UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"ELABORACION DEL P.S.I DE LA EMPRESA DISTRIBUCIONES QUISPE SAC"

INFORME PRÁCTICO DE SUFICIENCIA

PARA OPTAR EL TÍTULO DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

Presentado por el Bachiller:

Tony Charles Guardia Chanchari

Asesor: Grover Pablo Vásquez Rengifo

IQUITOS – PERU

2011

DEDICATORIA

“A Dios por guiarme en cada etapa de mi vida, y darme las fuerzas necesarias para seguir adelante”

“A Mi señor Padre un ejemplo de carisma, alegría entusiasmo a seguir para lograr las metas en la vida en los buenos y malos momentos nunca nos abandono.”

“A mi señora madre por el amor, el apoyo incondicional, la confianza que puso en mi, si no fuera por ella no estaría donde estoy ahora.

“A mis Tios que fueron mi guía durante la ausencia de mis padres en especial Luis por su apoyo incondicional hacia mi persona que fue él la base fundamental para llegar hacer un hombre de bien.

“A mis,amigos en especial al sr. Danilo por darme la oportunidad de aplicar lo aprendido.”

Tony Charles.

AGRADECIMIENTO

Expreso mi mas cordial y fraternal agradecimiento a los Docentes de la Escuela de Ingeniería de Sistemas e Informática por los conocimientos y enseñanzas impartidas durante mi ACTUALIZACON ACADEMICA quienes lograron mi sólida formación académica y profesional.

El presente informe a sido elaborado bajo el asesoramiento del Ing. Grover Pablo Vásquez Rengifo, a quien agradezco por su valioso apoyo en la dirección durante la realización del presente informe.

Así mismo expreso mi mas fraterno agradecimiento a todas las personas en general que pusieron su confianza y apoyo incondicional para llegar a alcanzar unos de mis grandes anhelos en mi vida profesional.

RESUMEN

Propongo:

El presente trabajo práctico consiste en la Elaboración del P.S.I de la EMPRESA Distribuciones Quispe S.A.C, el cual permitirá reducir la posibilidad de ocurrencia de amenazas a sus activos y desarrollar los procedimientos de recuperación. Sirviendo el estudio de este análisis como base para definir los lineamientos para promover la implementación de un modelo de seguridad en toda la organización.

Este trabajo práctico se fundamenta en la realización **del Análisis de riesgo de La seguridad lógica y física de la información** de LA EMPRESA DISTRIBUCIONES QUISPE SAC con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una Política de Seguridad, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la organización

Las herramientas utilizadas para la Elaboración del P.S.I fueron pilar como herramienta estándar en el análisis cualitativo del riesgo

Al final de este informe se logró como resultado la Elaboración del P.S.I para la Empresa Distribuciones Quispe S.A.C, logrando que la información sirva como base para la ejecución de la elaboración antes mencionada.

El desarrollo del proyecto, está dividido en dos Secciones, de tal forma que posibilite la secuencia lógica:

En la Sección I, se detalla los datos generales del proyecto.

En la Sección II, se detalla la visión general de la solución propuesta, la cual está compuesta por IX capítulos:

- Capítulo I: se hace referencia a la parte introductoria, a la realidad problemática por la que atraviesan los activos de la Empresa y los objetivos que se deben alcanzar con el desarrollo del proyecto.
- Capítulo II: se describe el diseño de la solución, las técnicas empleadas para la recolección de datos, la metodología empleada para el análisis de la solución, las herramientas a emplear para la solución del proyecto, se describe el desarrollo de la solución y se identifican los indicadores de evaluación de la solución.

- Capítulo III: se realiza la investigación haciendo uso de la metodología Magerit para el desarrollo de la solución del proyecto.

Palabras clave: Activos, Amenazas, Salvaguardas, Riesgos, Incidentes, Seguridad.

ABSTRACT

I propose:

The present practical work consists of the Production of the P.S.I of the Company Distributions Quispe S.A.C which will allow to reduce the possibility of occurrence of the threats to his assets and to develop the procedures of recovery .Serving the study of this analysis as base to define the limits to promote the implementation of a safety model in the whole organization.

This practical work bases on the accomplishment of the Analysis of risk of The logical safety and physics of the information of THE COMPANY DISTRIBUTIONS QUISPE SAC in order to reveal the existing vulnerabilities in the relative thing to safety controls, as way for the development of a Security policy, where the limits will be defined to promote the implementation of a safety model in the whole organization

The tools used for the Production of the P.S.I were a prop as standard tool in the qualitative analysis of the risk

At the end of this report the Production of the P.S.I achieved like proved for the Company Distributions Quispee S.A.C, achieving that the information is serve as base for the execution of the production before mentioned.

The development of the project, it is divided in two Sections, in such a way that it makes the logical sequence possible

The development of project is divided in two sections, to make possible the logical sequence:

At the Section I: is detailed the general data of the Project.

At the Section II: is detailed the general vision of the proposed solution that is composing for IX chapters:

- Chapter I: is related to the introduction of the reality problematical that is going through the manual processes and the objectives to get with the development of the project.
- Chapter II: Are described the design of the solution, the techniques acquired to recollect data, the methodology acquired for the analysis of the solution of the project, is described as well the development of the solution and the indicators for evaluation of the solution are identified.

- Chapter III: the investigation is making using the methodology MAGERIT for the development of the solution of the project.

Key words: Assets, Threats, Safeguards, Risks, Incidents, Security.

ÍNDICE GENERAL

SECCION I
DATOS GENERALES

I. Generalidades

1. Titulo

"ELABORACION DEL P.S.I DE LA EMPRESA DISTRIBUCIONES QUISPE SAC"

2 Área de Desarrollo.

Departamento de informática y sistema de DISTRIBUCIONES QUISPE SAC.

3 Generalidades de la Institución.

3.1 Razón Social.

DISTRIBUCIONES QUISPE SAC.

3.2 Ubicación de la Empresa.

3.2.1 Ubicación geográfica:

La Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana está ubicada en:

País	**:**	Perú.
Región	**:**	Loreto.
Distrito	**:**	Iquitos.
Dirección	**:**	Jr. Prospero N°935.
Referencia	**:**	Frente Esquina Cia. Bomberos de Belén.

3.2.2 Plano de ubicación:

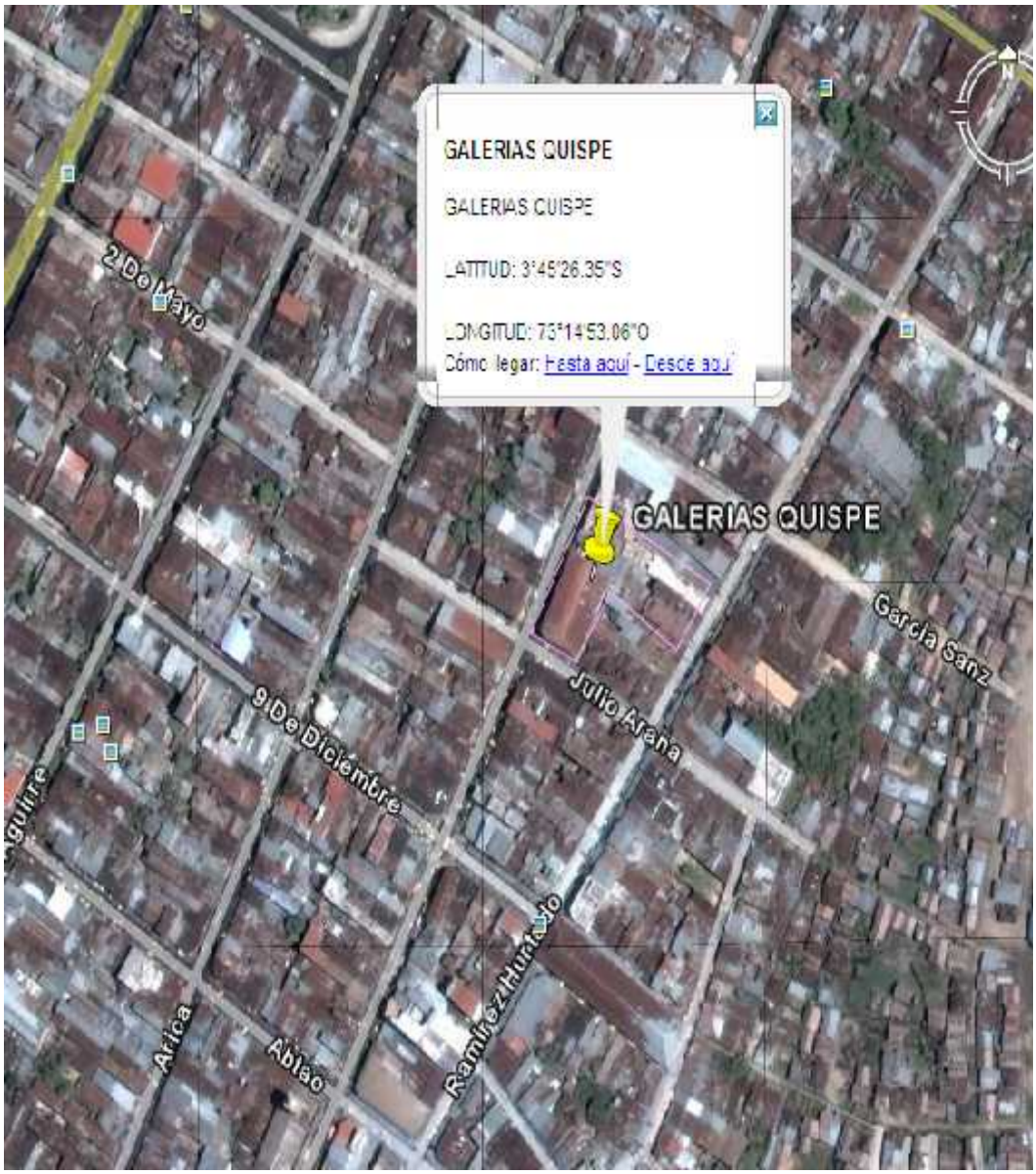
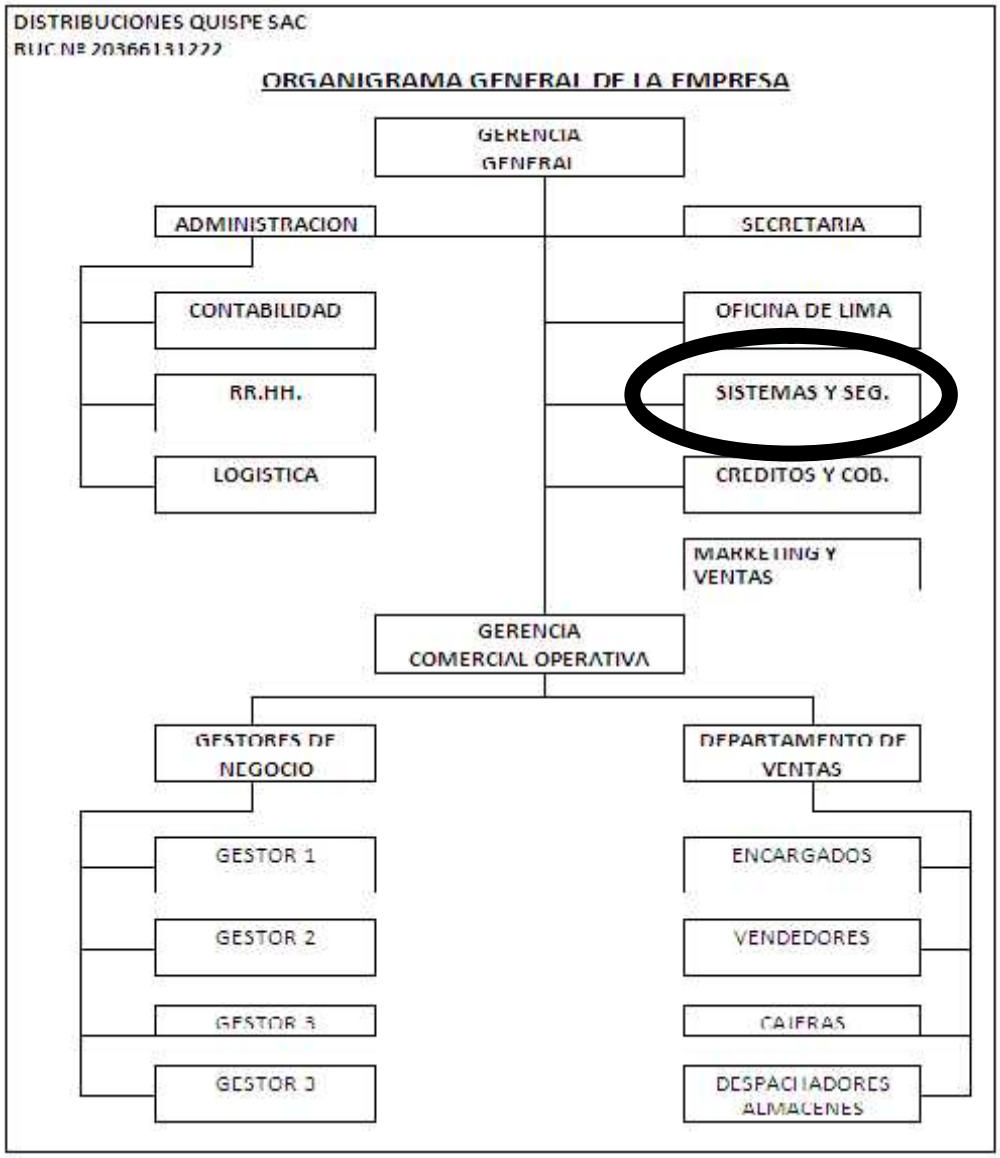


Figura N° 01: Plano de Ubicación de la DISTRIBUCIONES QUISPE SAC.
Fuente: GoogleEarth.

3.3 Organigrama Funcional.



3.4 Funciones de la Oficina o Área

- Mantener la disponibilidad del parque instalado de PCs (incluida conectividad y comunicaciones) por medio de mantenimiento preventivo y acciones correctivas ante fallas.

- Instalar nuevo hardware con su software de base.

- Cumplir con el esquema de mantenimiento preventivo recomendado por lo proveedores para los diferentes equipos, o supervisar el cumplimiento de éste por parte de terceros.

- Solucionar cualquier tipo de contingencia de hardware ya sea por medios propios, solicitud del trabajo a terceros o solicitud del cumplimiento de garantías.

- Instalar, o supervisar la instalación por parte del proveedor, de todo nuevo hardware con su software de base. Evacuar consultas de los usuarios.

- Mantener la operatividad de los usuarios en el uso de aplicaciones básicas por medio de la respuesta a sus consultas.

- Desarrollar guías de ayuda.

- Entrenar al nuevo personal no informático en las particularidades del sistema de la empresa para el uso de aplicaciones básicas.

- Evacuar las consultas de todo el personal de la empresa.

- Tratar de determinar cuándo una anomalía se trata de una impericia o una falla, interactuando con el área de soporte técnico.

4 Bachiller:

Guardia Chanchari, Tony Charles

5 Asesor:

Ing. Grover Pablo Vásquez Rengifo

6 Colaboradores:

- Tco. José Ochoa Isuiza.
- Est. Ing. Danilo Jara Vela.
- Ing. Lee Frank Mendoza López

7 Duración estimada de ejecución del proyecto

Item	Nombre de tarea	Duración	Comienzo	Fin	Predece
1	Estudio de la metodología MAGERIT	24dias	01/12/2010	24/12/2010	
2	Identificación de activos	20dias	25/12/2010	14/01/2011	1
3	Dependencia entre activos	3dias	14/01/2011	17/01/2011	2
4	Valoración de los activos	3dias	18/01/2011	21/01/2011	3
5	Identificación de las amenazas	3dias	22/01/2011	25/01/2011	4
6	Valoración de las amenazas	2dias	26/01/2011	28/01/2011	5
7	identificación de las salvaguardas existentes	1dia	29/01/2011	30/01/2011	6
8	valoración de las salvaguardas existentes	2dias	31/01/2011	01/02/2011	7
9	estimación del impacto	1dia	02/02/2011	03/02/2011	8
10	estimación del riesgo	1dia	03/02/2011	04/02/2011	9

Fuente: Elaboración propia

2 Presupuesto Estimado

Descripción	CANTIDAD	Costo Total	
Bienes		**S./**	**1300.00**
- Equipo de cómputo *	1	**S./**	1200.00
- Impresora *	1	**S./**	100.00
- Software	1	**S./**	0.00
Recursos Humanos		**S./**	**2700.00**
- Personal de Investigación *	1	**S./**	2700.00
Insumos		**S./**	**100.00**
- Material de escritorio	VARIOS	**S./**	20.00
- Materiales de impresión	VARIOS	**S./**	80.00
Servicios		**S./**	**180.00**
- Movilidad Local	VARIOS	**S./**	180.00
Total		**S./**	**4,280.00**

* **PROPIEDAD DEL BACHILLER**

Fuente: Elaboración propia

SECCION II

VISIÓN GENERAL DE LA SOLUCIÓN PROPUESTA

CAPÍTULO I

1. INTRODUCCION.

1.1 Contexto:

La Empresa Distribuciones Quispe S.A.C. empresa líder en comercialización de productos diversos en la Amazonía.
Desde sus inicios desde la década de los años 80 empezando por una tienda de abarrotes a un centro comercial uno de los más grandes de la ciudad de Iquitos en la actualidad, se ha distinguido por la sencillez, agilidad y seguridad donde todo lo encuentras en un mismo lugar, lo que permite brindar un valor agregado en sus servicios de atención al cliente.

Distribuciones Quispe S.A.C., no es ajena a este proceso evolutivo y es consciente de la seguridad de la información e infraestructura tecnológica (hardware, software, comunicaciones, etc.), además de considerar los procesos de implementación y actualización de las acciones a seguir en su Seguridad Informática.

Siendo para ello uno de los procesos más importante el **Análisis de riesgo de La seguridad lógica y física de la información,** para poder determinar el nivel de criticidad de los activos de la empresa. Sirviendo esto como base para la implementación de un PSI – PLAN DE SEGURIDAD DE INFORMACION.

1.2 PROBLEMÁTICA OBJETO DE LA APLICACIÓN

Con la ELABORACION DEL P.S.I DE LA EMPRESA DISTRIBUCIONES QUISPE SAC, se pretende reducir la posibilidad de ocurrencia de las amenazas a sus activos y desarrollar los procedimientos de recuperación a seguir en caso que se presentara alguna amenaza

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de la organización. De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades.

1.2.1 PROBLEMA GENERAL

1. ¿Es factible la ELABORACION DEL P.S.I DE LA EMPRESA DISTRIBUCIONES QUISPE SAC?

1.2.2 PROBLEMÁTICA ESPECÍFICA.

1. ¿Cuáles serían los principales activos a identificar para el correcto funcionamiento dentro de LA EMPRESA DISTRIBUCIONES QUISPE SAC?

2. ¿Cómo se determinaría las amenazas que están expuestas a dichos activos, y estimar su valor cualitativo en LA EMPRESA DISTRIBUCIONES QUISPE SAC?

3. ¿Qué salvaguardas serian apropiadas para que pretenda impedir la ocurrencia de las amenazas en LA EMPRESA DISTRIBUCIONES QUISPE SAC?

4. ¿Cuál sería perfil necesario de las personas que se encargaran del diseño de los lineamientos de seguridad en LA EMPRESA DISTRIBUCIONES QUISPE SAC?

1.3 OBJETIVOS DEL PROYECTO

1.3.1 **OBJETIVO** GENERAL.

El objetivo general consiste en la realización **del Análisis de riesgo de La seguridad lógica y física de la información** de LA EMPRESA DISTRIBUCIONES QUISPE SAC con el fin de revelar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una Política de Seguridad, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la organización.

1.3.2 **OBJETIVOS** ESPECIFICOS.

1. Identificar los activos necesarios para el correcto funcionamiento de LA EMPRESA DISTRIBUCIONES QUISPE SAC.

2. Determinar que amenazas están expuestas dichos activos, y estimar su valor

3. Proponer las salvaguardas apropiadas que pretenda impedir la ocurrencia de las amenazas.

4. Definir en LA EMPRESA DISTRIBUCIONES QUISPE SAC, los perfiles de las personas que se encargaran del diseño de los lineamientos de seguridad.

CAPITULO II

DESCRIPCIÓN DEL DISEÑO DE LA SOLUCIÓN

2.1. Técnicas de recolección de datos a emplear.

Para la recolección de información se realizó mediante observación directa, documentación de auditoría realizada anteriormente a la EMPRESA DISTRIBUCIONES QUISPE SAC.

2.2. Metodología y herramientas a emplear.

2.2.1 METODOLOGIA

Para la Análisis de riesgo de La seguridad lógica y física de la información, de LA EMPRESA DISTRIBUCIONES QUISPE SAC existen diversas metodologías
Como son:

2.2.1.1 MAGERIT

MAGERIT: Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica Española.

Se trata de una metodología abierta, dispone de una herramienta de soporte, PILAR (Proceso Informatico-Logico para el Análisis y la Gestión de Riesgos)

La metodología Magerit se puede resumir gráficamente de la siguiente forma:

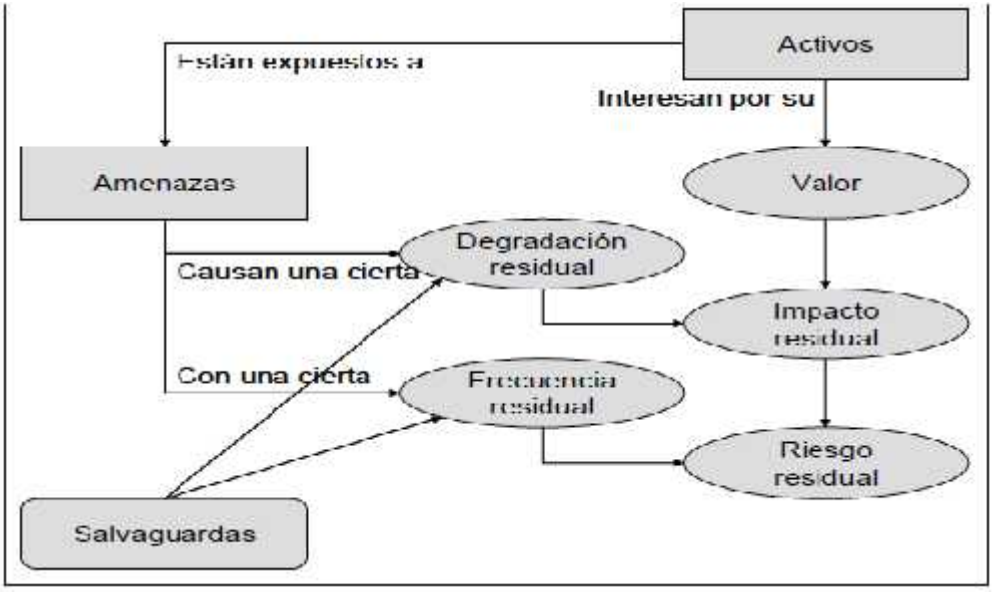


Figura 1. Grafico Metodología Magerit

2.2.1.2 OCTAVE -Operationally Critical threat, Asset and Vulnerability Evaluation

Octave: Es un modelo para la creación de metodologías de análisis de riesgos
Desarrollado por la Universidad de Carnegie Mellón
Las fases del proceso Octave se puede resumir en el siguiente gráfico:

Figura 2. Grafico Metodología OCTAVE

2.2.1.3 CRAMM- CCTA Risk Analysis and Management Method

CRAMM-CCTA Es la metodología de análisis de riesgo desarrollada en el Reino Unido por la agencia Central de Cómputo y Telecomunicaciones (CCTA)

El modelo de análisis y gestión de riesgos de CRAMM se puede resumir en el siguiente gráfico:

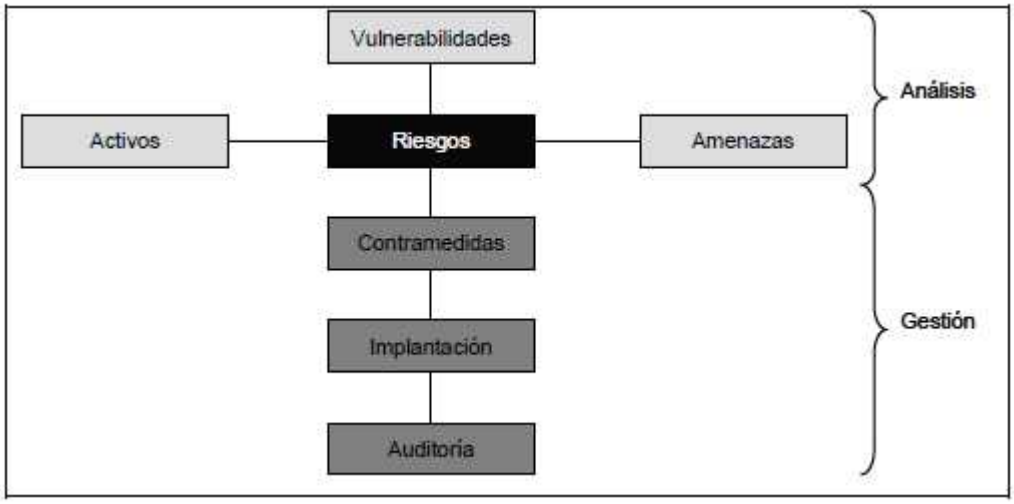


Figura 3. Grafico Metodología CRAMM

De las cuales se procedió a la elección de la siguiente:

MAGERIT Version 2

.

.

2.2.2 HERRAMIENTAS

Para el Análisis de riesgo de La seguridad lógica y física de la información, de LA EMPRESA DISTRIBUCIONES QUISPE SAC se utilizó las siguientes herramientas como son:

HERRAMIENTAS	DESCRIPCION	PROVEEDOR	VERSION	FABRICANTE	AÑO
⁾ PILAR	HERRAMIENTA DE ANALISI DE GESTION DE RIESGO	MINISTERIO DE ADMINISTRACION PUBLICA DE ESPAÑA	4.4.4	CSAE-CONSEJO ADMINISTRACION ELECTRONICA DE ESPAÑA	2010
⁾ JAVA-J2SE	HERRAMIENTA DE DESARROLLO-SERVICIOS WEB	SUN MICROSYSTEM	6.0	SUN MICROSYSTEM	2006

Tabla 1. Características de las HERRAMIENTAS DE ANALISIS Y GESTION DE RIESGOS

2.3. Descripción de la solución propuesta.

El desarrollo de la solución es un análisis de gestión de riesgos de la seguridad lógica y física de la empresa distribuciones QUISPE SAC que
Con el fin de revelar las vulnerabilidades existentes, como medio para el desarrollo de una Política de Seguridad como utilizando para el análisis de gestión de riesgo la herramienta de software de PILAR V2.0 el cual servirá para el análisis cualitativo asignándole para ello valores numéricos que se detallaran a medida que se lee el informe.

2.4. Indicadores de evaluación de la solución:

Los indicadores para la evaluación de la solución son indicadores cualitativos teniendo como escala de valores lo siguiente:

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

2.5. Relación de Entregables:

- ✓ INFORME FINAL
- ✓ SOFTWARE

CAPITULO III

DESARROLLO DE LA SOLUCIÓN PROPUESTA

3.1. Planificación.

Item	Nombre de tarea	Duración	Comienzo	Fin	Predece
1	Estudio de la metodología MAGERIT	24dias	01/12/2010	24/12/2010	
2	Identificación de activos	20dias	25/12/2010	14/01/2011	1
3	Dependencia entre activos	3dias	14/01/2011	17/01/2011	2
4	Valoración de los activos	3dias	18/01/2011	21/01/2011	3
5	Identificación de las amenazas	3dias	22/01/2011	25/01/2011	4
6	Valoración de las amenazas	2dias	26/01/2011	28/01/2011	5
7	identificación de las salvaguardas existentes	1dia	29/01/2011	30/01/2011	6
8	valoración de las salvaguardas existentes	2dias	31/01/2011	01/02/2011	7
9	estimación del impacto	1dia	02/02/2011	03/02/2011	8
10	estimación del riesgo	1dia	03/12/2011	04/12/2011	9

3.1.1. Determinación del dominio y límites.

3.1.1.1. Dominio

El Análisis de riesgo de La seguridad lógica y física de la información tiene como DOMINIO BASE la sede central que se encuentra en la ciudad de Iquitos Jr Prospero N° 935

3.1.1.2. Limites

El Análisis de riesgo de La seguridad lógica y física de la información abarcara:

Seguridad lógica

- Identificación – id's-usuarios
- Autenticación
- Password

Seguridad física

- Equipamiento
- Control de acceso físico al Centro de Cómputos
- Control de acceso a equipos
- Dispositivos de Soporte
- Estructura del edificio
- Cableado estructurado

3.1.2. Dimensiones.

[D] disponibilidad

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

[I] integridad de los datos

Garantía de la exactitud y completitud de la información y los métodos de su procesamiento

[C] confidencialidad de los datos

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

[A_S] autenticidad de los usuarios del servicio

Aseguramiento de la identidad u origen.

[A_D] autenticidad del origen de los datos

Aseguramiento de la identidad u origen.

[T_S] trazabilidad del servicio.

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué
momento.

[T_D] trazabilidad de los datos.

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué
momento.

3.2. **Análisis de riesgo**

La evaluación de riesgos supone considerar los factores inmediatos de riesgo, imaginándose que puede ir mal y estimar el coste que supondría la ocurrencia e impacto, sean estas accidentales o intencionales.

En tal sentido se realizaron las evaluaciones de los posibles riesgos y sus probabilidades de ocurrencia en el entorno informático de Distribuciones Quispe S.A.C.

Los principales riesgos en la seguridad informática a los que se enfrenta nuestra empresa son:

3.2.1. **Caracterización de los activos.**

3.2.1.1**. Identificación los activos a proteger.**

Seguridad lógica

- IDENTIFICACIÓN – ID'S-Usuarios
  Este activo está relacionado a perfiles de usuarios del personal que interactua con el sistema de ventas

- AUTENTICACIÓN

  Este activo está relacionado al nivel de seguridad en control de acceso al sistema de ventas

- PASSWORD

  Este activo está relacionado a las características mínimas de los claves de acceso

SEGURIDAD FÍSICA

- EQUIPAMIENTO.

  Este activo está relacionado a la protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos de la empresa

- CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTOS

  Este activo está relacionado en cuanto a la restricción y seguridad, monitoreo, control de acceso a las instalaciones del centro de cómputo

- CONTROL DE ACCESO A EQUIPOS

  Este activo está relacionado en cuanto a la restricción y seguridad, monitoreo, control de acceso a las a los pc's, servidores, switch

- DISPOSITIVOS DE SOPORTE

  Este activo está relacionado en cuanto a seguridad, monitoreo, control de los sistemas de alarmas, energía, aire acondicionado dispositivos que contribuyan al correcto y continuo funcionamiento de la Empre

- ESTRUCTURA DEL EDIFICIO

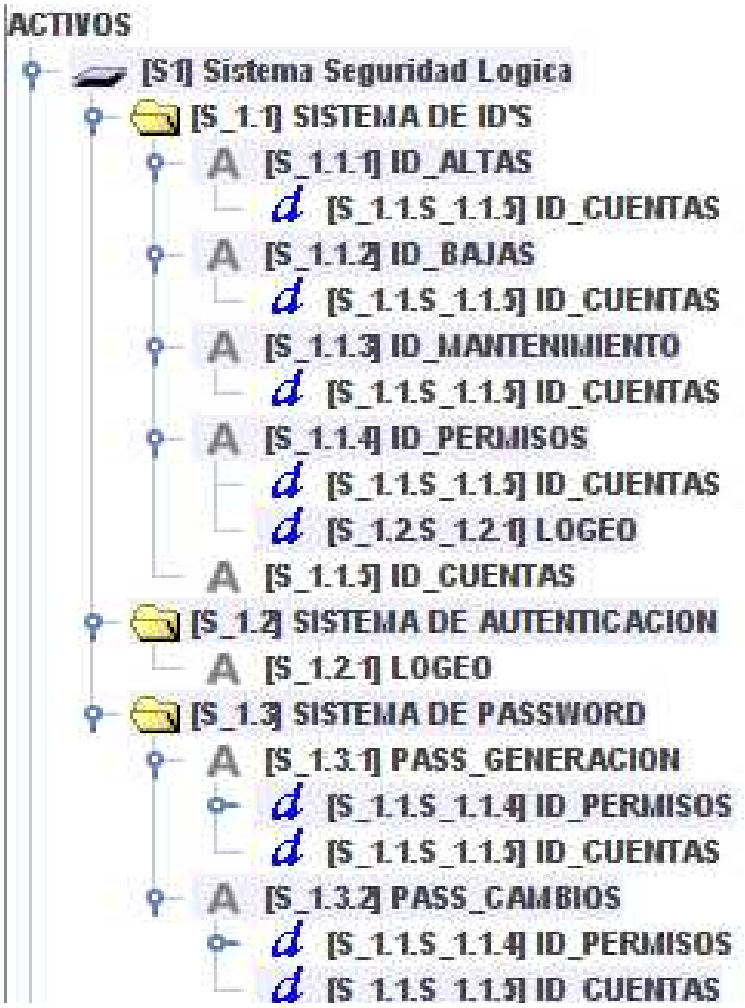
  Este activo está relacionado en cuanto al diseño y la ubicación de las distintas áreas de la empresa y el centro de cómputo.

- CABLEADO ESTRUCTURADO

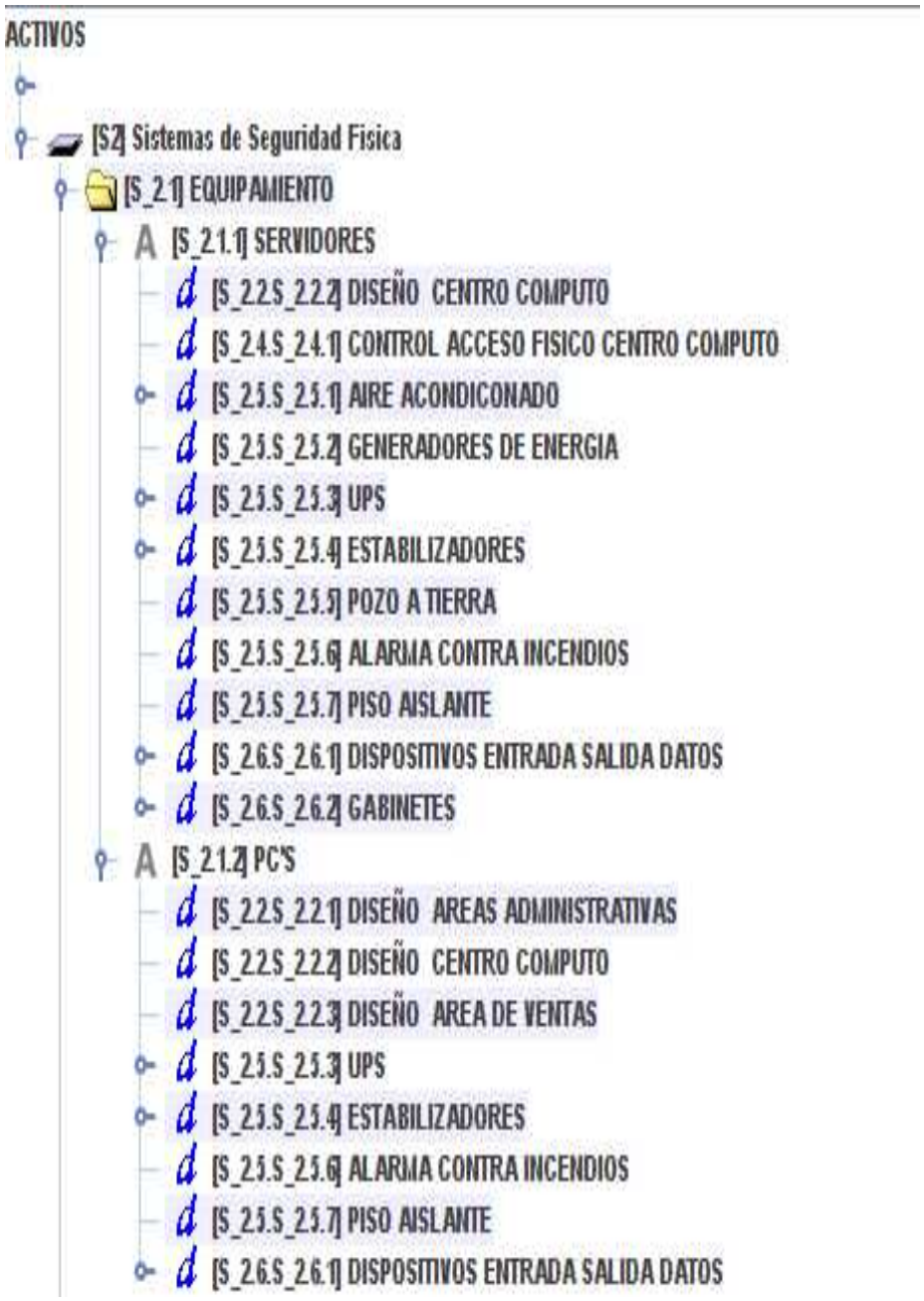
  Este activo está relacionado en cuanto a la estructuración de la red LAN de la empresa.

3.2.1.2. **Establecimiento de las dependencias de los Activos.**

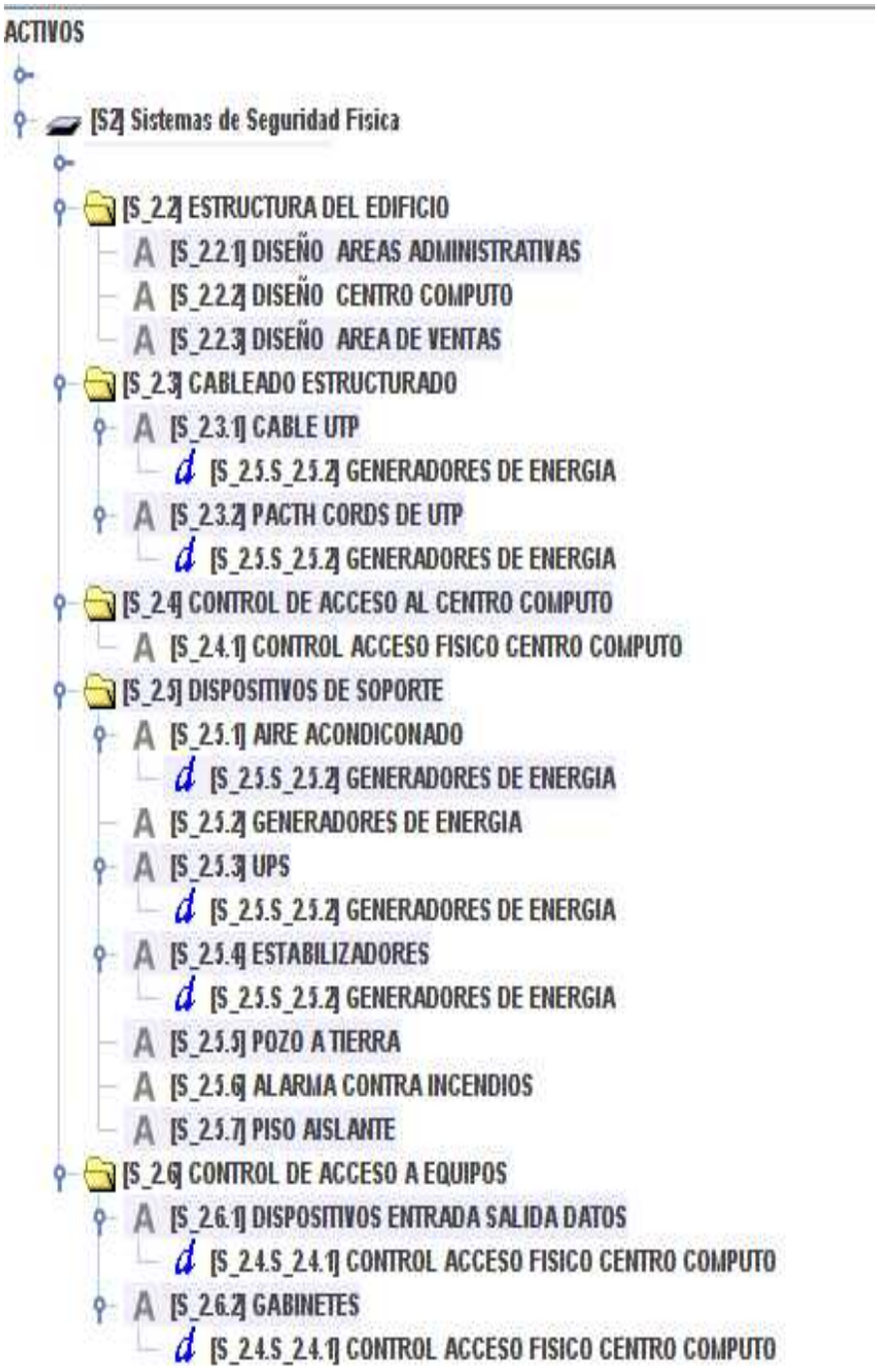
Dependencia sistema seguridad lógica



Dependencia sistema seguridad física



Dependencia sistema seguridad física



3.2.1.3 **Valoración de activos**

Sistemas de seguridad lógica

Identificación – id's-usuarios

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_1.1]sistema de id's							
❖ [S_1.1.1]id_altas	4(1)	4(2)	9(3)	4(4)		4(5)	
❖ [S_1.1.2]id_bajas	7(6)	4(7)	4(8)	7(9)		7(10)	
❖ [S_1.1.3]id_mantenimiento	7(11)	4(12)	4(13)	7(14)		7(15)	
❖ [S_1.1.4]id_permisos	5(16)	7(17)	7(18)	7(19)		4(20)	
❖ [S_1.1.5]id_cuentas	7(21)	7(22)	9(23)	7(24)		7(25)	

1. [4] [pi1] Información personal: probablemente afecte a un grupo de individuos
2. [4] [pi1] Información personal: probablemente afecte a un grupo de individuos
3. [9] [si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
4. [4][pi1] Información personal: probablemente afecte a un grupo de individuos
   [4][ps] Seguridad de las personas: probablemente cause daños menores a varios individuos
5. [4][pi1] Información personal: probablemente afecte a un grupo de individuos
6. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
   [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
7. [4][pi1] Información personal: probablemente afecte a un grupo de individuos
   [4][ps] Seguridad de las personas: probablemente cause daños menores a varios individuos

8. [4] [pi1] Información personal: probablemente afecte a un grupo de individuos
   [4] [pi2] Información personal: probablemente quebrante leyes o regulaciones
9. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras
   organizaciones
   [7][lg] Probablemente causaría una publicidad negativa generalizada
10. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
    [7][cei] Intereses comerciales o económicos:
11. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
12. [4][pi1] Información personal: probablemente afecte a un grupo de individuos
    [4][ps] Seguridad de las personas: probablemente cause daños menores a varios individuos
13. [4] [pi1] Información personal: probablemente afecte a un grupo de individuos
    [4] [pi2] Información personal: probablemente quebrante leyes o regulaciones
14. [7][lg] Probablemente causaría una publicidad negativa generalizada
15. [7][cei] Intereses comerciales o económicos:
16. [5][pi1] Información personal: probablemente afecte gravemente a un individuo
17. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
    [7][cei] Intereses comercial o económico:
18. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización
    con un impacto significativo en otras organizaciones
    [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
19. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización
    con un impacto significativo en otras organizaciones
    [7][lg] Probablemente causaría una publicidad negativa generalizada
20. [4][pi1] Información personal: probablemente afecte a un grupo de individuos
21. [7][cei] Intereses comerciales o económicos:

22. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
    [7][cei] Intereses comerciales o económicos:
23. [da] Probablemente cause una interrupción excepcionalmente seria de las actividades
    [cei] Intereses comerciales o económicos:
24. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización
    [7] [cei] Intereses comerciales o económicos:
    [7] [ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
25. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización

Sistemas de seguridad lógica

Autenticación

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_1.2]sistema de autenticación							
❖ [S_1.1.1]logeo	5(1)	7(2)	7(3)	7(4)		9(5)	

1. [5] [adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización
2. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización
3. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
4. [7][lg] Probablemente causaría una publicidad negativa generalizada
5. [9][cei] Intereses comerciales o económicos:

Sistemas de seguridad lógica

Password

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_1.3] PASSWORD							
❖ [S_1.1.1]generación	4(1)	4(2)	9(3)	4(4)		4(5)	
❖ [S_1.1.2]cambios	7(6)	7(7)	7(8)	7(9)		7(10)	

1. [4] [pi1] Información personal: probablemente afecte a un grupo de individuos
2. [4] [pi1] Información personal: probablemente afecte a un grupo de individuos
3. [9] [si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
4. [4][ps] Seguridad de las personas: probablemente cause daños menores a varios individuos
5. [4][pi1] Información personal: probablemente afecte a un grupo de individuos
6. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
7. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización
8. [7][da] Probablemente cause una interrupción seria de las actividades propias de la Organización
9. [7] [cei] Intereses comerciales o económicos
10. [7][adm] Administración y gestión: probablemente impediría la operación efectiva de la organización

Sistemas de seguridad física

Equipamiento.

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.1] equipamiento							
❖ [S_2.1.1] servidores	$10^{(1)}$	$10^{(2)}$	$10^{(3)}$	$9^{(4)}$		$10^{(5)}$	
❖ [S_2.1.2] pc's	$10^{(6)}$	$10^{(7)}$	$10^{(8)}$	$9^{(9)}$		$10^{(10)}$	

1. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
2. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
3. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
4. [9][da] Probablemente cause una interrupción excepcionalmente seria de las actividades
5. [10][olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
6. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
7. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
8. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9. [9][da] Probablemente cause una interrupción excepcionalmente seria de las actividades
10. [10][olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

Sistemas de seguridad física

Estructura del edificio.

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.2] ESTRUCTURA DEL EDIFICIO							
❖ [S_2.1.1] área administrativa							
❖ [S_2.1.2] centro computo							
❖ [S_2.1.3] área ventas	5(1)						

1. [5][lg] Probablemente sea causa una cierta publicidad negativa

Sistemas de seguridad física

Cableado estructurado

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.3] CABLEADO ESTRUCTRADO							
❖ [S_2.3.1] cable utp	-	-	-	-	-	-	-
❖ [S_2.3.2] patch cords de utp	-	-	-	-	-	-	-

Sistemas de seguridad física

Control de acceso al centro de cómputo

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.4] control acceso centro de computo	$10^{(1)}$	$10^{(2)}$	$10^{(3)}$				

1. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
2. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
3. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

Sistemas de seguridad física

Dispositivos de soporte

ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.5] dispositivos de soporte							
❖ [S_2.5.1] aire acondicionado	$10^{(1)}$	$10^{(2)}$					
❖ [S_2.5.2] generador de energía	$10^{(1)}$	$10^{(2)}$					
❖ [S_2.5.3] ups	$10^{(1)}$	$10^{(2)}$					
❖ [S_2.5.4] estabilizador	$10^{(1)}$	$10^{(2)}$					
❖ [S_2.5.1] pozo a tierra	$10^{(1)}$	$10^{(2)}$					
❖ [S_2.5.2] alarma de contra incendio	$10^{(1)}$	$10^{(2)}$					
❖ [S_2.5.3] piso aislante	$10^{(1)}$	$10^{(2)}$					

1. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
2. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
3. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
4. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
5. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
6. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
7. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
8. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
10. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

Sistemas de seguridad física

Control de acceso a equipos

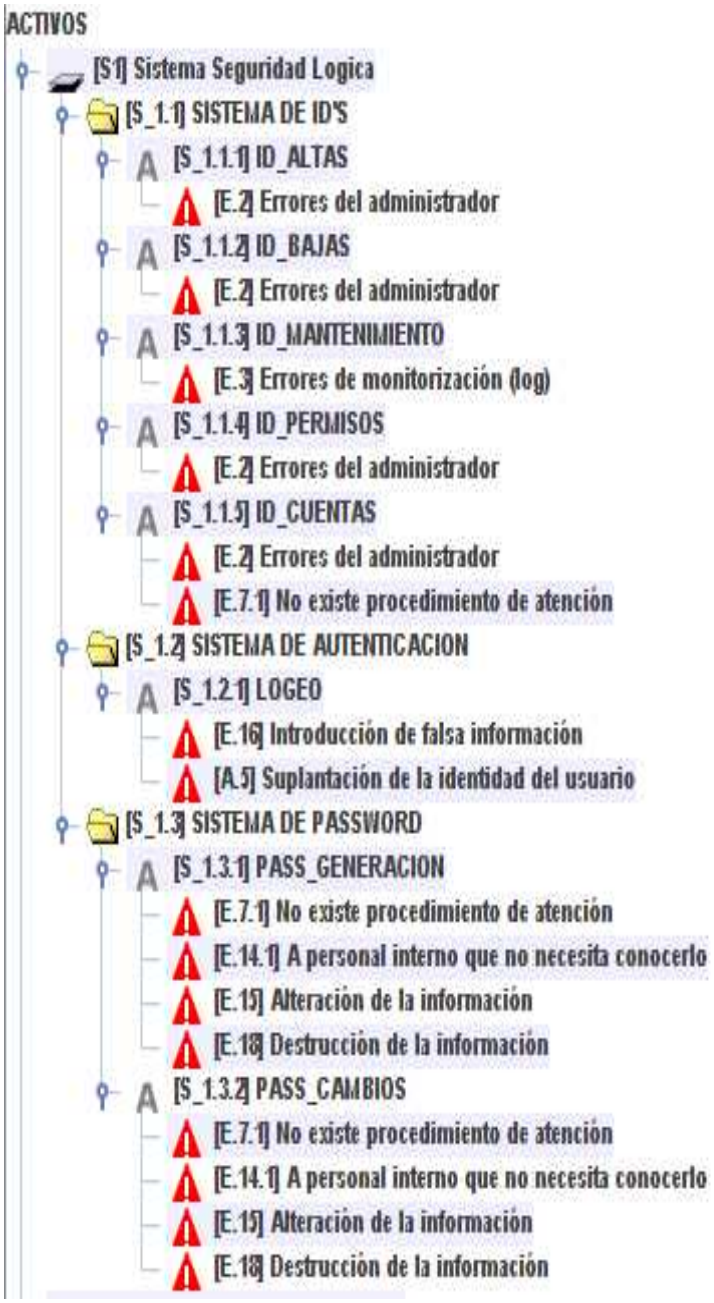
ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.6] acceso a equipos							
❖ [S_2.1.1] dispositivos e/s de datos	$10^{(1)}$	$10^{(2)}$	$10^{(3)}$				
❖ [S_2.1.2] GABINETES	$10^{(4)}$	$10^{(5)}$	$10^{(6)}$				

1. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
2. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
3. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
4. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
5. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
6. [10] [olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

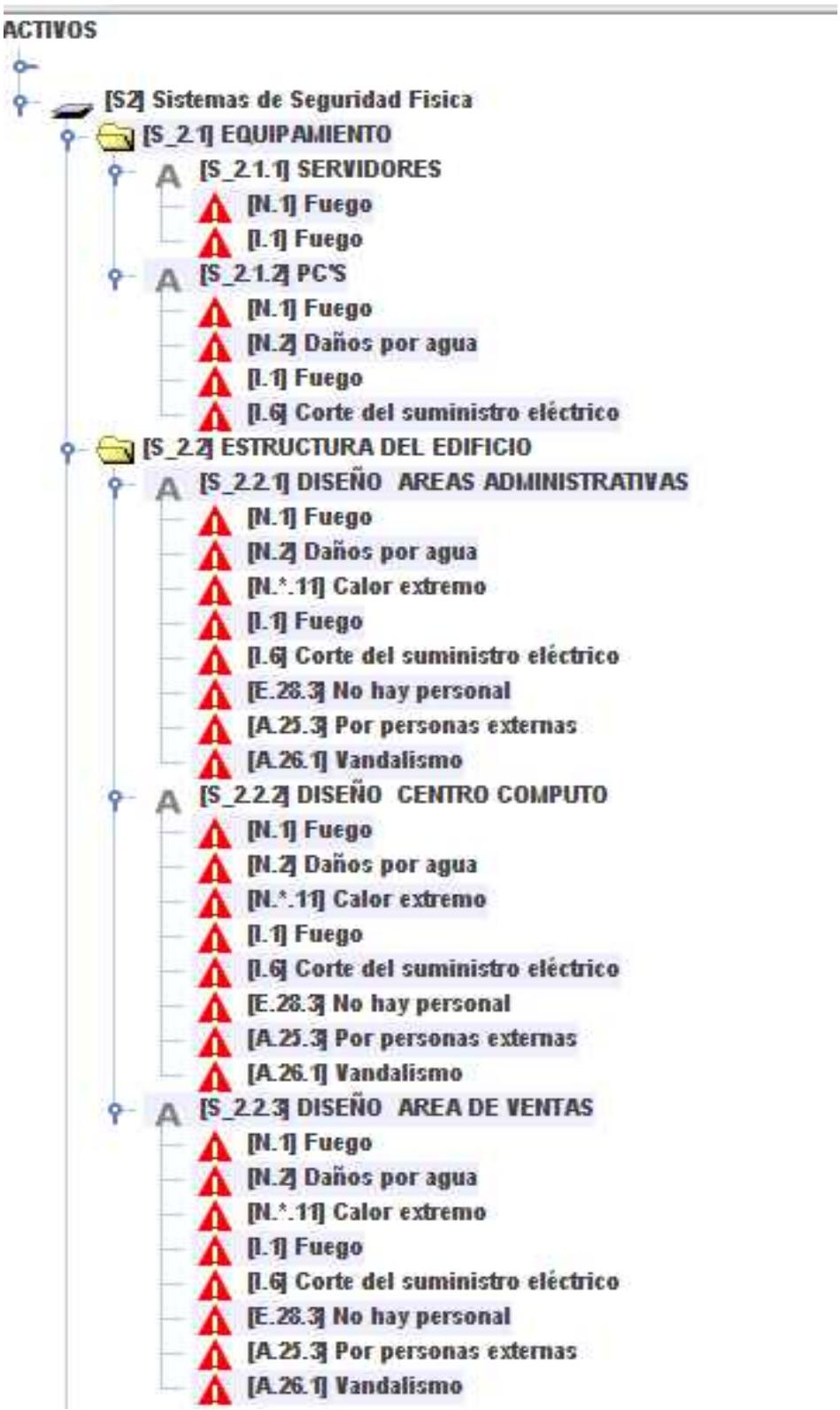
3.2.2. **Caracterización de las amenazas.**

3.2.2.1. Identificación de las amenazas.

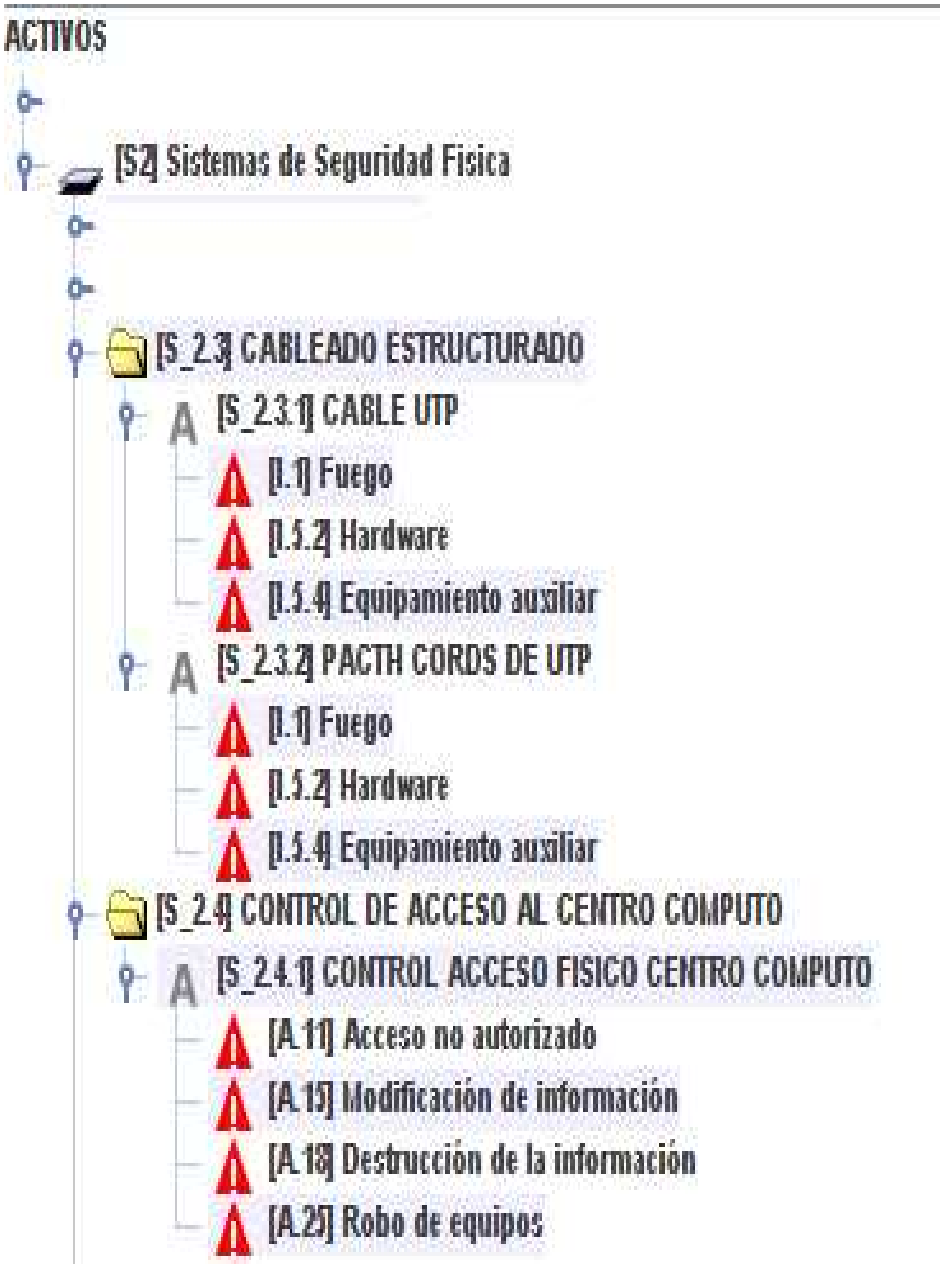
Sistema de seguridad lógica



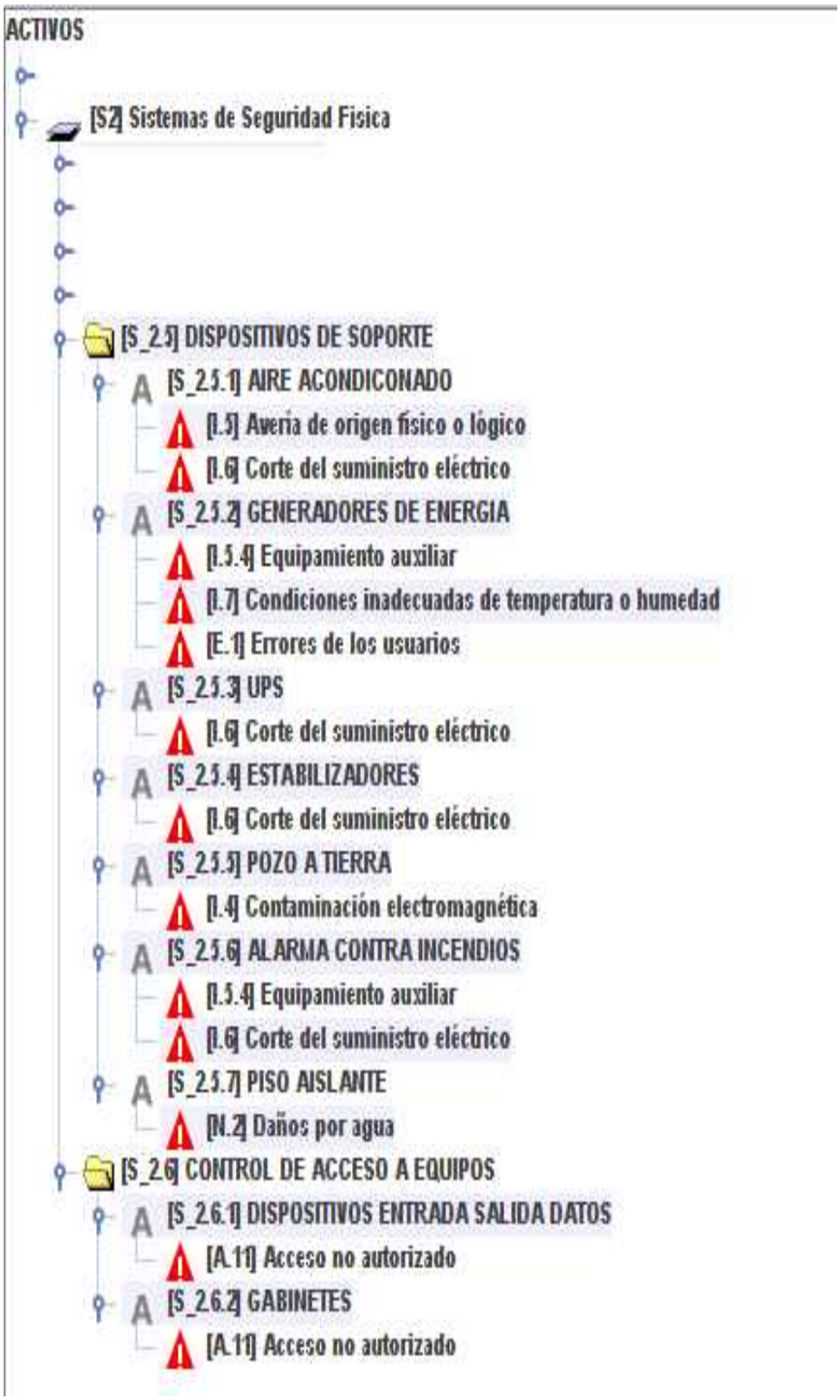
SISTEMA DE SEGURIDAD FISICA



SISTEMA DE SEGURIDAD FISICA



SISTEMA DE SEGURIDAD FISICA



3.2.2.2. VALORACIÓN DE LAS AMENAZAS.

VALORACION

CRITERIO	FRECUENCIA
1 VEZ AL DIA	1
5 VECES AL DIA	5
1 VEZ POR SEMANA	0.5
1VEZ AL MES	0.25
1VEZ AL AÑO	0.125
2 VECES AL AÑO	0.625

SISTEMAS DE SEGURIDAD LOGICA

IDENTIFICACIÓN – ID'S-Usuarios

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_1.1]SISTEMA DE ID'S								
❖ [S_1.1.1]ID_ALTAS		100%						
[E.2]Errores de Administrador	0,25	100%						
❖ [S_1.1.2]ID_BAJAS		50%						
[E.2]Errores de Administrador	0,25	50%						
❖ [S_1.1.3]ID_MANTENIMIENTO		50%						
[E.3]Errores de monitorización	0,25	50%						
❖ [S_1.1.4]ID_PERMISOS		100%						
[E.2]Errores de Administrador	5	100%						
❖ [S_1.1.5]ID_CUENTAS		100%						
[E.2]Errores de Administrador	5	100%						
[E.7.1]No existe procedimiento de atención	5	100%						

Sistemas de seguridad lógica

Autenticación

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_1.2]SISTEMA DE LOGEO		50%						
❖ Introducción de falsa información	0,5	50%						
❖ Suplantación de identidad de usuario	0,25	50%						

Sistemas de seguridad logica

Password

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_1.3] PASSWORD								
[S_1.1.1]GENERACION		100%						
[E.7.1]No existe procedimiento de atención	0,125	100%						
[E.14.1]A personal interno que no necesita conocerlo	0,125	100%						
[E.15]Alteración de la información	0,125	50%						
[E.18]Destrucción de la información	0,125	100%						
[S_1.1.2]CAMBIOS		100%						
[E.7.1]No existe procedimiento de atención	0,125	100%						
[E.14.1]A personal interno que no necesita conocerlo	0,125	100%						
[E.15]Alteración de la información	0,125	100%						
[E.18]Destrucción de la información	0,125	100%						

Sistemas de seguridad física

Equipamiento.

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.1] equipamiento								
❖ [S_2.1.1] servidores		10%						25%
[I.1]Fuego	0,625	10%						25%
❖ [S_2.1.2] pc's		90%						90%
[N.2] Daños por agua	0,625	10%						10%
[I.1] Fuego	0,125	25%						25%
[I.6] Corte del suministro eléctrico	1	90%						90%

Sistemas de seguridad física

Estructura del edificio

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.2] ESTRUCTURA DEL EDIFICIO								
❖ [S_2.1.1] AREA ADMINISTRATIVA		90%						90%
[N.1]Fuego	0,625	90%						25%
[N.2]Daños por agua	0,125	25%						25%
[N.11]Calor extremo	0,25	25%						25%
[I.1]Fuego	1	25%						5%
[I.6]Corte de suministro eléctrico	0,25	10%						10%
[E.28.3]No hay personal		90%						90%
❖ [S_2.1.2] CENTRO COMPUTO	0,625	90%						25%
[N.1]Fuego	0,125	25%						25%
[N.2]Daños por agua	0,25	25%						25%
[N.11]Calor extremo	0,125	25%						25%
[I.5.4]Equipamiento auxiliar		90%						90%
❖ [S_2.1.3] AREA VENTAS	0,625	90%						90%
[N.1]Fuego	0,125	25%						25%
[N.2]Daños por agua	0,25	25%						25%
[N.11]Calor extremo	1	90%						5%
[I.6]Corte de suministro eléctrico	0,25	10%						5%
[E.28.3]No hay personal	0,125	90%						90%

SISTEMAS DE SEGURIDAD FISICA

❖ CABLEADO ESTRUCTURADO

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.3] cableado estructrado								
❖ [S_2.3.1] cable utp		10%						
Hardware	0,25	5%						
Fuego	0,625	10%						
❖ [S_2.3.2] pacth cords de utp		10%						
Hardware	0,25	10%						
Fuego	0,625	5%						

Sistemas de seguridad física

Control de acceso al centro de cómputo

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.4] control acceso centro de computo		50%	10%	20%				70%
[A.11]Acceso no autorizado	0,125	50%	10%	20%				70%
[A.15]Modificación de la información	0,125	10%	10%	20%				25%
[A.18]Destrucción de la información	0,125	5%	5%	5%				10%

SISTEMAS DE SEGURIDAD FISICA

DISPOSITIVOS DE SOPORTE.

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.5] dispositivos de soporte								
❖ [S_2.5.1] aire acondicionado		50%						50%
[I.5]Avería de origen físico o lógico	0,25	50%						50%
[I.6]Corte de suministro eléctrico	0,5	50%						50%
❖ [S_2.5.2] generador de energía		50%	50%	50%	50%			50%
[I.5.4]Equipamiento auxiliar	0,25	50%						50%
[I.7]Condiciones inadecuadas de temperatura o humedad	0,125	25%						50%
[E.1]Errores de los usuarios	0,125	50%	50%	50%	50%			50%
❖ [S_2.5.3] ups		50%						
[I.6]Corte de suministro eléctrico	0,25	50%						
❖ [S_2.5.4] estabilizador		50%						
[I.6]Corte de suministro eléctrico	0,5	50%						
❖ [S_2.5.1] pozo a tierra		50%						
[I.4]Contaminación electromagnética	0,125	50%						
❖ [S_2.5.2] alarma incendios		50%						
[I.5.4]Equipamiento auxiliar	0,125	25%						
[I.6]Corte suministro eléctrico	0,5	50%						
❖ [S_2.5.3] piso aislante		25%						
[N.2] Daños por agua	0,25	25%						

Sistemas de seguridad física

Control de acceso a equipos

Amenaza	Frecuencia	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_2.6] acceso a equipos								
❖ [S_2.1.1] dispositivos e/s de datos		50%	50%	50%				25%
[A.11]Acceso no autorizado	0,25	50%	50%	50%				25%
❖ [S_2.1.2] gabinetes		25%	25%					25%
[A.11]Acceso no autorizado	0,125	25%	25%					25%

3.2.3. **Caracterización de las salvaguardas**.

3.2.3.1. **Identificación de las salvaguardas**.

[Quispe] centro comercial galerías Quispe Distribuciones Quispe sac

[QUISPE]	**Distribuciones Quispe sac**
DESCRIPCION	Área encargada de ti y sistemas
PROPIETARIO	Sr. Remigio Quispe choque
ORGANIZACIÓN	Distribuciones Quispe sac
VERSION	1.0
FECHA	Mar-11
BIBLIOTECA	[std]Biblioteca INFOSEC (22.1.2009)

LICENCIA

[Evaluación]

NIVELES 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

DOMINIOS

- [base]Base

FASES

- [f1] situación actual
- [f2] situación deseado

MARCO DE GESTION

SALVAGUARDA
Organización
Coordinación De La Seguridad De Información
Asignación De Responsabilidades Para La Seguridad De Información
Roles Identificados
Cooperación Entre Organizaciones
Normativa De Seguridad
Marco Legal
Política De Seguridad
Documentación De Seguridad De Información
Procedimientos Operativos
Criterios De Aceptación Para Versiones O Sistemas Nuevos
Gestión De Privilegios
Identificación Y Autenticación
Identificación De Usuarios
Control De Acceso Lógico
Restricción De Acceso A La Información
Registro De Usuarios
Gestión De Incidencias
Procedimientos De Gestión De Incidentes
Comunicación De Los Fallos Del Software
Registro De Fallos Y Revisión De Medidas Correctoras
Se Aprende De Los Incidentes Y Se Propone Mejoras
Registro Y Auditoria

RELACIONES CON TERCEROS

SALVAGUARDA
Seguridad En Los Accesos A Terceras Partes
Establecimientos De Acuerdo Para Intercambio De Información Y Software
Inclusión De Clausulas De Confidencialidad En Los Contratos En Otras Empresas

SERVICIOS

SALVAGUARDA
Inventario De Servicios
Disponibilidad
Desarrollo
Despliegue
Aplicación De Perfiles De Seguridad
Explotación
Gestión De Servicios Externos
Terminación

DATOS/INFORMACION

SALVAGUARDA
Inventario De Activos De Información
Clasificación De La Información
Disponibilidad
Integridad
Criptografía

APLICACIONES INFORMATICAS (SW)

SALVAGUARDA
Inventario de aplicaciones
Copias de seguridad
Adquisición
Desarrollo
Puesta en producción
Aplicación de perfiles de seguridad

EQUIPOS INFORMATICOS (HW)

SALVAGUARDA
Inventario de equipos
Disponibilidad
Adquisición de HW
Instalación
Aplicación de perfiles de seguridad

SOPORTE DE INFORMACION

SALVAGUARDA
Inventario de soportes
Disponibilidad
Adquisición de soportes
Gestión de soportes

ELEMENTOS AUXILIARES

SALVAGUARDA
Inventario de equipamiento auxiliar
Disponibilidad
Suministro eléctrico
Gestión de soportes
Protección de cableado
Otros suministros

SEGURIDAD FISICA

SALVAGUARDA
Inventario de instalaciones
Normativa
Procedimientos
Diseño
Control de acceso físico
Protección de perímetro
Vigilancia
Iluminación de seguridad
Protección frente a desastres

PERSONAL

SALVAGUARDA
Relación de personal
Puestos de trabajo
Contratación
Formación

3.2.3.2. VALORACIÓN DE LAS SALVAGUARDAS.

[QUISPE] **CENTRO COMERCIAL GALERIAS QUISPE**
DISTRIBUCIONES QUISPE SAC

[QUISPE]	**DISTRIBUCIONES QUISPE SAC**
DESCRIPCION	AREA ENCARGADA DE T.I Y SISTEMAS
PROPIETARIO	SR. REMIGIO QUISPE CHOQUE
ORGANIZACIÓN	DISTRIBUCIONES QUISPE SAC
VERSION	1.0
FECHA	mar-11
BIBLIOTECA	[std]Biblioteca INFOSEC (22.1.2009)

LICENCIA

[Evaluación]

NIVELES 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

DOMINIOS

- [base]Base

FASES

- [f1] situación actual
- [f2] situación deseado

MARCO DE GESTION

SALVAGUARDA	[f1]	[f2]
Organización	L1	L3
Coordinación de la seguridad de información	L0	L5
Asignación de responsabilidades para la seguridad de información	L0	L3
Roles identificados	L1	L3
Cooperación entre organizaciones	na	na
Normativa de seguridad	L0	L3
Marco legal	L1	L3
Política de seguridad	L0	L3
Documentación de seguridad de información	L0	L3
Procedimientos operativos	L1	L3
Criterios de aceptación para versiones o sistemas nuevos	L1	L3
Gestión de Privilegios	L0	L3
Identificación y autenticación	L1	L3
Identificación de usuarios	L1	L3
Control de acceso lógico	L1	L3
Restricción de acceso a la información	L1	L3
Registro de usuarios	L1	L3
Gestión de incidencias	L1	L5
Procedimientos de gestión de incidentes	L1	L3
Comunicación de los fallos del software	L2	L3
Registro de fallos y revisión de medidas correctoras	L1	L3
Se aprende de los incidentes y se propone mejoras	L1	L3
Registro y auditoria	L1	L3

RELACIONES CON TERCEROS

SALVAGUARDA	[f1]	[f2]
Seguridad en los accesos a terceras partes	na	na
Establecimientos de acuerdo para intercambio de información y software	na	na
Inclusión de clausulas de confidencialidad en los contratos en otras empresas	na	na

SERVICIOS

SALVAGUARDA	[f1]	[f2]
Inventario de servicios	na	na
Disponibilidad	na	na
Desarrollo	na	na
Despliegue	na	na
Aplicación de perfiles de seguridad	na	na
Explotación	na	na
Gestión de servicios externos	na	na
Terminación	na	na

DATOS/INFORMACION

SALVAGUARDA	[f1]	[f2]
Inventario de activos de información	L1	L3
Clasificación de la información	L1	L3
Disponibilidad	L1	L3
Integridad	L1	L3
Criptografía	na	na

APLICACIONES INFORMATICAS (SW)

SALVAGUARDA	[f1]	[f2]
Inventario de aplicaciones	na	na
Copias de seguridad	na	na
Adquisición	na	na
Desarrollo	na	na
Puesta en producción	na	na
Aplicación de perfiles de seguridad	na	na

EQUIPOS INFORMATICOS (HW)

SALVAGUARDA	[f1]	[f2]
Inventario de equipos	L1	L5
Disponibilidad	L1	L3
Adquisición de HW	L1	L3
Instalación	L1	L5
Aplicación de perfiles de seguridad	L0	L3

SOPORTE DE INFORMACION

SALVAGUARDA	[f1]	[f2]
Inventario de soportes	na	na
Disponibilidad	na	na
Adquisición de soportes	na	na
Gestión de soportes	na	na

ELEMENTOS AUXILIARES

SALVAGUARDA	[f1]	[f2]
Inventario de equipamiento auxiliar	L1	L3
Disponibilidad	L1	L3
Suministro eléctrico	L1	L5
Gestión de soportes	L0	L5
Protección de cableado	L1	L5
Otros suministros	L1	L3

SEGURIDAD FISICA

SALVAGUARDA	[f1]	[f2]
Inventario de instalaciones	L1	L3
Normativa	L0	L3
Procedimientos	L0	L5
Diseño	L0	L5
Control de acceso físico	L1	L5
Protección de perímetro	L1	L5
Vigilancia	L1	L3
Iluminación de seguridad	L1	L3
Protección frente a desastres	L0	L5

PERSONAL

SALVAGUARDA	**[f1]**	**[f2]**
Relación de personal	na	na
Puestos de trabajo	na	na
Contratación	na	na
Formación	na	na

3.2.4. **Caracterización del impacto**.

Muestra los niveles de impacto y riesgo potenciales (que sufrirían los activos si no se aplicara ninguna salvaguarda para gestionarlos).

- **IMPACTO ACUMULADO**

  El impacto acumulado refleja el impacto del activo y de aquellos activos hijo de los que depende.

  Este valor se obtiene como resultado de la siguiente fórmula:

  Impacto acumulado = valor acumulado del activo * degradación que le provocaría la amenaza

  La valoración del impacto acumulado se muestran con la siguiente escala de colores según su valor:

|**Activos**: Muestra todos los activos (organizados por las capas y grupos de activos) dentro de cada uno, todas las amenazas definidas.

Impacto en cada dimensión: Muestra el impacto acumulado en cada dimensión que esté valorando.
Generalmente se mostrará:

- [D]: Muestra el impacto en la Disponibilidad.
- [I]: Muestra el impacto en la Integridad.
- [C]: Muestra el impacto en la Confidencialidad.
- [A]: Muestra el impacto en la Autenticidad.
- [T]: Muestra el impacto en la Trazabilidad.

IMPACTO ACUMULADO

SISTEMAS DE SEGURIDAD LOGICA

IDENTIFICACIÓN – ID'S-Usuarios

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_1.1]SISTEMA DE ID'S	7				
❖ [S_1.1.1]ID_ALTAS	4				
[E.2]Errores de Administrador	4				
❖ [S_1.1.2]ID_BAJAS	6				
[E.2]Errores de Administrador	6				
❖ [S_1.1.3]ID_MANTENIMIENTO	6				
[E.3]Errores de monitorización	6				
❖ [S_1.1.4]ID_PERMISOS	7				
[E.2]Errores de Administrador	7				
❖ [S_1.1.5]ID_CUENTAS	7				
[E.2]Errores de Administrador	7				
[E.7.1]No existe procedimiento de atención	7				

IMPACTO ACUMULADO

Sistemas de seguridad lógica

Autenticación

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_1.2]SISTEMA DE LOGEO	6				
[E.16]Introducción de falsa información	6				
[A.5]Suplantación de identidad de usuario	6				

IMPACTO ACUMULADO

Sistemas de seguridad lógica

Password

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_1.3] PASSWORD	7				
[S_1.1.1]GENERACION	4				
[E.7.1]No existe procedimiento de atención	4				
[E.14.1]A personal interno que no necesita conocerlo	4				
[E.15]Alteración de la información	3				
[E.18]Destrucción de la información	4				
❖ [S_1.1.2]CAMBIOS	7				
[E.7.1]No existe procedimiento de atención	7				
[E.14.1]A personal interno que no necesita conocerlo	7				
[E.15]Alteración de la información	7				
[E.18]Destrucción de la información	7				

IMPACTO ACUMULADO

Sistemas de seguridad física

Equipamiento.

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_2.1] equipamiento					
❖ [S_2.1.1] servidores	7				8
[N.1]Fuego	7				8
[I.1]Fuego	7				8
❖ [S_2.1.2] pc's	10				10
[N.1] Fuego	7				7
[N.2] Daños por agua	8				8
[I.1] Fuego	7				7
[I.6] Corte del suministro eléctrico	10				10

IMPACTO ACUMULADO

Sistemas de seguridad física

Estructura del edificio

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_2.2] ESTRUCTURA DEL EDIFICIO					
❖ [S_2.1.1] AREA ADMINISTRATIVA	10				10
[N.1]Fuego	7				8
[N.2]Daños por agua	8				8
[N.11]Calor extremo	8				8
[I.1]Fuego	7				8
[I.6]Corte de suministro eléctrico	10				10
[E.28.3]No hay personal	7				7
❖ [S_2.1.2] CENTRO COMPUTO	10				10
[N.1]Fuego	7				8
[N.2]Daños por agua	8				8
[N.11]Calor extremo	8				8
[I.5.4]Equipamiento auxiliar					
❖ [S_2.1.3] AREA VENTAS	10				10
[N.1]Fuego	7				8
[N.2]Daños por agua	8				8
[N.11]Calor extremo	8				8
[I.6]Corte de suministro eléctrico	10				10
[E.28.3]No hay personal	7				7
[A.26.1]Vandalismo	6				6

IMPACTO ACUMULADO

SISTEMAS DE SEGURIDAD FISICA

- CABLEADO ESTRUCTURADO

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_2.3] cableado estructrado					
❖ [S_2.3.1] cable utp					
Hardware					
Fuego					
❖ [S_2.3.2] pacth cords de utp					
Hardware					
Fuego					

IMPACTO ACUMULADO

Sistemas de seguridad física

Control de acceso al centro de cómputo

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_2.4] control acceso centro de computo	9	7	8		10
[A.11]Acceso no autorizado	9	7	8		10
[A.15]Modificación de la información	7	7	8		10
[A.18]Destrucción de la información	6	6	6		7

IMPACTO ACUMULADO

SISTEMAS DE SEGURIDAD FISICA

DISPOSITIVOS DE SOPORTE.

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_2.5] dispositivos de soporte					
❖ [S_2.5.1] aire acondicionado	9				9
[I.5]Avería de origen físico o lógico	9				9
[I.6]Corte de suministro eléctrico	9				9
❖ [S_2.5.2] generador de energía	9	9	9	9	9
[I.5.4]Equipamiento auxiliar	9				9
[I.7]Condiciones inadecuadas de temperatura o humedad	8				9
[E.1]Errores de los usuarios	9	9	9	8	9
❖ [S_2.5.3] ups	9				
[I.6]Corte de suministro eléctrico	9				
❖ [S_2.5.4] estabilizador	9				
[I.6]Corte de suministro eléctrico	9				
❖ [S_2.5.1] pozo a tierra	9				
[I.4]Contaminación electromagnética	9				
❖ [S_2.5.2] alarma incendios	9				
[I.5.4]Equipamiento auxiliar	8				
[I.6]Corte suministro eléctrico	8				
❖ [S_2.5.3] piso aislante	9				
[N.2] Daños por agua	8				

IMPACTO ACUMULADO

Sistemas de seguridad física

Control de acceso a equipos

ACTIVOS	[D]	[I]	[C]	[A]	[T]
[S_2.6] acceso a equipos					
❖ [S_2.1.1] dispositivos e/s de datos	9	9	9		8
[A.11]Acceso no autorizado	9	8	9		8
❖ [S_2.1.2] gabinetes	8	8			8
[A.11]Acceso no autorizado	8	8			8

➢ IMPACTO REPERCUTIDO

ACTIVOS	D	I	C	A	T
[S_1.1.1]id_altas	[4]				
[S_1.1.2]id_bajas	[7]				
[S_1.1.3]id_mantenimiento	[7]				
[S_1.1.4]id_permisos	[5]				
[S_1.1.5]id_cuentas	[7]				
[S_1.1.1]logeo	[4]				
[S_1.1.1]generación	[4]				
[S_1.1.2]cambios	[7]				
[S_2.1.1] servidores	[10]	[9]	[9]	[8]	[10]
[S_2.1.2] pc's	[10]	[9]	[9]	[8]	[10]
[S_2.1.1] diseño area de ventas	[9]				
[S_2.1.2] control acceso fisico centro computo	[9]	[6]	[7]		
[S_2.1.3] aire acondicionado	[8]	[8]			
[S_2.5.2] generador de energía	[8]	[8]			
[S_2.5.3] ups	[8]	[8]			
[S_2.5.4] estabilizador	[8]	[8]			
[S_2.5.1] pozo a tierra	[8]				
[S_2.5.2] alarma de contra incendio	[8]				
[S_2.5.3] piso aislante	[7]				
[S_2.1.1] dispositivos e/s de datos	[9]	[8]	[8]		
[S_2.1.2] gabinetes	[9]	[7]	[7]		

3.2.5. **Caracterización del Riesgo**

.

- **RIESGO ACUMULADO**

ACTIVO	AMENAZA	D	V	VA	D	I	F	RIESGO
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.6] Corte del suministro eléctrico	[T]		[10]	90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[I.6] Corte del suministro eléctrico	[T]	[10]	[10]	90%	[10]	1	{6.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.6] Corte del suministro eléctrico	[D]		[10]	90%	[10]	1	{6.7}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.6] Corte del suministro eléctrico	[T]		[10]	90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[I.6] Corte del suministro eléctrico	[D]	[10]	[10]	90%	[10]	1	{6.7}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.6] Corte del suministro eléctrico	[D]	[9]	[10]	90%	[10]	1	{6.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.6] Corte del suministro eléctrico	[T]		[10]	90%	[10]	1	{6.7}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.6] Corte del suministro eléctrico	[D]		[10]	90%	[10]	1	{6.7}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.6] Corte del suministro eléctrico	[T]		[10]	50%	[9]	0,5	{6.0}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.6] Corte del suministro eléctrico	[D]	[9]	[10]	50%	[9]	0,5	{6.0}
[S_2.5.S_2.5.4] ESTABILIZADORES	[I.6] Corte del suministro eléctrico	[D]	[9]	[10]	50%	[9]	0,5	{6.0}
[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.6] Corte del suministro eléctrico	[D]	[9]	[10]	50%	[9]	0,5	{6.0}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[T]		[10]	70%	[10]	0,125	{5.8}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	[10]	50%	[9]	0,25	{5.8}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.5] Avería de origen físico o lógico	[D]	[9]	[10]	50%	[9]	0,25	{5.8}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[C]	[9]	[10]	50%	[9]	0,25	{5.8}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[I]	[9]	[10]	50%	[9]	0,25	{5.8}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[D]	[10]	[10]	50%	[9]	0,25	{5.8}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.5] Avería de origen físico o lógico	[T]		[10]	50%	[9]	0,25	{5.8}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[T]		[10]	50%	[9]	0,25	{5.8}
[S_2.5.S_2.5.3] UPS	[I.6] Corte del suministro eléctrico	[D]	[9]	[10]	50%	[9]	0,25	{5.8}
[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.4] ID_PERMISOS	[E.2] Errores del administrador	[D]	[5]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	[7]	100%	[7]	5	{5.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.1] Fuego	[T]		[10]	25%	[8]	0,63	{5.6}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.1] Fuego	[T]		[10]	25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.1] SERVIDORES	[I.1] Fuego	[T]	[10]	[10]	25%	[8]	0,63	{5.6}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.1] Fuego	[T]		[10]	25%	[8]	0,63	{5.6}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.1] Fuego	[T]		[10]	25%	[8]	0,63	{5.6}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.1] Fuego	[T]		[10]	25%	[8]	0,63	{5.6}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.1] Fuego	[T]		[10]	25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.1] SERVIDORES	[N.1] Fuego	[T]	[10]	[10]	25%	[8]	0,63	{5.6}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[C]		[10]	50%	[9]	0,125	{5.5}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[T]		[10]	50%	[9]	0,125	{5.5}

[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	[10]	50%	[9]	0,125	{5.5}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	[10]	50%	[9]	0,125	{5.5}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[T]		[10]	50%	[9]	0,125	{5.5}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[D]	[10]	[10]	50%	[9]	0,125	{5.5}
[S_2.5.S_2.5.5] POZO A TIERRA	[I.4] Contaminación electromagnética	[D]	[9]	[10]	50%	[9]	0,125	{5.5}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[T]		[10]	25%	[8]	0,25	{5.2}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.*.11] Calor extremo	[T]		[10]	25%	[8]	0,25	{5.2}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.*.11] Calor extremo	[D]		[10]	25%	[8]	0,25	{5.2}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.*.11] Calor extremo	[D]	[9]	[10]	25%	[8]	0,25	{5.2}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.*.11] Calor extremo	[D]		[10]	25%	[8]	0,25	{5.2}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.*.11] Calor extremo	[T]		[10]	25%	[8]	0,25	{5.2}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.*.11] Calor extremo	[T]		[10]	25%	[8]	0,25	{5.2}
[S_2.5.S_2.5.7] PISO AISLANTE	[N.2] Daños por agua	[D]	[9]	[10]	25%	[8]	0,25	{5.2}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[10]	25%	[8]	0,125	{5.0}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.2] Daños por agua	[D]	[9]	[10]	25%	[8]	0,125	{5.0}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.2] Daños por agua	[D]		[10]	25%	[8]	0,125	{5.0}
[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[T]		[10]	25%	[8]	0,125	{5.0}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.2] Daños por agua	[T]		[10]	25%	[8]	0,125	{5.0}
[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[I]	[9]	[10]	25%	[8]	0,125	{5.0}
[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[D]	[10]	[10]	25%	[8]	0,125	{5.0}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.2] Daños por agua	[T]		[10]	25%	[8]	0,125	{5.0}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[T]		[10]	25%	[8]	0,125	{5.0}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.2] Daños por agua	[T]		[10]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[N.2] Daños por agua	[D]	[10]	[10]	25%	[8]	0,125	{5.0}
[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.5.4] Equipamiento auxiliar	[D]	[9]	[10]	25%	[8]	0,125	{5.0}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.2] Daños por agua	[D]		[10]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[N.2] Daños por agua	[T]	[10]	[10]	25%	[8]	0,125	{5.0}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[A]		[9]	50%	[8]	0,125	{4.9}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.1] Fuego	[D]		[10]	10%	[7]	0,63	{4.9}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.1] Fuego	[D]		[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[I.1] Fuego	[T]	[10]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[N.1] Fuego	[D]	[10]	[10]	10%	[7]	0,63	{4.9}

[S_2.1.S_2.1.2] PC'S	[N.1] Fuego	[T]	[10]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[I.1] Fuego	[D]	[10]	[10]	10%	[7]	0,63	{4.9}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.1] Fuego	[D]	[9]	[10]	10%	[7]	0,63	{4.9}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.1] Fuego	[D]		[10]	10%	[7]	0,63	{4.9}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.1] Fuego	[D]	[9]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[I.1] Fuego	[D]	[10]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[N.1] Fuego	[D]	[10]	[10]	10%	[7]	0,63	{4.9}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.1] Fuego	[D]		[10]	10%	[7]	0,63	{4.9}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[C]	[9]	[10]	20%	[8]	0,125	{4.8}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[C]	[9]	[10]	20%	[8]	0,125	{4.8}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[E.28.3] No hay personal	[T]		[10]	10%	[7]	0,25	{4.5}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[E.28.3] No hay personal	[T]		[10]	10%	[7]	0,25	{4.5}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[E.28.3] No hay personal	[D]	[9]	[10]	10%	[7]	0,25	{4.5}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[E.28.3] No hay personal	[D]		[10]	10%	[7]	0,25	{4.5}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[E.28.3] No hay personal	[D]		[10]	10%	[7]	0,25	{4.5}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[E.28.3] No hay personal	[T]		[10]	10%	[7]	0,25	{4.5}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[T]		[10]	10%	[7]	0,125	{4.3}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[I]	[9]	[10]	10%	[7]	0,125	{4.3}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[D]	[10]	[10]	10%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.18] Destrucción de la información	[D]	[7]	[7]	100%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.14.1] A personal interno que no necesita conocerlo	[D]	[7]	[7]	100%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.15] Alteración de la información	[D]	[7]	[7]	100%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.7.1] No existe procedimiento de atención	[D]	[7]	[7]	100%	[7]	0,125	{4.3}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[I]	[9]	[10]	10%	[7]	0,125	{4.3}
[S_1.2.S_1.2.1] LOGEO	[E.16] Introducción de falsa información	[D]	[5]	[7]	50%	[6]	0,5	{4.3}
[S_1.2.S_1.2.1] LOGEO	[A.5] Suplantación de la identidad del usuario	[D]	[5]	[7]	50%	[6]	0,25	{4.0}
[S_1.1.S_1.1.3] ID_MANTENIMIENTO	[E.3] Errores de monitorización (log)	[D]	[7]	[7]	50%	[6]	0,25	{4.0}
[S_1.1.S_1.1.2] ID_BAJAS	[E.2] Errores del administrador	[D]	[7]	[7]	50%	[6]	0,25	{4.0}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.25.3] Por personas externas	[T]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.25.3] Por personas externas	[T]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.26.1] Vandalismo	[D]		[10]	5%	[6]	0,125	{3.7}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[C]	[9]	[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.25.3] Por personas externas	[D]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.26.1] Vandalismo	[T]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.25.3] Por personas externas	[D]	[9]	[10]	5%	[6]	0,125	{3.7}

[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[D]	[10]	[10]	5%	[6]	0,125	{3.7}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[I]	[9]	[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.26.1] Vandalismo	[T]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.25.3] Por personas externas	[D]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.26.1] Vandalismo	[D]	[9]	[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.26.1] Vandalismo	[T]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.25.3] Por personas externas	[T]		[10]	5%	[6]	0,125	{3.7}
[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.26.1] Vandalismo	[D]		[10]	5%	[6]	0,125	{3.7}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.25] Robo de equipos	[D]	[10]	[10]	1%	[4]	0,63	{3.1}
[S_1.1.S_1.1.1] ID_ALTAS	[E.2] Errores del administrador	[D]	[4]	[4]	100%	[4]	0,25	{2.8}
[S_1.3.S_1.3.1] PASS_GENERACION	[E.7.1] No existe procedimiento de atención	[D]	[4]	[4]	100%	[4]	0,125	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[E.18] Destrucción de la información	[D]	[4]	[4]	100%	[4]	0,125	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[E.14.1] A personal interno que no necesita conocerlo	[D]	[4]	[4]	100%	[4]	0,125	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[E.15] Alteración de la información	[D]	[4]	[4]	50%	[3]	0,125	{2.0}

➢ RIESGO REPERCUTIDO

PADRE	HIJO	AMENAZA	D	V	D	I	F	R
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.6] Corte del suministro eléctrico	[T]		90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[I.6] Corte del suministro eléctrico	[T]	[10]	90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.6] Corte del suministro eléctrico	[D]		90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.6] Corte del suministro eléctrico	[D]		90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.6] Corte del suministro eléctrico	[D]	[9]	90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.6] Corte del suministro eléctrico	[T]		90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.6] Corte del suministro eléctrico	[T]		90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[I.6] Corte del suministro eléctrico	[D]	[10]	90%	[10]	1	{6.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.6] Corte del suministro eléctrico	[D]		90%	[10]	1	{6.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.6] Corte del suministro eléctrico	[T]		90%	[10]	1	{6.7}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.6] Corte del suministro eléctrico	[D]	[9]	90%	[9]	1	{6.2}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,5	{6.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.4] ESTABILIZADORES	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,5	{6.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,5	{6.0}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.4] ESTABILIZADORES	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,5	{6.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.6] Corte del suministro eléctrico	[T]		50%	[9]	0,5	{6.0}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,5	{6.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[T]		70%	[10]	0,125	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[T]		70%	[10]	0,125	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[C]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[T]		50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.5] Avería de origen físico o lógico	[T]		50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[I]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.3] UPS	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,25	{5.8}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[I]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.5] Avería de origen físico o lógico	[D]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[T]		50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[C]	[9]	50%	[9]	0,25	{5.8}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.3] UPS	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[9]	0,25	{5.8}

[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.3] ID_MANTENIMIENTO	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.3] ID_MANTENIMIENTO	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[7]	5	{5.7}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.5] ID_CUENTAS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.2] ID_BAJAS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.5] ID_CUENTAS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[7]	5	{5.7}
[S_1.1.S_1.1.2] ID_BAJAS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[7]	5	{5.7}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.1.S_1.1.4] ID_PERMISOS	[E.2] Errores del administrador	[D]	[5]	100%	[7]	5	{5.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.1.S_2.1.1] SERVIDORES	[I.1] Fuego	[T]	[10]	25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.1.S_2.1.1] SERVIDORES	[N.1] Fuego	[T]	[10]	25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.1] Fuego	[T]		25%	[8]	0,63	{5.6}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[T]		50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[C]		50%	[9]	0,125	{5.5}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[T]		50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.5] POZO A TIERRA	[I.4] Contaminación electromagnética	[D]	[9]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[T]		50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[C]		50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[T]		50%	[9]	0,125	{5.5}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,125	{5.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[D]	[10]	50%	[9]	0,125	{5.5}
[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[8]	0,5	{5.4}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[8]	0,5	{5.4}

[S_2.5.S_2.5.4] ESTABILIZADORES	[S_2.5.S_2.5.4] ESTABILIZADORES	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[8]	0,5	{5.4}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[T]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.*.11] Calor extremo	[T]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.*.11] Calor extremo	[D]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.7] PISO AISLANTE	[N.2] Daños por agua	[D]	[9]	25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.*.11] Calor extremo	[T]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.*.11] Calor extremo	[T]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.*.11] Calor extremo	[D]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.*.11] Calor extremo	[T]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[T]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.*.11] Calor extremo	[D]	[9]	25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.*.11] Calor extremo	[D]		25%	[8]	0,25	{5.2}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.7] PISO AISLANTE	[N.2] Daños por agua	[D]	[9]	25%	[8]	0,25	{5.2}
[S_2.5.S_2.5.3] UPS	[S_2.5.S_2.5.3] UPS	[I.6] Corte del suministro eléctrico	[D]	[9]	50%	[8]	0,25	{5.2}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	50%	[8]	0,25	{5.2}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[C]	[9]	50%	[8]	0,25	{5.2}
[S_2.5.S_2.5.4] ESTABILIZADORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	50%	[8]	0,25	{5.2}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	50%	[8]	0,25	{5.2}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[S_2.5.S_2.5.1] AIRE ACONDICONADO	[I.5] Avería de origen físico o lógico	[D]	[9]	50%	[8]	0,25	{5.2}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[A.11] Acceso no autorizado	[I]	[9]	50%	[8]	0,25	{5.2}
[S_2.5.S_2.5.3] UPS	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.5.4] Equipamiento auxiliar	[D]	[9]	50%	[8]	0,25	{5.2}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.2] Daños por agua	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.2] Daños por agua	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.5.4] Equipamiento auxiliar	[D]	[9]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.2] Daños por agua	[D]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[N.2] Daños por agua	[T]	[10]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.2] Daños por agua	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[I]	[9]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[D]	[10]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.2] Daños por agua	[D]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.2] Daños por agua	[D]	[9]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	25%	[8]	0,125	{5.0}
[S_2.6.S_2.6.2] GABINETES	[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[D]	[10]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.2] Daños por agua	[T]		25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.2] Daños por agua	[D]		25%	[8]	0,125	{5.0}

[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[N.2] Daños por agua	[D]	[10]	25%	[8]	0,125	{5.0}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.5.4] Equipamiento auxiliar	[D]	[9]	25%	[8]	0,125	{5.0}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	50%	[8]	0,125	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[A]		50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.5] POZO A TIERRA	[S_2.5.S_2.5.5] POZO A TIERRA	[I.4] Contaminación electromagnética	[D]	[9]	50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.4] ESTABILIZADORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.4] ESTABILIZADORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	50%	[8]	0,125	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[A]		50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.3] UPS	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[I]	[9]	50%	[8]	0,125	{4.9}
[S_2.5.S_2.5.3] UPS	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[E.1] Errores de los usuarios	[D]	[9]	50%	[8]	0,125	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[N.1] Fuego	[D]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[N.1] Fuego	[D]		10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.1] Fuego	[D]		10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.1] Fuego	[D]	[9]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.1] Fuego	[D]	[9]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[I.1] Fuego	[D]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.1] Fuego	[D]		10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[I.1] Fuego	[D]		10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[I.1] Fuego	[T]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.1.S_2.1.1] SERVIDORES	[I.1] Fuego	[D]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[I.1] Fuego	[D]		10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.1.S_2.1.2] PC'S	[N.1] Fuego	[T]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.1.S_2.1.1] SERVIDORES	[N.1] Fuego	[D]	[10]	10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[N.1] Fuego	[D]		10%	[7]	0,63	{4.9}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[C]	[9]	20%	[8]	0,125	{4.8}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[C]	[9]	20%	[8]	0,125	{4.8}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[C]	[9]	20%	[8]	0,125	{4.8}

[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[C]	[9]	20%	[8]	0,125	{4.8}
[S_2.5.S_2.5.7] PISO AISLANTE	[S_2.5.S_2.5.7] PISO AISLANTE	[N.2] Daños por agua	[D]	[9]	25%	[7]	0,25	{4.6}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.*.11] Calor extremo	[D]	[9]	25%	[7]	0,25	{4.6}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[E.28.3] No hay personal	[T]		10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[E.28.3] No hay personal	[D]		10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[E.28.3] No hay personal	[T]		10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[E.28.3] No hay personal	[T]		10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[E.28.3] No hay personal	[D]	[9]	10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[E.28.3] No hay personal	[T]		10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[E.28.3] No hay personal	[D]		10%	[7]	0,25	{4.5}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[E.28.3] No hay personal	[D]		10%	[7]	0,25	{4.5}
[S_1.1.S_1.1.4] ID_PERMISOS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[5]	5	{4.5}
[S_1.1.S_1.1.4] ID_PERMISOS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[5]	5	{4.5}
[S_1.1.S_1.1.4] ID_PERMISOS	[S_1.1.S_1.1.4] ID_PERMISOS	[E.2] Errores del administrador	[D]	[5]	100%	[5]	5	{4.5}
[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	25%	[7]	0,125	{4.4}
[S_2.5.S_2.5.4] ESTABILIZADORES	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	25%	[7]	0,125	{4.4}
[S_2.5.S_2.5.1] AIRE ACONDICONADO	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	25%	[7]	0,125	{4.4}
[S_2.6.S_2.6.2] GABINETES	[S_2.6.S_2.6.2] GABINETES	[A.11] Acceso no autorizado	[I]	[9]	25%	[7]	0,125	{4.4}
[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[S_2.5.S_2.5.6] ALARMA CONTRA INCENDIOS	[I.5.4] Equipamiento auxiliar	[D]	[9]	25%	[7]	0,125	{4.4}
[S_2.5.S_2.5.3] UPS	[S_2.5.S_2.5.2] GENERADORES DE ENERGIA	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	25%	[7]	0,125	{4.4}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.2] Daños por agua	[D]	[9]	25%	[7]	0,125	{4.4}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[D]	[10]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[T]		10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[I]	[9]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[D]	[10]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[I]	[9]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[D]	[10]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[I]	[9]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[T]		10%	[7]	0,125	{4.3}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[D]	[10]	10%	[7]	0,125	{4.3}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[D]	[10]	10%	[7]	0,125	{4.3}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[I]	[9]	10%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.15] Alteración de la información	[D]	[7]	100%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.18] Destrucción de la información	[D]	[7]	100%	[7]	0,125	{4.3}

[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.3.S_1.3.2] PASS_CAMBIOS	[E.14.1] A personal interno que no necesita conocerlo	[D]	[7]	100%	[7]	0,125	{4.3}
[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.2.S_1.2.1] LOGEO	[E.16] Introducción de falsa información	[D]	[5]	50%	[6]	0,5	{4.3}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[N.1] Fuego	[D]	[9]	10%	[6]	0,63	{4.3}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[I.1] Fuego	[D]	[9]	10%	[6]	0,63	{4.3}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[C]	[9]	20%	[7]	0,125	{4.2}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[C]	[9]	20%	[7]	0,125	{4.2}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[C]	[9]	20%	[7]	0,125	{4.2}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[C]	[9]	20%	[7]	0,125	{4.2}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[C]	[9]	20%	[7]	0,125	{4.2}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[C]	[9]	20%	[7]	0,125	{4.2}

[S_1.3.S_1.3.2] PASS_CAMBIOS	[S_1.2.S_1.2.1] LOGEO	[A.5] Suplantación de la identidad del usuario	[D]	[5]	50%	[6]	0,25	{4.0}
[S_1.1.S_1.1.2] ID_BAJAS	[S_1.1.S_1.1.2] ID_BAJAS	[E.2] Errores del administrador	[D]	[7]	50%	[6]	0,25	{4.0}
[S_1.1.S_1.1.3] ID_MANTENIMIENTO	[S_1.1.S_1.1.3] ID_MANTENIMIENTO	[E.3] Errores de monitorización (log)	[D]	[7]	50%	[6]	0,25	{4.0}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[E.28.3] No hay personal	[D]	[9]	10%	[6]	0,25	{3.9}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[4]	5	{3.9}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[4]	5	{3.9}
[S_1.1.S_1.1.1] ID_ALTAS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.2] Errores del administrador	[D]	[7]	100%	[4]	5	{3.9}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.1.S_1.1.4] ID_PERMISOS	[E.2] Errores del administrador	[D]	[5]	100%	[4]	5	{3.9}
[S_1.1.S_1.1.1] ID_ALTAS	[S_1.1.S_1.1.5] ID_CUENTAS	[E.7.1] No existe procedimiento de atención	[D]	[7]	100%	[4]	5	{3.9}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.25.3] Por personas externas	[T]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.26.1] Vandalismo	[D]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.25.3] Por personas externas	[T]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[D]	[10]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[I]	[9]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[C]	[9]	5%	[6]	0,125	{3.7}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[D]	[10]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.25.3] Por personas externas	[D]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.26.1] Vandalismo	[D]	[9]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.25.3] Por personas externas	[T]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.26.1] Vandalismo	[D]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.26.1] Vandalismo	[T]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[C]	[9]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.25.3] Por personas externas	[D]	[9]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[I]	[9]	5%	[6]	0,125	{3.7}

[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[D]	[10]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.25.3] Por personas externas	[D]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.1] DISEÑO AREAS ADMINISTRATIVAS	[A.26.1] Vandalismo	[T]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.26.1] Vandalismo	[T]		5%	[6]	0,125	{3.7}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[D]	[10]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.26.1] Vandalismo	[D]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.26.1] Vandalismo	[T]		5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.2] PC'S	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.25.3] Por personas externas	[T]		5%	[6]	0,125	{3.7}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[D]	[10]	5%	[6]	0,125	{3.7}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.2.S_2.2.2] DISEÑO CENTRO COMPUTO	[A.25.3] Por personas externas	[D]		5%	[6]	0,125	{3.7}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[I]	[9]	10%	[6]	0,125	{3.7}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[I]	[9]	10%	[6]	0,125	{3.7}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[I]	[9]	10%	[6]	0,125	{3.7}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[I]	[9]	10%	[6]	0,125	{3.7}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.11] Acceso no autorizado	[I]	[9]	10%	[6]	0,125	{3.7}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.15] Modificación de información	[I]	[9]	10%	[6]	0,125	{3.7}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[C]	[9]	5%	[5]	0,125	{3.1}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[I]	[9]	5%	[5]	0,125	{3.1}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.26.1] Vandalismo	[D]	[9]	5%	[5]	0,125	{3.1}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[C]	[9]	5%	[5]	0,125	{3.1}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[C]	[9]	5%	[5]	0,125	{3.1}
[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[S_2.2.S_2.2.3] DISEÑO AREA DE VENTAS	[A.25.3] Por personas externas	[D]	[9]	5%	[5]	0,125	{3.1}

[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[I]	[9]	5%	[5]	0,125	{3.1}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.18] Destrucción de la información	[I]	[9]	5%	[5]	0,125	{3.1}
[S_1.1.S_1.1.4] ID_PERMISOS	[S_1.2.S_1.2.1] LOGEO	[E.16] Introducción de falsa información	[D]	[5]	50%	[4]	0,5	{3.1}
[S_1.2.S_1.2.1] LOGEO	[S_1.2.S_1.2.1] LOGEO	[E.16] Introducción de falsa información	[D]	[5]	50%	[4]	0,5	{3.1}
[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.25] Robo de equipos	[D]	[10]	1%	[4]	0,63	{3.1}
[S_2.6.S_2.6.1] DISPOSITIVOS ENTRADA SALIDA DATOS	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.25] Robo de equipos	[D]	[10]	1%	[4]	0,63	{3.1}
[S_2.1.S_2.1.2] PC'S	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.25] Robo de equipos	[D]	[10]	1%	[4]	0,63	{3.1}
[S_2.1.S_2.1.1] SERVIDORES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.25] Robo de equipos	[D]	[10]	1%	[4]	0,63	{3.1}
[S_2.6.S_2.6.2] GABINETES	[S_2.4.S_2.4.1] CONTROL ACCESO FISICO CENTRO COMPUTO	[A.25] Robo de equipos	[D]	[10]	1%	[4]	0,63	{3.1}
[S_1.1.S_1.1.4] ID_PERMISOS	[S_1.2.S_1.2.1] LOGEO	[A.5] Suplantación de la identidad del usuario	[D]	[5]	50%	[4]	0,25	{2.8}
[S_1.2.S_1.2.1] LOGEO	[S_1.2.S_1.2.1] LOGEO	[A.5] Suplantación de la identidad del usuario	[D]	[5]	50%	[4]	0,25	{2.8}

[S_1.1.S_1.1.1] ID_ALTAS	[S_1.1.S_1.1.1] ID_ALTAS	[E.2] Errores del administrador	[D]	[4]	100%	[4]	0,25	{2.8}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.3.S_1.3.1] PASS_GENERACION	[E.14.1] A personal interno que no necesita conocerlo	[D]	[4]	100%	[4]	0,125	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.3.S_1.3.1] PASS_GENERACION	[E.7.1] No existe procedimiento de atención	[D]	[4]	100%	[4]	0,125	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.3.S_1.3.1] PASS_GENERACION	[E.18] Destrucción de la información	[D]	[4]	100%	[4]	0,125	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.2.S_1.2.1] LOGEO	[E.16] Introducción de falsa información	[D]	[5]	50%	[3]	0,5	{2.5}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.2.S_1.2.1] LOGEO	[A.5] Suplantación de la identidad del usuario	[D]	[5]	50%	[3]	0,25	{2.2}
[S_1.3.S_1.3.1] PASS_GENERACION	[S_1.3.S_1.3.1] PASS_GENERACION	[E.15] Alteración de la información	[D]	[4]	50%	[3]	0,125	{2.0}

3.3. **Gestión de Riesgo**

3.3.1. Plan de Contingencia.

El Plan de Contingencias considera un análisis detallado de los posibles riesgos y amenazas a los cuales pueden estar expuestos nuestra organización y afines y toda la información contenida en los diversos medios de almacenamiento; estos nos permitirán determinar cómo reducir impacto ante la posibilidad de ocurrencia; así mismo se consideran cada de uno de los procedimientos de recuperación y restablecimiento a seguir en caso que se presentara el problema.

A - SEGURIDAD LÓGICA

1. IDENTIFICACIÓN – ID'S

- Deberá existir una herramienta para la administración y el control de acceso a los datos. Debe existir una **política formal de control de acceso** a datos donde se detalle como mínimo:
  - el nivel de confidencialidad de los datos y su sensibilidad,
  - los procedimientos de otorgamiento de claves de usuarios para el ingreso al sistema de ventas y contable

- Para **registrar un usuario** al sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos:
  - identificación del usuario, deberá ser única e irrepetible,
  - password, debe ser personal e ingresado por el usuario.
  - nombre y apellido completo.
  - sector donde se desempeña.
  - fecha de anulación de la cuenta
  - contador de intentos fallidos.

- Deben asignarse los **permisos mínimos** y necesarios para que cada usuario desempeñe su función.

- Deberá restringirse el acceso al sistema o la utilización de recursos en un **rango horario definido**, teniendo en cuenta que:
  - las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan,
  - durante las vacaciones o licencias las cuentas de usuarios deben desactivarse,
  - en días feriados las cuentas de usuarios administrativos, a excepción de los del departamento de ventas, deben permanecer desactivadas.
- Deben restringirse las conexiones de los usuarios sólo a los puntos de venta **autorizadas**.

- El **administrador del sistema comercial debe poder logearse** solamente desde el terminal que se encuentre encargado de administrarlo.

- El administrador del sistema comercial deberá realizar un **chequeo mensual de los usuarios** del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos.

- El área de recursos humanos deberá comunicar al administrador los **cambios de personal** que se produzcan.

- Para **dar de baja un usuario** deberá existir un procedimiento formal por escrito, a través del cual los datos del usuario no se eliminarán sino que se actualizará la fecha de anulación de su cuenta, quedando estos datos registrados en el histórico.

- Además, se debe llevar a cabo una **política de desvinculación del personal**, evitando un posible acto de vandalismo por insatisfacción.

- El sistema deberá **finalizar toda sesión interactiva** cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de cinco minutos, deberá deslogear al usuario y limpiar la pantalla.

- Las PC´s deben tener instalado un **protector de pantalla con contraseña**.

- Los usuarios del sistema solamente podrán abrir **una sesión de cada aplicación**, y no podrán abrir varias sesiones de la misma aplicacion en diferentes terminales ni en la misma terminal.

- Se deberá impedir la existencia de **perfiles de usuarios genéricos**, en todos los sistemas operativos y en el sistema comercial de la Empresa.

- Se deberá minimizar la generación y el uso de perfiles de **usuario con máximos privilegios**. Todos los usos de estas clases de perfiles deberán ser registrados y revisados por el administrador del sistema comercial.

- Los administradores que realizan tareas de mantenimiento, deberán tener otro perfil, con un nivel de acceso menor, denominado **mantenimiento**, para ser utilizado en tareas cotidianas que no requieran privilegios de administrador.

- Si se realiza **mantenimiento externo**, deberá crearse una cuenta de usuario especial para esta tarea, con los permisos mínimos necesarios para desempeñar las funciones; una vez finalizado el mantenimiento el administrador del sistema deberá modificar la contraseña de esta cuenta. Cada vez que sea necesario realizar mantenimiento, el administrador deberá proporcionar esta clave al personal externo.

- Periódicamente el administrador del sistema deberá **chequear** las acciones desempeñadas con las cuentas de administradores y de mantenimiento.

2. AUTENTICACIÓN

- La **pantalla de logeo** del sistema deberá mostrar los siguientes datos:
  - nombre de usuario,
  - password,

- Mientras el usuario está **ingresando su contraseña**, esta no debe ser mostrada por pantalla.

- Cuando el **usuario logra logearse** al sistema deberán mostrase los siguientes datos:
  - nombre de usuario,
  - fecha y hora de la última conexión,
  - localización de la última conexión (Ej. número de terminal),

- La **aplicación para administrar los datos de usuarios** solo deberá ejecutarse en máquinas designadas del centro de cómputos.

- Deberán **encriptarse**:
  - la lista de control de accesos,
  - los passwords y datos de las cuentas de usuarios,

3. PASSWORD

- Los passwords deberán tener las siguientes **características**:
  - conjunto de caracteres alfa-numérico,
  - longitud mínima de 6 y máxima de 10 caracteres.

- La **fecha de expiración** del password deberá ser de cuatro meses. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.

- El password **no deberá contener** el nombre de la empresa, el nombre del usuario, ni palabras reservadas.

- Bloquear el perfil de todo usuario que haya intentado **acceder al sistema en forma fallida** por más de **cinco** veces consecutivas.

- El usuario debe poder **modificar su password** cuantas veces considere necesario, sin seguir ningún procedimiento formal de aviso.

- Controlar que el password ingresado sea **diferente a los últimas cinco utilizados**.

- El password deberá tener un **período de duración mínimo** de 30 días. El sistema no permitirá el cambio de password si este período no se ha cumplido.

- Si un usuario **olvida el password**, la aplicación no deberá mostrarle el Password .el administrador de sistema, es la única persona con atribuciones para poder generar un password nuevo al usuario y esta a su vez le permitirá que al próximo inicio de sesión sea cambiado desde su terminal, la próxima vez que intente logearse.

B. SEGURIDAD FÍ SICA

1. EQUIPAMIENTO

|

- Deberá existir una adecuada protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos de la empresa.

2. CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTOS

|

- Se deberá restringir el acceso físico a las **áreas críticas** a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.

|

- Se deberá asegurar que todos los **individuos** que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.

|

- Cualquier **persona ajena a la empresa** que necesite ingresar al centro de cómputos deberá anunciarse en la puerta de entrada, personal de sistemas designado deberá escoltarlo desde la puerta hacia el interior del edificio, acompañándolo durante el transcurso de su tarea, hasta que éste concluya.

|

- El **área del centro de cómputos** donde se encuentran los servidores, el switch central y demás equipamiento crítico solo debe tener permitido el acceso a las personas encargadas.

|

3 CONTROL DE ACCESO A EQUIPOS

- Las **disqueteras y lectoras de CD** deberán deshabilitarse en aquellas máquinas en que no se necesiten.
- Los servidores deberán tener una **llave de bloqueo** de hardware.
- Cualquier **dispositivo externo** que no se encuentre en uso, deberá permanecer guardado bajo llave dentro del centro de cómputos.
- Los **gabinetes** donde se ubican los switches de cada una de los sectores, deberán permanecer guardados bajo llave, y fuera del alcance de personal no autorizado.
- El administrador o algún encargado de cómputos designado deberá realizar **chequeos periódicos** para comprobar:
  - la correcta instalación de los dispositivos de los equipos.
  - su buen funcionamiento.
  - sus números de series corresponden con los datos registrados por el administrador al momento de la instalación.
- Los **servidores deberán apagarse** automáticamente una vez que han cerrado todas las sucursales de la empresa.

4 DISPOSITIVOS DE SOPORTE

- Deberán existir los siguientes **dispositivos de soporte** en la empresa:
  - **Aire acondicionado**: en el centro de cómputos la temperatura debe mantenerse entre 19º C y 20º C.
  - **Extintores**: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación,
    - deberán estar instalados en lugares estratégicos de la empresa,
    - el centro de cómputos deberá contar con uno propio ubicado en la habitación de los servidores.
  - **Alarmas contra intrusos**: deberán contar con una alarma que se active en horarios no comerciales. Ésta deberá poder activarse manualmente en horarios laborales ante una emergencia.
  - **Estabilizador de tensión**: deberá existir al menos un estabilizador de tensión que atienda la línea de energía eléctrica independiente del centro de cómputos.
  - **Descarga a tierra**: deberán existir métodos de descarga a tierra para el edificio y otra independiente para el centro de cómputos.
- Todos estos dispositivos deberán ser **evaluados periódicamente** por personal de mantenimiento.
- Deberá existir una **llave de corte de energía general** en la salida de emergencias del edificio.
- Deberán existir procedimientos detallados a seguir por el personal en **caso de emergencias**, indicando responsables, quiénes deben estar adecuadamente capacitados.

5 ESTRUCTURA DEL EDIFICIO

- El centro de cómputos deberá ubicarse en un **piso superior** del edificio. Debe tener protecciones contra ruidos e interferencias electromagnéticas y visuales.
- Todas las **salidas hacia el exterior** del centro de cómputos deberán estar protegidas con rejas y métodos que impidan la visión.
- En el diseño del centro de cómputos deberá tenerse en cuenta el **futuro crecimiento** de la empresa, permitiendo la expansión del mismo y predisponiéndolo a reinstalaciones, conservando siempre recursos redundantes.
- Los **sectores administrativos y contables** de la empresa deberán estar divididos entre sí, con un medio que restrinja la visión.

6 CABLEADO ESTRUCTURADO

- El cableado debe seguir las normas del **cableado estructurado**, que garantizan el funcionamiento eficiente de la red.
- Si el tendido del cableado se **tercериza**, la empresa encargada debe prestar garantías escritas sobre su trabajo.
- Se deberá **documentar** en planos los canales de tendidos de cables y las bocas de red existentes.
- Debe existir tendido de **cableado redundante** para futuros puestos de trabajo. Estos cables no deben tener bocas de red instaladas.
- Deberá medirse periódicamente el **nivel de interferencia** que existe en la red. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.
- Deberá medirse periódicamente **nivel de ancho de banda** de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.

- Ante un **corte del suministro de energía** eléctrica deberán apagarse los equipos del centro de cómputos de forma segura, como medida de prevención.

SERVICIOS INTERNOS

SERVICIOS
1. OUTSOURCIN G
2. REFRIGERACION
3. ELECTRICO
4. VIGILANCIA
5. LIMPIEZA
6. VENTAS
7. ADMINISTRATIVOS

EQUIPAMIENTO

- **APLICACIONES**

CARACTERISTICAS DE LOS SISTEMAS DE INFORMACION

SISTEMAS	LENGUAJE	BASE DE DATOS	USUARIOS	NIVEL DE IMPORTANCIA	RESTORE
Sistema Comercial SOFTCOM	Visual Basic 6.0	SQL SERVER 2000	⌡ Ventas ⌡ Administración ⌡ Contabilidad	ALTO	Manual 01
Sistema Contable CONCAR	Visual Basic 6.0	SQL SERVER 2000	⌡ Administración ⌡ Contabilidad	ALTO	Manual 02
Sistema de RR.HH	Visual Basic .NET 2008	SQL SERVER 2005	⌡ Administración ⌡ RR.HH	ALTO	Manual 03
Sistema de Control Biométrico	Visual Basic .NET 2008	SQL SERVER 2000	⌡ RR.HH	ALTO	Manual 04

- **EQUIPOS**

UBICACIÓN DE LOS EQUIPOS DE CÓMPUTO

ÁREA	TIPO DE EQUIPO					
	PC	SERVIDORES	LAPTOP	IMPRESORA	SCANNER	OTROS
Administración	5		3	1	1	1
Contabilidad	15			5		
Sistemas	1	4		1		
Tienda	35			6		
Ferretería	15			1		
Almacenes	6					

- **COMUNICACIONES**

ÁREA	TIPO DE EQUIPO			
	Switch	Acces point	router	
Administración	1	1		
Contabilidad	1			
Sistemas	2	1	1	
Tienda	8			
Ferretería	1			
Almacenes				

➢ ELEMENTOS AUXILIARES

INFORMACION DE RESPALDO DE APLICACIONES

BACKUP APLICACIONES	MEDIO DE ALMACENAMIENTO	PERÍODO	UBICACIÓN	NIVEL DE IMPORTANCIA	RESTORE
Sistema Comercial SOFTCOM	Disco Duro Externo	Mensual	Informática	ALTO	Manual 01
Sistema Contable CONCAR	Disco Duro Externo	Mensual	Informática	ALTO	Manual 02
Sistema de RR.HH	Disco Duro Externo	Mensual	Informática	ALTO	Manual 03

INFORMACION DE RESPALDO DE BASES DE DATOS

BACKUP BASE DE DATOS	MEDIO DE ALMACENAMIENTO	PERÍODO	UBICACIÓN	NIVEL DE IMPORTANCIA	RESTORE
SOFTCOM	Disco Duro Externo	Diario	Informática	ALTO	Cartilla Operativa 01
CONCAR	Disco Duro Externo	Diario	Informática	ALTO	Cartilla Operativa 02
RR.HH	Disco Duro Externo	Diario	Informática	ALTO	Cartilla Operativa 03

MANUALES Y CARTILLAS OPERATIVAS

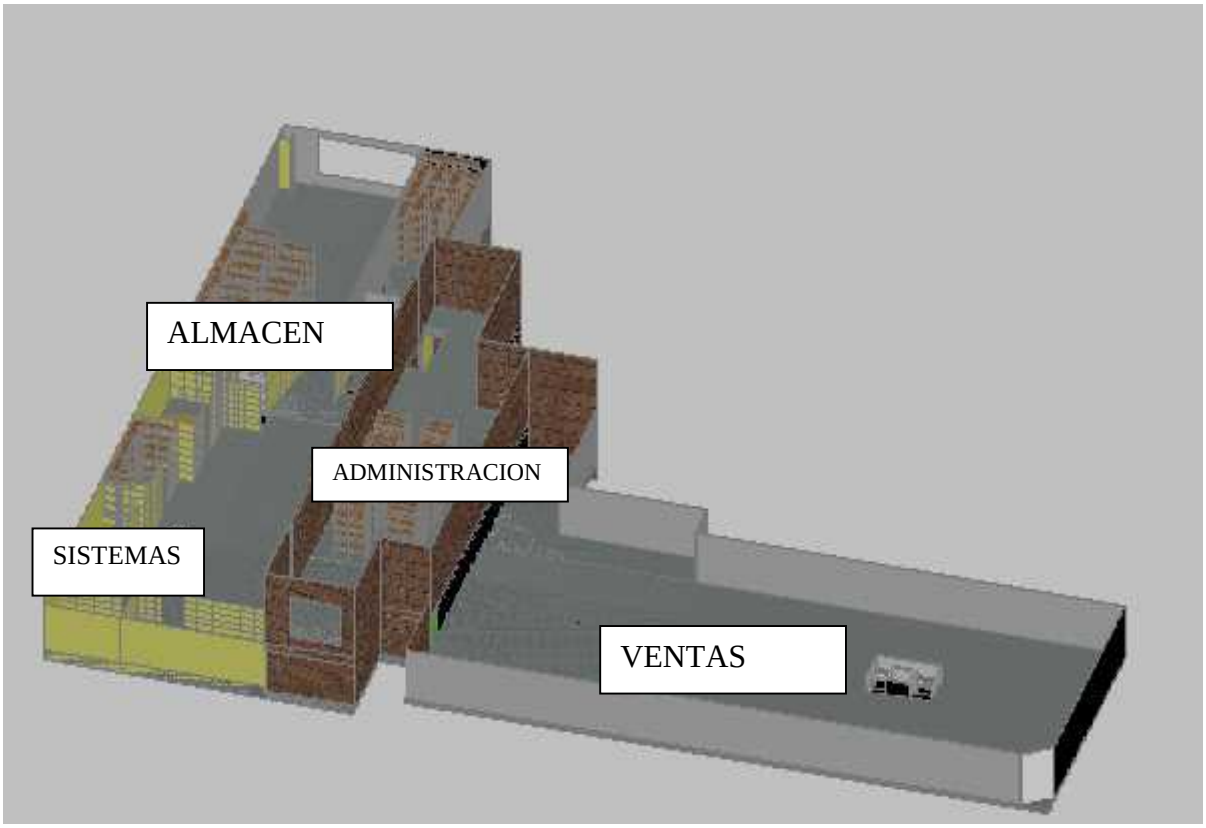
DOCUMENTO	NOMBRE	UBICACIÓN	NIVEL DE IMPORTANCIA
Manual 01	Instalación y Gestión del Sistema Comercial SOFTCOM	Informática	ALTO
Manual 02	Instalación y Gestión del Sistema Contable CONCAR	Informática	ALTO
Manual 03	Instalación y Gestión del Sistema de RR.HH – SAFNET	Informática	ALTO
Manual 04	Instalación y Gestión del Sistema de Control Biométrico	Informática	ALTO
Cartilla Operativa 01	Gestión de Base de Datos SOFTCOM	Informática	ALTO
Cartilla Operativa 02	Gestión de Base de Datos CONCAR	Informática	ALTO
Cartilla Operativa 03	Gestión de Base de Datos SAFTNET	Informática	ALTO

- **PERSONAL**

AREAS	PERSONAL
Administración	10
Contabilidad	12
Sistemas	3
Tienda	40
Ferretería	10

- **INSTALACIÓNES**

AREAS
8. Administración
9. Contabilidad
10. Sistemas
11. Tienda
12. Ferretería



Resultados y Discusiones

- **I** **S**e identificó los siguientes activos con mayor índice de riesgo potencial el cual es un factor determinante para la priorización en seguridad inmediata

Activos

1 ID_BAJAS
2 ID_MANTENIMIENTO
3 ID_CUENTAS
4 PASS_CAMBIOS

- **II** Se Determinó las siguiente amenazas que están expuestas dichos activos encontrados.

Amenazas

1. Errores de Administrador
2. Errores de monitorización
3. No existe procedimiento de atención
4. personal interno que no necesita conocerlo
5. Alteración de la información
6. Destrucción de la información

III **Las Salvaguardas** seleccionadas para este trabajo se encuentran seleccionadas en el desarrollo del presente informe en el tema **Caracterización de las salvaguardas pag.51**.

- **IV** Se propone 3 perfiles para el personal del CENTRO COMERCIAL DISTRIBUCIONES QUISPE SAC las cuales son: JEFE DE SISTEMAS, SUPERVISOR DE SOPORTE, SUPERVISOR DE HELPDESK

Conclusiones

La implementación de una política de seguridad informática en DISTRIBUCIONES QUISPE SAC. Implica un gran desafío:

1. La seguridad informatica no es un proceso absoluto por tal motivo se debe realizar anualmente un analisis de riesgo de las nuevas tecnologias a ser adquiridas.

2. El analisis de riesgo es fundamental para los procesos de evolucion, certificacion,auditoria en la empresa DISTRIBUCIONES QUISPE SAC.

3. La elaboración de este PSI debe servir como base para mejorar los procedimientos preventivos y correctivos.

4. El plan de contingencia establecida en el presente trabajo debe servir de base para mejorar los procedimientos preventivos y correctivos en futuras contingencias.

Ponemos de manifiesto que los resultados obtenidos fueron muy satisfactorios. Una vez concluido el desarrollo del presente trabajo, la empresa se mostró muy conforme con las recomendaciones sugeridas, y reveló su intención de poner en práctica el plan de seguridad generado.
La comunicación con los usuarios del sistema es la clave para hacer que esta política sea efectiva y se genere una “cultura de la seguridad”.

Por último, espero con este trabajo generar en los egresados de la escuela profesional de Sistemas e Informática una inquietud que incite a futuras investigaciones o proyectos que profundicen en el campo de la seguridad informática

Recomendaciones

1. Crear las políticas de seguridad que apoyen a los procedimientos descritos en el plan de contingencia

2. Adoptar MAGERIT como metodología que permita establecer fases que ayudara la implementación de seguridad de información

3. Capacitar de forma constante al personal que asumirá los roles de seguridad de información

4. Concientización al personal de la empresa de las diversas amenazas en seguridad lógica, física y demás activos de seguridad de información.

5. Debe de contarse con el personal indicado para asumir los roles sugeridos en el presente trabajo

GLOSARIO DE TÉRMINOS

AUDITORÍA: llevar a cabo una inspección y examen independiente de los registros del Sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y Procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

AMENAZA: cualquier cosa que pueda interferir con el funcionamiento adecuado de una Computadora personal o equipo informático, o causar la difusión no autorizada de Información confiada a una computadora. Ejemplo: fallas de suministro eléctrico, virus, Saboteadores o usuarios descuidados.

CRIPTOGRAFÍA: (encriptación) es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.

INCIDENTE: cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

PSI: Plan de seguridad de información

RIESGO: Medida del daño probable sobre un sistema.

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, puedan ser Modificados, destruidos o simplemente divulgados

SALVAGUARDA: Procedimiento o mecanismo tecnológico que reduce el riesgo.

BIBLIOGRAFIA

- [MAGERIT-I-METODO:2006]
  Ministerio de administraciones públicas
  Madrid, 20 de junio de 2006, ¨MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, I - Métodos ¨ versión 2.0
  Http://publicaciones.administracion.es, 154paginas.

- [MAGERIT-II-CATALOGO DE ELEMENTOS:2006]
  Ministerio de administraciones públicas
  Madrid, 20 de junio de 2006, ¨MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, II - Catalogo de elementos ¨ versión 2.0
  Http://publicaciones.administracion.es 87paginas.

- [MAGERIT-III-GUIA DE TECNICAS:2006]
  Ministerio de administraciones públicas
  Madrid, 20 de junio de 2006, ¨MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, III – Guía de técnicas ¨ versión 2.0
  Http://publicaciones.administracion.es, 72paginas.

- [ANALISIS DE RIESGO Y PLAN DE CONTINGENCIA PARA EL CENTRO DE COMUNICACIONES DE LA UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA:2007]
  UNAP
  Nauta, 2007, Informe técnico del examen de suficiencia previa actualización académica para optar el título de ingeniero de sistemas e informática - Bach. Elva Silvana rojas shapiama