Intranet de docentes	[6] <sup>(6)</sup>	[5] <sup>(7)</sup>	[2] <sup>(8)</sup>	[6] <sup>(9)</sup>	[6] <sup>(10)</sup>
[sga] Sistema de gestión académica	[7] <sup>(11)</sup>	[7] <sup>(12)</sup>	[6] <sup>(13)</sup>	[7] <sup>(14)</sup>	[7] <sup>(15)</sup>

Cuadro 02. Valoración de activos – Servicios internos

Fuente. Elaboración propia

- (1) [5.lg] Probablemente sea causa una cierta publicidad negativa.
- (2) [7.lg] Probablemente causaría una publicidad negativa generalizada.
- (3) [4.pi1] Información personal: probablemente afecte a un grupo de individuos.
- (4) [6.pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
- (5) [6.ps] Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo.
- (6) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.
- (7) [5.lg.b] por afectar negativamente a las relaciones con el público.
- (8) [2.ps] Seguridad de las personas: pudiera causar daño menor a varios individuos.
- (9) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.
- (10) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.
- (11) [7.adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización.

[7.lg] Probablemente causaría una publicidad negativa generalizada.

- (12) [7.ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos.
- (13) [6.pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
- (14) [7.ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos.
- (15) [7.ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos.

### [E] Equipamiento

<i>activo</i>	[D]	[I]	[C]	[A]	[T]
[SW.WS] Windows Server 2003	[7] <sup>(1)</sup>	[9] <sup>(2)</sup>	[7] <sup>(3)</sup>		
[SW.FB] FreeBSD	[7] <sup>(4)</sup>	[10] <sup>(5)</sup>	[10] <sup>(6)</sup>		
[SW.SBA] Unix	[7] <sup>(7)</sup>	[10] <sup>(8)</sup>	[10] <sup>(9)</sup>		
[SW.AS] Apache	[7] <sup>(10)</sup>	[10] <sup>(11)</sup>	[10] <sup>(12)</sup>		
[HW.SA] Servidor de aplicaciones y Base de Datos	[10] <sup>(13)</sup>	[10] <sup>(14)</sup>	[10] <sup>(15)</sup>	[10] <sup>(16)</sup>	[10] <sup>(17)</sup>
[HW.SC] Servidor de correo	[5] <sup>(18)</sup>			[7] <sup>(19)</sup>	
[HW.FR] Firewall	[10] <sup>(20)</sup>	[10] <sup>(21)</sup>	[10] <sup>(22)</sup>	[10] <sup>(23)</sup>	[10] <sup>(24)</sup>
[HW.SDM] Servidor DMZ	[7] <sup>(25)</sup>			[7] <sup>(26)</sup>	
[HW.SWC] Switch Core	[10] <sup>(27)</sup>				
[HW.WA] Punto de acceso wireless	[10] <sup>(28)</sup>			[10] <sup>(29)</sup>	[10] <sup>(30)</sup>
[HW.SW3] Switch 3 Com			[10] <sup>(31)</sup>	[10] <sup>(32)</sup>	
[HW.SBC] Servidor de Backup	[10] <sup>(33)</sup>	[10] <sup>(34)</sup>	[10] <sup>(35)</sup>	[10] <sup>(36)</sup>	[10] <sup>(37)</sup>
[COM.RADIO] Red inalámbrica	[5] <sup>(38)</sup>				
[COM.LAN] Red Lan	[3] <sup>(39)</sup>				
[AUX.UPS] Sistema de alimentacion ininterrumpida	[5] <sup>(40)</sup>				
[AUX.WIRE] Cable UTP	[5] <sup>(41)</sup>				
[AUX.FIBER] Fibra optica	[7] <sup>(42)</sup>				

Cuadro 03. Valoración de activos – Equipamiento

Fuente. Elaboración propia

- (1) [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
- (2) [9.ii] Probablemente cause serios daños a misiones muy importantes de inteligencia o información.
- (3) [7.adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización.
- (4) [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.

- (5) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (6) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (7) [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
- (8) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (9) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (10) [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
- (11) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (12) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (13) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (14) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (15) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (16) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (17) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (18) [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
- (19) [7.si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
- (20) [10.si] Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
- (21) [10.si] Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.

- (22) [10.si] Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
- (23) [10.si] Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
- (24) [10.si] Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
- (25) [7.lg] Probablemente causaría una publicidad negativa generalizada.
- (26) [7.si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
- (27) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (28) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (29) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (30) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (31) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (32) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (33) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (34) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (35) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (36) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (37) [10.iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
- (38) [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
- (39) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa.

- (40) [5.adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización.
- (41) [5.adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización.
- (42) [7.adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización.

**[P] Personal**

<i>activo</i>	[D]	[I]	[C]	[A]	[T]
[ADSD] Administrador de sistemas y Base de datos	[5] <sup>(1)</sup>				
[ADCO] Administrador de comunicaciones	[5] <sup>(2)</sup>				
[OP] Operadores	[3] <sup>(3)</sup>				

Cuadro 04. Valoración de activos – Personal  
 Fuente. Elaboración propia

- (1) [5.lg] Probablemente sea causa una cierta publicidad negativa.
- (2) [5.lg] Probablemente sea causa una cierta publicidad negativa.
- (3) [3.iiio] Probablemente cause algún daño menor a misiones importantes de inteligencia o información.

### 3.2.2. Caracterización de las amenazas

#### 3.2.2.1. Identificación de amenazas

Las amenazas son identificadas según:

- ↳ [IS] Servicios internos
  - ↳ [email] Correo electrónico de docentes
    - ⚠ [E.1] Errores de los usuarios
    - ⚠ [E.2] Errores del administrador
    - ⚠ [E.3] Errores de monitorización (log)
    - ⚠ [E.4] Errores de configuración
    - ⚠ [E.7] Deficiencias en la organización
    - ⚠ [E.9] Errores de [re-]encaminamiento
    - ⚠ [E.10] Errores de secuencia
    - ⚠ [E.24] Caída del sistema por agotamiento de recursos
    - ⚠ [A.4] Manipulación de la configuración
    - ⚠ [A.5] Suplantación de la identidad del usuario
    - ⚠ [A.6] Abuso de privilegios de acceso
    - ⚠ [A.7] Uso no previsto
    - ⚠ [A.9] [Re-]encaminamiento de mensajes
    - ⚠ [A.10] Alteración de secuencia
    - ⚠ [A.11] Acceso no autorizado
    - ⚠ [A.13] Repudio
    - ⚠ [A.24] Denegación de servicio

Figura 09. Identificación de amenazas – Servicios internos – Correo electrónico de Docentes.

Fuente. Elaboración propia





- ⊙ **A [intd] Intranet de docentes**
- ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.3] Errores de monitorización (log)
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.13] Repudio
  - ▲ [A.24] Denegación de servicio

Figura 10. Identificación de amenazas – Servicios internos – Intranet de Docentes.

Fuente. Elaboración propia

- ⊙ **A [sga] Sistema de gestión académica**
- ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.3] Errores de monitorización (log)
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.13] Repudio
  - ▲ [A.24] Denegación de servicio

Figura 11. Identificación de amenazas – Servicios internos – Sistema de Gestión Académica.

Fuente. Elaboración propia

- ☞ [SW] Aplicaciones
  - 📍 [WS] Windows Server 2003
    - ▲ [L5] Avería de origen físico o lógico
    - ▲ [E.1] Errores de los usuarios
    - ▲ [E.2] Errores del administrador
    - ▲ [E.3] Errores de monitorización (log)
    - ▲ [E.4] Errores de configuración
    - ▲ [E.7] Deficiencias en la organización
    - ▲ [E.8] Difusión de software dañino
    - ▲ [E.9] Errores de [re-]encaminamiento
    - ▲ [E.10] Errores de secuencia
    - ▲ [E.15] Alteración de la información
    - ▲ [E.16] Introducción de falsa información
    - ▲ [E.18] Destrucción de la información
    - ▲ [E.19] Divulgación de información
    - ▲ [E.20] Vulnerabilidades de los programas (software)
    - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
    - ▲ [A.4] Manipulación de la configuración
    - ▲ [A.5] Suplantación de la identidad del usuario
    - ▲ [A.6] Abuso de privilegios de acceso
    - ▲ [A.7] Uso no previsto
    - ▲ [A.8] Difusión de software dañino
    - ▲ [A.9] [Re-]encaminamiento de mensajes
    - ▲ [A.10] Alteración de secuencia
    - ▲ [A.11] Acceso no autorizado
    - ▲ [A.14] Interceptación de información (escucha)
    - ▲ [A.15] Modificación de información
    - ▲ [A.16] Introducción de falsa información
    - ▲ [A.18] Destrucción de la información
    - ▲ [A.19] Divulgación de información
    - ▲ [A.22] Manipulación de programas

Figura 12. Identificación de amenazas – Aplicaciones – Windows Server 2003.

Fuente. Elaboración propia

- ♀ **A** [FB] FreeBSD
- ▲ [L5] Avería de origen físico o lógico
  - ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.3] Errores de monitorización (log)
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.8] Difusión de software dañino
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.15] Alteración de la información
  - ▲ [E.16] Introducción de falsa información
  - ▲ [E.18] Destrucción de la información
  - ▲ [E.19] Divulgación de información
  - ▲ [E.20] Vulnerabilidades de los programas (software)
  - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.8] Difusión de software dañino
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.15] Modificación de información
  - ▲ [A.16] Introducción de falsa información
  - ▲ [A.18] Destrucción de la información
  - ▲ [A.19] Divulgación de información
  - ▲ [A.22] Manipulación de programas

Figura 13. Identificación de amenazas – Aplicaciones – FreeBSD.  
Fuente. Elaboración propia

- ⊕ *A* [SBA] Unix
- ▲ [L5] Avería de origen físico o lógico
  - ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.8] Difusión de software dañino
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.20] Vulnerabilidades de los programas (software)
  - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.8] Difusión de software dañino
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.22] Manipulación de programas

Figura 14. Identificación de amenazas – Aplicaciones – UNIX.  
Fuente. Elaboración propia

- ⊕ *A* [AS] Apache
- ▲ [L5] Avería de origen físico o lógico
  - ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.3] Errores de monitorización (log)
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.8] Difusión de software dañino
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.20] Vulnerabilidades de los programas (software)
  - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.8] Difusión de software dañino
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.22] Manipulación de programas

Figura 15. Identificación de amenazas – Aplicaciones – Apache.  
Fuente. Elaboración propia

- ☐ [HW] Equipos
  - ☐ [SA] Servidor de aplicaciones y Base de Datos
    - ▲ [N.1] Fuego
    - ▲ [N.2] Daños por agua
    - ▲ [N.\*] Desastres naturales
    - ▲ [L.1] Fuego
    - ▲ [L.2] Daños por agua
    - ▲ [L.\*] Desastres industriales
    - ▲ [L.3] Contaminación mecánica
    - ▲ [L.4] Contaminación electromagnética
    - ▲ [L.5] Avería de origen físico o lógico
    - ▲ [L.6] Corte del suministro eléctrico
    - ▲ [L.7] Condiciones inadecuadas de temperatura o humedad
    - ▲ [L.11] Emanaciones electromagnéticas
    - ▲ [E.1] Errores de los usuarios
    - ▲ [E.2] Errores del administrador
    - ▲ [E.3] Errores de monitorización (log)
    - ▲ [E.4] Errores de configuración
    - ▲ [E.7] Deficiencias en la organización
    - ▲ [E.8] Difusión de software dañino
    - ▲ [E.9] Errores de [re-]encaminamiento
    - ▲ [E.10] Errores de secuencia
    - ▲ [E.20] Vulnerabilidades de los programas (software)
    - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
    - ▲ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
    - ▲ [E.24] Caída del sistema por agotamiento de recursos
    - ▲ [E.25] Pérdida de equipos
    - ▲ [A.4] Manipulación de la configuración
    - ▲ [A.5] Suplantación de la identidad del usuario
    - ▲ [A.6] Abuso de privilegios de acceso
    - ▲ [A.7] Uso no previsto
    - ▲ [A.8] Difusión de software dañino
    - ▲ [A.9] [Re-]encaminamiento de mensajes
    - ▲ [A.10] Alteración de secuencia
    - ▲ [A.11] Acceso no autorizado
    - ▲ [A.14] Interceptación de información (escucha)
    - ▲ [A.22] Manipulación de programas
    - ▲ [A.24] Denegación de servicio
    - ▲ [A.25] Robo de equipos
    - ▲ [A.26] Ataque destructivo

Figura 16. Identificación de amenazas – Equipos – Servidor de aplicaciones y Base de Datos.

Fuente. Elaboración propia

- ⊕ **A** [SC] Servidor de correo
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L1] Fuego
  - ▲ [L2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L3] Contaminación mecánica
  - ▲ [L4] Contaminación electromagnética
  - ▲ [L5] Avería de origen físico o lógico
  - ▲ [L6] Corte del suministro eléctrico
  - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L11] Emanaciones electromagnéticas
  - ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.3] Errores de monitorización (log)
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.8] Difusión de software dañino
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.20] Vulnerabilidades de los programas (software)
  - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
  - ▲ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [E.25] Pérdida de equipos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.8] Difusión de software dañino
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.22] Manipulación de programas
  - ▲ [A.24] Denegación de servicio
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 17. Identificación de amenazas – Equipos – Servidor de correo.  
Fuente. Elaboración propia

- ⊕ *A* [FR] Firewall
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L1] Fuego
  - ▲ [L2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L3] Contaminación mecánica
  - ▲ [L4] Contaminación electromagnética
  - ▲ [L5] Avería de origen físico o lógico
  - ▲ [L6] Corte del suministro eléctrico
  - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L11] Emanaciones electromagnéticas
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [E.25] Pérdida de equipos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.24] Denegación de servicio
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 18. Identificación de amenazas – Equipos – Firewall.  
Fuente. Elaboración propia

- ⊙ *A* [SDM] Servidor DMZ
- ▲ [L5] Avería de origen físico o lógico
  - ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.8] Difusión de software dañino
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.20] Vulnerabilidades de los programas (software)
  - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.7] Uso no previsto
  - ▲ [A.8] Difusión de software dañino
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.22] Manipulación de programas

Figura 19. Identificación de amenazas – Equipos – Servidor DMZ.  
Fuente. Elaboración propia

- ⊙ *A* [SWC] Switch Core
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L.1] Fuego
  - ▲ [L.2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L.3] Contaminación mecánica
  - ▲ [L.4] Contaminación electromagnética
  - ▲ [L.5] Avería de origen físico o lógico
  - ▲ [L.6] Corte del suministro eléctrico
  - ▲ [L.7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L.11] Emanaciones electromagnéticas
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [E.25] Pérdida de equipos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.24] Denegación de servicio
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 20. Identificación de amenazas – Equipos – Switch core.  
Fuente. Elaboración propia



- ⊕ **[WA] Punto de acceso wireless**
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L1] Fuego
  - ▲ [L2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L3] Contaminación mecánica
  - ▲ [L4] Contaminación electromagnética
  - ▲ [L5] Avería de origen físico o lógico
  - ▲ [L6] Corte del suministro eléctrico
  - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L11] Emanaciones electromagnéticas
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [E.25] Pérdida de equipos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.24] Denegación de servicio
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 21. Identificación de amenazas – Equipos – Punto de acceso wireless.

Fuente. Elaboración propia

- ⊕ **A [SW3] Switch 3 Com**
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L.1] Fuego
  - ▲ [L.2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L.3] Contaminación mecánica
  - ▲ [L.4] Contaminación electromagnética
  - ▲ [L.5] Avería de origen físico o lógico
  - ▲ [L.6] Corte del suministro eléctrico
  - ▲ [L.7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L.11] Emanaciones electromagnéticas
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [E.25] Pérdida de equipos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.24] Denegación de servicio
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 22. Identificación de amenazas – Equipos – Switch 3 com  
Fuente. Elaboración propia

- ⊙ **A** [SBC] Servidor de Backup
- ▲ [L5] Avería de origen físico o lógico
  - ▲ [E.1] Errores de los usuarios
  - ▲ [E.2] Errores del administrador
  - ▲ [E.3] Errores de monitorización (log)
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.8] Difusión de software dañino
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.20] Vulnerabilidades de los programas (software)
  - ▲ [E.21] Errores de mantenimiento / actualización de programas (software)
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.8] Difusión de software dañino
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.11] Acceso no autorizado
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.22] Manipulación de programas

Figura 23. Identificación de amenazas – Equipos – Servidor de Backup  
Fuente. Elaboración propia

- ☞ [COM] Comunicaciones
  - ☞ [RADIO] Red inalámbrica
    - ▲ [N.1] Fuego
    - ▲ [N.2] Daños por agua
    - ▲ [N.\*] Desastres naturales
    - ▲ [L1] Fuego
    - ▲ [L2] Daños por agua
    - ▲ [L.\*] Desastres industriales
    - ▲ [L3] Contaminación mecánica
    - ▲ [L4] Contaminación electromagnética
    - ▲ [L5] Avería de origen físico o lógico
    - ▲ [L6] Corte del suministro eléctrico
    - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
    - ▲ [L8] Fallo de servicios de comunicaciones
    - ▲ [L11] Emanaciones electromagnéticas
    - ▲ [E.2] Errores del administrador
    - ▲ [E.4] Errores de configuración
    - ▲ [E.7] Deficiencias en la organización
    - ▲ [E.9] Errores de [re-]encaminamiento
    - ▲ [E.10] Errores de secuencia
    - ▲ [E.24] Caída del sistema por agotamiento de recursos
    - ▲ [A.4] Manipulación de la configuración
    - ▲ [A.5] Suplantación de la identidad del usuario
    - ▲ [A.6] Abuso de privilegios de acceso
    - ▲ [A.7] Uso no previsto
    - ▲ [A.9] [Re-]encaminamiento de mensajes
    - ▲ [A.10] Alteración de secuencia
    - ▲ [A.11] Acceso no autorizado
    - ▲ [A.12] Análisis de tráfico
    - ▲ [A.14] Interceptación de información (escucha)
    - ▲ [A.24] Denegación de servicio
    - ▲ [A.25] Robo de equipos
    - ▲ [A.26] Ataque destructivo

Figura 24. Identificación de amenazas - Comunicaciones - Red inalámbrica  
Fuente. Elaboración propia

- ⊕ *A* [LAN] Red Lan
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L1] Fuego
  - ▲ [L2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L3] Contaminación mecánica
  - ▲ [L4] Contaminación electromagnética
  - ▲ [L5] Avería de origen físico o lógico
  - ▲ [L6] Corte del suministro eléctrico
  - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L8] Fallo de servicios de comunicaciones
  - ▲ [L11] Emanaciones electromagnéticas
  - ▲ [E.2] Errores del administrador
  - ▲ [E.4] Errores de configuración
  - ▲ [E.7] Deficiencias en la organización
  - ▲ [E.9] Errores de [re-]encaminamiento
  - ▲ [E.10] Errores de secuencia
  - ▲ [E.24] Caída del sistema por agotamiento de recursos
  - ▲ [A.4] Manipulación de la configuración
  - ▲ [A.5] Suplantación de la identidad del usuario
  - ▲ [A.6] Abuso de privilegios de acceso
  - ▲ [A.7] Uso no previsto
  - ▲ [A.9] [Re-]encaminamiento de mensajes
  - ▲ [A.10] Alteración de secuencia
  - ▲ [A.12] Análisis de tráfico
  - ▲ [A.14] Interceptación de información (escucha)
  - ▲ [A.24] Denegación de servicio
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 25. Identificación de amenazas – Comunicaciones – Red Lan  
Fuente. Elaboración propia

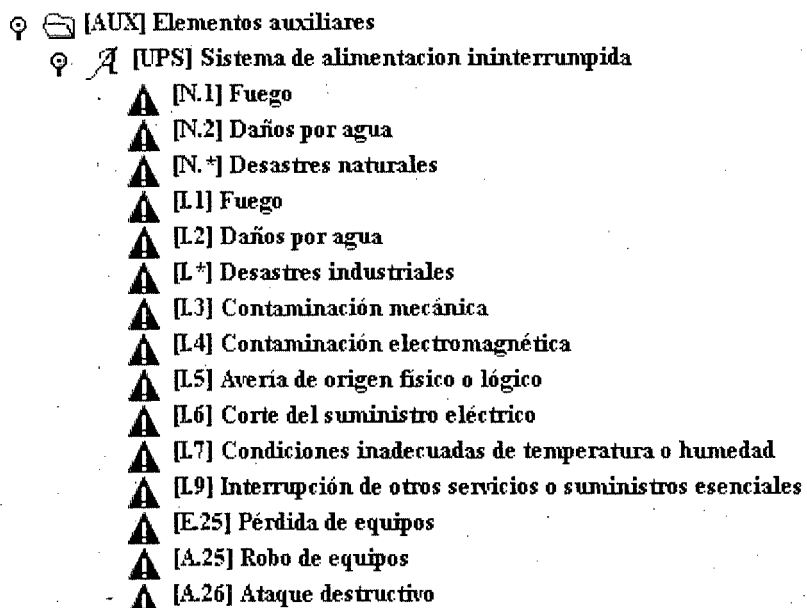


Figura 26. Identificación de amenazas – Elementos auxiliares – UPS  
Fuente. Elaboración propia

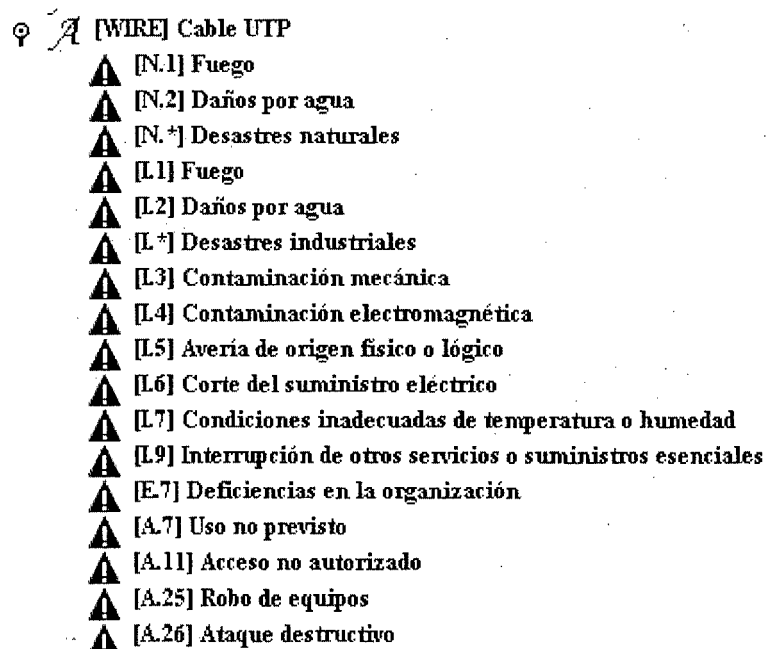


Figura 27. Identificación de amenazas - Elementos auxiliares  
Cable UTP  
Fuente. Elaboración propia

- ⊙ **A [FIBER] Fibra optica**
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L1] Fuego
  - ▲ [L2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L3] Contaminación mecánica
  - ▲ [L5] Avería de origen físico o lógico
  - ▲ [L6] Corte del suministro eléctrico
  - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L9] Interrupción de otros servicios o suministros esenciales
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 28. Identificación de amenazas- Elementos auxiliares - Fibra óptica  
Fuente. Elaboración propia

- ⊙ **A [TRA] Transformador de aislamiento**
- ▲ [N.1] Fuego
  - ▲ [N.2] Daños por agua
  - ▲ [N.\*] Desastres naturales
  - ▲ [L1] Fuego
  - ▲ [L2] Daños por agua
  - ▲ [L.\*] Desastres industriales
  - ▲ [L3] Contaminación mecánica
  - ▲ [L4] Contaminación electromagnética
  - ▲ [L5] Avería de origen físico o lógico
  - ▲ [L6] Corte del suministro eléctrico
  - ▲ [L7] Condiciones inadecuadas de temperatura o humedad
  - ▲ [L9] Interrupción de otros servicios o suministros esenciales
  - ▲ [E.25] Pérdida de equipos
  - ▲ [A.25] Robo de equipos
  - ▲ [A.26] Ataque destructivo

Figura 29. Identificación de amenazas- Elementos auxiliares -  
Transformador de aislamiento  
Fuente. Elaboración propia

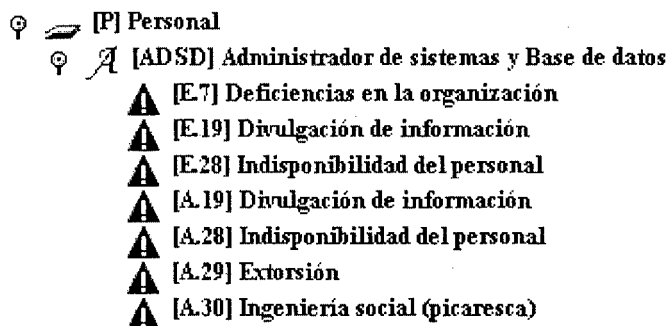


Figura 30. Identificación de amenazas- Personal- Administrador de sistemas y BD.

Fuente. Elaboración propia

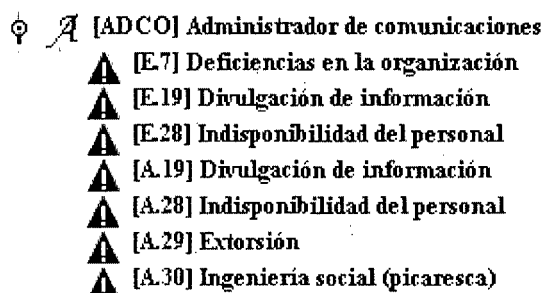


Figura 31. Identificación de amenazas- Personal- Administrador de comunicaciones.

Fuente. Elaboración propia

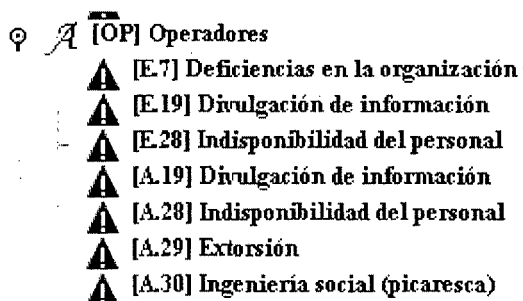


Figura 32. Identificación de amenazas- Personal- Operadores.

Fuente. Elaboración propia



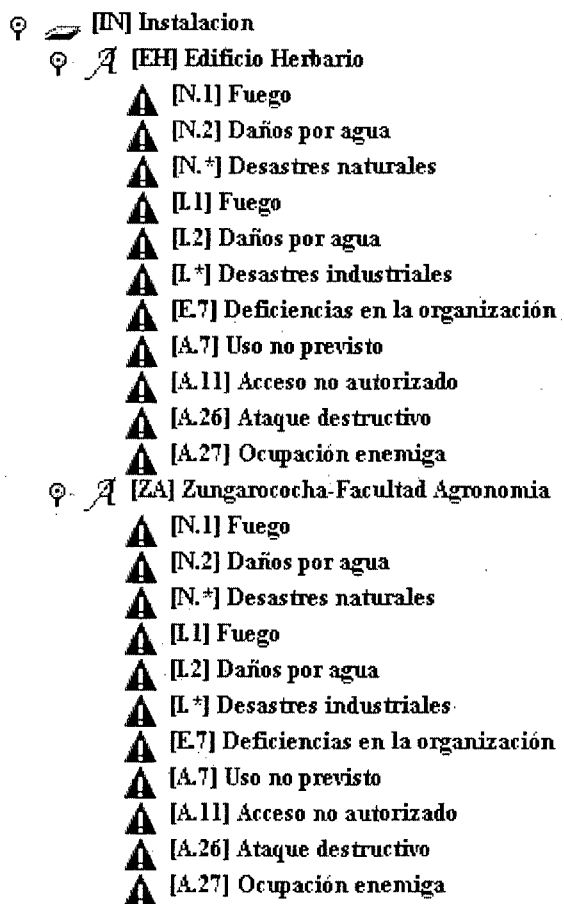


Figura 33. Identificación de amenazas- Instalaciones  
Fuente. Elaboración propia

### 3.2.2.2. Valoración de las amenazas

Después de determinar las amenazas por activo, ahora se evaluará la vulnerabilidad del activo frente a cada amenaza identificada.

- **Dimensiones:**
  - [D] disponibilidad
  - [I] integridad de los datos
  - [C] confidencialidad de los datos
  - [A] autenticidad de los usuarios y la información
  - [T] trazabilidad del servicio y de los datos
  
- **Valoración:**
  - 0,1 : Cada 10 años.
  - 0,5 : Cada 2 años.
  - 0,33 : Cada 3 años.
  - 0,05 : Cada 20 años.
  - 1 : Una vez al año.
  - 5 : Cinco veces al año.
  - 2 : Dos veces al año.
  - 10 : Diez veces al año.
  - 20 : Veinte veces al año.
  - 100 : Cien veces al año.

A continuación se muestra el resumen de valoración de las amenazas por activos:

**[email] Correo electrónico de docentes**

<b>amenaza</b>	<b>frecuencia</b>	<b>[D]</b>	<b>[I]</b>	<b>[C]</b>	<b>[A]</b>	<b>[T]</b>
[E.1] Errores de los usuarios	10	10%	10%	10%	-	-
[E.2] Errores del administrador	1	20%	20%	10%	10%	20%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	0,5	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.9] Errores de [re-]encaminamiento	1	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,5	-	10%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[A.4] Manipulación de la configuración	0,1	50%	10%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	100	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	10	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.9] [Re-]encaminamiento de mensajes	10	-	10%	50%	50%	50%
[A.10] Alteración de secuencia	0,1	-	50%	-	-	-
[A.11] Acceso no autorizado	100	100%	10%	50%	50%	-
[A.13] Repudio	10	-	-	-	-	100%
[A.24] Denegación de servicio	10	50%	-	-	-	-

Cuadro 05. Valoración de amenazas - Correo electrónico de docentes  
Fuente. Elaboración propia

**[intd] Intranet de docentes**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[E.1] Errores de los usuarios	10	10%	10%	10%	-	-
[E.2] Errores del administrador	1	20%	20%	10%	10%	20%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	0,5	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.9] Errores de [re-]encaminamiento	1	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,5	-	10%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[A.4] Manipulación de la configuración	0,1	50%	10%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	100	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	10	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.9] [Re-]encaminamiento de mensajes	10	-	10%	50%	50%	50%
[A.10] Alteración de secuencia	0,1	-	50%	-	-	-
[A.11] Acceso no autorizado	100	100%	10%	50%	50%	-
[A.13] Repudio	10	-	-	-	-	100%
[A.24] Denegación de servicio	10	50%	-	-	-	-

Cuadro 06. Valoración de amenazas – Intranet de docentes  
 Fuente. Elaboración propia

**[sga] Sistema de gestión académica**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[E.1] Errores de los usuarios	10	10%	10%	10%	-	-
[E.2] Errores del administrador	1	20%	20%	10%	10%	20%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	0,5	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.9] Errores de [re-]encaminamiento	1	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,5	-	10%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[A.4] Manipulación de la configuración	0,1	50%	10%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	100	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	10	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.9] [Re-]encaminamiento de mensajes	10	-	10%	50%	50%	50%
[A.10] Alteración de secuencia	0,1	-	50%	-	-	-
[A.11] Acceso no autorizado	100	100%	10%	50%	50%	-
[A.13] Repudio	10	-	-	-	-	100%
[A.24] Denegación de servicio	10	50%	-	-	-	-

Cuadro 07. Valoración de amenazas – Sistema de gestión académica  
Fuente. Elaboración propia

[SW.WS] Windows Server 2003

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[E.1] Errores de los usuarios	10	10%	10%	10%	-	-
[E.2] Errores del administrador	1	20%	20%	10%	10%	20%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	0,5	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.9] Errores de [re-]encaminamiento	1	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,5	-	10%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[A.4] Manipulación de la configuración	0,1	50%	10%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	100	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	10	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.9] [Re-]encaminamiento de mensajes	10	-	10%	50%	50%	50%
[A.10] Alteración de secuencia	0,1	-	50%	-	-	-
[A.11] Acceso no autorizado	100	100%	10%	50%	50%	-
[A.24] Denegación de servicio	10	50%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[E.1] Errores de los usuarios	20	10%	10%	10%	-	-
[E.2] Errores del administrador	2	20%	20%	10%	50%	50%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.15] Alteración de la información	10	-	1%	-	-	-
[E.16] Introducción de falsa información	100	-	1%	-	-	-
[E.18] Destrucción de la información	10	1%	-	-	-	-
[E.19] Divulgación de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%

Cuadro 08. Valoración de amenazas – Windows Server 2003

Fuente. Elaboración propia

**[SW.FB] FreeBSD**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[E.1] Errores de los usuarios	20	10%	10%	10%	-	-
[E.2] Errores del administrador	2	20%	20%	10%	50%	50%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.15] Alteración de la información	10	-	1%	-	-	-
[E.16] Introducción de falsa información	100	-	1%	-	-	-
[E.18] Destrucción de la información	10	1%	-	-	-	-
[E.19] Divulgación de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	5	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.10] Alteración de secuencia	0,05	-	50%	-	-	-
[A.11] Acceso no autorizado	100	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	10	-	-	50%	-	-
[A.15] Modificación de información	10	-	50%	-	-	-
[A.16] Introducción de falsa información	20	-	50%	-	-	-
[A.18] Destrucción de la información	10	50%	-	-	-	-
[A.19] Divulgación de información	10	-	-	100%	-	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%

Cuadro 09. Valoración de amenazas – FreeBSD

Fuente. Elaboración propia

[SW.SBA] Unix

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[E.1] Errores de los usuarios	20	1%	10%	10%	-	-
[E.2] Errores del administrador	2	20%	20%	10%	50%	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	5	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.10] Alteración de secuencia	0,05	-	50%	-	-	-
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,5	-	-	50%	-	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%

Cuadro 10. Valoración de amenazas – Unix

Fuente. Elaboración propia



[SW.AS] Apache

<i>amenaza</i>	<i>Frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[E.1] Errores de los usuarios	20	1%	10%	10%	-	-
[E.2] Errores del administrador	2	20%	20%	10%	50%	50%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	5	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.10] Alteración de secuencia	0,05	-	50%	-	-	-
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,5	-	-	50%	-	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%

Cuadro 11. Valoración de amenazas – Apache  
Fuente. Elaboración propia

**[HW.SA] Servidor de aplicaciones y Base de Datos**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,1	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	20	100%	-	-	-	1%
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.1] Errores de los usuarios	20	1%	10%	10%	-	-
[E.2] Errores del administrador	2	50%	20%	10%	50%	50%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	100%	-	10%	-	100%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	5	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.10] Alteración de secuencia	0,05	-	50%	-	-	-
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,5	-	-	50%	-	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%
[A.24] Denegación de servicio	10	100%	-	-	-	-
[A.25] Robo de equipos	1	100%	-	10%	-	100%
[A.26] Ataque destructivo	0,1	100%	-	-	-	-

Cuadro 12. Valoración de amenazas – Servidor de aplicaciones y Base de datos

Fuente. Elaboración propia

[HW.SC] Servidor de correo

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,1	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	20	100%	-	-	-	1%
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.1] Errores de los usuarios	20	1%	10%	10%	-	-
[E.2] Errores del administrador	2	50%	20%	10%	50%	50%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	100%	-	10%	-	100%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	5	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.10] Alteración de secuencia	0,05	-	50%	-	-	-
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,5	-	-	50%	-	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%
[A.24] Denegación de servicio	10	100%	-	-	-	-
[A.25] Robo de equipos	1	100%	-	10%	-	100%
[A.26] Ataque destructivo	0,1	100%	-	-	-	-

Cuadro 13. Valoración de amenazas – Servidor de Correo

Fuente. Elaboración propia

**[HW.FR] Firewall**

<i>Amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,1	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	20	100%	-	-	-	1%
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.2] Errores del administrador	1	50%	1%	10%	10%	50%
[E.4] Errores de configuración	1	50%	1%	10%	10%	50%
[E.7] Deficiencias en la organización	1	100%	-	10%	10%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	20%	-	-	-	-
[A.4] Manipulación de la configuración	0,5	50%	10%	20%	10%	100%
[A.6] Abuso de privilegios de acceso	0,5	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	-	10%	10%	50%
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,1	-	-	20%	-	-
[A.24] Denegación de servicio	10	100%	-	-	-	-
[A.25] Robo de equipos	1	20%	-	-	-	-
[A.26] Ataque destructivo	0,1	100%	-	-	-	-

Cuadro 14. Valoración de amenazas – Firewall

Fuente. Elaboración propia

**[HW.SDM] Servidor DMZ**

<i>Amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[E.1] Errores de los usuarios	20	1%	10%	10%	-	-
[E.2] Errores del administrador	2	20%	20%	10%	50%	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%

Cuadro 15. Valoración de amenazas – Servidor DMZ

Fuente. Elaboración propia

[HW.SWC] Switch Core

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,1	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	20	100%	-	-	-	1%
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.2] Errores del administrador	1	50%	1%	10%	10%	50%
[E.4] Errores de configuración	1	50%	1%	10%	10%	50%
[E.7] Deficiencias en la organización	1	100%	-	10%	10%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	20%	-	-	-	-
[A.4] Manipulación de la configuración	0,5	50%	10%	20%	10%	100%
[A.6] Abuso de privilegios de acceso	0,5	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	-	10%	10%	50%
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,1	-	-	20%	-	-
[A.24] Denegación de servicio	10	100%	-	-	-	-
[A.25] Robo de equipos	1	20%	-	-	-	-
[A.26] Ataque destructivo	0,1	100%	-	-	-	-

Cuadro 16. Valoración de amenazas – Switch core  
Fuente. Elaboración propia

**[HW.WA] Punto de acceso wireless**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,1	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	20	100%	-	-	-	1%
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.2] Errores del administrador	1	50%	1%	10%	10%	50%
[E.4] Errores de configuración	1	50%	1%	10%	10%	50%
[E.7] Deficiencias en la organización	1	100%	-	10%	10%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	20%	-	-	-	-
[A.4] Manipulación de la configuración	0,5	50%	10%	20%	10%	100%
[A.6] Abuso de privilegios de acceso	0,5	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	-	10%	10%	50%
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,1	-	-	20%	-	-
[A.24] Denegación de servicio	10	100%	-	-	-	-
[A.25] Robo de equipos	1	20%	-	-	-	-
[A.26] Ataque destructivo	0,1	100%	-	-	-	-

Cuadro 17. Valoración de amenazas – Punto de acceso wireless

Fuente. Elaboración propia

[HW.SW3] Switch 3 Com

<i>Amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,1	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	20	100%	-	-	-	1%
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.2] Errores del administrador	1	50%	1%	10%	10%	50%
[E.4] Errores de configuración	1	50%	1%	10%	10%	50%
[E.7] Deficiencias en la organización	1	100%	-	10%	10%	50%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	20%	-	-	-	-
[A.4] Manipulación de la configuración	0,5	50%	10%	20%	10%	100%
[A.6] Abuso de privilegios de acceso	0,5	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	-	10%	10%	50%
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,1	-	-	20%	-	-
[A.24] Denegación de servicio	10	100%	-	-	-	-
[A.25] Robo de equipos	1	20%	-	-	-	-
[A.26] Ataque destructivo	0,1	100%	-	-	-	-

Cuadro 18. Valoración de amenazas – Switch 3 com

Fuente. Elaboración propia



**[HW.SBC] Servidor de Backup**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[E.1] Errores de los usuarios	20	1%	10%	10%	-	-
[E.2] Errores del administrador	2	20%	20%	10%	50%	50%
[E.3] Errores de monitorización (log)	1	-	-	-	-	50%
[E.4] Errores de configuración	2	50%	10%	10%	50%	50%
[E.7] Deficiencias en la organización	1	100%	10%	10%	10%	50%
[E.8] Difusión de software dañino	100	10%	10%	10%	10%	10%
[E.9] Errores de [re-]encaminamiento	0,5	-	1%	10%	1%	1%
[E.10] Errores de secuencia	0,1	-	10%	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	1%	10%	10%
[A.4] Manipulación de la configuración	1	50%	50%	50%	100%	100%
[A.5] Suplantación de la identidad del usuario	20	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	5	-	10%	10%	-	-
[A.7] Uso no previsto	1	100%	10%	10%	10%	50%
[A.8] Difusión de software dañino	10	100%	100%	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	0,1	-	10%	100%	50%	50%
[A.10] Alteración de secuencia	0,05	-	50%	-	-	-
[A.11] Acceso no autorizado	5	100%	10%	50%	50%	-
[A.14] Interceptación de información (escucha)	0,5	-	-	50%	-	-
[A.22] Manipulación de programas	20	-	100%	100%	100%	100%

Cuadro 19. Valoración de amenazas – Servidor de Backup

Fuente. Elaboración propia

[COM.RADIO] Red inalámbrica

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,05	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	10	100%	-	-	-	1%
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.2] Errores del administrador	1	50%	1%	10%	10%	50%
[E.4] Errores de configuración	1	50%	1%	10%	10%	50%
[E.7] Deficiencias en la organización	1	100%	-	10%	10%	50%
[E.9] Errores de [re-]encaminamiento	5	-	1%	1%	1%	1%
[E.10] Errores de secuencia	2	-	10%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.4] Manipulación de la configuración	1	50%	10%	20%	10%	100%
[A.5] Suplantación de la identidad del usuario	2	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	-	10%	10%	50%
[A.9] [Re-]encaminamiento de mensajes	2	-	10%	10%	10%	10%
[A.10] Alteración de secuencia	0,5	-	10%	-	-	-
[A.11] Acceso no autorizado	10	100%	10%	50%	50%	-
[A.12] Análisis de tráfico	0,33	-	-	2%	-	-
[A.14] Interceptación de información (escucha)	10	-	-	50%	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-
[A.25] Robo de equipos	10	50%	-	50%	-	-
[A.26] Ataque destructivo	1	50%	-	-	-	-

Cuadro 20. Valoración de amenazas – Red inalámbrica  
Fuente. Elaboración propia

[COM.LAN] Red Lan

<i>Amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,05	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	50%
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	10	100%	-	-	-	1%
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[E.2] Errores del administrador	1	50%	1%	10%	10%	50%
[E.4] Errores de configuración	1	50%	1%	10%	10%	50%
[E.7] Deficiencias en la organización	1	100%	-	10%	10%	50%
[E.9] Errores de [re-]encaminamiento	5	-	1%	1%	1%	1%
[E.10] Errores de secuencia	2	-	10%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.4] Manipulación de la configuración	1	50%	10%	20%	10%	100%
[A.5] Suplantación de la identidad del usuario	2	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	50%	-	-
[A.7] Uso no previsto	1	100%	-	10%	10%	50%
[A.9] [Re-]encaminamiento de mensajes	2	-	10%	10%	10%	10%
[A.10] Alteración de secuencia	0,5	-	10%	-	-	-
[A.11] Acceso no autorizado	10	100%	10%	50%	50%	-
[A.12] Análisis de tráfico	0,33	-	-	2%	-	-
[A.14] Interceptación de información (escucha)	2	-	-	100%	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-
[A.25] Robo de equipos	10	50%	-	50%	-	-
[A.26] Ataque destructivo	1	50%	-	-	-	-

Cuadro 21. Valoración de amenazas – Red Lan

Fuente. Elaboración propia

**[AUX.UPS] Sistema de alimentación ininterrumpida**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,5	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	10%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	10%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	5	10%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	10%	-	-	-	-
[E.25] Pérdida de equipos	10	10%	-	-	-	-
[A.25] Robo de equipos	1	10%	-	-	-	-
[A.26] Ataque destructivo	1	10%	-	-	-	-

Cuadro 22. Valoración de amenazas – Sistema de alimentación ininterrumpida  
Fuente. Elaboración propia

**[AUX.WIRE] Cable UTP**

<i>Amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,5	50%	-	-	-	50%
[I.4] Contaminación electromagnética	10	10%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%	-	-	-	-
[E.7] Deficiencias en la organización	1	100%	-	1%	1%	10%
[A.7] Uso no previsto	1	100%	-	1%	1%	10%
[A.11] Acceso no autorizado	1	-	10%	50%	50%	-
[A.25] Robo de equipos	10	100%	-	-	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

Cuadro 23. Valoración de amenazas – Cable UTP  
Fuente. Elaboración propia

**[AUX.FIBER] Fibra óptica**

<i>Amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,5	50%	-	-	-	50%
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	10%
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%	-	-	-	-
[A.25] Robo de equipos	10	100%	-	-	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

Cuadro 24. Valoración de amenazas – Fibra óptica  
Fuente. Elaboración propia

**[AUX.TRA] Transformador de aislamiento**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	50%
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,1	100%	-	-	-	50%
[I.3] Contaminación mecánica	0,5	50%	-	-	-	50%
[I.4] Contaminación electromagnética	1	10%	-	-	-	10%
[I.5] Avería de origen físico o lógico	1	10%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	10%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	5	10%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	10%	-	-	-	-
[E.25] Pérdida de equipos	10	10%	-	-	-	-
[A.25] Robo de equipos	1	10%	-	-	-	-
[A.26] Ataque destructivo	1	10%	-	-	-	-

Cuadro 25. Valoración de amenazas – Transformador de aislamiento  
Fuente. Elaboración propia

**[ADSD] Administrador de sistemas y Base de datos**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[E.7] Deficiencias en la organización	5	20%	-	50%	50%	50%
[E.19] Divulgación de información	1	-	-	40%	40%	-
[E.28] Indisponibilidad del personal	1	10%	-	-	-	-
[A.19] Divulgación de información	1	-	-	50%	50%	-
[A.28] Indisponibilidad del personal	0,5	20%	-	-	-	-
[A.29] Extorsión	0,9	50%	100%	100%	100%	100%
[A.30] Ingeniería social (picaresca)	0,5	50%	100%	100%	100%	100%

Cuadro 26. Valoración de amenazas – Administrador de sistemas y Base de datos  
 Fuente. Elaboración propia

**[ADCO] Administrador de comunicaciones**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[E.7] Deficiencias en la organización	5	20%	-	50%	50%	50%
[E.19] Divulgación de información	1	-	-	40%	40%	-
[E.28] Indisponibilidad del personal	1	10%	-	-	-	-
[A.19] Divulgación de información	1	-	-	50%	50%	-
[A.28] Indisponibilidad del personal	0,5	20%	-	-	-	-
[A.29] Extorsión	0,9	50%	100%	100%	100%	100%
[A.30] Ingeniería social (picaresca)	0,5	50%	100%	100%	100%	100%

Cuadro 27. Valoración de amenazas – Administrador de comunicaciones  
 Fuente. Elaboración propia

**[OP] Operadores**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[E.7] Deficiencias en la organización	1	20%	-	10%	10%	10%
[E.19] Divulgación de información	1	-	-	10%	10%	-
[E.28] Indisponibilidad del personal	1	30%	-	-	-	-
[A.19] Divulgación de información	1	-	-	10%	10%	-
[A.28] Indisponibilidad del personal	0,5	50%	-	-	-	-
[A.29] Extorsión	0,9	20%	10%	10%	10%	50%
[A.30] Ingeniería social (picaresca)	0,5	20%	20%	20%	20%	50%

Cuadro 28. Valoración de amenazas – Operadores  
Fuente. Elaboración propia

**[EH] Edificio Herbario**

<i>amenaza</i>	<i>frecuencia</i>	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	1	100%	-	-	-	10%
[N.2] Daños por agua	1	100%	-	-	-	10%
[N.*] Desastres naturales	0,5	100%	-	-	-	10%
[I.1] Fuego	1	100%	-	-	-	10%
[I.2] Daños por agua	1	100%	-	-	-	10%
[I.*] Desastres industriales	1	100%	-	-	-	10%
[E.7] Deficiencias en la organización	1	100%	50%	50%	50%	50%
[A.7] Uso no previsto	1	100%	50%	50%	50%	50%
[A.11] Acceso no autorizado	5	10%	10%	10%	10%	10%
[A.26] Ataque destructivo	0,1	100%	-	-	-	10%
[A.27] Ocupación enemiga	1	100%	50%	50%	50%	50%

Cuadro 29. Valoración de amenazas – Edificio Herbario  
Fuente. Elaboración propia

### 3.2.3. Caracterización de las salvaguardas

#### 3.2.3.1. Identificación de las salvaguardas

Las salvaguardas se clasifican según:

##### **Protecciones generales**

- Identificación y autenticación
- Mecanismo de autenticación
- Control de acceso lógico
- Herramientas de seguridad
- Gestión de incidencias (TIC)
- Registro y auditoría

##### **Protección de los servicios**

- Inventario de servicios
- Aseguramiento de la disponibilidad
- Adquisición o desarrollo
- Aceptación
- Aplicación de perfiles de seguridad (servicios)
- Explotación
- Gestión de cambios (mejoras y sustituciones)
- Definición del proceso de cambio de forma que minimice la interrupción del servicio
- Registro de toda actualización de servicios
- Terminación
- Protección del correo electrónico
- Identificación de los usuarios
- Teletrabajo
- Acuerdo de seguridad

##### **Protección de la información**

- Inventario de activos de información
- Clasificación de la información
- Normativa de retención de datos
- Aseguramiento de la disponibilidad
- Aseguramiento de la integridad
- Protección criptográfica de la información

##### **Protección de las aplicaciones informáticas (SW)**

- Normativa sobre el uso correcto de las aplicaciones
- Procedimientos de uso de las aplicaciones
- Inventario de aplicaciones
- Copias de seguridad (backup) (SW)
- Adquisición de aplicaciones SW
- Aplicación de perfiles de seguridad (SW)
- Explotación
- Cambios (actualizaciones y mantenimiento)
- Terminación



### **Protección de los equipos informáticos**

- Normativa sobre el uso correcto de los equipos
- Procedimientos de uso del equipamiento
- Inventario de equipos
- Aseguramiento de la disponibilidad
- Adquisición de HW
- Desarrollo de HW
- Aplicación de perfiles de seguridad (HW)
- Instalación
- Operación
- Cambios (actualizaciones y mantenimiento)
- Terminación
- Protección de los cortafuegos (firewall)

### **Protección de las comunicaciones**

- Normativa sobre el uso correcto de las comunicaciones
- Procedimientos de uso de las comunicaciones
- Inventario de servicios de comunicación
- Aseguramiento de la disponibilidad
- Adquisición o contratación (COM)
- Aplicación de perfiles de seguridad (COM)
- Protección criptográfica del canal (COM)
- Operación
- Cambios (actualizaciones y mantenimiento)
- Terminación
- Seguridad Wireless (WiFi)

### **Elementos auxiliares**

- Inventario de equipamiento auxiliar
- Aseguramiento de la disponibilidad
- Instalación
- Suministro eléctrico
- Climatización
- Protección del cableado
- Contenedores de seguridad

### **Protección de las instalaciones**

- Inventario de instalaciones
- Normativa
- Procedimientos
- Diseño
- Control de los accesos físicos
- Protección del perímetro
- Vigilancia
- Protección frente a desastres
- La seguridad de la instalación no es responsabilidad de un único guardia.

### **Gestión del Personal**

- Política de gestión de personal (en materia de seguridad)
- Procedimientos de gestión de personal (en materia de seguridad)
- Relación de personal
- Puestos de trabajo
- Cambio de puesto de trabajo
- Contratación
- Formación y concienciación
- Protección del usuario frente a coacciones

### **Organización**

- Organización interna
- Documentación del sistema
- Normativa de seguridad (política, ...)
- Planificación de seguridad
- Continuidad del negocio (contingencia)
- Inspecciones de seguridad
- Protección de los activos fuera de las instalaciones
- Salvaguarda de los registros de la Organización

### **Relaciones externas**

- Acuerdos para intercambio de información y software
- Revisión del cumplimiento de acuerdos y contratos

### **3.2.3.2. Valoración de las salvaguardas**

Para evaluar las salvaguardas se utiliza como parámetros los niveles de madurez y fase.

#### **Nivel de madurez**

- L0 - 0 - inexistente
- L1 - 1 - inicial / ad hoc
- L2 - 2 - reproducible, pero intuitivo
- L3 - 3 - proceso definido
- L4 - 4 - gestionado y medible
- L5 - 5 – optimizado

#### **Fases**

- [f1] situación actual
- [f2] situación objetivo

A continuación se muestra la valoración de las salvaguardas:

### Protecciones generales

<i>Salvaguarda</i>	[f1]	[f2]
Identificación y autenticación	L0	L3
Normativa de identificación y autenticación	L3	L3
Procedimientos de identificación y autenticación	L3	L3
Identificación de los usuarios	L5	L5
Gestión de la identificación y autenticación de usuario	L2	L3
Registro de las identificaciones	L2	L3
Alta, activación, modificación y baja de las cuentas de usuario	L2	L3
Proceso de alta: creación de nuevas cuentas	L2	L3
Proceso de activación	L2	L3
Comprobación previa de la identidad de los usuarios y de los privilegios requeridos	L2	L3
Limitación del número de autenticadores necesarios por usuario	L2	L3
Verificación de la identidad de los usuarios previa entrega del autenticador	L2	L3
Distribución segura de los autenticadores	L2	L3
Compromiso escrito de mantener la confidencialidad del autenticador	L2	L3
Confirmación de la recepción de los autenticadores por los interesados	L2	L3
Control de los autenticadores por los interesados	L2	L3
Comunicación de incidentes que afecten a los autenticadores (pérdida, vulneración, etc.)	L2	L3
Las cuentas se suspenden al ser comprometidas o existir sospecha de ello	L2	L3
Mecanismo de autenticación	L3	L3
Contraseñas	L3	L3
Control de acceso lógico	L3	L3
Normativa para el control de accesos	L3	L3
Restricción de acceso a la información	L3	L3
Restricción de uso de las utilidades del sistema	L3	L3
Segregación de tareas	L3	L3
Gestión de privilegios	L3	L3
Revisión de los derechos de acceso de los usuarios	L2	L3
Mecanismo de control de acceso	L3	L3
Canal seguro de autenticación	L3	L3
Limitación del número de sesiones concurrentes de un usuario	L2	L3
Equipo informático de usuario desatendido	L2	L3
Desconexión automática de terminales	L2	L3
Herramientas de seguridad	L2	L3
Herramienta contra código dañino	L2	L3
Herramienta de detección / prevención de intrusión	L2	L3
Herramienta de monitorización de tráfico	L2	L3
Herramienta de análisis de vulnerabilidades	L2	L3
Herramienta para análisis de logs	L2	L3
Gestión de incidencias (TIC)	L0	L3
Definición de procedimientos a seguir para todos los tipos potenciales de incidencias	L0	L3
Comunicación de las incidencias de seguridad	L0	L3
Comunicación de las deficiencias de seguridad	L0	L3
Comunicación de los fallos del software	L0	L3
Registro de fallos y revisión de las medidas correctoras	L0	L3
Control formal del proceso de recuperación ante el incidente	L0	L3
Concienciación en la detección y reporte de incidentes	L0	L3
Formación en detección y gestión de incidentes	L0	L3
Registro y auditoría	L0	L3

Cuadro 30. Valoración de las salvaguardas – Protecciones generales

Fuente. Elaboración propia

### Protección de los servicios

<i>salvaguarda</i>	[f1]	[f2]
Inventario de servicios	L2	L4
Aseguramiento de la disponibilidad	L1	L3
Adquisición o desarrollo	L1	L3
Aceptación	L1	L3
Aplicación de perfiles de seguridad (servicios)	L1	L3
Explotación	L1	L3
Uso de servicios criptográficos	L1	L3
Gestión de cambios (mejoras y sustituciones)	L1	L3
Definición del proceso de cambio de forma que minimice la interrupción del servicio	L1	L3
Registro de toda actualización de servicios	L0	L3
Terminación	L1	L3
Protección del correo electrónico	L3	L5
Identificación de los usuarios	L2	L4
Teletrabajo	L2	L5
Acuerdo de seguridad	L1	L5

Cuadro 31. Valoración de las salvaguardas – Protección de los servicios  
Fuente. Elaboración propia

### Protección de la información

<i>salvaguarda</i>	[f1]	[f2]
Inventario de activos de información	n.a.	n.a.
Clasificación de la información	n.a.	n.a.
Normativa de retención de datos	n.a.	n.a.
Aseguramiento de la disponibilidad	n.a.	n.a.
Aseguramiento de la integridad	n.a.	n.a.
Protección criptográfica de la información	n.a.	n.a.

Cuadro 32. Valoración de las salvaguardas – Protección de la información  
Fuente. Elaboración propia

**Protección de las aplicaciones informáticas (SW)**

<i>Salvaguarda</i>	[f1]	[f2]
Normativa sobre el uso correcto de las aplicaciones	L2	L3
Procedimientos de uso de las aplicaciones	L2	L3
Inventario de aplicaciones	L2	L3
Protección de los derechos de propiedad intelectual (IPR)	L2	L3
Copias de seguridad (backup) (SW)	L2	L3
Adquisición de aplicaciones SW	L2	L3
Aplicación de perfiles de seguridad (SW)	L2	L3
Explotación	L2	L3
Cambios (actualizaciones y mantenimiento)	L2	L3
Seguimiento permanente de actualizaciones y parches (SW)	L2	L3
Evaluación del impacto potencial del cambio	L2	L3
Definición del proceso de cambio de forma que minimice la interrupción del servicio	L2	L3
Control de versiones de toda actualización del software	L2	L3
Realización por personal debidamente autorizado	L2	L3
Retención de versiones anteriores de software como medida de precaución para contingencias	L2	L3
Retención de versiones anteriores de configuración (SW)	L2	L3
Pruebas de regresión	L2	L3
Procedimientos de control de cambios	L2	L3
Registro de toda actualización de SW	L2	L3
Documentación	L2	L3
Actualización de todos los procedimientos de explotación afectados	L2	L3
Actualización de los planes de continuidad (SW)	L2	L3
Terminación	L2	L3

Cuadro 33. Valoración de las salvaguardas – Protección de las aplicaciones informáticas.

Fuente. Elaboración propia

**Protección de los equipos informáticos**

<i>Salvaguarda</i>	<b>[f1]</b>	<b>[f2]</b>
Normativa sobre el uso correcto de los equipos	L2	L3
Procedimientos de uso del equipamiento	L2	L3
Inventario de equipos	L2	L3
Aseguramiento de la disponibilidad	L2	L3
Adquisición de HW	L5	L5
Desarrollo de HW	L2	L3
Aplicación de perfiles de seguridad (HW)	L2	L3
Contenedores criptográficos (HW, HW virtual)	L2	L3
Instalación	L2	L3
Operación	L2	L3
Proceso de autorización de recursos para el tratamiento de la información	L2	L3
Protección física de los equipos	L2	L3
Seguridad del equipamiento de oficina	L2	L3
Seguridad de los equipos fuera de las instalaciones	L2	L3
Protección de los dispositivos de red	L2	L3
Cambios (actualizaciones y mantenimiento)	L2	L3
Terminación	L2	L3
Protección de los cortafuegos (firewall)	L2	L3
Se controla el tráfico entrante y saliente	L2	L3
Se ocultan las direcciones IP internas (servicio NAT o similar)	L2	L3
Se ocultan los puertos internos (servicio PAT o similar)	L2	L3
Se controla el producto	L2	L3
Configuración segura	L2	L3
Voz, facsímil y video	L2	L3
Prohibición de establecimiento de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección	L2	L3
Prohibición de dejar mensajes confidenciales en contestadores automáticos	L2	L3
Formación y concienciación en el uso seguro de los sistemas y recursos	L2	L3
Control sobre el envío de documentos y mensajes a números equivocados	L2	L3

Cuadro 34. Valoración de las salvaguardas – Protección de los equipos informáticos.  
 Fuente. Elaboración propia

**Protección de las comunicaciones**

<i>salvaguarda</i>	[f1]	[f2]
Normativa sobre el uso correcto de las comunicaciones	L2	L3
Procedimientos de uso de las comunicaciones	L2	L3
Inventario de servicios de comunicación	L2	L3
Aseguramiento de la disponibilidad	L2	L3
Adquisición o contratación (COM)	L2	L3
Aplicación de perfiles de seguridad (COM)	L2	L3
Protección criptográfica del canal (COM)	L2	L3
Norma de uso de los controles criptográficos	L2	L3
Mecanismo de integridad	L2	L3
Mecanismo de cifrado	L2	L3
Operación	L2	L3
Control de acceso a la red	L2	L3
Desconexión	L2	L3
Seguridad de los servicios de red	L2	L3
Protección frente a análisis del tráfico	L2	L3
Protección frente a emanaciones electromagnéticas (COM)	L2	L3
Cambios (actualizaciones y mantenimiento)	L2	L3
Terminación	L2	L3
Seguridad Wireless (WiFi)	L2	L3
Autorización previa de puntos de acceso	L2	L3
Eliminar claves por defecto en tarjetas y puntos de accesos antes de su despliegue	L2	L3
Deshabilitar los protocolos de gestión no esenciales	L2	L3
Comprobación periódica de los puntos de acceso (mediante broadcast o herramientas)	L2	L3
Desactivación del modo de conexión ad-hoc en los dispositivos de usuario	L2	L3
Autenticación de dispositivos wireless (filtrado MAC, servidor de autenticación, etc.)	L2	L3
Restricciones del protocolo SNMP en redes wireless	L2	L3
Control de direcciones IP	L2	L3

Cuadro 35. Valoración de las salvaguardas – Protección de las comunicaciones.  
 Fuente. Elaboración propia

### Elementos auxiliares

<i>salvaguarda</i>	[f1]	[f2]
Inventario de equipamiento auxiliar	L1	L3
Aseguramiento de la disponibilidad	L1	L3
Instalación	L1	L3
Suministro eléctrico	L1	L3
Climatización	L1	L3
Dimensionamiento adecuado del sistema	L1	L3
Control de temperatura	L1	L3
Control de humedad	L1	L3
Revisión y mantenimiento periódicos	L1	L3
Sistema de climatización redundante	L1	L3
Protección del cableado	L1	L3
Contenedores de seguridad	L1	L3

Cuadro 36. Valoración de las salvaguardas – Elementos auxiliares.

Fuente. Elaboración propia

### Protección de las instalaciones

<i>Salvaguarda</i>	[f1]	[f2]
Inventario de instalaciones	L1	L3
Normativa	L1	L3
Procedimientos	L1	L3
Diseño	L1	L3
Diseño observando reglas y normas relevantes sobre salud y sanidad	L1	L3
Separación de áreas de seguridad y de acceso público	L1	L3
Situar equipos sensibles en áreas separadas	L1	L3
Evitar que el acceso físico para operación y mantenimiento abra el acceso a otros activos	L1	L3
Separación de áreas gestionadas por otros	L1	L3
Separación de las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura, depósitos de combustible, etc.)	L1	L3
Separación de accesos para personas y vehículos	L1	L3
Carga / descarga	L1	L3
Procedimiento para la identificación visible de las personas	L1	L3
Instalaciones discretas minimizando indicaciones sobre su propósito	L1	L3
Las áreas no se identifican en directorios telefónicos y vestíbulos	L1	L3
Acceso a través de un área de recepción	L1	L3
Control de los accesos físicos	L1	L3
Protección del perímetro	L1	L3
Vigilancia	L1	L3
Protección frente a desastres	L1	L3
Iluminación de emergencia cubre todas las áreas necesarias para garantizar la continuidad de las misiones críticas	L1	L3
Protección frente a incendios	L1	L3
Protección frente a inundaciones	L1	L3
Protección frente a accidentes naturales e industriales	L1	L3
Protección frente a explosivos	L1	L3
Seguros	L1	L3
La seguridad de la instalación no es responsabilidad de un único guardia	L1	L3

Cuadro 37. Valoración de las salvaguardas – Protección de las instalaciones.

Fuente. Elaboración propia



### Gestión del Personal

<i>salvaguarda</i>	[f1]	[f2]
Política de gestión de personal (en materia de seguridad)	L1	L3
Procedimientos de gestión de personal (en materia de seguridad)	L1	L3
Relación de personal	L1	L3
Puestos de trabajo	L1	L3
Cambio de puesto de trabajo	L1	L3
Contratación	L1	L3
Formación y concienciación	L0	L3
Política de formación y concienciación	L0	L3
Procedimientos de formación y concienciación	L0	L3
Plan de formación y concienciación	L0	L3
Concienciación	L0	L3
Formación	L0	L3
Procedimientos relevantes de seguridad: emergencias, incidencias, ...	L1	L3
Prevención y reacción frente a extorsión	L1	L3
Prevención y reacción frente a ingeniería social	L1	L3
Protección del usuario frente a coacciones	L1	L3

Cuadro 38. Valoración de las salvaguardas – Gestión del Personal.  
Fuente. Elaboración propia

### Organización

<i>salvaguarda</i>	[f1]	[f2]
Organización interna	L0	L3
Comité de gestión de seguridad de la información	L0	L3
Coordinación interna	L0	L3
Roles identificados	L0	L3
Asignación de responsabilidades para la seguridad de la información	L0	L3
Cooperación con otras organizaciones	L0	L3
Se dispone de asesoramiento especializado en seguridad	L0	L3
Documentación del sistema	L0	L3
Normativa de seguridad (política, ...)	L0	L3
Planificación de seguridad	L0	L3
Continuidad del negocio (contingencia)	L0	L3
Gestión de la continuidad	L0	L3
Plan de continuidad	L0	L3
Seguros contra interrupciones en el negocio	L0	L3
Inspecciones de seguridad	L0	L3
Protección de los activos fuera de las instalaciones	L0	L3
Salvaguarda de los registros de la Organización	L0	L3

Cuadro 39. Valoración de las salvaguardas – Organización.  
Fuente. Elaboración propia

### Relaciones externas

<i>Salvaguarda</i>	[f1]	[f2]
Acuerdos para intercambio de información y software	L0	L3
Revisión del cumplimiento de acuerdos y contratos	L0	L3

Cuadro 40. Valoración de las salvaguardas – Relaciones externas.  
Fuente. Elaboración propia

### 3.2.4. Caracterización del Impacto

#### 3.2.4.1. Impacto acumulado

El impacto acumulado es el calculado sobre un activo teniendo en cuenta:

- Su valor acumulado (el propio mas el acumulado de los activos que depende de él).
- Las amenazas a que esta expuesto.

#### Dimensiones:

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

#### Fases:

- potencial
- [f1] situación actual
- [f2] situación objetivo

#### a) [D] disponibilidad

##### [IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[5]	[5]	[1]
[intd] Intranet de docentes	[6]	[6]	[2]
[sga] Sistema de gestión académica	[7]	[7]	[3]

Cuadro 41. Impacto acumulado – [D] disponibilidad - [IS] Servicios internos  
Fuente. Elaboración propia

### [E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[7]	[7]	[1]
[SW.WS] Windows Server 2003	[7]	[7]	[1]
[SW.FB] FreeBSD	[7]	[7]	[1]
[SW.SBA] Unix	[7]	[7]	[1]
[SW.AS] Apache	[7]	[7]	[1]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[9]	[4]
[HW.SC] Servidor de correo	[7]	[6]	[1]
[HW.FR] Firewall	[10]	[9]	[4]
[HW.SDM] Servidor DMZ	[7]	[7]	[1]
[HW.SWC] Switch Core	[10]	[9]	[4]
[HW.WA] Punto de acceso wireless	[10]	[9]	[4]
[HW.SW3] Switch 3 Com	[10]	[9]	[4]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[7]	[7]	[1]
[COM.RADIO] Red inalambrica	[7]	[6]	[1]
[COM.LAN] Red Lan	[7]	[7]	[1]
[AUX] Elementos auxiliares	[10]	[10]	[4]
[AUX.UPS] Sistema de alimentacion ininterrumpida	[10]	[10]	[4]
[AUX.WIRE] Cable UTP	[7]	[7]	[2]
[AUX.FIBER] Fibra optica	[7]	[7]	[2]
[AUX.TRA] Transformador de aislamiento	[10]	[10]	[4]

Cuadro 42. Impacto acumulado - [D] disponibilidad - [E] Equipamiento  
Fuente. Elaboración propia

### [P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[9]	[9]	[3]
[ADCO] Administrador de comunicaciones	[9]	[9]	[3]
[OP] Operadores	[6]	[6]	[0]

Cuadro 43. Impacto acumulado - [D] disponibilidad - [P] Personal  
Fuente. Elaboración propia

### [IN] Instalaciones

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	[10]	[10]	[4]
[ZA] Zungarococha-Facultad Agronomia	[10]	[10]	[4]
[AC] Almacen Central	[7]	[7]	[1]
[FQ] Facultad Quimica	[7]	[7]	[1]
[FD] Facultad Derecho	[7]	[7]	[1]

Cuadro 44. Impacto acumulado - [D] disponibilidad - [IN] Instalaciones  
Fuente. Elaboración propia

**b) [I] integridad de los datos**

**[IS] Servicios internos**

<i>activo</i>	potencial	[f1]	[f2]
[email] Correo electrónico de docentes	[6]	[5]	[2]
[intd] Intranet de docentes	[4]	[4]	[1]
[sga] Sistema de gestión académica	[6]	[6]	[2]

Cuadro 45. Impacto acumulado - [I] integridad de los datos - [IN] Servicios internos.

Fuente. Elaboración propia

**[E] Equipamiento**

<i>activo</i>	potencial	[f1]	[f2]
[SW] Aplicaciones	[10]	[9]	[4]
[SW.WS] Windows Server 2003	[9]	[8]	[3]
[SW.FB] FreeBSD	[10]	[9]	[4]
[SW.SBA] Unix	[10]	[9]	[4]
[SW.AS] Apache	[10]	[9]	[4]
[HW] Equipos	[10]	[9]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[8]	[4]
[HW.SC] Servidor de correo	[10]	[8]	[4]
[HW.FR] Firewall	[7]	[5]	[1]
[HW.SDM] Servidor DMZ	[0]	[0]	[0]
[HW.SWC] Switch Core	[7]	[5]	[1]
[HW.WA] Punto de acceso wireless	[4]	[2]	[0]
[HW.SW3] Switch 3 Com	[7]	[5]	[1]
[HW.SBC] Servidor de Backup	[10]	[9]	[4]
[COM] Comunicaciones	[4]	[3]	[0]
[COM.RADIO] Red inalambrica	[4]	[3]	[0]
[COM.LAN] Red Lan	[4]	[3]	[0]
[AUX] Elementos auxiliares	[4]	[4]	[0]
[AUX.UPS] Sistema de alimentacion ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[4]	[4]	[0]
[AUX.FIBER] Fibra optica	[0]	[0]	[0]
[AUX.TRA] Transformador de aislamiento	[0]	[0]	[0]

Cuadro 46. Impacto acumulado - [I] integridad de los datos - [E] Equipamiento

Fuente. Elaboración propia

**[P] Personal**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[10]	[10]	[4]
[ADCO] Administrador de comunicaciones	[10]	[10]	[4]
[OP] Operadores	[5]	[5]	[0]

Cuadro 47. Impacto acumulado - [I] integridad de los datos - [P] Personal  
 Fuente. Elaboración propia

**[IN] Instalaciones**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	[9]	[9]	[3]
[ZA] Zungarococha-Facultad Agronomía	[6]	[6]	[0]
[AC] Almacén Central	[6]	[6]	[0]
[FQ] Facultad Química	[6]	[6]	[0]
[FD] Facultad Derecho	[6]	[6]	[0]

Cuadro 48. Impacto acumulado - [I] integridad de los datos - [IN] Instalaciones  
 Fuente. Elaboración propia

**e) [C] confidencialidad de los datos**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[3]	[2]	[0]
[intd] Intranet de docentes	[1]	[1]	[0]
[sga] Sistema de gestión académica	[5]	[5]	[1]

Cuadro 49. Impacto acumulado - [C] confidencialidad de los datos - [IS] Servicios internos.  
 Fuente. Elaboración propia

### [E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[10]	[10]	[4]
[SW.WS] Windows Server 2003	[7]	[7]	[1]
[SW.FB] FreeBSD	[10]	[10]	[4]
[SW.SBA] Unix	[10]	[10]	[4]
[SW.AS] Apache	[10]	[10]	[4]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[8]	[4]
[HW.SC] Servidor de correo	[10]	[8]	[4]
[HW.FR] Firewall	[9]	[7]	[3]
[HW.SDM] Servidor DMZ	[0]	[0]	[0]
[HW.SWC] Switch Core	[9]	[7]	[3]
[HW.WA] Punto de acceso wireless	[5]	[3]	[0]
[HW.SW3] Switch 3 Com	[9]	[7]	[3]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[6]	[4]	[0]
[COM.RADIO] Red inalambrica	[5]	[4]	[0]
[COM.LAN] Red Lan	[6]	[4]	[0]
[AUX] Elementos auxiliares	[5]	[5]	[0]
[AUX.UPS] Sistema de alimentacion ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[5]	[5]	[0]
[AUX.FIBER] Fibra optica	[0]	[0]	[0]
[AUX.TRA] Transformador de aislamiento	[0]	[0]	[0]

Cuadro 50. Impacto acumulado - [C] confidencialidad de los datos - [E] Equipamiento.

Fuente. Elaboración propia

### [P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[10]	[10]	[4]
[ADCO] Administrador de comunicaciones	[10]	[10]	[4]
[OP] Operadores	[4]	[4]	[0]

Cuadro 51. Impacto acumulado - [C] confidencialidad de los datos - [P] Personal.

Fuente. Elaboración propia

### [IN] Instalaciones

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	[9]	[9]	[3]
[ZA] Zungarococha-Facultad Agronomía	[5]	[5]	[0]
[AC] Almacén Central	[5]	[5]	[0]
[FQ] Facultad Química	[5]	[5]	[0]
[FD] Facultad Derecho	[5]	[5]	[0]

Cuadro 52. Impacto acumulado - [C] confidencialidad de los datos - [IN] Instalaciones.

Fuente. Elaboración propia

**d) [A] autenticidad de los usuarios y de la información**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[6]	[5]	[2]
[intd] Intranet de docentes	[6]	[6]	[2]
[sga] Sistema de gestión académica	[7]	[7]	[3]

Cuadro 53. Impacto acumulado - [A] autenticidad de los usuarios y de la información - [IS] Servicios internos.

Fuente. Elaboración propia

**[E] Equipamiento**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[7]	[7]	[1]
[SW.WS] Windows Server 2003	[7]	[7]	[1]
[SW.FB] FreeBSD	[6]	[6]	[0]
[SW.SBA] Unix	[0]	[0]	[0]
[SW.AS] Apache	[6]	[6]	[0]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[8]	[4]
[HW.SC] Servidor de correo	[7]	[5]	[1]
[HW.FR] Firewall	[9]	[7]	[3]
[HW.SDM] Servidor DMZ	[7]	[7]	[1]
[HW.SWC] Switch Core	[9]	[7]	[3]
[HW.WA] Punto de acceso wireless	[9]	[7]	[3]
[HW.SW3] Switch 3 Com	[9]	[7]	[3]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[7]	[6]	[1]
[COM.RADIO] Red inalambrica	[7]	[5]	[1]
[COM.LAN] Red Lan	[7]	[6]	[1]
[AUX] Elementos auxiliares	[6]	[6]	[0]
[AUX.UPS] Sistema de alimentacion ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[6]	[6]	[0]
[AUX.FIBER] Fibra optica	[0]	[0]	[0]
[AUX.TRA] Transformador de aislamiento	[0]	[0]	[0]

Cuadro 54. Impacto acumulado - [A] autenticidad de los usuarios y de la información - [E] Equipamiento.

Fuente. Elaboración propia

**[P] Personal**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[10]	[10]	[4]
[ADCO] Administrador de comunicaciones	[10]	[10]	[4]
[OP] Operadores	[5]	[5]	[0]

Cuadro 55. Impacto acumulado - [A] autenticidad de los usuarios y de la información - [P] Personal.

Fuente. Elaboración propia

**[IN] Instalaciones**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	[9]	[9]	[3]
[ZA] Zungarococha-Facultad Agronomía	[9]	[9]	[3]
[AC] Almacén Central	[6]	[6]	[0]
[FQ] Facultad Química	[6]	[6]	[0]
[FD] Facultad Derecho	[6]	[6]	[0]

Cuadro 56. Impacto acumulado - [A] autenticidad de los usuarios y de la información - [IN] Instalaciones.

Fuente. Elaboración propia

**e) [T] trazabilidad del servicio y de los datos**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[6]	[5]	[2]
[intd] Intranet de docentes	[6]	[6]	[3]
[sga] Sistema de gestión académica	[7]	[7]	[4]

Cuadro 57. Impacto acumulado - [T] trazabilidad del servicio y de los datos - [IS] Servicios internos.

Fuente. Elaboración propia



### [E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[7]	[7]	[1]
[SW.WS] Windows Server 2003	[7]	[7]	[1]
[SW.FB] FreeBSD	[6]	[6]	[0]
[SW.SBA] Unix	[0]	[0]	[0]
[SW.AS] Apache	[6]	[6]	[0]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[8]	[4]
[HW.SC] Servidor de correo	[6]	[4]	[0]
[HW.FR] Firewall	[10]	[8]	[4]
[HW.SDM] Servidor DMZ	[0]	[0]	[0]
[HW.SWC] Switch Core	[10]	[8]	[4]
[HW.WA] Punto de acceso wireless	[10]	[8]	[4]
[HW.SW3] Switch 3 Com	[10]	[8]	[4]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[7]	[6]	[1]
[COM.RADIO] Red inalámbrica	[7]	[6]	[1]
[COM.LAN] Red Lan	[7]	[6]	[1]
[AUX] Elementos auxiliares	[9]	[9]	[3]
[AUX.UPS] Sistema de alimentación ininterrumpida	[9]	[9]	[3]
[AUX.WIRE] Cable UTP	[6]	[6]	[0]
[AUX.FIBER] Fibra óptica	[0]	[0]	[0]
[AUX.TRA] Transformador de aislamiento	[9]	[9]	[3]

Cuadro 58. Impacto acumulado - [T] trazabilidad del servicio y de los datos -  
[E] Equipamiento.

Fuente. Elaboración propia

### [P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[10]	[10]	[4]
[ADCO] Administrador de comunicaciones	[10]	[10]	[4]
[OP] Operadores	[6]	[6]	[0]

Cuadro 59. Impacto acumulado - [T] trazabilidad del servicio y de los datos -  
[P] Personal

Fuente. Elaboración propia

### [IN] Instalaciones

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	[9]	[9]	[3]
[ZA] Zungarococha-Facultad Agronomía	[9]	[9]	[3]
[AC] Almacén Central	[6]	[6]	[0]
[FQ] Facultad Química	[6]	[6]	[0]
[FD] Facultad Derecho	[6]	[6]	[0]

Cuadro 60. Impacto acumulado - [T] trazabilidad del servicio y de los datos -  
[IN] Instalaciones.

Fuente. Elaboración propia

### 3.2.4.2. Impacto repercutido

El impacto repercutido es el calculado sobre un activo teniendo en cuenta:

- Su valor propio.
- Las amenazas a las que están expuestos los activos de los que depende.

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

#### Dimensiones:

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

#### Fases:

- potencial
- [f1] situación actual
- [f2] situación objetivo

#### a) [D] disponibilidad

##### [IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[5]	[5]	[1]
[intd] Intranet de docentes	[6]	[6]	[2]
[sga] Sistema de gestión académica	[7]	[7]	[3]

Cuadro 61. Impacto repercutido - [D] disponibilidad - [IS] Servicios internos  
Fuente. Elaboración propia

### [E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[7]	[7]	[1]
[SW.WS] Windows Server 2003	[7]	[7]	[1]
[SW.FB] FreeBSD	[7]	[7]	[1]
[SW.SBA] Unix	[7]	[7]	[1]
[SW.AS] Apache	[7]	[7]	[1]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[10]	[4]
[HW.SC] Servidor de correo	[5]	[5]	[0]
[HW.FR] Firewall	[10]	[10]	[4]
[HW.SDM] Servidor DMZ	[7]	[7]	[1]
[HW.SWC] Switch Core	[10]	[10]	[4]
[HW.WA] Punto de acceso wireless	[10]	[10]	[4]
[HW.SW3] Switch 3 Com	[0]	[0]	[0]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[5]	[5]	[0]
[COM.RADIO] Red inalámbrica	[5]	[5]	[0]
[COM.LAN] Red Lan	[3]	[3]	[0]
[AUX] Elementos auxiliares	[7]	[7]	[2]
[AUX.UPS] Sistema de alimentación ininterrumpida	[5]	[5]	[0]
[AUX.WIRE] Cable UTP	[5]	[5]	[0]
[AUX.FIBER] Fibra óptica	[7]	[7]	[2]

Cuadro 62. Impacto repercutido - [D] disponibilidad - [E] Equipamiento  
Fuente. Elaboración propia

### [P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[4]	[4]	[0]
[ADCO] Administrador de comunicaciones	[4]	[4]	[0]
[OP] Operadores	[2]	[2]	[0]

Cuadro 63. Impacto repercutido - [D] disponibilidad - [P] Personal  
Fuente. Elaboración propia

**b) [I] integridad de los datos**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[7]	[7]	[2]
[intd] Intranet de docentes	[5]	[5]	[1]
[sga] Sistema de gestión académica	[7]	[7]	[2]

Cuadro 64. Impacto repercutido - [I] integridad de los datos - [IS] Servicios internos.

Fuente. Elaboración propia

**[E] Equipamiento**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[10]	[10]	[4]
[SW.WS] Windows Server 2003	[9]	[9]	[3]
[SW.FB] FreeBSD	[10]	[10]	[4]
[SW.SBA] Unix	[10]	[10]	[4]
[SW.AS] Apache	[10]	[9]	[4]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[10]	[4]
[HW.SC] Servidor de correo	[0]	[0]	[0]
[HW.FR] Firewall	[10]	[10]	[4]
[HW.SDM] Servidor DMZ	[0]	[0]	[0]
[HW.SWC] Switch Core	[0]	[0]	[0]
[HW.WA] Punto de acceso wireless	[0]	[0]	[0]
[HW.SW3] Switch 3 Com	[0]	[0]	[0]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[0]	[0]	[0]
[COM.RADIO] Red inalámbrica	[0]	[0]	[0]
[COM.LAN] Red Lan	[0]	[0]	[0]
[AUX] Elementos auxiliares	[0]	[0]	[0]
[AUX.UPS] Sistema de alimentación ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[0]	[0]	[0]
[AUX.FIBER] Fibra óptica	[0]	[0]	[0]

Cuadro 65. Impacto repercutido - [I] integridad de los datos - [E] Equipamiento.

Fuente. Elaboración propia

**[P] Personal**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[0]	[0]	[0]
[ADCO] Administrador de comunicaciones	[0]	[0]	[0]
[OP] Operadores	[0]	[0]	[0]

Cuadro 66. Impacto repercutido - [I] integridad de los datos - [P] Personal.

Fuente. Elaboración propia

**c) [C] confidencialidad de los datos**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[4]	[4]	[0]
[intd] Intranet de docentes	[2]	[2]	[0]
[sga] Sistema de gestión académica	[6]	[6]	[1]

Cuadro 67. Impacto repercutido - [C] confidencialidad de los datos - [IS] Servicios internos.

Fuente. Elaboración propia

**[E] Equipamiento**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[10]	[10]	[4]
[SW.WS] Windows Server 2003	[7]	[7]	[1]
[SW.FB] FreeBSD	[10]	[10]	[4]
[SW.SBA] Unix	[10]	[10]	[4]
[SW.AS] Apache	[10]	[10]	[4]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[10]	[4]
[HW.SC] Servidor de correo	[0]	[0]	[0]
[HW.FR] Firewall	[10]	[10]	[4]
[HW.SDM] Servidor DMZ	[0]	[0]	[0]
[HW.SWC] Switch Core	[0]	[0]	[0]
[HW.WA] Punto de acceso wireless	[0]	[0]	[0]
[HW.SW3] Switch 3 Com	[10]	[10]	[4]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[0]	[0]	[0]
[COM.RADIO] Red inalámbrica	[0]	[0]	[0]
[COM.LAN] Red Lan	[0]	[0]	[0]
[AUX] Elementos auxiliares	[0]	[0]	[0]
[AUX.UPS] Sistema de alimentación ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[0]	[0]	[0]
[AUX.FIBER] Fibra óptica	[0]	[0]	[0]

Cuadro 68. Impacto repercutido - [C] confidencialidad de los datos - [E] Equipamiento.

Fuente. Elaboración propia

**[P] Personal**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[0]	[0]	[0]
[ADCO] Administrador de comunicaciones	[0]	[0]	[0]
[OP] Operadores	[0]	[0]	[0]

Cuadro 69. Impacto repercutido - [C] confidencialidad de los datos - [P] Personal.

Fuente. Elaboración propia

**d) [A] autenticidad de los usuarios y de la información**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[6]	[6]	[2]
[intd] Intranet de docentes	[6]	[6]	[2]
[sga] Sistema de gestión académica	[7]	[7]	[3]

Cuadro 70. Impacto repercutido - [A] autenticidad de los usuarios y la información - [IS] Servicios internos.

Fuente. Elaboración propia

**[E] Equipamiento**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[0]	[0]	[0]
[SW.WS] Windows Server 2003	[0]	[0]	[0]
[SW.FB] FreeBSD	[0]	[0]	[0]
[SW.SBA] Unix	[0]	[0]	[0]
[SW.AS] Apache	[0]	[0]	[0]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[10]	[4]
[HW.SC] Servidor de correo	[7]	[7]	[1]
[HW.FR] Firewall	[10]	[10]	[4]
[HW.SDM] Servidor DMZ	[7]	[7]	[1]
[HW.SWC] Switch Core	[0]	[0]	[0]
[HW.WA] Punto de acceso wireless	[10]	[10]	[4]
[HW.SW3] Switch 3 Com	[10]	[10]	[4]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[0]	[0]	[0]
[COM.RADIO] Red inalámbrica	[0]	[0]	[0]
[COM.LAN] Red Lan	[0]	[0]	[0]
[AUX] Elementos auxiliares	[0]	[0]	[0]
[AUX.UPS] Sistema de alimentación ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[0]	[0]	[0]
[AUX.FIBER] Fibra optica	[0]	[0]	[0]

Cuadro 71. Impacto repercutido - [A] autenticidad de los usuarios y la información - [E] Equipamiento.

Fuente. Elaboración propia

**[P] Personal**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[0]	[0]	[0]
[ADCO] Administrador de comunicaciones	[0]	[0]	[0]
[OP] Operadores	[0]	[0]	[0]

Cuadro 72. Impacto repercutido - [A] autenticidad de los usuarios y la información - [P] Personal.

Fuente. Elaboración propia

**e) [T] trazabilidad del servicio y de los datos**

**[IS] Servicios internos**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	[6]	[6]	[2]
[intd] Intranet de docentes	[6]	[6]	[3]
[sga] Sistema de gestión académica	[7]	[7]	[4]

Cuadro 73. Impacto repercutido - [T] trazabilidad del servicio y de los datos - [IS] Servicios internos.

Fuente. Elaboración propia

**[E] Equipamiento**

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	[0]	[0]	[0]
[SW.WS] Windows Server 2003	[0]	[0]	[0]
[SW.FB] FreeBSD	[0]	[0]	[0]
[SW.SBA] Unix	[0]	[0]	[0]
[SW.AS] Apache	[0]	[0]	[0]
[HW] Equipos	[10]	[10]	[4]
[HW.SA] Servidor de aplicaciones y Base de Datos	[10]	[10]	[4]
[HW.SC] Servidor de correo	[0]	[0]	[0]
[HW.FR] Firewall	[10]	[10]	[4]
[HW.SDM] Servidor DMZ	[0]	[0]	[0]
[HW.SWC] Switch Core	[0]	[0]	[0]
[HW.WA] Punto de acceso wireless	[10]	[10]	[4]
[HW.SW3] Switch 3 Com	[0]	[0]	[0]
[HW.SBC] Servidor de Backup	[10]	[10]	[4]
[COM] Comunicaciones	[0]	[0]	[0]
[COM.RADIO] Red inalámbrica	[0]	[0]	[0]
[COM.LAN] Red Lan	[0]	[0]	[0]
[AUX] Elementos auxiliares	[0]	[0]	[0]
[AUX.UPS] Sistema de alimentación ininterrumpida	[0]	[0]	[0]
[AUX.WIRE] Cable UTP	[0]	[0]	[0]
[AUX.FIBER] Fibra optica	[0]	[0]	[0]

Cuadro 74. Impacto repercutido - [T] trazabilidad del servicio y de los datos - [E] Equipamiento.

Fuente. Elaboración propia

### [P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	[0]	[0]	[0]
[ADCO] Administrador de comunicaciones	[0]	[0]	[0]
[OP] Operadores	[0]	[0]	[0]

Cuadro75. Impacto repercutido - [T] trazabilidad del servicio y de los datos –  
[P] Personal.

Fuente. Elaboración propia

## 3.2.5. Caracterización del Riesgo

### 3.2.5.1. Riesgo acumulado

El riesgo acumulado es el calculado sobre un activo teniendo en cuenta:

- El impacto acumulado sobre un activo debido a una amenaza.
- La frecuencia de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

#### Nivel de criticidad

- {0} := despreciable
- {1} := bajo
- {3} := medio
- {5} := alto
- {7} := muy alto
- {10} := crítico

#### Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

#### Fases

- potencial
- [f1] situación actual
- [f2] situación objetivo



**a) [D] disponibilidad**

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{5.7}	{4.7}	{1.9}
[intd] Intranet de docentes	{6.2}	{5.8}	{2.6}
[sga] Sistema de gestión académica	{6.8}	{6.4}	{3.2}

Cuadro76. Riesgo acumulado - [D] disponibilidad - [IS] Servicios internos  
Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{6.8}	{5.7}	{1.6}
[SW.WS] Windows Server 2003	{6.8}	{5.7}	{1.6}
[SW.FB] FreeBSD	{6.8}	{5.7}	{1.6}
[SW.SBA] Unix	{5.9}	{5.1}	{0.7}
[SW.AS] Apache	{5.9}	{5.1}	{0.7}
[HW] Equipos	{8.0}	{6.9}	{2.6}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.1}	{2.6}
[HW.SC] Servidor de correo	{6.2}	{4.3}	{0.8}
[HW.FR] Firewall	{8.0}	{5.9}	{2.6}
[HW.SDM] Servidor DMZ	{5.9}	{5.1}	{0.7}
[HW.SWC] Switch Core	{8.0}	{6.0}	{2.6}
[HW.WA] Punto de acceso wireless	{8.0}	{6.0}	{2.6}
[HW.SW3] Switch 3 Com	{8.0}	{6.0}	{2.6}
[HW.SBC] Servidor de Backup	{7.7}	{6.9}	{2.4}
[COM] Comunicaciones	{5.9}	{4.8}	{0.7}
[COM.RADIO] Red inalámbrica	{5.9}	{4.5}	{0.7}
[COM.LAN] Red Lan	{5.9}	{4.8}	{0.7}
[AUX] Elementos auxiliares	{6.6}	{6.6}	{1.3}
[AUX.UPS] Sistema de alimentación ininterrumpida	{6.6}	{6.6}	{1.3}
[AUX.WIRE] Cable UTP	{5.9}	{5.9}	{0.7}
[AUX.FIBER] Fibra óptica	{5.9}	{5.9}	{0.7}
[AUX.TRA] Transformador de aislamiento	{6.6}	{6.6}	{1.3}

Cuadro77. Riesgo acumulado - [D] disponibilidad - [E] Equipamiento  
Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	{6.3}	{6.1}	{1.0}
[ADCO] Administrador de comunicaciones	{6.3}	{6.1}	{1.0}
[OP] Operadores	{4.3}	{4.2}	{0.0}

Cuadro78. Riesgo acumulado - [D] disponibilidad - [P] Personal  
Fuente. Elaboración propia

[IN] Instalación

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	{6.8}	{6.8}	{1.6}
[ZA] Zungarococha-Facultad Agronomía	{6.8}	{6.8}	{1.6}
[AC] Almacén Central	{5.1}	{5.0}	{0.0}
[FQ] Facultad Química	{5.1}	{5.0}	{0.0}
[FD] Facultad Derecho	{5.1}	{5.0}	{0.0}

Cuadro79. Riesgo acumulado - [D] disponibilidad - [I] Instalación  
Fuente. Elaboración propia

**b) [I] integridad de los datos**

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{6.3}	{5.3}	{2.9}
[intd] Intranet de docentes	{5.1}	{4.8}	{2.0}
[sga] Sistema de gestión académica	{6.3}	{5.9}	{3.1}

Cuadro80. Riesgo acumulado - [I] integridad de los datos - [IS] Servicios internos.  
Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{8.0}	{6.9}	{2.7}
[SW.WS] Windows Server 2003	{7.4}	{6.3}	{2.1}
[SW.FB] FreeBSD	{8.0}	{6.9}	{2.7}
[SW.SBA] Unix	{8.0}	{6.8}	{2.7}
[SW.AS] Apache	{8.0}	{6.9}	{2.7}
[HW] Equipos	{8.0}	{6.9}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.1}	{2.6}
[HW.SC] Servidor de correo	{8.0}	{6.1}	{2.6}
[HW.FR] Firewall	{5.7}	{4.2}	{0.3}
[HW.SDM] Servidor DMZ	-	-	-
[HW.SWC] Switch Core	{5.7}	{4.2}	{0.3}
[HW.WA] Punto de acceso wireless	{3.9}	{2.5}	{0.0}
[HW.SW3] Switch 3 Com	{5.7}	{4.2}	{0.3}
[HW.SBC] Servidor de Backup	{8.0}	{6.9}	{2.7}
[COM] Comunicaciones	{4.2}	{3.1}	{0.0}
[COM.RADIO] Red inalámbrica	{4.2}	{3.0}	{0.0}
[COM.LAN] Red Lan	{4.2}	{3.1}	{0.0}
[AUX] Elementos auxiliares	{3.3}	{3.3}	{0.0}
[AUX.UPS] Sistema de alimentación ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	{3.3}	{3.3}	{0.0}
[AUX.FIBER] Fibra optica	-	-	-
[AUX.TRA] Transformador de aislamiento	-	-	-

Cuadro81. Riesgo acumulado - [I] integridad de los datos - [E] Equipamiento.  
Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	{6.8}	{6.4}	{1.5}
[ADCO] Administrador de comunicaciones	{6.8}	{6.4}	{1.5}
[OP] Operadores	{3.6}	{3.2}	{0.0}

Cuadro82. Riesgo acumulado - [I] integridad de los datos - [P] Personal.  
Fuente. Elaboración propia

[IN] Instalación

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	{6.3}	{6.2}	{1.1}
[ZA] Zungarococha-Facultad Agronomía	{4.5}	{4.5}	{0.0}
[AC] Almacén Central	{4.5}	{4.5}	{0.0}
[FQ] Facultad Química	{4.5}	{4.5}	{0.0}
[FD] Facultad Derecho	{4.5}	{4.5}	{0.0}

Cuadro83. Riesgo acumulado - [I] integridad de los datos - [IN] Instalación.  
Fuente. Elaboración propia

c) [C] confidencialidad de los datos

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{4.5}	{3.8}	{1.2}
[intd] Intranet de docentes	{3.4}	{3.0}	{0.3}
[sga] Sistema de gestión académica	{5.7}	{5.4}	{2.6}

Cuadro84. Riesgo acumulado - [C] confidencialidad de los datos - [IS] Servicios internos.  
Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{8.1}	{7.2}	{2.8}
[SW.WS] Windows Server 2003	{6.3}	{5.4}	{1.1}
[SW.FB] FreeBSD	{8.1}	{7.2}	{2.8}
[SW.SBA] Unix	{8.0}	{7.0}	{2.7}
[SW.AS] Apache	{8.0}	{7.0}	{2.7}
[HW] Equipos	{8.0}	{7.0}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.1}	{2.6}
[HW.SC] Servidor de correo	{8.0}	{6.1}	{2.6}
[HW.FR] Firewall	{6.9}	{5.4}	{1.6}
[HW.SDM] Servidor DMZ	-	-	-
[HW.SWC] Switch Core	{6.9}	{5.5}	{1.5}
[HW.WA] Punto de acceso wireless	{4.6}	{3.1}	{0.0}
[HW.SW3] Switch 3 Com	{6.9}	{5.5}	{1.5}
[HW.SBC] Servidor de Backup	{8.0}	{7.0}	{2.7}
[COM] Comunicaciones	{4.8}	{3.8}	{0.0}
[COM.RADIO] Red inalambrica	{4.8}	{3.6}	{0.0}
[COM.LAN] Red Lan	{4.8}	{3.8}	{0.0}
[AUX] Elementos auxiliares	{3.9}	{3.9}	{0.0}
[AUX.UPS] Sistema de alimentación ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	{3.9}	{3.9}	{0.0}
[AUX.FIBER] Fibra óptica	-	-	-
[AUX.TRA] Transformador de aislamiento	-	-	-

Cuadro85. Riesgo acumulado - [C] confidencialidad de los datos - [E] Equipamiento.

Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	{6.9}	{6.8}	{1.7}
[ADCO] Administrador de comunicaciones	{6.9}	{6.8}	{1.7}
[OP] Operadores	{3.0}	{2.6}	{0.0}

Cuadro86. Riesgo acumulado - [C] confidencialidad de los datos - [P] Personal.

Fuente. Elaboración propia

[IN] Instalación

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	{6.3}	{6.2}	{1.1}
[ZA] Zungarococha-Facultad Agronomía	{3.9}	{3.9}	{0.0}
[AC] Almacén Central	{3.9}	{3.9}	{0.0}
[FQ] Facultad Química	{3.9}	{3.9}	{0.0}
[FD] Facultad Derecho	{3.9}	{3.9}	{0.0}

Cuadro87. Riesgo acumulado - [C] confidencialidad de los datos - [IN] Instalación.

Fuente. Elaboración propia

**d) [A] autenticidad de los usuarios y de la información**

[IS] Servicios internos

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{6.2}	{5.3}	{2.9}
[intd] Intranet de docentes	{6.2}	{5.9}	{3.1}
[sga] Sistema de gestión académica	{6.8}	{6.5}	{3.7}

Cuadro88. Riesgo acumulado - [A] autenticidad de los usuarios y la información - [IS] Servicios internos.

Fuente. Elaboración propia

[E] Equipamiento

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{6.3}	{5.4}	{1.1}
[SW.WS] Windows Server 2003	{6.3}	{5.4}	{1.1}
[SW.FB] FreeBSD	{5.7}	{4.8}	{0.5}
[SW.SBA] Unix	-	-	-
[SW.AS] Apache	{5.6}	{4.7}	{0.3}
[HW] Equipos	{8.0}	{7.0}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.1}	{2.6}
[HW.SC] Servidor de correo	{6.2}	{4.4}	{0.8}
[HW.FR] Firewall	{6.9}	{5.4}	{1.6}
[HW.SDM] Servidor DMZ	{6.2}	{5.2}	{0.9}
[HW.SWC] Switch Core	{6.9}	{5.5}	{1.5}
[HW.WA] Punto de acceso wireless	{6.9}	{5.5}	{1.5}
[HW.SW3] Switch 3 Com	{6.9}	{5.5}	{1.5}
[HW.SBC] Servidor de Backup	{8.0}	{7.0}	{2.7}
[COM] Comunicaciones	{5.4}	{4.4}	{0.2}
[COM.RADIO] Red inalambrica	{5.4}	{4.2}	{0.2}
[COM.LAN] Red Lan	{5.4}	{4.4}	{0.2}
[AUX] Elementos auxiliares	{4.5}	{4.5}	{0.0}
[AUX.UPS] Sistema de alimentacion ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	{4.5}	{4.5}	{0.0}
[AUX.FIBER] Fibra optica	-	-	-
[AUX.TRA] Transformador de aislamiento	-	-	-

Cuadro89. Riesgo acumulado - [A] autenticidad de los usuarios y la información - [E] Equipamiento.

Fuente. Elaboración propia

[P] Personal

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	{6.9}	{6.8}	{1.7}
[ADCO] Administrador de comunicaciones	{6.9}	{6.8}	{1.7}
[OP] Operadores	{3.6}	{3.2}	{0.0}

Cuadro90. Riesgo acumulado - [A] autenticidad de los usuarios y la información - [P] Personal.

Fuente. Elaboración propia

[IN] Instalación

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	{6.3}	{6.2}	{1.1}
[ZA] Zungarococha-Facultad Agronomía	{6.3}	{6.2}	{1.1}
[AC] Almacén Central	{4.5}	{4.5}	{0.0}
[FQ] Facultad Química	{4.5}	{4.5}	{0.0}
[FD] Facultad Derecho	{4.5}	{4.5}	{0.0}

Cuadro91. Riesgo acumulado - [A] autenticidad de los usuarios y la información - [IN] Instalación.

Fuente. Elaboración propia

e) [T] trazabilidad del servicio y de los datos

[IS] Servicios internos

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{5.4}	{4.4}	{2.2}
[intd] Intranet de docentes	{5.4}	{5.0}	{2.4}
[sga] Sistema de gestión académica	{5.9}	{5.5}	{3.0}

Cuadro92. Riesgo acumulado - [T] trazabilidad del servicio y de los datos - [IS] Servicios internos.

Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{6.2}	{5.3}	{0.9}
[SW.WS] Windows Server 2003	{6.2}	{5.3}	{0.9}
[SW.FB] FreeBSD	{5.6}	{4.7}	{0.3}
[SW.SBA] Unix	-	-	-
[SW.AS] Apache	{5.6}	{4.7}	{0.3}
[HW] Equipos	{8.0}	{7.0}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.2}	{2.6}
[HW.SC] Servidor de correo	{5.6}	{3.8}	{0.2}
[HW.FR] Firewall	{6.6}	{5.2}	{1.2}
[HW.SDM] Servidor DMZ	-	-	-
[HW.SWC] Switch Core	{6.6}	{5.3}	{1.2}
[HW.WA] Punto de acceso wireless	{6.6}	{5.3}	{1.2}
[HW.SW3] Switch 3 Com	{6.6}	{5.3}	{1.2}
[HW.SBC] Servidor de Backup	{8.0}	{7.0}	{2.7}
[COM] Comunicaciones	{5.1}	{4.2}	{0.0}
[COM.RADIO] Red inalambrica	{5.1}	{3.9}	{0.0}
[COM.LAN] Red Lan	{5.1}	{4.2}	{0.0}
[AUX] Elementos auxiliares	{6.0}	{6.0}	{0.7}
[AUX.UPS] Sistema de alimentacion ininterrumpida	{6.0}	{6.0}	{0.7}
[AUX.WIRE] Cable UTP	{4.3}	{4.3}	{0.0}
[AUX.FIBER] Fibra optica	-	-	-
[AUX.TRA] Transformador de aislamiento	{6.0}	{6.0}	{0.7}

Cuadro93. Riesgo acumulado - [T] trazabilidad del servicio y de los datos –  
[E] Equipamiento.

Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	{6.9}	{6.8}	{1.7}
[ADCO] Administrador de comunicaciones	{6.9}	{6.8}	{1.7}
[OP] Operadores	{4.5}	{4.1}	{0.0}

Cuadro94. Riesgo acumulado - [T] trazabilidad del servicio y de los datos –  
[P] Personal.

Fuente. Elaboración propia

[IN] Instalación

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[EH] Edificio Herbario	{6.3}	{6.2}	{1.1}
[ZA] Zungarococha-Facultad Agronomía	{6.3}	{6.2}	{1.1}
[AC] Almacén Central	{4.5}	{4.5}	{0.0}
[FQ] Facultad Química	{4.5}	{4.5}	{0.0}
[FD] Facultad Derecho	{4.5}	{4.5}	{0.0}

Cuadro95. Riesgo acumulado - [T] trazabilidad del servicio y de los datos –  
[IN] Instalaciones.

Fuente. Elaboración propia

### 3.2.5.2. Riesgo repercutido

El riesgo repercutido es el calculado sobre un activo teniendo en cuenta:

- El impacto repercutido sobre un activo debido a la amenaza.
- La frecuencia de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza.

#### Nivel de criticidad

- {0} := despreciable
- {1} := bajo
- {3} := medio
- {5} := alto
- {7} := muy alto
- {10} := crítico

#### Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

#### Fases

- potencial
- [f1] situación actual
- [f2] situación objetivo

#### a) [D] disponibilidad

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{5.7}	{4.8}	{1.9}
[intd] Intranet de docentes	{6.2}	{5.8}	{2.6}
[sga] Sistema de gestión académica	{6.8}	{6.4}	{3.2}

Cuadro96. Riesgo repercutido - [D] disponibilidad - [IS] Servicios internos.

Fuente. Elaboración propia



[E] Equipamiento

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{6.8}	{5.7}	{1.6}
[SW.WS] Windows Server 2003	{6.8}	{5.7}	{1.6}
[SW.FB] FreeBSD	{6.8}	{5.7}	{1.6}
[SW.SBA] Unix	{5.9}	{5.1}	{0.7}
[SW.AS] Apache	{5.9}	{5.1}	{0.7}
[HW] Equipos	{8.0}	{6.9}	{2.6}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.8}	{2.6}
[HW.SC] Servidor de correo	{5.0}	{3.8}	{0.0}
[HW.FR] Firewall	{8.0}	{6.8}	{2.6}
[HW.SDM] Servidor DMZ	{6.2}	{5.1}	{0.8}
[HW.SWC] Switch Core	{8.0}	{6.8}	{2.6}
[HW.WA] Punto de acceso wireless	{8.0}	{6.8}	{2.6}
[HW.SW3] Switch 3 Com	-	-	-
[HW.SBC] Servidor de Backup	{7.7}	{6.9}	{2.4}
[COM] Comunicaciones	{5.0}	{3.8}	{0.0}
[COM.RADIO] Red inalambrica	{5.0}	{3.8}	{0.0}
[COM.LAN] Red Lan	{3.6}	{3.6}	{0.0}
[AUX] Elementos auxiliares	{5.9}	{5.9}	{0.7}
[AUX.UPS] Sistema de alimentacion ininterrumpida	{3.6}	{3.6}	{0.0}
[AUX.WIRE] Cable UTP	{4.8}	{4.8}	{0.0}
[AUX.FIBER] Fibra optica	{5.9}	{5.9}	{0.7}

Cuadro97. Riesgo repercutido - [D] disponibilidad - [E] Equipamiento.  
Fuente. Elaboración propia

[P] Personal

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	{3.3}	{3.2}	{0.0}
[ADCO] Administrador de comunicaciones	{3.3}	{3.2}	{0.0}
[OP] Operadores	{1.9}	{1.9}	{0.0}

Cuadro98. Riesgo repercutido - [D] disponibilidad - [P] Personal.  
Fuente. Elaboración propia

**b) [I] integridad de los datos**

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{6.3}	{5.3}	{2.9}
[intd] Intranet de docentes	{5.1}	{4.8}	{2.0}
[sga] Sistema de gestión académica	{6.3}	{6.0}	{3.1}

Cuadro99. Riesgo repercutido - [I] integridad de los datos - [IS] Servicios internos.

Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{8.0}	{6.9}	{2.7}
[SW.WS] Windows Server 2003	{7.4}	{6.3}	{2.1}
[SW.FB] FreeBSD	{8.0}	{6.9}	{2.7}
[SW.SBA] Unix	{8.0}	{6.9}	{2.7}
[SW.AS] Apache	{8.0}	{6.9}	{2.7}
[HW] Equipos	{8.0}	{6.9}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.4}	{2.6}
[HW.SC] Servidor de correo	-	-	-
[HW.FR] Firewall	{6.8}	{6.4}	{1.5}
[HW.SDM] Servidor DMZ	-	-	-
[HW.SWC] Switch Core	-	-	-
[HW.WA] Punto de acceso wireless	-	-	-
[HW.SW3] Switch 3 Com	-	-	-
[HW.SBC] Servidor de Backup	{8.0}	{6.9}	{2.7}
[COM] Comunicaciones	-	-	-
[COM.RADIO] Red inalámbrica	-	-	-
[COM.LAN] Red Lan	-	-	-
[AUX] Elementos auxiliares	-	-	-
[AUX.UPS] Sistema de alimentación ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	-	-	-
[AUX.FIBER] Fibra óptica	-	-	-

Cuadro100. Riesgo repercutido - [I] integridad de los datos - [E] Equipamiento

Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	-	-	-
[ADCO] Administrador de comunicaciones	-	-	-
[OP] Operadores	-	-	-

Cuadro101. Riesgo repercutido - [I] integridad de los datos - [P] Personal

Fuente. Elaboración propia

c) [C] **confidencialidad de los datos**

[IS] Servicios internos

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{4.5}	{3.8}	{1.2}
[intd] Intranet de docentes	{3.4}	{3.0}	{0.3}
[sga] Sistema de gestión académica	{5.7}	{5.4}	{2.6}

Cuadro102. Riesgo repercutido - [C] confidencialidad de los datos - [IS]  
Servicios internos.

Fuente. Elaboración propia

[E] Equipamiento

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	{8.1}	{7.2}	{2.8}
[SW.WS] Windows Server 2003	{6.3}	{5.4}	{1.1}
[SW.FB] FreeBSD	{8.1}	{7.2}	{2.8}
[SW.SBA] Unix	{8.0}	{7.0}	{2.7}
[SW.AS] Apache	{8.0}	{7.0}	{2.7}
[HW] Equipos	{8.0}	{7.0}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.8}	{2.6}
[HW.SC] Servidor de correo	-	-	-
[HW.FR] Firewall	{6.9}	{6.8}	{1.7}
[HW.SDM] Servidor DMZ	-	-	-
[HW.SWC] Switch Core	-	-	-
[HW.WA] Punto de acceso wireless	-	-	-
[HW.SW3] Switch 3 Com	{6.9}	{6.8}	{1.7}
[HW.SBC] Servidor de Backup	{8.0}	{7.0}	{2.7}
[COM] Comunicaciones	-	-	-
[COM.RADIO] Red inalambrica	-	-	-
[COM.LAN] Red Lan	-	-	-
[AUX] Elementos auxiliares	-	-	-
[AUX.UPS] Sistema de alimentacion ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	-	-	-
[AUX.FIBER] Fibra optica	-	-	-

Cuadro103. Riesgo repercutido - [C] confidencialidad de los datos - [E]  
Equipamiento.

Fuente. Elaboración propia

[P] Personal

<b>activo</b>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	-	-	-
[ADCO] Administrador de comunicaciones	-	-	-
[OP] Operadores	-	-	-

Cuadro104. Riesgo repercutido - [C] confidencialidad de los datos - [P]  
Personal.

Fuente. Elaboración propia

**d) [A] autenticidad de los usuarios y de la información**

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{6.2}	{5.3}	{2.9}
[intd] Intranet de docentes	{6.2}	{5.9}	{3.1}
[sga] Sistema de gestión académica	{6.8}	{6.5}	{3.7}

Cuadro105. Riesgo repercutido - [A] autenticidad de los usuarios y la información - [IS] Servicios internos.

Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	-	-	-
[SW.WS] Windows Server 2003	-	-	-
[SW.FB] FreeBSD	-	-	-
[SW.SBA] Unix	-	-	-
[SW.AS] Apache	-	-	-
[HW] Equipos	{8.0}	{7.0}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.8}	{2.6}
[HW.SC] Servidor de correo	{6.2}	{5.0}	{0.8}
[HW.FR] Firewall	{6.9}	{6.8}	{1.7}
[HW.SDM] Servidor DMZ	{6.2}	{5.2}	{0.9}
[HW.SWC] Switch Core	-	-	-
[HW.WA] Punto de acceso wireless	{6.9}	{6.8}	{1.7}
[HW.SW3] Switch 3 Com	{6.9}	{6.8}	{1.7}
[HW.SBC] Servidor de Backup	{8.0}	{7.0}	{2.7}
[COM] Comunicaciones	-	-	-
[COM.RADIO] Red inalámbrica	-	-	-
[COM.LAN] Red Lan	-	-	-
[AUX] Elementos auxiliares	-	-	-
[AUX.UPS] Sistema de alimentación ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	-	-	-
[AUX.FIBER] Fibra óptica	-	-	-

Cuadro106. Riesgo repercutido - [A] autenticidad de los usuarios y la información - [E] Equipamiento.

Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	-	-	-
[ADCO] Administrador de comunicaciones	-	-	-
[OP] Operadores	-	-	-

Cuadro107. Riesgo repercutido - [A] autenticidad de los usuarios y la información - [P] Personal.

Fuente. Elaboración propia

e) [T] trazabilidad del servicio y de los datos

[IS] Servicios internos

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[email] Correo electrónico de docentes	{5.6}	{4.7}	{2.2}
[intd] Intranet de docentes	{5.6}	{5.0}	{2.4}
[sga] Sistema de gestión académica	{6.2}	{5.5}	{3.0}

Cuadro 108. Riesgo repercutido - [T] trazabilidad del servicio y de los datos  
- [IS] Servicios internos.

Fuente. Elaboración propia

[E] Equipamiento

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[SW] Aplicaciones	-	-	-
[SW.WS] Windows Server 2003	-	-	-
[SW.FB] FreeBSD	-	-	-
[SW.SBA] Unix	-	-	-
[SW.AS] Apache	-	-	-
[HW] Equipos	{8.0}	{7.0}	{2.7}
[HW.SA] Servidor de aplicaciones y Base de Datos	{8.0}	{6.8}	{2.6}
[HW.SC] Servidor de correo	-	-	-
[HW.FR] Firewall	{6.9}	{6.8}	{1.7}
[HW.SDM] Servidor DMZ	-	-	-
[HW.SWC] Switch Core	-	-	-
[HW.WA] Punto de acceso wireless	{6.9}	{6.8}	{1.7}
[HW.SW3] Switch 3 Com	-	-	-
[HW.SBC] Servidor de Backup	{8.0}	{7.0}	{2.7}
[COM] Comunicaciones	-	-	-
[COM.RADIO] Red inalámbrica	-	-	-
[COM.LAN] Red Lan	-	-	-
[AUX] Elementos auxiliares	-	-	-
[AUX.UPS] Sistema de alimentación ininterrumpida	-	-	-
[AUX.WIRE] Cable UTP	-	-	-
[AUX.FIBER] Fibra optica	-	-	-

Cuadro 109. Riesgo repercutido - [T] trazabilidad del servicio y de los datos  
- [E] Equipamiento.

Fuente. Elaboración propia

[P] Personal

<i>activo</i>	<b>potencial</b>	<b>[f1]</b>	<b>[f2]</b>
[ADSD] Administrador de sistemas y Base de datos	-	-	-
[ADCO] Administrador de comunicaciones	-	-	-
[OP] Operadores	-	-	-

Cuadro 110. Riesgo repercutido - [T] trazabilidad del servicio y de los datos  
- [P] Personal

Fuente. Elaboración propia

### **3.3. Gestión de Riesgos**

#### **3.3.1. Plan de Contingencia**

##### **3.3.1.1. Servicios internos**

#### **A. Procedimientos a desarrollar ante una falla o carencia de uno de los servicios que se prestan a través de la red.**

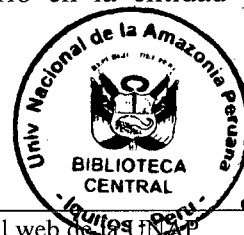
**a.1. Falta de correo electrónico de docentes.** Para garantizar el flujo de la correspondencia se debe recurrir al flujo del documento físico o verbal (llamada telefónica al personal encargado de verificar el problema en la Oficina de Sistemas Informáticos y de Comunicaciones) hasta que restablezca el servicio; cuando se utilice el documento físico se deberá manejar dos copias del documento; una para el destinatario y otra para el remitente en la cual se debe registrar el recibido.

**a.2. Falta de Intranet de docentes.** Dada que la intranet es un servicio para la divulgación de la información, su carencia no genera mayores traumas al interior de la organización. Al momento de presentarse problemas con este servicio debe procederse así:

- Tomar posesión del computador alternativa para restablecer el funcionamiento de este servicio.
- Realizar la configuración necesaria en el computador a fin de que los cambios no generen problemas con los usuarios finales.
- Instalar todos los archivos necesarios para restablecer el servicio.

**a.3. Falta de sistema de gestión académica.** La carencia de elementos de software desarrollados se debe a fallas en servidores o software de desarrollo, estas fallas por lo general son de soluciones demoradas, el procedimiento a seguir ante esta eventualidad es:

- Evaluar la magnitud del problema contra la necesidad del aplicativo.
- Contactar al responsable de la administración del sistema de gestión académica.
- Configurar el ambiente de trabajo necesario en la entidad para instalar los aplicativos.
- Probar la funcionalidad de los aplicativos.



- Definir horarios de trabajo y asignar responsable para el procesamiento de la información.
- Realizar las tareas de backup necesarios para garantizar la integridad de la información.

### **3.3.1.2. Equipamiento**

#### **3.3.1.2.1. Aplicaciones**

##### **A. Procedimientos Preventivos**

1. Toda aplicación utilizada deberá tener una licencia de uso, no está permitido la instalación de ningún software que no esté autorizado por OSIC.
2. Se considera una falta grave y posible de sanción la instalación no autorizada de software.
3. Para mantener la integridad de las aplicaciones se deberá utilizar controles y administración de la configuración de los equipos para monitorear toda la instalación de software y actualización en los equipos críticos de la red.
4. Se deberá mantener el software original (sistemas operativos, sistemas de aplicación y otros.)
5. El administrador de correo electrónico deberá coordinar con el personal de soporte técnico la correcta configuración del cliente de correo.
6. Los usuarios sólo podrán ingresar a las aplicaciones autorizadas, desde sus puestos de trabajo y dentro del horario establecido para el desempeño de sus labores.
7. Toda información acerca de las aplicaciones de la UNAP es confidencial y de carácter restringido, por lo que está prohibido su divulgación y salidas de la institución.
8. No se implementará ningún servicio o aplicación accesible desde el exterior o internet, que brinde información de la institución sin la debida autorización de OSIC.
9. La base de datos de las aplicaciones que involucren información crítica, valiosa o confidencial, deberán permanecer encriptado en todos los locales externos y su desencriptación deberá ser realizada sólo por las aplicaciones que trabajen con dicha aplicación.
10. Toda aplicación deberá permitir el cambio periódico del password a los usuarios.

### 3.3.1.2.2. Equipos

#### A. Procedimientos Preventivos

1. Para el software básico almacenado en los Servidores, tener una relación con los requerimientos de hardware mínimos necesarios para su instalación, en caso de ocurrir una eventualidad con uno de los servidores y deba ser instalada en otra máquina para ser reemplazada momentáneamente al Servidor.
2. Tener identificados e inventariado otros equipos que puedan reemplazar a los Servidores en un momento dado, teniendo en cuenta la información del punto anterior.
3. Mantener la configuración básica de los Servidores respaldada en un archivo e impreso tanto dentro como fuera del Centro de Comunicaciones de la Universidad Nacional de la Amazonía Peruana.
4. Colocar contraseñas mayor a 8 caracteres, éstas deben contener símbolos, números, mayúsculas y minúsculas, a las consolas y a monitores.
5. Las contraseñas de administración deben ser conocidas por el administrador y el grupo encargado de redes, y deben estar documentadas en forma confidencial.
6. Estructurar formatos donde se tenga de forma clara y concisa la siguiente información para cada uno de los servidores:
  - Discos duros: cantidad, capacidad, tecnología, nombre y número de volúmenes por discos, cantidad de discos que se puedan adicionar, drivers que lo controlan.
  - Memoria: marca, referencia, cantidad actual, posible expansión, tabla de distribución de SIMM suministrada por el proveedor.
  - Main Board: arquitectura, procesador, velocidad, coprocesador, número y tipo de slots.
  - Tarjeta de red: tipo, drivers, tipo de bus, configuración (puerto, interrupción, DMA), tipo de conector, topología.
  - Unidades de Almacenamiento: CD ROM (tecnología, velocidad interna o externa drivers, tipo de controladora) Floppy driver(tipo, capacidad), tape backup (tipo, capacidad, controladora).
7. Actualizar inventarios de suministros y formatos de información cada 2 meses.



8. La ubicación debe ser un lugar cerrado de acceso restringido, preferiblemente en el cuarto destinado a todos los equipos de comunicación.
9. Estructurar formatos de software instalados en los servidores como sistema operativo, antivirus y aplicaciones en general.
10. Proteger los interruptores de encendido/apagado para que éstos no sean activados/desactivados accidentalmente.
11. Mantener copia de los disquetes de licencia y de los registros de los servidores.
12. Estructurar formatos de software instalados en los servidores como sistema operativo, antivirus y aplicaciones en general.
13. Instalar un adecuado antivirus que sea residente en memoria, y configurarlo para que chequee continuamente todas las acciones realizadas sobre los archivos.
14. Actualizar constantemente el antivirus, ya sea a través del Internet o a través del distribuidor.
15. Verificar una vez por semana el espacio en disco de los diferentes volúmenes.
16. Borrar semanalmente la información innecesaria.
17. Verificar en horas de alta demanda el porcentaje de utilización del servidor mediante la utilización de la herramienta Monitor del Sistema.
18. Semestralmente realizar limpieza al interior de los servidores, unidades de CD.
19. Para aquellos Servidores que son críticos y no pueden estar fuera de servicio, se recomienda implementar un sistema de tolerancia a fallas.
20. Definir políticas de respaldo que aseguren la integridad y la pronta recuperación en caso de una posible pérdida total o parcial de la información.
21. Tener un estricto control sobre los usuarios, derechos sobre filesystem y sobre los objetos.
22. En caso de retiro de algún funcionario, desactivar su usuario de la red o cambiar su contraseña y borrar todos los datos sobre el mismo que no se requieran en el volumen de los Servidores.
23. Mantener la estructura organizacional, eliminando objetos o unidades organizacionales que ya no existan.

24. Purgar los Servidores una vez cada 15 días vaciando la papelera de reciclaje para liberar espacio en memoria para borrar físicamente los archivos que han sido borrados lógicamente y no se necesitan.
25. Apagar los servidores cada 15 días para liberar espacio en memoria que haya quedado por otros procesos.
26. Siempre apagar los servidores mediante el proceso adecuado antes de apagarlos físicamente, para evitar que tanto el sistema operativo como las aplicaciones que estén abiertas sufran algún daño.
27. Verificar a través de la utilidad Monitor del Sistema la utilización de memoria y confirmar que ésta no sobrepase el 80%, en tal caso se debe proponer por aumentar la memoria RAM del Servidor.
28. Nunca apagar el servidor mientras haya usuarios conectados a este.
29. Utilizar el Panel de Control para configurar los protocolos y tarjetas de red de tal manera que se garantice la mejor administración de los dispositivos.
30. Definir un número máximo de conexiones simultáneas a la red por usuario. Máximo 2 conexiones.
31. Restringir en lo posible el acceso a la red de un usuario a través de la misma estación.
32. Limitar el número de conexiones simultáneas de usuarios a un recurso de red.
33. Crear tablas que relacionen características de los Servidores contra número máximo de usuarios, garantizando el rendimiento eficiente de cada servidor.
34. Verificar mensualmente el funcionamiento del sistema de ventilación de los equipos, evitando el sobrecalentamiento.
35. Implementar un sistema de seguridad para que los Servidores no sean abiertos fácilmente.
36. Homogenizar el acceso a la red mediante el uso de unidades lógicas a todos los recursos de la red.
37. FIREWALL
  - Se deberá delegar un responsable para la configuración del Firewall.
  - Se deberá bloquear todo el tráfico, excepto el explícitamente aprobado.
  - Se deberá revisar semanalmente el tráfico autorizado.
  - Se deberá revisar diariamente las trazas de actividad.
  - Se deberá ocultar los puertos internos.

- Se deberá instalar las nuevas versiones del fabricante del producto.
- Se deberá instalar los parches del fabricante del producto.
- Se deberá realizar pruebas de regresión antes de instalar una nueva versión o parche.

### 38. SERVIDOR DE BASE DE DATOS

- Aplicar Service Packs y revisions.
  - Utilizar MBSA(Microsoft Baseline Security Analyzer) para detectar las actualizaciones de SQL no aplicadas.
- Deshabilitar los servicios que no se utilicen
  - MSSQLSERVER (obligatorio)
  - SQLSERVERAGENT
  - MSSQLServerADHelper
  - Microsoft Search
  - Microsoft DTC
- Limitar SQL Server para que utilice TCP/IP.
- Reforzar la pila TCP/IP.
- Configure la cuenta de servicio de SQL Server con los mínimos permisos posibles.
- Elimine o deshabilite las cuentas que no se utilicen.
- Proteja el tráfico de autenticación.
- Eliminar la cuenta de usuario invitado (guest) de SQL.
- Eliminar el login BUILTIN\Administradores .
- Habilitar la auditoría de inicios de sesión de SQL Server.
- Habilitar la auditoría general de SQL Server.
- Eliminar las bases de datos de ejemplo.
- Proteger los procedimientos almacenados.
- Proteger los procedimientos almacenados extendidos.
- Limitar el acceso de cmdExec a la función sysadmin.
- No conceda permisos para el rol público.

39. OTRAS TAREAS A REALIZAR SON:

- Actualizar periódicamente los discos de Reparación de cada uno de los Servidores con el fin de corregir los problemas menores que se presenten.
  - Verificar el correcto funcionamiento del arreglo de disco de cada uno de los servidores mediante las utilidades proporcionada por cada fabricante.
  - Mantener actualizada la relación de impresoras de red con sus respectivos puertos y nombres previamente definidos.
  - Liberar espacio en los discos en cada uno de los Servidores; para ello:
    - Vaciar la papelera de reciclaje.
    - Reducir el espacio utilizado por la papelera de reciclaje.
    - Hacer copias de seguridades no se necesiten a un disco auxiliar y borrar los del disco duro.
    - Buscar y eliminar archivos temporales.
    - Crear más espacio en disco usando la compresión de disco en volúmenes NTFS.
    - Desfragmentar el disco o volumen.
40. Crear grupos de trabajo de manera que la capacitación y la experiencia no sea individualizada.
41. Tener varias componentes de respaldo (un stock de repuestos) como discos duros, tarjetas de red, memorias, controladoras en un lugar seguro y de acceso restringido.
42. Cada Servidor debe poseer una dirección IP de acuerdo al mapa de direcciones IP definido.
43. Utilizar el Visor de Eventos para monitorear la hora interna del Servidor y su sincronización con los demás.
44. Tener el máximo de los recursos en red como impresoras, scanner, servicio de fax.
45. Mantener actualizado el sistema operativo de la red, aplicaciones críticas que se tengan y software utilitarios.
46. Reducir el tiempo de acceso y tráfico WAN colocando la información en un único servidor al que el usuario pueda acceder y manejar copia de la información en el cliente.

47. Estandarizar el nombre del objeto “usuario”, debe ser familiar y tratar de ser igual al del correo electrónico para obtener un nombre común exclusivo.
48. Las particiones se deben efectuar solo si proporcionan mejor funcionamiento o tolerancia a fallos en la red.

SWITCHES:

49. Instalar los switches en gabinete cerrado con seguro, para impedir el acceso de personal no autorizado.
50. Marcar adecuadamente los puertos de switches mediante un código que tenga relación con la estructura de la red.
51. Todos los slots que no estén siendo usados deben estar protegidos por faceplate (tapa).
52. Al instalar un módulo en los switches, con este equipo encendido, asegúrese de no introducir objetos extraños dentro del slot.
53. Después de insertar un módulo verificar, que el LED de encendido quede finalmente en verde para garantizar su buena instalación.
54. Revisar periódicamente los LEDS ubicados en la parte frontal de los switches, que indica el estado de operación del mismo y de sus componentes. Estos LEDS pueden ser muy útiles en determinados casos, especificando las causas de determinados problemas.
55. Habilitar el protocolo RIP para que genere sus tablas de enrutamiento con los routers y los Servidores que trabajan con dichos protocolos.
56. Segmentar el tráfico de subredes, definiendo grupos de 40 usuarios como máximos, para minimizar el tráfico que fluye a través del switch congestionando la red.
57. Habilitar el protocolo ARP para que los switches interactúen con los diferentes routers que se encuentran en la red.
58. Se deberá configurar direcciones estáticas a los módulos y sus puertos como una forma de dar seguridad a la red.
59. En casos que existan segmentos que trabajen con protocolos que sólo se requieren en dicho segmento, se podrían habilitar filtros para evitar su tráfico en otros segmentos.
60. Implementar filtros que eviten la comunicación de determinadas estaciones y segmentos con otros, con el objeto de dar mayor seguridad a la red.

## **B. Procedimientos Correctivos**

1. Antes de destapar el equipo verificar si tiene garantía y en caso tal llamar al proveedor.
2. Verificar que la correa de datos esté bien conectada tanto al disco duro como en la controladora.
3. Verifique que el disco duro tenga la potencia bien conectada.
4. Verificar que la tarjeta controladora esté haciendo buen contacto en el spot.
5. Conecte el disco duro en otro equipo de similares características para descartar daño de otros elementos.
6. Reiniciar el equipo con un disquete que tenga DOS de la misma versión que hay grabada en el disco duro.
7. Transferir los archivos del sistema a la partición del sistema operativo.
8. En caso de poder ver la información hacer respaldo.
9. Correr un antivirus actualizado a la participación del sistema operativo.
10. Ejecutar FDISK para verificar si la partición del sistema operativo está activa.
11. Borrar la partición del sistema operativo y volver a crear.
12. Formatear la partición del sistema operativo con sistema.
13. Restaurar todos los archivos de la partición del sistema operativo, archivos de arranque, archivos de configuración, controladores de disco etc., desde el backup si se tiene ó si no desde el CD de instalación, teniendo precaución de seleccionar los controladores de disco apropiado.
14. Verificar que los controladores para el disco duro o controladora del arreglo (\*.dsk), no estén defectuosos, o sean adecuados, en tal caso reemplazarlos y reinstalar nuevamente.
15. Arrancar el servidor y hacer Backup total.
16. Restaurar la información mínima necesaria en otro servidor como solución transitoria para evitar paro de funciones.
17. Adecuar las estaciones y asignar derechos necesarios para el acceso al servidor transitorio.
18. Enviar el disco Duro a empresas especializadas en recuperar la información.
19. Instalar un disco duro nuevo.
20. Instalar el Sistema Operativo que le corresponde y ubicar el servidor en el contexto donde estaba anteriormente.

21. Reestablecer la información en sus volúmenes.
  22. Verificar si el directorio SYSTEM no ha sido borrado o ha perdido información.
  23. Arrancar el servidor y dirigir manualmente los datos solicitados por el.
  24. Cargar manualmente los controladores para manejo de la tarjeta de red, con los parámetros adecuados desde la partición del sistema operativo.
  25. Entrar al servidor a través de una estación y restaurar el sub directorio SYSTEM desde el último backup o copiarlo desde otro servidor adecuándolo para que realice correctamente sus funciones anteriores.
  26. Hacer chequeo de la superficie del Disco teniendo cuidado previamente de:
    - Realizar backup previamente de toda la información en los volúmenes o al menos de los datos.
    - Demostrar los volúmenes que contenga el disco en cuestión.
    - Hacer el chequeo no destructivo para garantizar la integridad de los datos.
- Tarjetas de Red
    27. Verificar que la tarjeta de red esté haciendo buen contacto con el bus de datos.
    28. Verificar que el Patch Cord esté bien conectado y en buen estado.
    29. Verificar que el controlador de la tarjeta de red esté cargado.
    30. Verificar que los parámetros especificados lógicamente en los archivos de configuración coincidan realmente con la ubicación y configuración física.
    31. En caso de que no cargue la tarjeta de red o reporte problemas con el controlador, sustituirlo.
    32. Reemplazar la tarjeta de red, para descartar un posible daño en la tarjeta.
  - Main Board
    33. Revisar todos los conectores para asegurar que estén conectados en forma completa.
    34. Confirme que el suministro de energía sea el adecuado.
    35. Buscar elementos extraños que hayan caído en la tarjeta, como por ejemplo tornillos.
    36. Realice una limpieza total de la tarjeta.
    37. Confirme que las posiciones de los interruptores en la tarjeta del sistema estén correctas.

38. Haga trabajar la prueba de tarjeta del sistema, del programa de diagnóstico avanzado.
  39. Revisar si existen códigos de error que aparecen en la pantalla como son fallas de interrupción, reloj, memoria u otras, ayuda sustancialmente a elegir un diagnóstico.
  40. Comprobar el voltaje de alimentación para ver si existe 2,4 a 5 voltios entre las terminales de entrada de del sistema.
  41. Emplee una tarjeta adaptadora de códigos de pruebas de autodiagnóstico.
  42. Chequear el funcionamiento del procesador, cambiar por otro de similares características.
  43. Cambiar la tarjeta madre por otra, teniendo en cuenta de que esta posea la misma arquitectura y soporte del sistema.
- MEMORIA
44. Apagar adecuadamente el servidor y cambiar los módulos de memoria RAM uno a uno para determinar si existe uno defectuoso, en caso tal reemplazarlo por uno de idénticas características.
  45. Verificar que las especificaciones de los módulos de memoria RAM correspondan con las requeridas por el equipo (capacidad, velocidad, paridad etc.).
  46. Verifique que la distribución de memoria en los slot correspondan con las especificaciones por el fabricante. En caso de no tener manuales hacer las pruebas respectivas.
  47. En todos los cambios de memoria se debe configurar el equipo a través del setup, diskette o CD de configuración del equipo.
  48. Reiniciar el equipo, restaurar el servidor y verificar que realice normalmente sus funciones (Conteo de memoria, ejecución de aplicaciones etc.).
  49. Para solucionar el problema temporalmente reducir el valor de “minimum cache buffers”.
  50. Aumentar la capacidad de memoria, teniendo en cuenta de especificar correctamente el número de pines, velocidad, capacidad, marca y modelo del equipo.



- Fuente
  51. Verifique la potencia de entrada.
  52. Verifique que el cable de potencia esté bien conectados en ambos extremos.
  53. Verifique el voltaje de salida de la fuente (+/- 12 y +/- 5).
  54. Cambiar la fuente de potencia por otra según la marca y modelo del equipo.
- Archivos de Arranque y Configuración.
  55. Cargar manualmente la tarjeta de red y el protocolo (TCP/IP) para que permita el acceso al Servidor.
  56. Entra al servidor con un usuario que tenga los derechos necesarios y verifique que el Autoexec se encuentra dentro del directorio System del volumen SYS.
  57. Restaurar el archivo Autoexec dentro del directorio SYS:SYSTEM desde el backup correspondiente.
  58. Verificar que el archivo Initsys se encuentre en el directorio System.
  59. Restaurar el archivo Initsys desde el último backup correspondiente.
- SWITCHES:
  60. Verificar que los niveles de voltaje de alimentación sean los correctos, posiblemente el software del Switch no está funcionando correctamente, llamar al distribuidor del equipo o a la empresa encargada del mantenimiento.
  61. Verificar que la temperatura ambiente donde se encuentra instalado el Switch cumpla con los requerimientos del sistema.
  62. En caso de que la temperatura sea muy alta, tomar las medidas necesarias de acuerdo a la situación para asegurar el correcto funcionamiento del equipo.
  63. Reiniciar el equipo.
  64. Remover el módulo LMM del sistema.
  65. Encender el sistema. Si el sistema opera por lo menos 10 minutos sin apagarse, reemplazar el módulo.
  66. Si el sistema todavía se apaga, el problema probablemente es el sensor térmico, Backpane o la fuente de potencia. En este caso llame a su distribuidor o empresa encargada de su mantenimiento.
  67. Verifique que los cables UTP estén bien conectados a los puertos RJ-45 de los módulos ESM.
  68. Remueve el módulo en cuestión, instálelo de nuevo y reinicie el equipo.

69. Accesar al Switch a través de Telnet con el usuario administrador, y corre la opción de diagnóstico sobre el módulo en cuestión.
70. Verifique la integridad de los cables que están conectados a los puertos del módulo.
71. Si el puerto continúa en amarillo contacte a su distribuidor o empresa de mantenimiento.
72. Verifique que los cables de potencia estén finalmente conectados al equipo y que haya suministro de energía.
73. Verifique que el interruptor de encendido se encuentre en posición "ON".
74. Reinicialice el equipo apagando y encendiendo repetidamente a través del interruptor de encendido.
75. Verificar que las rejillas de ventilación estén limpias y despejadas.
76. Verifique que el ventilador del equipo estén funcionando correctamente (Ver manual "setup guide").
77. Verifique que el sistema esté conectado debidamente al suministro de AC y al voltaje adecuado.
78. Conectar los equipos (Servidores, consolas, etc.) más necesarias a los Switches.

### **3.3.1.2.3. Comunicaciones**

#### **A. Procedimientos Preventivos**

1. No se debe realizar empates, es decir, múltiples apariciones del mismo par de cables en diversos puntos de distribución.
2. El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25 cm.
3. En la ruta del cableado de los closet a los nodos se debe evitar el paso por dispositivos eléctricos como equipos de soldaduras, aire acondicionado, ventiladores, intercomunicadores, luces fluorescentes y balastos; debe pasar mínimo a una distancia de 12 cm.
4. El cableado debe pasar mínimo a 1.2 m de los motores eléctricos grandes o transformadores.
5. El cableado debe estar distantes de los cables de corriente alterna con 2KVA o menos de 13cm, de cables de 2KVA a 5KVA debe estar distante 30cm y de cables de 5KVA mínimo 91cm.

6. Ubicar en el centro de comunicaciones el diagrama del cableado de red, éste debe indicar claramente el diagrama de distribución, el puerto asignado a cada toma de información, a cada servidor y en general a cada una de las conexiones.
- Red inalámbrica:
  7. Los puntos de acceso deben permanecer apagados en los horarios que no se utilicen por ejemplo: fines de semanas y feriados.
  8. Cambiar los parámetros por defectos de los punto de acceso, por ejemplo: SSID, contraseñas, etc.
  9. Utilizar encriptamiento WAP.
  10. Deshabilitar el broadcast del SSID en los puntos de acceso.
  11. No usar una SSID que contenga información útil para un atacante.
  12. Utilizar canales libres para evitar interferencias entre nuestros propios dispositivos o dispositivos de redes próximas.
  13. Deshabilitar todos los protocolos y servicios no utilizados en los puntos de acceso.
  14. Instalar y confirmar adecuadamente un cortafuego entre el segmento cableado y el segmento inalámbrico de nuestra red.
  15. Instalar y configurar adecuadamente un sistema de detección de intrusos con finalidades específicas para redes inalámbrica.
  16. Aplicar lista de control de acceso por dirección MAC en los puntos de acceso.
  17. Desplegar VPN basadas en IPsec entre los clientes inalámbricos y la infraestructura.
  18. La identificación para el acceso administrativo, a los puntos de acceso; se utilizará una contraseña mayor de 8 caracteres, las cuales deben contener símbolos, números, mayúsculas y minúsculas.
  19. Deshabilitar la posibilidad de utilizar ad-hoc en todos los clientes.
  20. Utilizar direcciones IP estático en la infraestructura.

## **B. Procedimientos Correctivos**

1. Revise la conexión del Patch Cord desde el punto de la red hasta la estación de trabajo.
2. Verificar el estado de conector RJ-45 y los colores estándar utilizados en la conexión.

3. Conectar otro equipo al Terminal del RJ45; comprobar si esté realiza todas las operaciones en la red.
4. Por medio de un chequeador de cableado, comprobar el funcionamiento del cable según el estándar EIA/TIA 568B desde el punto de la red hasta el Patch panel donde se encuentra ubicado el centro del cableado.
5. Verificar el estado de conexión en el concentrador respectivo.
6. Observar si existe cables de energía cerca, y evaluar la influencia de estos sobre el par trenzado del cable UTP.
7. Llevar un cable desde el puerto de conexión ubicado en el centro de cableado, hasta la tarjeta de red del equipo y verificar su funcionamiento de red.
8. Si el equipo funciona luego del procedimiento anterior, cambiar el cable UTP que va por el tendido horizontal.

#### **3.3.1.2.4. Elementos auxiliares**

##### **A. Procedimientos Preventivos**

1. Revisar periódicamente todos los mensajes y el menú de control del UPS, para precisar el estado general de la misma, sus parámetros de medición, el estado de la batería y alarmas y la configuración del sistema. Para luego confrontarlo con los valores requeridos y recomendados por el proveedor.
2. Asegurar la buena ventilación y alimentación del UPS.
3. Definir una política de finalización de tareas con el objetivo de disminuir gradualmente la carga del uso del UPS, en el momento de una interrupción eléctrica, según las necesidades identificadas y la potencia de las baterías.
4. Emplear la toma que estén conectados al UPS sólo para conectar los equipos de comunicación de misión crítica, en ningún momento pueden ser conectados lámparas, ventiladores, hornos microondas y otros.
5. El UPS tiene una fuente propia de energía (baterías), cuando no está conectado a una fuente de corriente directa, pueden estar presentes altos voltajes en los terminales 9 y 10 (terminales para conexión remota de la batería), cuando el UPS está funcionando con la batería.
6. Al des energizar completamente el UPS, disparar el breque de salida. Luego dispara el breque de entrada y el breque de la batería.
7. Se corre el riesgo de una descarga eléctrica al instalar la batería, esta tarea debe ser realizada por personal de servicio especializado.

8. No disponer de las baterías en caso de presentarse un incendio. Las baterías pueden explotar al estar expuestas a las llamas.
9. Todos los gabinetes donde se encuentren equipos de comunicaciones deben ser de seguridad.
10. Una batería puede presentar riesgo de una fuerte descarga eléctrica, por esta causa puede quemarse o explotar. Se debe tener todas las precauciones.
11. Proteger colocando una banda en el botón Emergency Power – Off para evitar que sea presionado por personal no autorizado.
12. Se debe instalar un generador de respaldo para los nodos que conforman el Back Bone de Fibra Óptica e Inalámbrica.
  - Pozo a Tierra para Descarga Eléctrica
13. La inspección de los pozos a tierra para descargas eléctricas, se realizará cada trimestre; para elegir el día de la inspección se debe de tomar en cuenta que no haya llovido por lo menos tres días antes; para garantizar poca humedad en los suelos para evaluar la resistencia y las conexiones de los pozos.

#### **B. Procedimientos Correctivos**

1. Si el fallo de energía es de un periodo prolongado se debe activar el generador de respaldo:
  - Pozo a Tierra para Descarga Eléctrica
2. Los trabajos para el mantenimiento de los pozos a tierra para descarga eléctrica, se debe realizar con la Supervisión de un Ingeniero Electrónico o Eléctrico y un Personal de Apoyo para cubrir todos los alcances y medidas de seguridad que permitan realizar estos con la Confiabilidad y Seguridad Eléctrica, que amerite un óptimo trabajo.
3. Se usará para mediciones de resistividad del terreno y de voltaje (para casos que exista alguna línea de voltaje cercana al pozo, o voltajes indirectos que se refleje en el pozo) un medidor digital, Instrumento que facilita efectuar 02 tipos de medición (medición normal y método corto).
4. De acuerdo a los resultados medidos iniciales en cada uno de los pozos; éstos serán agrupados o clasificados para la realización del trabajo de mantenimiento, cumpliendo las especificaciones técnicas estandarizadas.
5. En las mediciones de cada uno de los pozos se tendrá agrupado en:
  - Buena resistividad del Terreno

- Regular resistividad del Terreno
  - Mala resistividad del Terreno
6. Se atenderá y se dedicará mayor tiempo de trabajo a los pozos que tengan mala y regular resistividad. Realizando una limpieza general de los Pozos, cambio de conectores, relleno o reemplazo con tierra vegetal, suministrando mejores mezclas electrolíticas, materiales no metálicos, 2 dosis de Thourgel de buena calidad para obtener mejores resultados finales.
  7. Se realizará monitoreos de mediciones previos e intermedios al inicio del trabajo y durante el uso de los pozos a fin de poder obtener resultados de los mantenimientos realizados.
  8. Concluidos los trabajos en las diferentes sedes se realizará las mediciones, que verifiquen y garanticen que éstos están dentro de los parámetros estipuladas por las Normas Técnicas de Conductividad y Resistividad.
    - Para Pozos de Comunicaciones e Informática:  $< 05 \text{ W}$  (ohmios).
  9. Se presentará un Informe Final de todos los trabajos realizados, con las conclusiones y recomendaciones de cada pozo para el Historial de éstos.

### **3.3.1.3. Personal**

#### **A. Procedimientos Preventivos**

1. Capacitar continuamente al personal de sistemas para que tengan conocimientos sobre la tecnología de punta.
2. Otorgar o retirar el acceso de personas a las tecnologías de información y cómo se controla el mismo.
3. Asignar o retirar derechos permisos sobre los archivos y datos a los usuarios.
4. Autorizar o denegar servicios a los usuarios.
5. Definir perfiles de trabajo.
6. Autorización y control de la entrada/salida de las tecnologías de información.
7. Gestionar las claves de acceso considerando para cada nivel el tipo de clave.
8. Garantizar que los mantenimientos de los equipos, soporte y datos se realice en presencia y bajo la supervisión de personal responsable.
9. Permitir sólo el acceso al personal que realice labores de operación, administración de sistemas y base de datos y al administrador de la red.
10. No manipular equipos en estado de embriaguez ni bajo efecto de sustancias alucinógenas.

11. Destinar un sitio seguro y de acceso restringido para guardar manuales, software de instalación, documentos de los equipos, ejerciendo un estricto control sobre su uso.
12. Los equipos sólo deben ser manipulados por el personal que tenga los suficientes conocimientos sobre ellos.
13. Tener actualizada la información de los proveedores y empresas que brindan soporte y mantenimiento de los diferentes equipos.
14. No fumar en lugares donde se concentran los equipos y especialmente en el centro de cableados.
15. Nunca consumir alimentos ni ingerir bebidas cerca de los equipos.
16. El personal deberá firmar acuerdos de confidencialidad o no divulgación como parte de sus términos o condiciones de trabajo.
17. Todo el personal, tanto interno como externo a la institución, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
18. Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médicos y tener muy en cuenta sus antecedentes de trabajo, ya que un centro de cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.

#### **3.3.1.4. Instalación**

##### **A. Procedimientos Preventivos**

11. Debe existir un cuarto de comunicaciones capaz de albergar equipos de telecomunicaciones, terminales de cables y cableado de interconexión asociado.
12. El cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones.
13. El cuarto de comunicaciones debe tener acceso controlado y sólo debe permitir el acceso al administrador de la red y de los servicios de comunicaciones.
14. La altura mínima recomendada para un cuarto de comunicaciones es de 2,6 metros.
15. Se debe de evitar polvo y electricidad estática utilizando piso de concreto, terraza, loza o similar, nunca utilizar alfombra.

16. En cuartos que no posean equipos electrónicos la temperatura debe mantenerse continuamente entre 10 y 33 grados centígrados y la humedad relativa mantenerse en 85%.
17. Todos los sitios donde le encuentren ubicados equipos informáticos deben de estar dotados de las medidas de seguridad adecuadas que garanticen su protección, por ejemplo:
  - Sistema de aire acondicionado
  - Extintor.
  - Material no combustible
  - Sistema eléctrico con protección a tierra
  - Control de acceso restringido a los equipos
  - Control que detecte variaciones de temperatura y humedad relativa
  - Señalización adecuada
18. No debe existir alguna tubería de agua pasando por, sobre o alrededor del cuarto de comunicaciones.
19. Las paredes deben estar pintadas de un color claro para mejorar la iluminación.
20. Se recomienda mantener una distancia promedio de 46 metros para ubicar el cuarto de comunicaciones lo más cerca posible del área de trabajo.
21. Debe de existir un mínimo de 2 tomacorrientes dobles de 220 v corriente alterna dedicados de 3 hilos, deben ser circuitos separados de 15 a 20 amperios, y deben estar prevenidos a 1.8 metros mínimo de distancia de uno a otro.
22. Se debe contar con alimentación de emergencia de activación automática (UPS).
23. Se debe mantener el cuarto con llave en todo momento, asignando llaves al personal que debe laborar allí.
24. El cuarto en todo instante debe encontrarse limpio y ordenado.
25. Debe existir mínimo 1 metro de espacio libre para trabajar con el equipo en partes expuestas sin aislamiento.
26. Las paredes deben ser pintadas con pinturas resistente al fuego, lavable, mate y color claro.
27. Realizar mantenimientos preventivos a las instalaciones.
28. Realizar mediciones periódicas a las instalaciones eléctricas y de telecomunicaciones.
29. Hacer chequeos previos a las instalaciones eléctricas, de comunicaciones y datos antes de instalar los equipos informáticos.



30. Colocar avisos de no fumar, no ingerir bebidas ni alimentos en todos los lugares donde se encuentren ubicados equipos informáticos.
  31. Evitar adecuar en forma improvisada sitios para equipos informáticos o colocar equipos informáticos en sótanos.
  32. El entorno físico debe facilitar que los equipos sean ubicados en lugares aireados, no muy cercanos a ventanas, que no reciban directamente los rayos del sol o demasiado polvo.
- En el anexo # 6 se muestran algunos formatos para el control y seguridad en el acceso a los sistemas de información.

## Capítulo IV: Resultados y Discusiones

1. Se identificó 4 grupos de activos necesarios para el correcto funcionamiento de la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana, los cuales son:
  - Servicios internos (correo electrónico de docentes, intranet de docentes y sistema de gestión académica)
  - Equipamiento (aplicaciones, equipos, comunicaciones y elementos auxiliares)
  - Personal (administrador de comunicaciones, administrador de sistemas y base de datos y operadores)
  - Instalaciones.
  
2. Se identificaron las siguientes amenazas:

• Para el servicio de correo electrónico de docentes	20 amenazas
• Para la intranet de docentes	20 amenazas
• Para el sistema de gestión académica	20 amenazas
• Para las aplicaciones se ha identificado	30 amenazas
• Para los equipos se ha identificado	40 amenazas
• Para las comunicaciones se ha identificado	30 amenazas
• Para los elementos auxiliares se ha identificado	20 amenazas
• Para el personal se ha identificado	20 amenazas
• Para las instalaciones	20 amenazas
  
3. Se ha identificado que los controles existentes son pocos efectivos frente a las amenazas encontradas.
  
4. Las salvaguardas seleccionadas fueron desarrollados en el informe Plan de Contingencia.
  
5. La elaboración del plan de contingencia establece procedimientos o medidas necesarias ante la ocurrencia de eventos no favorables, para garantizar un nivel óptimo de disponibilidad de los sistemas de información.

## **Capítulo V: Conclusiones**

1. La seguridad informática es muy importante para la continuidad del servicio, por tal motivo debe realizarse anualmente un análisis de riesgo de las nuevas tecnologías a ser adquiridas por la Universidad Nacional de la Amazonía Peruana.
2. Mediante el análisis de riesgo se determina de manera precisa cuales son los riesgos a los que se encuentran expuestos los activos de la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana.
3. Este Plan de Contingencia es un documento que contiene los procedimientos preventivos y correctivos para proteger y salvaguardar la integridad y seguridad de la información que maneja la Intranet y Portal web de la UNAP.
4. El personal encargado de la Intranet y Portal web de la UNAP, son los responsables de ejecutar los procedimientos en los cuales estén involucrados para superar las contingencias detalladas en el presente procedimiento.
5. Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración y mantenimiento de un Plan de Contingencia.

## **Capítulo VI: Recomendaciones**

1. Hacer de conocimiento al personal informático el contenido del presente Análisis de Riesgos y Plan de Contingencia, con la finalidad de instruirlos adecuadamente.
2. El personal que asumirá los roles establecidos en el plan de contingencia debe ser capacitado anualmente en sus funciones.
3. Se debe tener una adecuada política de seguridad orientada a proteger todos los recursos informáticos.
4. El Plan de Contingencia debe ser actualizado anualmente, así mismo revisado/evaluado cuando se materialice u ocurra una amenaza.
5. Elaboración de los Manuales de Procedimientos de los activos mencionados en el Plan de contingencias.



00025

## Capítulo VII: Bibliografía

- ✓ **[Magerit-I-Metodo:2006]**  
Ministerio de Administración Públicas, Madrid 20 Junio del 2006, “MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, I – Método”, Versión 1.1, MAP, <http://publicaciones.administracion.es>, 154 páginas.
  
- ✓ **[Magerit-II- Catálogo de Elementos:2006]**  
Ministerio de Administración Públicas, Madrid 20 Junio del 2006, “MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, II – Catálogo de Elementos”, Versión 1.1, MAP, <http://publicaciones.administracion.es>, 87 páginas.
  
- ✓ **[Magerit-III- Guía de Técnicas :2006]**  
Ministerio de Administración Públicas, Madrid 20 Junio del 2006, “MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, III – Guía de Técnicas”, Versión 1.1, MAP, <http://publicaciones.administracion.es>, 72 páginas.
  
- ✓ **[Contingencia :2005]**  
Plan de Contingencia para los Bienes Informáticos.pdf. Versión 3. Medellín: Unidad de Sistemas e Informática; 2005, 99 páginas.
  
- ✓ **[Contingencia :2008]**  
Plan de Contingencias InformáticosCCDGA.pdf. Versión 1.1. Universidad Nacional de San Antonio Abad del Cusco: Dirección General de Administración; 2008, 17 páginas.
  
- ✓ **[Contingencia :2008]**  
Plan de Contingencia UADY.pdf. Secretaria General Coordinación Administrativa de Tecnologías de Información; 2008, 27 páginas.

- ✓ **[Recavarren Benites :2009]**  
Seguridad de Tecnologías de Información, Mg. Ing. Miguel Robles-Recavarren Benites, Curso de Actualización Académica Profesional, Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana, del 20 de Abril al 10 de Octubre del 2009.
  
- ✓ **[URL 01 :2009]**  
Oficina Nacional, fecha de acceso el 02 de diciembre del 2009, URL disponible en: <http://www.ongei.gob.pe>
  
- ✓ **[URL 02 :2009]**  
Guía Práctica para el desarrollo de Planes de Contingencia de Sistemas de Información, fecha de acceso el 05 de diciembre del 2009, URL disponible en: <http://www.inei.gob.pe>
  
- ✓ **[URL 03 :2009]**  
Normas Técnica Peruana, fecha de acceso el 15 de diciembre del 2009, URL disponible en: <http://www.ongei.gob.pe>

## ANEXO

## ANEXOS

### Anexo N° 1

#### Estimación de costos del proyecto

A continuación se muestran los costos directos e indirectos que se han generado:

#### **Recursos Humanos**

Nombre	Disponibilidad para el trabajo	Tiempo que requiere el proyecto	Conocimiento de las herramientas	Remuneración
Guadalupe Pizango Ytala	90%	2 meses y medio	0%	-----

**TOTAL: S. / 0.00**

**Cuadro 111:** Estimación de costos en recursos humanos

Fuente: Elaboración propia

#### **Software**

Descripción	Precio	Cantidad	TOTAL
Pilar versión 4.3	S/.1,614.84	1	S/.1,614.84
Microsoft Office Word 2003	S/.450.00		S/.450.00
Sistema Operativo Windows XP Profesional Service Pack 2	S/.600.00		S/.600.00

**TOTAL: S. / 2,664.84**

**Cuadro 112:** Estimación de costos en software

Fuente: Elaboración propia

#### **Hardware**

Descripción	Precio	Cantidad	TOTAL
Computadora Intel Pentium "D"	S/. 2300.00	1	S/. 2300.00
Impresora	S/.200.00	1	S/.200.00
Cartuchos	S/.150.00	2	S/.150.00

**TOTAL: S. / 2,650.00**

**Cuadro 113:** Estimación de costos en hardware

Fuente: Elaboración propia



**Varios**

<b>Descripción</b>	<b>Precio</b>	<b>Cantidad</b>	<b>TOTAL</b>
Luz	S./ 40	1	S./ 80
Teléfono	S./ 50	1	S./ 100
Internet	S./ 2	60	S./ 120
Memoria USB de 2GB	S./ 80	1	S./ 80
Papel bond	S./35	2	S./ 70

**TOTAL: S. / 450.00****Cuadro 114:** Estimación de costos varios

Fuente: Elaboración propia

**COSTO TOTAL DEL PROYECTO: S/. 5,764.84**

## Anexo N° 2

Cuestionario efectuado al: Ing. Marvin Díaz Montenegro

Fecha: 3/10/2009

Hora: 11:00 am

Lugar: Oficina de Sistemas Informáticos y Comunicaciones

1. ¿Que activos intervienen en el correcto funcionamiento de la Intranet y Portal web de la Universidad Nacional de la Amazonia Peruana?
  - a. Correo electrónico de docentes
  - b. Intranet de docentes
  - c. Sistema de gestión académica
  - d. Servidores de aplicaciones, correos y firewall
  - e. Red Lan e inalámbrica
  - f. Switches, UPS y transformador de aislamiento
  - g. Personal e instalaciones
  
2. ¿Cuáles son los activos que desea proteger la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana?

Todos los activos que se han mencionado.
  
3. ¿Quiénes son los profesionales encargados de administrar la Intranet y el Portal web de la Universidad Nacional de la Amazonía Peruana?
  - a. El administrador de sistemas y Base de datos
  - b. El administrador de comunicaciones
  
4. ¿Es importante proteger estos activos para la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana? ¿Por qué?

Si, estos servicios mejoran la productividad de los trabajadores administrativos, facilitan al docente la elaboración de trabajos de investigaciones y brindar un adecuado servicio de comunicaciones al estudiante, que es el principal protagonista del que hacer diario en la Universidad.

5. ¿Existe un Plan de Contingencia para la Intranet y Portal web de la Universidad Nacional de la Amazonía Peruana?

La universidad no cuenta con un plan de prevención y recuperación de desastres basados en un plan de contingencia debido a hay autoridades que desconocen el tema y no tiene visión de este aspecto. Existen normas de seguridad que no se aplican en su totalidad, es necesario resaltar esto porque los desastres pueden suceder en cualquier instante, es prioritario contar con un plan de contingencia que sea parte esencial de una efectiva estrategia de seguridad. Sobre todo para las oficinas de la universidad, la cual tiene áreas críticas.

### **Anexo N° 3**

#### **Observación realizada a las instalaciones del Centro de Comunicaciones de la UNAP**

De acuerdo a las observaciones que se han efectuado entre el 4/10/2009 y el 05/10/2009 se pueden determinar las siguientes conclusiones:

- Existen los equipos informáticos: servidores, firewall, switches, UPS.
- Existen las aplicaciones informáticas: servidores de correos, aplicaciones y otros.
- Existen las redes de comunicaciones: red Lan, red inalámbrica.
- Existen los servicios: correo electrónico de docentes, intranet de docentes y sistema de gestión académica.
- Existe el personal informático asignado a la intranet y el portal web de la Unap.

## Descripción de la metodología y herramienta

### **Descripción Magerit versión 2**

Magerit es una metodología de carácter público, perteneciente al ministerio de administraciones públicas del gobierno español. Dicha metodología es un método formal para investigar los riesgos que soportan los sistemas de información y para recomendar las medidas apropiadas que deberían adoptarse para controlar dichos riesgos.

Magerit v1 fue publicado en 1997. Magerit v2 fue publicado en 2006.

Algunas de las razones por las cuales se selecciono como base esta metodología son las siguientes:

- Es un método desarrollado íntegramente en castellano.
- Es de carácter público y su uso no requiere autorización previa.
- Es un método sistemático para analizar riesgos. Las fases del método apoyaron:
  - \*Identificación del riesgo:
    - Activos: identificación, clasificación, dependencia entre los activos, y valoración.
    - Amenazas: identificación, relación con los activos y evaluación de la vulnerabilidad.
    - Salvaguardas: identificación y evaluación. Ayuda de la herramienta.
  - \*Análisis del riesgo:
    - Impacto y riesgo acumulado. Impacto y riesgo desviado. Ayuda de la herramienta.
    - Evaluación del riesgo: De riesgos técnicos en riesgos de negocio.
- Es soportada por una herramienta de software denominada Pilar (entorno para el análisis de riesgo).
- Su conformidad con estándares de TI, tales como:
  - ISO/IEC 27002/2005
  - ISO/IEC 27001/2005
  - ISO/IEC 15408/2005
  - ISO/IEC 17799/2005
  - ISO/IEC 13335/2004

- Indirectamente, preparar a la organización para procesos de evaluación, auditoría, certificación o el acreditación, según corresponda cada caso.

Magerit v2 se ha estructurado en tres libros:

**Libro I:** Metodología. Describe los pasos y las tareas básicas, para realizar un proyecto para el análisis y la gestión del riesgo; la descripción formal del proyecto; el uso al desarrollo los sistemas y de él de información proporciona una gran cantidad de pistas prácticas, así como las fundaciones teóricas, junto con una cierta otra información complementaria.

**Libro II:** Catálogo de elementos. Proporciona elementos y los criterios estándares para los sistemas de información y modelar del riesgo: clases del activo, dimensiones de la valuación, criterios de la valuación, amenazas típicas, y salvaguardas que se considerarán; también describe los informes que contienen los resultados y las conclusiones (modelo del valor, mapa del riesgo, evaluación de la salvaguardia, estado del riesgo, deficiencias informe y plan de la seguridad), así contribuyendo para alcanzar uniformidad.

**Libro III:** Técnicas prácticas. Describe las técnicas usadas con frecuencia para realizar proyectos del análisis y de la gerencia del riesgo por ejemplo: análisis tabular y algorítmico; árboles de la amenaza, análisis de costes y beneficios, diagramas del flujo de datos, cartas de proceso, técnicas gráficas, planeamiento del proyecto, sesiones del funcionamiento (entrevistas, reuniones, presentaciones), y análisis de Delphi.

### **Descripción de la herramienta PILAR versión 4.3**

PILAR, acrónimo de “Procedimiento Informático-Lógico para el Análisis de Riesgos” es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.

Evalúa el estado de seguridad de un sistema que requiere un modelado del mismo, identificando y valorando sus activos e identificando y valorando las amenazas que se ciernen sobre ellos. De este modelado surge una estimación del riesgo potencial al que está expuesto el sistema.

La herramienta soporta todas las fases del método Magerit:

- Caracterización de los activos: identificación, dependencias y valoración.
- Caracterización de las amenazas: identificación y valoración.
- Caracterización de las salvaguardas: identificación y valoración.

**Comparación de Magerit con otras Metodologías y Ponderación de Característica**

**Método de Ponderación:**

Se tomara en cuenta la siguiente valoración:

- Herramientas que apoyan a la metodología: 1 punto por cada herramienta.
- Idioma: 1 punto al que está disponible en español, 0 puntos al que está en otro idioma.
- Habilidades necesarias: 1 punto por cada habilidad estándar.
- Conformidad con estándares de TIC: 1 por cada estándar que cumpla.

<b>CRAMM</b>	<b>SP800-30(NIST)</b>	<b>MAGERIT VERSION 2</b>
<b>Herramienta que apoya a la metodología</b>		
Herramientas no comerciales <ul style="list-style-type: none"> <li>• Ninguno</li> </ul> Herramientas comerciales <ul style="list-style-type: none"> <li>• CRAMM Expreso</li> <li>• CRAMM Experto</li> </ul> 2 Puntos	Herramientas no comerciales <ul style="list-style-type: none"> <li>• Ninguno</li> </ul> Herramientas comerciales <ul style="list-style-type: none"> <li>• Ninguno</li> </ul> 0 Puntos	Herramientas no comerciales <ul style="list-style-type: none"> <li>• Ninguno</li> </ul> Herramientas comerciales <ul style="list-style-type: none"> <li>• PILAR</li> </ul> 1 Punto
<b>Idiomas</b>		
<ul style="list-style-type: none"> <li>• Inglés, holandés, checo</li> </ul> 0 Puntos	<ul style="list-style-type: none"> <li>• Inglés</li> </ul> 0 Puntos	<ul style="list-style-type: none"> <li>• Español, inglés, italiano</li> </ul> 1 Punto
<b>Habilidades necesarias</b>		
<ul style="list-style-type: none"> <li>• Para introducir: Estándar</li> <li>• Para utilizar: Estándar</li> <li>• Para mantener: Especialista</li> </ul> 2 Puntos	<ul style="list-style-type: none"> <li>• Para introducir: Especialista.</li> <li>• Para utilizar: Especialista.</li> <li>• Para mantener: Especialista.</li> </ul> 0 Puntos	<ul style="list-style-type: none"> <li>• Para introducir: Estándar.</li> <li>• Para utilizar: Profesionales de TIC.</li> <li>• Para mantener: Habilidades de gerencia.</li> </ul> 1 Punto
<b>Conformidad con estándares de TI</b>		
<ul style="list-style-type: none"> <li>• ISO/IEC 17799</li> </ul> 1 Punto	<ul style="list-style-type: none"> <li>• N/A</li> </ul> 0 Puntos	<ul style="list-style-type: none"> <li>• ISO/IEC 27002/2005</li> <li>• ISO/IEC 27001/2005</li> <li>• ISO/IEC 15408/2005</li> <li>• ISO/IEC 17799/2005</li> <li>• ISO/IEC 13335/2004</li> </ul> 5 Puntos

**Cuadro 115: Características de las metodologías y puntajes.**

**Fuente: Elaboración propia**

## Anexo N° 5

### Glosario

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

**Acceso:** Es la recuperación o grabación de datos que han sido almacenados en un sistema de información.

**AGR:** Análisis y Gestión de Riesgos.

**Amenaza:** Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

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

**Autenticidad:** Aseguramiento de la identidad u origen.

**Base de datos:** Es un conjunto de datos organizados, entre los cuales existe una correlación.

**Certificación:** declarar públicamente que un producto, proceso o servicio es conforme con requisitos establecidos.

**Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

**Contraseña:** Palabra clave que identifica al usuario para proteger el acceso a un equipo, a una aplicación o aun modulo de una aplicación.

**Copia de seguridad:** Replicación periódica y almacenamiento externo (usualmente en discos, CDs, memorias USB, etc.) de datos y programas en previsión de posibles contingencias.



**Degradación:** Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

**Dimensión:** Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor.

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

**Frecuencia:** Tasa de ocurrencia de una amenaza.

**Firewall:** Sistema de seguridad utilizado como “cortafuego” controlando los accesos de los usuarios externos a una red local.

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

**Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza.

**Integridad:** Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

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

**Plan de Contingencia:** Es un documento que establece una estrategia de respuesta para atender en forma oportuna, eficiente y eficaz, un desastre, evento natural u otro, por culpa de algún incidente tanto interno como externo a la institución.

**Políticas de seguridad:** Conjunto de principios y reglas, propias de la organización, que declaran como se especificará y gestionará la protección de los activos de información de una manera consistente y segura.

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

**Riesgo residual:** Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.

**Riesgo acumulado:** Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.

**Riesgo repercutido:** Es el calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.

**Salvaguardas:** Procedimiento o mecanismo tecnológico que reduce el riesgo.

**Seguridad:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puede ser modificados, destruidos o simplemente divulgados.

**Sistema de información:** Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

**Trazabilidad:** Aseguramiento de que en todo momento se podrá determinar quién hizo, qué y en qué momento con el acceso a los datos.

**URL:** Abreviación de “Uniform Resoucer Locator” o en español, “Localizador de Recursos Uniformes”. Es el formato usado para describir la dirección de cada página en la WWW.

**Valor:** De un activo. Es una estimación del coste inducido por la materialización de una amenaza.

**Vulnerabilidad:** Estimación de la exposición efectiva de un activo a una amenaza.

## **Anexo N° 6**

Se muestra algunos formatos para mantener la seguridad y control en el acceso a los sistemas de información.

- Solicitud de nuevo usuario
- Inhabilitación o eliminación de usuario
- Bitácoras de incidencias
- Control de backup
- Entrada y salida al área restringida
- Solicitud de correo



**UNAP**

UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA

### Solicitud de Nuevo Usuario al Sistema de Gestion Academica

Jefe de la Unidad / Area Solicitante				
Correo Electrónico del Jefe de la Unidad / Area				
<b>Datos del Empleado</b>				
Nº	Apellidos y Nombres	Correo Electrónico	Area / Función que Realiza	Sustento para el Acceso al Sistema (Indicar los modulos a las que va acceder, de acuerdo a la función, cargo que tiene el usuario)
1				
2				
3				
4				
5				

**NOTA:** Deberá contar con la firma y sello del jefe del area solicitante.

\_\_\_\_\_  
Jefe de la Unidad solicitante



**UNAP**

UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA

**Eliminación y/o Inhabilitación de Usuario al Sistema de Gestion Academica**

Jefe de la Unidad / Area Solicitante						
Correo Electrónico del Jefe de la Unidad /Area						
<b>Datos del Empleado</b>						
Nº	Apellidos y Nombres	Correo Electrónico	Area	Función que Realiza (o)	Sustento para la inhabilitación al SGA (Vacaciones / Licencia)	Sustento para la eliminación al SGA (Cese de funciones / Cese de la Institución)
1						
2						
3						
4						
5						

**NOTA:** Deberá contar con la firma y sello del jefe del area solicitante.

\_\_\_\_\_  
Jefe del Area





**UNAP**

UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA

Unidad de Sistemas Informaticos y Comunicaciones.

**FORMATO DE CONTROL DE BACKUP Y RESGUARDO DE LA INFORMACIÓN.**

FECHA	HORA	EQUIPO				BACKUP		PROCESO		ERROR (ES)		DESCRIPCION DEL ERROR	OBSERVACIONES	RESPONSABLE	FIRMA
		PC	SERV	NOMBRE	IP.	DATA	APLIC.	AUTO.	MANU.	SI	NO				

\_\_\_\_\_  
Sello y Firma  
Jefe de Soporte Informático



**UNAP**

Oficina de Sistemas Informáticos y Comunicaciones

**FORMATO DE ENTRADA Y SALIDA DE PERSONAS AL AREA RESTRINGIDA  
CENTRO DE COMUNICACIONES**

Responsable del Centro de Comunicaciones / Area Restringida	
---	--

DATOS DE LA PERSONA						
APELLIDOS Y NOMBRES	AREA DE ORIGEN	FECHA	ENTRADA HORA	SALIDA HORA	FIRMA	MOTIVO DEL INGRESO

\_\_\_\_\_  
Sello y Firma  
Jefe Unidad de Soporte Informático





**UNAP**

**UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA**

Oficina de Sistemas Informaticos y Comunicaciones.

**FORMATO DE SOLICITUD DE CORREO ELECTRÓNICO**

DATOS A SER LLENADO POR EL SOLICITANTE DE LA CUENTA							Datos de Respuesta	
Nombres	Apellidos	Dependencia donde Labora	Función Principal que realiza	Persona que Solicita	Persona que Autoriza	Cargo de la Persona que Autoriza	Cuenta de Correo	Password de Cuenta

NOTA: Indicar al usuario de la cuenta que el cambio de su contraseña la podra realizar acercandose personalmente a OSIC.