



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES CARRERA DE TECNOLOGÍA SUPERIOR EN REDES Y TELECOMUNICACIONES

Trabajo de integración curricular, previo a la obtención del título de
Tecnólogo Superior en Redes y Telecomunicaciones

**Elaboración de un plan de contingencia para los sistemas
informáticos de las juntas administradoras de agua potable de la
parroquia de Pastocalle caso de estudio junta administradora de
agua “Miño San Antonio”**

AUTOR: Pilatuña Ramos Edgar Jefferson

DIRECTOR: Ing. Andaluz Espinoza Diego Fernando. MGTR.

Latacunga

2023



ÌNDICE

➤ **Antecedentes y planteamiento del problema**

➤ **Justificación**

➤ **Objetivos generales, específicos**

➤ **Alcance**

➤ **Marco teórico**

➤ **Conclusiones y recomendaciones**



ANTECEDENTES

La mayoría de instituciones a nivel nacional, desde la más grande hasta la más pequeña, cuentan con un infraestructura informática donde se realizan el procesamiento de los datos ya sea propios de la empresa o de los colaboradores, el mismo que debe cumplir con las especificaciones del fabricante y de las normativas internacionales para un correcto funcionamiento, la robustez de la infraestructura también viene acompañada con la seguridad, una de las especificaciones más importante y que muchas de las empresas no lo toman en cuenta



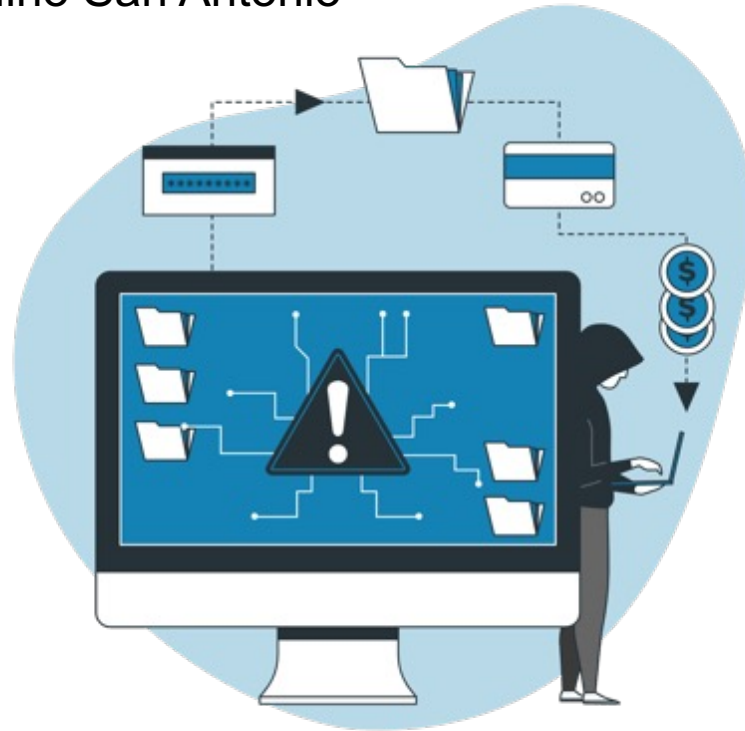
PLANTEAMIENTO DEL PROBLEMA

Actualmente, la junta administradora de agua potable Miño San Antonio, cuentan con un sistema informáticos para gestionar la información de los miembros que conforman el diferente número de juntas a su vez conformado una infraestructura tecnológica compuesta de activos físicos y lógicos para el procesamiento de los datos.



PLANTEAMIENTO DEL PROBLEMA

Debido a los eventos que se podrían desarrollarse y dejar sin operación al equipamiento tecnológico se es necesario que todos los activos estén ligados a un plan de contingencia, el mismo que por el momento no cuenta la junta administradora de agua Miño San Antonio



JUSTIFICACIÓN

La elaboración del plan de contingencia brinda una herramienta de apoyo realizada con el fin de tener una reacción oportuna por parte de los administradores de la institución hacia las amenazas, encontrándose disponible en todo momento de ser requerido.

El Este servicio ayudará a mitigar los riesgos que puede sufrir los sistemas informáticos, reactivando de esa forma los servicios más rápido y efectivo.



OBJETIVOS

GENERAL:

- ✓ Elaborar un plan de contingencia para sistemas informáticos de las juntas administradoras de agua potable Pastocalle, caso de estudio administrado de Junta Administradora de Agua Miño San Antonio.

ESPECÍFICOS:

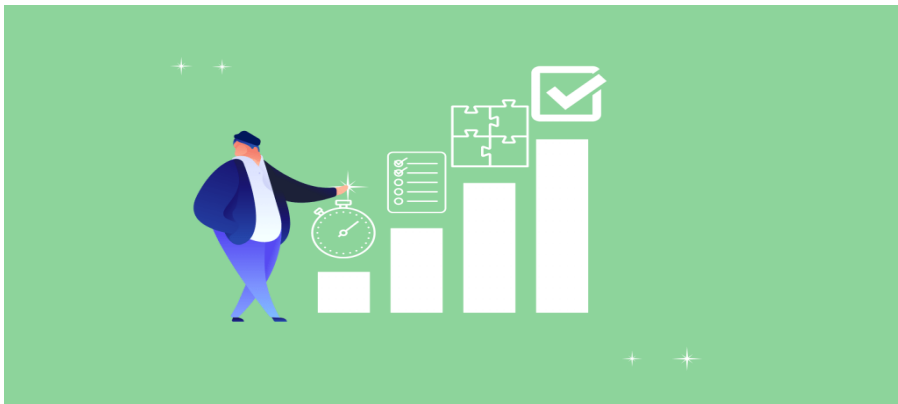
- ✓ Evaluar los riesgos de tecnología de la información y comunicación que afecten la continuidad del negocio en las instituciones.



- ✓ Determinar métricas que permiten gestionar los procesos críticos apoyados en las tecnologías de la información y comunicación.
- ✓ Generar procesos, procedimientos y políticas para mantener la operatividad de los servicios de tecnología de la información y comunicación.

ALCANCE

- Visita técnica a la comunidad participante para realizare un evaluó del estado y operación de los componentes de las oficinas de la institución, como son los activos lógicos y físicos del sistema informático para luego gestionar la tabulación y ingreso al software (EAR/PILAR), que será el encargado de realizar el barrido, validación de los activos para poder determinar los riesgos presentes dentro de los mismos.
- El proyecto tiene como fin, la creación de un plan de contingencia destinado a la junta administradora de agua Miño San Antonio se originará mediante una evaluación exhaustiva de los activos que poseen actualmente.



MARCO TEÓRICO

- **Plan de contingencia**



Objetivos del plan de contingencia

- Garantizar la integridad de los colaboradores y visitantes.
- Protección de los datos.
- Reanudación de las operaciones causado por error humano, destrucción intencional y falla del equipo. Mitigación de riesgos debido a desastres.
- Capacidad para continuar las operaciones posteriores a un evento desastroso.



- **Proceso de un plan de contingencia**

FASES PLAN DE CONTINGENCIA



AYUDALEYPROTECCIONDATOS.ES



Metodología para la gestión de riesgos tecnológicos



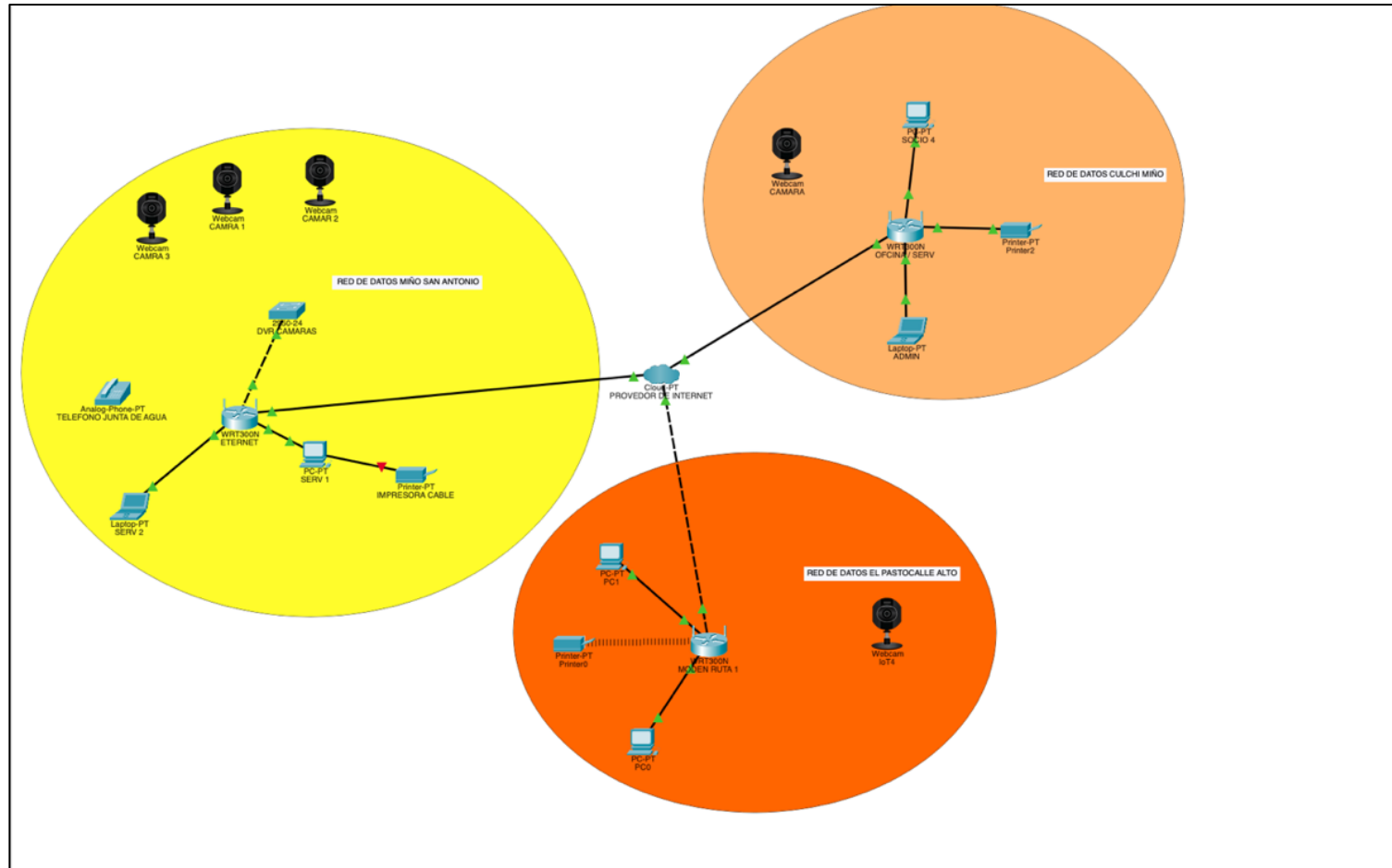
MAGERIT
inmobiliaria



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

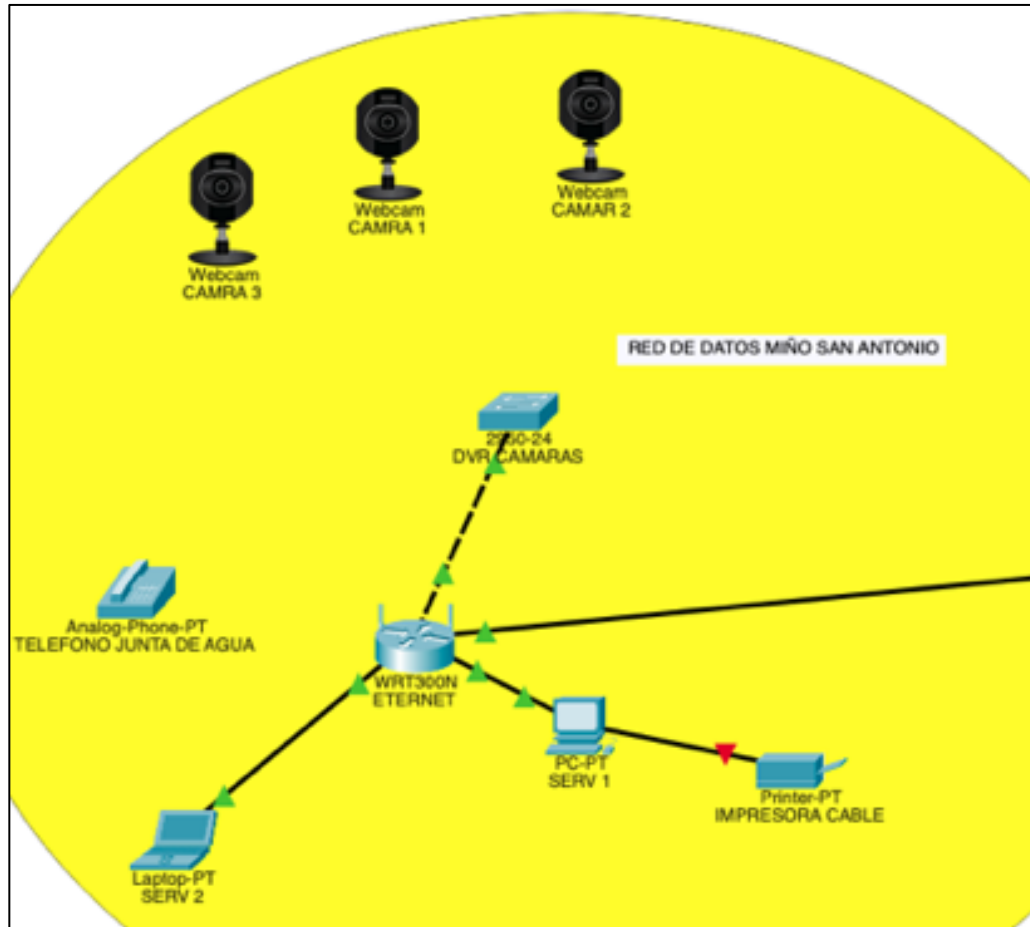
INFRAESTRUCTURA

- Bosquejo de las juntas aledañas



INFRAESTRUCTURA

- Bosquejo de la red “Miño San Antonio”



INFRAESTRUCTURA

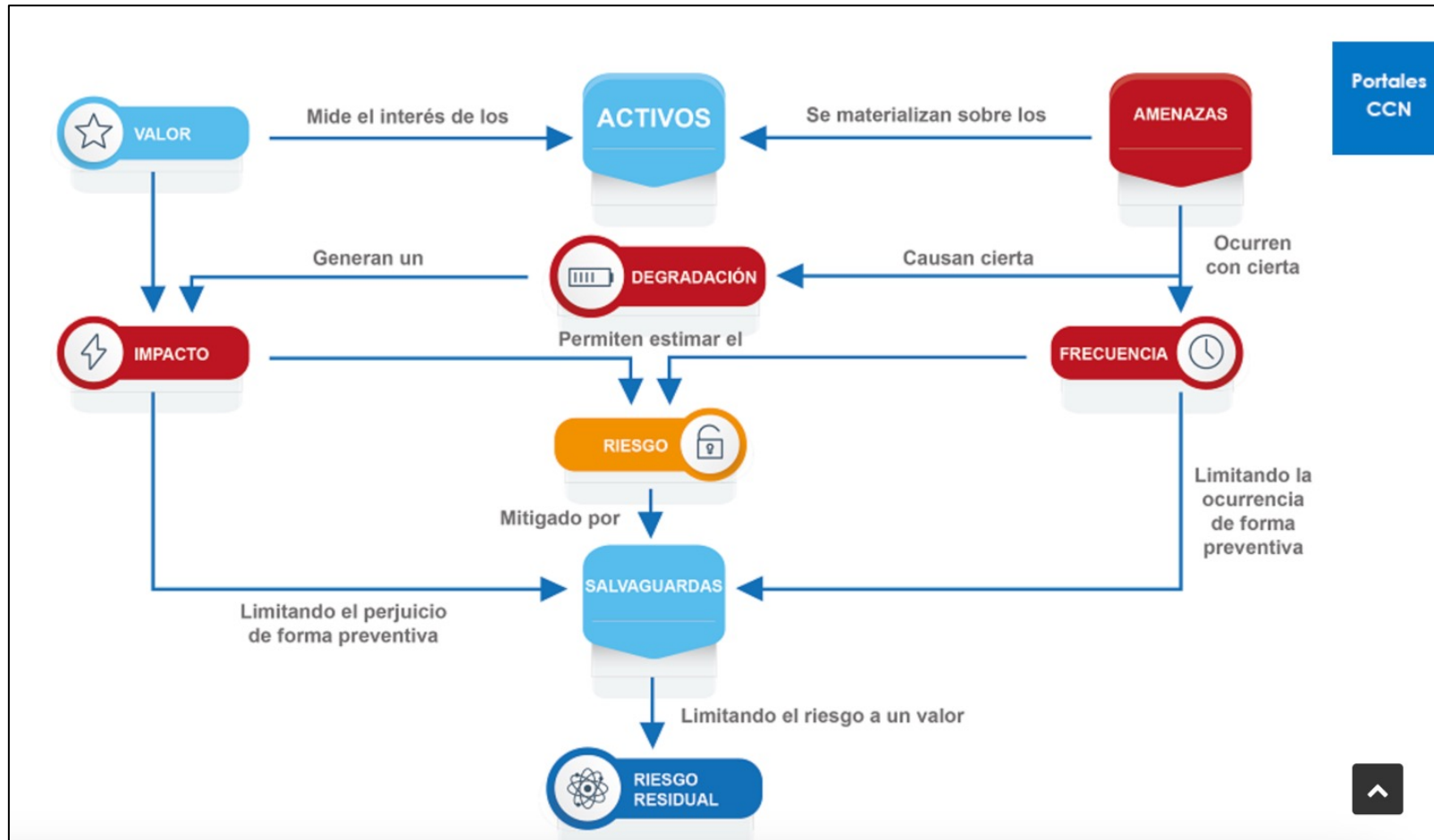
- **ACTIVOS JAMSA**

Activos	Tipo	Detalle	Cantidad
Software	Aplicativo web	Facturación	
Hardware	Switch	Comunicaciones	3
	Modem		
	Telefonía		
	Análoga		
Impresoras	1PC de	2 PCs de trabajo	
Estaciones de trabajo	administración		
Oficina			
Infraestructura		Matriz	1
Datos	Respaldos BDD	Documentos y registros	----- --



Desarrollo del tema

Procesos de ejecución del PILAR



Desarrollo del tema

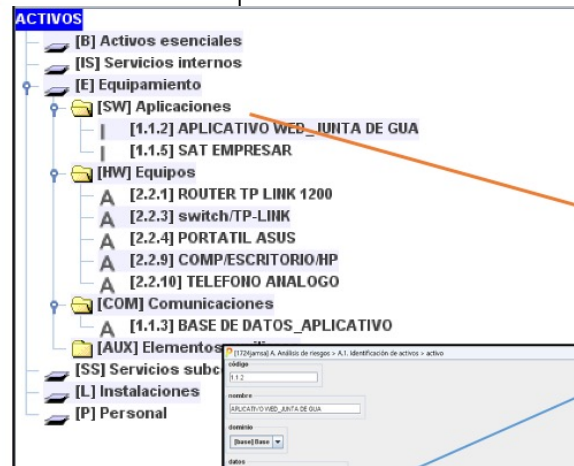
Proceso gestión de riesgos (ISO 27001 Y 31000_Magerit_Pilar)

[1724jamsa] Contexto

biblioteca [std] Biblioteca INFOSEC (12.12.2022) (std_20222.pl5)
código 1724jamsa
nombre JAMSA/ANALISIS DE RIESGOS
proyecto - clasificación DIFUSIÓN LIMITADA
RGPD contexto

código	nombre	valor
org	organisation	Junta administradora de agua Miño San Antonio
desc	description	Juntas administradoras de agua parroqui
author	Autor	autor
version	Versión	2
date	date	16-01-2023
owner	system owner	autor
ciso	chief information officer	system administration
resp	responsable	
ver	version	

descripción arriba abajo nueva eliminar estándar



se ingresa el activo en cada una de las carpetas con las valoraciones correspondientes.

[1724jamsa] A. Analisis de riesgos > A.1. Identificación de activos > activo

id: 112
nombre: APLICATIVO WEB_JUNTA DE GUA
dominio: [Seleccionar] >
datos:
descripcion: Ingreso de obras de agua potable
responsable: creador del software privado
servicio: facturación electrónica

ACTIVOS DE ACTIVOS

- [B] Activos esenciales
 - [B] Información
 - [B] Datos de acceso para el negocio
 - [B] Datos de acceso comercial
 - [B] Datos de la administración pública
 - [B] Datos vitales o críticos de la organización
 - [B] Datos personales
 - [B] Identificación clasificada
 - [B] Servicios
 - [B] Procesos de negocio
 - [B] Elementos de datos personales
- [IS] Servicios internos
 - [IS] Arquitectura del sistema
 - [IS] Información
 - [IS] Claves criptográficas
- [E] Equipamiento
 - [E] Aplicaciones (software)
 - [E] Operación propia (in-house)
 - [E] Desarrollo o modelo (subcontratado)
 - [E] Estándar (off-the-shelf)
 - [E] Herramientas de seguridad
 - [E] Equipamiento informático (hardware)
 - [E] Redes de comunicaciones
 - [E] Soportes de información
 - [E] Equipamiento móvil
- [L] Instalaciones
- [P] Personal
 - [P] Otros roles



VALORACIONES DE SEGURIDAD PARA ANÁLISIS

criterios de valoración	
<input type="checkbox"/>	Tiempo de Recuperación del Servicio:
<input type="checkbox"/>	Información Personal:
<input type="checkbox"/>	Obligaciones legales:
<input type="checkbox"/>	Seguridad:
<input type="checkbox"/>	Intereses Comerciales / Económicos:
<input type="checkbox"/>	Interrupción del servicio:
<input type="checkbox"/>	Orden Público:
<input type="checkbox"/>	Operaciones:
<input type="checkbox"/>	Administración y Gestión:
<input type="checkbox"/>	Pérdida de Confianza (Reputación):
<input type="checkbox"/>	Persecución de Delitos:
<input type="checkbox"/>	Seguridad de las personas
<input type="checkbox"/>	Datos personales
<input type="checkbox"/>	Información Clasificada:
...	
<input type="radio"/>	[7] Alto
<input type="radio"/>	[4] Medio
<input type="radio"/>	[1] Bajo
<input type="radio"/>	[0] Despreciable

ACTIVOS	AMENAZAS
[B] Activos esenciales	▲ [N] Desastres naturales
[IS] Servicios internos	▲ [I] De origen industrial
[E] Equipamiento	▲ [E] Errores y fallos no intencionados
[SW] Aplicaciones	▲ [A] Ataques deliberados
[1.1.2] APLICATIVO WED_JUNTA DE GUA	▲ [PR] Riesgos sobre la privacidad
[1.1.5] SAT EMPRESAR	
[HW] Equipos	
▲ [2.2.1] ROUTER TP LINK 1200	
▲ [2.2.3] switch/TP-LINK	
▲ [2.2.4] PORTATIL ASUS	
▲ [2.2.9] COMP/ESCRITORIO/HP	
▲ [N.1] Fuego	
▲ [N.2] Daños por agua	
▲ [N.] Desastres naturales	
▲ [L.1] Fuego	
▲ [L.2] Daños por agua	
▲ [L.] Desastres industriales	
▲ [L.3] Contaminación medioambiental	
▲ [L.4] Contaminación electromagnética	
▲ [L.5.2] Avería de origen físico	
▲ [L.6] Corte del suministro eléctrico	
▲ [L.7] Condiciones inadecuadas de temperatura o humedad	
▲ [L.11] Emanaciones electromagnéticas (TEMPEST)	
▲ [E.23] Errores de mantenimiento / actualización de equipos (hard	
▲ [E.24] Caída del sistema por agotamiento de recursos	
▲ [E.25] Pérdida de equipos	
▲ [A.7] Uso no previsto	
▲ [A.11] Acceso no autorizado	
▲ [A.23] Manipulación del hardware	
▲ [A.24] Denegación de servicio	
▲ [A.25] Robo de equipos	
▲ [A.26] Ataque destructivo	
▲ [2.2.10] TELEFONO ANALOGO	
[COM] Comunicaciones	
▲ [1.1.3] BASE DE DATOS_APLICATIVO	
[AUX] Elementos auxiliares	
[SS] Servicios subcontratados	
[L] Instalaciones	
[P] Personal	



Resultados

Valoración de impacto de los riesgos de los activos de JAMSA

Exportar

potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{7,2}	{7,5}	{7,5}	{8,6}	{6,3}
[1.1.2] APLICATIVO WED_JUNTA DE GUA	{4,8}	{6,3}	{6,9}	{5,7}	{6,3}
[1.1.5] SAT EMPRESAR	{4,2}	{7,5}	{6,9}	{6,8}	{4,5}
[2.2.1] ROUTER TP LINK 1200	{5,4}	{7,5}	{5,1}	{6,8}	{4,5}
[2.2.9] COMP/ESCRITORIO/HP	{7,2}	{4,5}	{5,7}		
[2.2.10] TELEFONO ANALOGO	{4,8}	{5,6}	{5,7}	{6,8}	
[1.1.3] BASE DE DATOS_APLICATIVO	{7,2}	{6,8}	{7,5}	{8,6}	

niveles de criticidad

- {9} - catástrofe
- {8} - desastre
- {7} - extremadamente crítico
- {6} - muy crítico
- {5} - crítico
- {4} - muy alto
- {3} - alto
- {2} - medio
- {1} - bajo
- {0} - despreciable

potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[R]	[V]
ACTIVOS	{10}	{9}	{8}	{10}	{6}	
[B] Activos esenciales						
[IS] Servicios internos						
[E] Equipamiento	{10}	{9}	{8}	{10}	{6}	
[SW] Aplicaciones	{6}	{9}	{8}	{7}	{6}	
[1.1.2] APLICATIVO WED_JUNTA DE GUA	{6}	{9}	{8}		{6}	
[1.1.5] SAT EMPRESAR	{0}	{8}	{7}	{7}	{6}	
[HW] Equipos	{10}	{8}	{8}	{10}	{6}	
[2.2.1] ROUTER TP LINK 1200	{5}	{7}	{7}	{7}	{6}	
[2.2.3] switch/TP-LINK	{6}	{7}	{7}	{7}		
[2.2.4] PORTATIL ASUS	{6}	{6}	{7}			
[2.2.9] COMP/ESCRITORIO/HP	{10}	{6}	{8}			
[2.2.10] TELEFONO ANALOGO	{5}	{8}	{8}	{10}		
[COM] Comunicaciones	{9}	{8}	{8}	{10}		
[1.1.3] BASE DE DATOS_APLICATIVO	{9}	{8}	{8}	{10}		
[AUX] Elementos auxiliares						
[SS] Servicios subcontratados						
[L] Instalaciones						
[P] Personal						



Contingentes:

- Eventos naturales como incendios, inundaciones, terremotos y erupción volcánica.
- Mal funciones en componentes de hardware y software.
- Acceso a la información por parte de individuos no autorizados.
- Corte de servicios internet/energía eléctrica

Procesos :

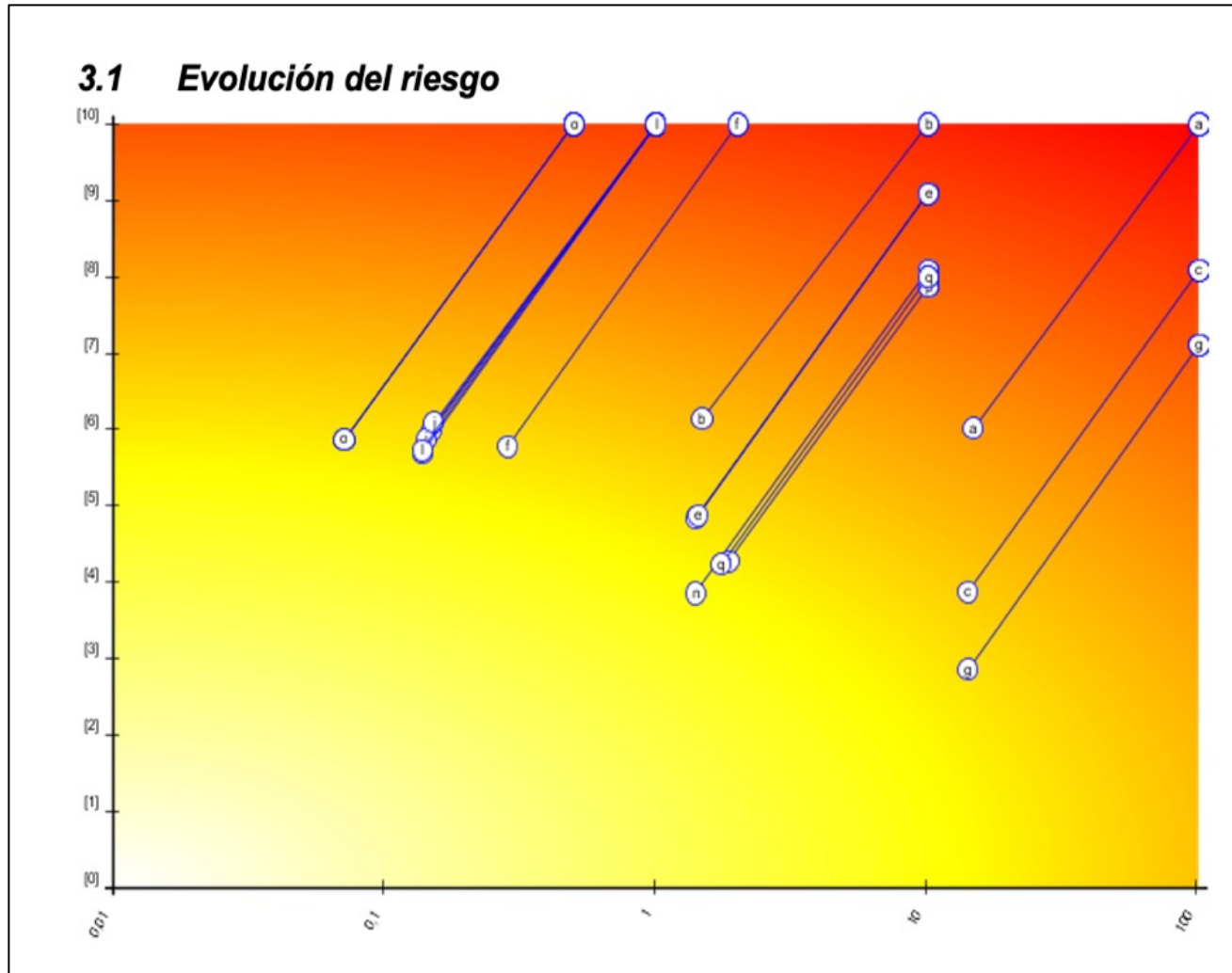
- Plan preventivo
- Plan en emergencia
- Plan restauración



Plan para continuidad de servicio

- ✓ Contar con Backus diarios y respaldo de información relevante para la institución.
- ✓ Revisar de manera periódica el estado del Software de todos los equipos.
- ✓ Mantener los equipos actualizados.
- ✓ Todos los computadores deben tener antivirus actualizados.
- ✓ Realizar un evaluó del físico de los activos.
- ✓ Realizar mantenimientos preventivos.





CONCLUSIONES

- ✓ Los planes de contingencia para servicios informáticos se enfocan en la creación de medidas que prevengan o reduzcan el efecto de una situación imprevista y permitan la recuperación de los servicios informáticos y/o tecnológicos afectados por dicha contingencia.
- ✓ Cabe destacar, que el ser una zona de riesgo debido al volcán Cotopaxi, se ha previsto que los respaldos se hagan de manera física y de manera digital (almacenamiento en la nube), y se recupere cualquier pérdida del sistema informático relacionado con la facturación a los socios de la Junta, que es de punto más crítico de la entidad.
- ✓ La validación de la propuesta mediante encuestas dirigidas tanto a los empleados como a los usuarios de la JAMSA, así como la realizada a expertos, ha arrojado resultados positivos. Los encuestados coinciden en que el plan de contingencia puede ser de gran ayuda para la Junta, permitiéndole preservar su información y operatividad en caso de sucesos tecnológicos y/o naturales.



RECOMENDACIONES

- ✓ Además, se sugiere que dado que la propuesta presentada es aplicable sin problemas en otras Juntas Administradoras de Agua Potable, se considere su implementación inmediata en estas instituciones.
- ✓ Según lo mencionado anteriormente, se sugiere la implementación inmediata de un plan de gestión de riesgos, así como de un plan de respaldo y contingencia que incluya diversas estrategias antes, durante y después de una posible infiltración o catastrofe. El propósito principal de estas medidas es proteger la información manejada por el sistema contable de la Junta Administradora de Agua Potable Pastocalle.



Gracias por su atención

