UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN
MODALIDAD: PROPUESTA METODOLÓGICA Y TECNOLÓGICA AVANZADA

Título:

ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO

Trabajo de titulación previo a la obtención del título de magister en Sistemas de Información

Autor:

Casa Guayta Carlos Welington

Tutor:

JOSÉ AUGUSTO CADENA MOREANO MSc.

LATACUNGA –ECUADOR

2020

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación "Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Guaytacama - caso de estudio Junta administradora de agua potable Pilacoto." presentado por Casa Guayta Carlos Welington, para optar por el título magíster en Sistemas de Información.

CERTIFICO

Que dicho trabajo de investigación ha sido revisado en todas sus partes y se considera que reúne los requisitos y méritos suficientes para ser sometido a la presentación para la valoración por parte del Tribunal de Lectores que se designe y su exposición y defensa pública.

Latacunga, Junio, 22, 2019.

……
MSc. JOSÉ AUGUSTO CADENA MOREANO
CC: 050155279-8

APROBACIÓN TRIBUNAL

El trabajo de Titulación: "Elaboración de un plan de contingencia para los sistemas informáticos de las Juntas administradoras de agua potable de la parroquia de Guaytacama - caso de estudio Junta administradora de agua potable Pilacoto", ha sido revisado, aprobado y autorizado su impresión y empastado, previo a la obtención del título de Magíster en Sistemas de Información; el presente trabajo reúne los requisitos de fondo y forma para que el estudiante pueda presentarse a la exposición y defensa.

Latacunga, Junio, 22, 2020.

……..
Mg.C Jorge Bladimir Rubio Peñaherrera
CC: 050222229-2
Presidente del tribunal

…….
Mg.C Manuel William Villa Quishpe
CC: 180338695-0
Lector 2

…….
Mg.C Alex Chistian Llano Casa
CC: 050258986-4
Lector 3

DEDICATORIA

En primer lugar, quiero dedicar este trabajo a Dios y a mi director de tesis José Cadena, por la dedicación y apoyo que ha brindado a este trabajo para culminar con éxito este proceso académico.

Agradezco mis hijos Monserrat y Carlitos Mathías porque son el motor fundamental en mi vida.

También a mi esposa Fernanda quien que fue una persona fundamental en este proceso.

Gracias a mi familia, a mis padres y a mis hermanas, porque son unas personas muy importantes en mi vida.

A mis suegros que son un apoyo para seguir superándome.

Y en especial a mis abuelitos que son un pilar fundamental en vida diaria.

Carlos

AGRADECIMIENTO

Mi agradecimiento profundo a la Universidad Técnica de Cotopaxi por permitir seguir estudiando esta maestría.

También a Dios y a mi familia que son el eje fundamental en mi vida diaria y profesional, quienes con sus palabras de aliento me impulsaron a continuar con mis estudios.

Y a la vez a la Junta Administradora de Agua Potable Pilacoto y a sus funcionarios, quienes me apoyaron con la información necesaria para esta investigación

Casa Guayta Carlos Welington

RESPONSABILIDAD DE AUTORÍA

Quien suscribe, declara que asume la autoría de los contenidos y los resultados obtenidos en el presente trabajo de titulación.

Latacunga, Junio, 22, 2019.

……
Ing. Casa Guayta Carlos Welington
CC: 0502352180

RENUNCIA DE DERECHOS

Quien suscribe, cede los derechos de autoría intelectual total y/o parcial del presente trabajo de titulación a la Universidad Técnica de Cotopaxi.

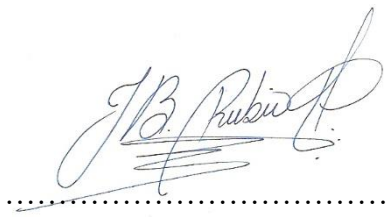
Latacunga, noviembre, 8, 2019.

……
Ing. Casa Guayta Carlos Welington
CC: 0502352180

AVAL DEL PRESIDENTE

Quien suscribe, declara que el presente Trabajo de Titulación: ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO, contiene las correcciones a las observaciones realizadas por los lectores en sesión científica del tribunal.

Latacunga, junio 26 del 2020



……

Mgs. Jorge Bladimir Rubio Peñaherrera

050222229-2

UNIVERSIDAD TÉCNICA DE COTOPAXI
DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN
‘

Título: ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO

Autor: Casa Guayta Carlos Welington
Tutor: José Augusto Cadena Moreano MSc.

RESUMEN

El presente proyecto plantea la **“ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO”**. Esta guía permitirá realizar la gestión adecuada de riesgos, así como ejecutar estrategias de recuperación para tecnologías de información, lo cual permitirán asegurar la continuidad de los servicios tecnológicos e informáticos, en este caso de la Junta Pilacoto, si fueran interrumpidos por algún tipo de incidente; la cual posteriormente podrá ser replicada en las demás Juntas Administradoras de agua potable de Guaytacama.

PALABRAS CLAVE: plan, contingencia, sistema, informático, junta, agua, Pilacoto

UNIVERSIDAD TECNICA DE COTOPAXI
DIRECCION DE POSGRADO

MAESTRIA EN SISTEMAS DE INFORMACION

Title: DEVELOPMENT OF A CONTINGENCY PLAN FOR THE COMPUTER SYSTEMS OF THE DRINKING WATER MANAGEMENT BOARDS OF THE PARISH OF GUAYTACAMA - CASE STUDY OF THE PILACOTO DRINKING WATER MANAGEMENT BOARD

Author: Casa Guayta Carlos Welington
Tutor: José Augusto Cadena Moreano MSc.

ABSTRACT

The present project proposes the "DEVELOPMENT OF A CONTINGENCY PLAN FOR THE COMPUTER SYSTEMS OF THE DRINKING WATER MANAGEMENT BOARDS OF THE PARISH OF GUAYTACAMA - CASE STUDY OF THE PILACOTO DRINKING WATER MANAGEMENT BOARD". This guide will allow for adequate risk management, as well as the implementation recovery strategies for information technology, which will ensure the continuity of technological and computer services, in this case of the Pilacoto Board, if they were interrupted by any type of incident; which can later be replicated in the other Drinking Water Management Boards of Guaytacama.

KEYWORD: plan, contingency, system, computer, board, water, Pilacoto

Nombres y apellidos **MARÍA ELISA COQUE CRUZ** con cédula de identidad número **0502638562** Licenciado/a en: **LICENCIADA EN CIENCIAS DE LA EDUCACIÓN MENCIÓN INGLÉS** con número de registro de la SENESCYT: **1010-08-807045**; **CERTIFICO** haber revisado y aprobado la traducción al idioma inglés del resumen del trabajo de investigación con el título: "**ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO",** de **CASA GUAYTA CARLOS WELINGTON**, aspirante a magister en SISTEMAS DE INFORMACIÓN

Latacunga, Febrero 7, 2020.

…….....
MARÍA ELISA COQUE CRUZ
CC: 0502638562

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El Planteamiento del problema constituye el hecho de que todas las entidades públicas y privadas deben cumplir normas y/o requisitos, por lo tanto, el Ministerio del Ambiente y Agua como institución pública está sujeto a la normativa del Estado ecuatoriano. De esta manera, y acatando las recomendaciones realizadas por los organismos de control, se tiene la necesidad de preparar un plan de contingencia para los sistemas informáticos, ya que, las Juntas administradoras de agua potable de Guaytacama, concretamente, la Junta de Pilacoto, poseen reducidos mecanismos de control de los sistemas de información, que lastimosamente no cuentan un estudio apropiado sobre el impacto en caso de desastres, ataques o incidentes. Por lo tanto, dichos mecanismos no permiten gestionar de manera adecuada, la prevención y la recuperación de los servicios informáticos y/o tecnológicos; de este modo, y considerando lo anteriormente expuesto, se puntualiza en el desarrollo de un plan de continuidad de los sistemas informáticos empleados en la institución en cuestión.

De lo anteriormente mencionado, se desprende la siguiente **formulación del problema**: En la Junta administradora de agua potable Pilacoto no existe un plan de contingencia para los sistemas informáticos que garantice su operatividad.

Así, el **objetivo general** del presente proyecto es, elaborar un Plan de Contingencia para Sistemas Informáticos de las Juntas administradoras de agua potable Guaytacama - Caso de estudio Junta administrado de agua potable Pilacoto.

Al respecto, los **objetivos específicos** correspondientes se detallan a continuación:

- Diagnosticar los riesgos de Tecnología de la Información y Comunicación que afecten la continuidad del negocio en la institución.
- Establecer métricas que permitan administrar los procesos críticos apoyados en las Tecnología de la Información y Comunicación.
- Generar procesos, procedimientos y/o políticas para mantener la operatividad de los servicios de Tecnología de la Información y Comunicación.

En este punto, es indispensable mencionar que, gran parte de instituciones públicas o privadas no cuentan con un plan de contingencia que permita responder exitosamente a las situaciones donde se afecten sus sistemas informáticos; por lo tanto, es indispensable realizar el estudio y elaboración de un plan de contingencia que pueda ser implantado en instituciones de diversa índole.

Tomando en cuenta que, el presente caso de estudio es para la Junta administradora de agua potable Pilacoto-Guaytacama, presentará una solución bien definida y estructurada que permitirá mantener la operatividad de las funciones informáticas de dicha Institución, cuando ocurra algún tipo de inocente sobre la infraestructura tecnológica que ésta posee. Por lo tanto, el plan de contingencia propondrá la aplicación de medidas preventivas y correctivas enfocadas a la preservación tanto de los activos físicos como de la información que se maneja, las cuales intentarán minimizar el impacto en caso de incidentes o eventos que generen algún riesgo para el cumplimiento de operaciones de la Junta.

En tal sentido, y para cumplir con lo planteado, se recurrirá al análisis y gestión de riesgos propuesto por la **metodología MAGERIT III** (aplicada mediante la **herramienta Pilar**), la cual consiste en la aplicación de mecanismos de control que permitan determinar el riesgo e impacto de amenazas en la institución. De esta manera, lo podrá determinar: las amenazas, las salvaguardas, el impacto, y el riesgo

De esta forma, la aplicación de esta metodología permitirá dar cumplimiento en lo establecido por los siguientes estándares internacionales, que de acuerdo a lo planteado en el presente proyecto, abarcan los siguientes:

- ISO 27001:2013 (SGSI -Sistema de gestión de seguridad de la información)
- ISO 27002:2013 (Seguridad de la información**)**
- ISO/ 27005:2018 (Gestión de riesgos de seguridad de la información)
- ISO 31000:2018 (Gestión del riesgo)

Adicionalmente, para validar para propuesta se ha recurrido al uso de la **técnica de la encuesta** aplicada mediante el **instrumento del cuestionario**, tanto a empleados como a usuarios de la Junta administradora de agua potable Pilacoto que, mediante el empleo de preguntas cerradas, se podrá obtener mediciones cuantitativas,

objetivas y subjetivas de la percepción de los encuestados y la ratificación correspondiente.

CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA

1.1 Antecedentes

En un estudio realizado por la Universidad de Minnesota, se ha demostrado que más del 60% de las empresas que sufren un desastre y que no tienen un plan de recuperación ya en funcionamiento, saldrán del negocio en dos o tres años. Mientras vaya en aumento la dependencia de la disponibilidad de los recursos informáticos, este porcentaje seguramente crecerá [1].

Por lo tanto, es importante destacar que, el plan de contingencia abarca el análisis de los riesgos a los cuales están expuestos los equipos de informáticos y/o tecnológicos, sistemas de información, incluyendo los datos propiamente dichos, con el propósito de disminuir las posibilidades de ocurrencia de éstos, así como determinar el procedimiento a seguir en caso que se presente un siniestro.

El plan de contingencia se hace énfasis al aspecto físico y lógico, es donde se concentra el mayor número de inconvenientes: pero también es establecer pruebas y verificaciones periódicas para que el plan de contingencia esté operativo y actualizado.

Las acciones que contemplan el plan de contingencia son: antes, durante y después, de manera que permita reducir: pérdidas financieras directas / indirectas perdidas de operatividad, pérdidas de usuarios finales, costos extras para apoyo, costos de compensación, pérdida de la infraestructura tecnológica, perdidas de sistemas de información, bases erróneas o pobres, entre otras [1].

La mayor dependencia de tecnologías que actualmente tienen las empresas públicas y privadas y que mueven la sustancia de su negocio sobre la tecnología, donde es necesario contar con una plataforma tecnológica confiable que colabore totalmente en la mejora del negocio. En este tipo de instituciones un suceso en la infraestructura tecnológica en pocos minutos puede haber un impacto catastrófico en los resultados económicos y por ende en el proceso de sus actividades.

Una catástrofe tecnológica no precisamente debe estar relacionado con un terremoto, inundaciones e incendios o cualquier otro suceso de gran dimensión causado por la naturaleza, también pueden ser causados por sí mismo tales como la penetración de un virus, ataques informáticos pueden causar la pérdida de información y en el peor de los escenarios, el daño definitivo de los sistemas informáticos y/o infraestructuras tecnológicas. De esta forma, existe otro tipo de incidentes que, pueden tener un impacto gravísimo y daños masivos para la institución como pueden ser daño a la infraestructura civil donde se encuentran los equipos tecnológicos, fallas eléctricas, fallas con los proveedores de los suministros informáticos.

Los resultados de estos sucesos sobre las instituciones que no cuentan con un plan de contingencia de los sistemas informáticos (TIs), pueden llegar a ocasionar la interrupción de los procesos institucionales, más aún si se tratan de empresas de recaudaciones de servicios básicos que mantienen las operaciones sobre las plataformas tecnológicas de la información, como es el caso de estudio en uno de los capítulos de esta tesis.

Por tal razón, es muy importante contar con un plan de contingencia para los sistemas informáticos que permita conseguir un mapa de acciones a tomar para la reducción de recuperación de infraestructura tecnológica, reanude efectivamente los servicios necesarios que permita integrar el funcionamiento de los sistemas que están en proceso y al mismo tiempo minimizar los costes y niveles operativos en el departamento.

El plan de contingencia ayudará a organizar y documentar los riesgos, responsabilidades y ordenamientos para la reparación segura de la infraestructura tecnológica.

Así, es primordial conocer los beneficios que tiene la institución al elaborar un plan de contingencia para los sistemas de información TIs, éstos son:

- Protección al enfrentar una interrupción mayor por cualquier tipo de desastre, mediante una estrategia y metodología de continuidad.
- Utilización de la infraestructura actual para el desarrollo del plan de contingencia.
- Utilización de la documentación actual de la institución
- Realización de un análisis de riesgo e impacto de los sistemas informáticos que posee la institución
- Verificación de los sitios más críticos y sensibles de los procesos de los sistemas informáticos en la institución
- Organización para el Plan de Contingencia de los sistemas de información en TIC.
- Consolidación de la documentación necesaria para cualquier auditoría.

Por otro lado, los problemas que se podrían presentar son:

- Falta de compromiso del personal de la institución, incluido directivos
- Complicación en la recolección de datos
- Diseño del plan sin evaluación adecuada del riesgo.
- Falta de un simulacro de prueba
- Limitaciones de presupuesto.

1.2 Plan de Contingencia

Se puede definir a un plan de contingencia como una estrategia que abarca un conjunto de lineamientos y/o procedimientos que permitan solucionar prontamente la restitución de los servicios de una institución u organización ante alguna eventualidad, la cual paralice sus actividades, ya sea parcial o

total. Específicamente, el plan de contingencias de los sistemas y equipos informáticos puede ser definido como "una herramienta que ayudará a que los procesos críticos continúen funcionando a pesar de una posible falla en los sistemas de información" [2].

Todas las instituciones están expuestas a diversos tipos de riesgos en sus sistemas de información, tanto físicos (fuego, inundación, sabotaje, Entre otros) como lógicos (virus, problemas de seguridad en la información, calidad de software, almacenamiento de datos inapropiado, entre otros), que pueden paralizar parcial o totalmente la normal actividad de los mismos, con el consiguiente perjuicio para la organización.

Una eventualidad en los sistemas y equipos informáticos tendrá diferente impacto en la organización según la criticidad de los servicios afectados, pudiendo afectar a la supervivencia de la propia institución, si no tiene definidas previamente diversas medidas que minimicen dicho impacto.

El plan de contingencia se basa en la minimización del impacto que pueda tener un siniestro en los sistemas de informáticos de la compañía, asegurando la continuidad del servicio, la satisfacción del cliente y la productividad a pesar de una catástrofe, tratando de alcanzar una alta disponibilidad para la infraestructura crítica [3].

Considerando la Norma ISO 27001 (Sistema de Gestión de Seguridad de la Información), son varios pilares que deben ser considerados en su implementación, y así, garantizar la disponibilidad de las infraestructuras de informáticas y/o tecnológicas, y no se detenga la operatividad ante un incidente [4]:

Figura 1 Pilares para la implementación de un plan de contingencia
Fuente: [4]

De igual forma, para la ejecución de un plan de contingencias Informático es necesario aplicar el ciclo de vida iterativo PDCA, el cual mediante la retroalimentación de información permite obtener una mejora continua de los procesos institucionales u organizacionales. El ciclo PDCA enseña a las entidades a planear una acción, hacerla, revisarla para ver cómo se adecua al plan y actuar en base a lo que se ha aprendido.

1.2.1 Ciclo de vida PDCA

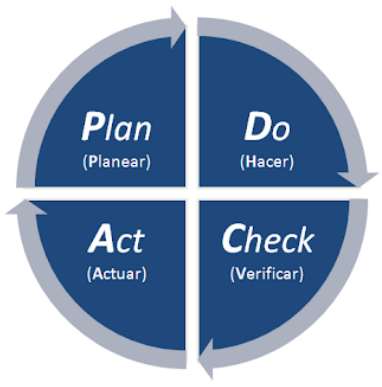


Figura 2 Ciclo de Vida PDCA
Fuente: [5]

El ciclo de vida PDCA, en inglés “Plan, Do, Check, Act”, o en español “Planificar, Hacer, Verificar”, es asimismo llamado ciclo de mejora

continua o círculo de Deming (por su autor). Esta metodología contiene cuatro pasos sistemáticos para alcanzar la mejora continua o calidad. Al llegar a la etapa final, se debe empezar con la primera nuevamente y así, repetir el ciclo, reevaluando el ciclo como tal e incorporando mejoras necesarias [6].

1.2.2 Objetivos del plan de contingencia

El objetivo principal de un plan de contingencia es permitir que una organización vuelva a sus actividades cotidianas tan pronto como sea posible después de un acontecimiento imprevisto. Además, entre los objetivos secundarios de un plan de contingencia se pueden detallar los siguientes:

- Garantizar la seguridad de todos los empleados y visitantes.
- Proteger la información sensible
- Asegurar las instalaciones
- Salvaguardar los materiales, suministros y equipos necesarios para garantizar la rápida recuperación de las operaciones
- Reducir el riesgo resultado de desastres causados por errores humanos, la destrucción deliberada y/o las fallas de los equipos
- Garantizar la capacidad de la organización para seguir funcionando después de un desastre.
- Recuperar la información perdida o dañada después de un desastre.

1.2.3 Metodología del plan de contingencia

La elaboración del plan de contingencia debe ser guiada por la metodología que permita adaptarse tanto a la infraestructura y servicios que posea y ofrezca la institución; un proyecto de plan de contingencia consiste en realizar:

Figura 3 Fases del plan de contingencia
Fuente: [7]

Existen algunos aspectos importantes en el modelamiento e implementación del plan de contingencia que son los siguientes:

- Es recomendable utilizar una herramienta para efectuar el análisis de riesgos.
- Es necesario definir los procesos de continuidad y disponibilidad de TI que permitan mantener actualizado el plan frente a los cambios continuos.
- También, es necesario definir los criterios de activación del plan.
- Es indispensable definir además, las estrategias de recuperación que cumplan con los criterios de continuidad del negocio [7].

1.2.4 Diferencia entre un plan de contingencia informático y plan de continuidad del negocio

El ámbito y alcance del Plan de contingencia informático se concentran en conseguir que las los servicios informáticos y tecnológicos, se restablezcan lo más pronto posible poniendo en funcionamiento tanto las estrategias de recuperación como el personal de contingencia; en cambio, en el plan de continuidad involucra la infraestructura necesaria para que el uso sistemas de información, es decir la organización de continuidad.

Una organización necesita de la suma de los dos para disponer de una cobertura completa, si bien no siempre un incidente obliga a activar ambos planes; pero es importante destacar que, la gestión de crisis y continuidad comprende las prácticas que se centran y orientan a las decisiones y las acciones necesarias para prevención, mitigación, preparación, respuesta a, reanudar, recuperar, restaurar y tránsito a partir de un evento de crisis.

1.3 Riesgos

El riesgo se define como "la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular" [8]; en lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo, de perder datos debido a ruptura de un disco duro, virus informático, etc.) [9].

1.3.1 Evaluación, tratamiento y monitoreo del riesgo

Para De Freitas, conocer el riesgo a los que están sometidos los activos es fundamental para poder gestionarlos, razón por la cual han surgido una variedad de guías, métodos y herramientas que buscan objetivar el análisis para saber cuán seguros o inseguros son o están dichos activos [8].

En los actuales momentos la serie de la norma ISO 27000, presenta un compendio de lineamientos que proporcionan una base los sistemas de gestión de seguridad de la información, asimismo la ISO 31000 se enfoca en la gestión del riesgo propiamente dicho; por lo que proporcionan información vital para que una entidad conozca sobre el riesgo que corren sus activos de información, así esté preparada para evitar su ocurrencia.

De esta serie, para el respectivo desarrollo se consideran las siguientes ISO:

- ISO 27001:2013 (SGSI -Sistema de gestión de seguridad de la información)
- ISO 27002:2013 (Seguridad de la información**)**
- ISO/ 27005:2018 (Gestión de riesgos de seguridad de la información)
- ISO 31000:2018 (Gestión del riesgo)

Dichas normas indican en resumen que, los activos de información deben ser valorados para identificar su impacto; luego se debe realizar un análisis para determinar qué activos están bajo riesgo.; y "es en ese momento que se deben tomar decisiones en relación a qué riesgos aceptará la organización y qué controles serán implantados para mitigar el riesgo" [8].

Para el análisis o evaluación de riesgos, se deben considerar los elementos para la evaluación de la amenaza latente, lo que puede realizarse a partir de las siguientes preguntas básicas:

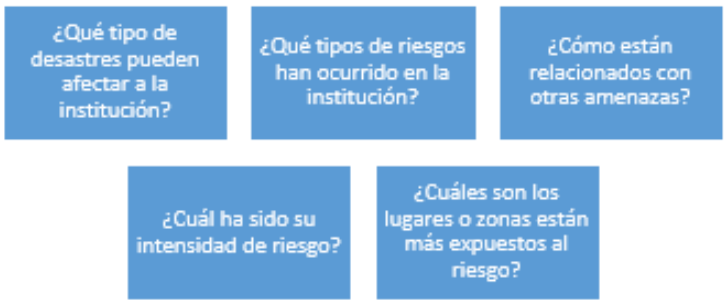


Figura 4 Preguntas básicas para la evaluación de riesgos
Fuente: [10].

Así mismo, se deben determinar las características de la amenaza, las cuales deben considerar:

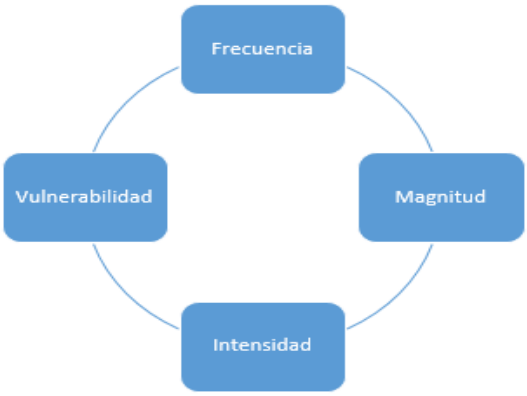


Figura 5 Características de las amenazas a considerar
Fuente: [10].

Adicionalmente, otro factor importante para la evaluación del riesgo, consiste en evaluar la vulnerabilidad, la cual puede realizarse mediante la identificación los principales elementos de vulnerabilidad que componen una amenaza y en una descripción de la importancia de cada una en las posibles pérdidas que generaría una amenaza determinada; de esta manera, el análisis de vulnerabilidad corresponde a la descripción de las condiciones relacionadas con los factores de vulnerabilidad según el tipo de amenaza [10].

Posteriormente, se debe aplicar el tratamiento de riesgo, que se define como "el conjunto de decisiones tomadas con cada activo de información" [8]; entre las medidas a atribuir se tienen: evitar, optimizar, transferir o retener el riesgo [8]. Para plantear los parámetros para la evaluación de los controles dependiendo de las medidas a asignar, se consideran las siguientes áreas:

- Administración de los recursos de TI
- Seguridad Física y Seguridad de Información
- Desarrollo y Mantenimiento de Sistemas de Información de la Entidad
- Continuidad de SI de la Entidad [11].

Con respecto al monitoreo y revisión de la gestión de riesgos, es necesario recalcar que, éstos se deben dar con regularidad y deben ser constantes; además, los responsables del monitoreo deben estar claramente definidos. Para que estos procesos sean exitosos, deberán comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar que los controles son eficaces y eficientes tanto en el diseño como en la operación.
- Obtener información adicional para mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos (incluyendo los cuasi accidentes), los cambios, las tendencias, los éxitos y los fracasos.
- Identificar los riesgos emergentes [12].

Además, se debe “detectar cambios en el contexto externo e interno, incluyendo los cambios en los criterios del riesgo y en el riesgo mismo que puedan exigir revisión de los tratamientos del riesgo y las prioridades” [13].

1.3.2 Metodología para la gestión de riesgos tecnológicos

Existen otras metodologías que ayudan en la implementación de la gestión de riesgos tecnológicos, las principales son:

1.3.2.1 Octave

Metodología del Software Engineering Institute (SEI) que abarca los temas organizacionales y los técnicos, además examina como la gente usa la infraestructura en su trabajo diario. “El objetivo de OCTAVE es el riesgo organizacional y el foco son los temas relativos a la estrategia y a la práctica” [14].

1.3.2.2 Cramm

Basado en la ISO 27001 se orienta a que los responsables de la seguridad estén en condiciones, “bien de evitar o aceptar riesgos individuales o bien en reducir los riesgos a aceptables” [15].

1.3.2.3 Risk It

Es una metodología de Information Systems Audit and Control Association (ISACA), la cual “ahorra tiempo, costos y esfuerzos al brindar

un método claro para concentrarse en los riesgos comerciales relacionados con la tecnología de la información" [16].

1.3.2.4 MAGERIT

Considerando la normativa ISO 31000, Magerit responde a: "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos"; es decir, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno puedan tomar decisiones teniendo presentes los riesgos procedentes del uso de tecnologías de la información [17].

Para la implementación del proceso de gestión de riesgos utilizando MAGERIT, se emplea el siguiente marco de trabajo:

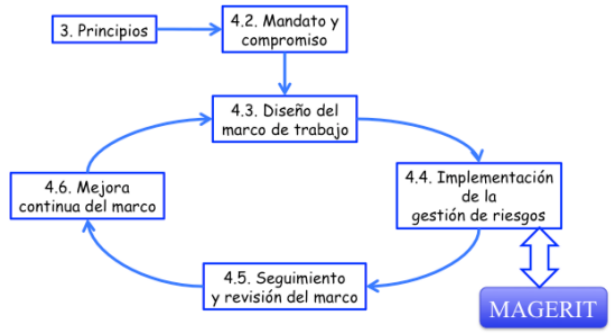


Figura 6 Marco de trabajo Magerit
Fuente: [17]

Figura 7 Lógica de Magerit
Fuente: [18]

Para la implementación de MAGERIT, se va a emplear la herramienta PILAR, que "es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT" [17].

La herramienta soporta todas las fases del método MAGERIT:

- Caracterización de los activos y de las amenazas
- Evaluación de las salvaguardas
- Estimación del estado de riesgo [17].

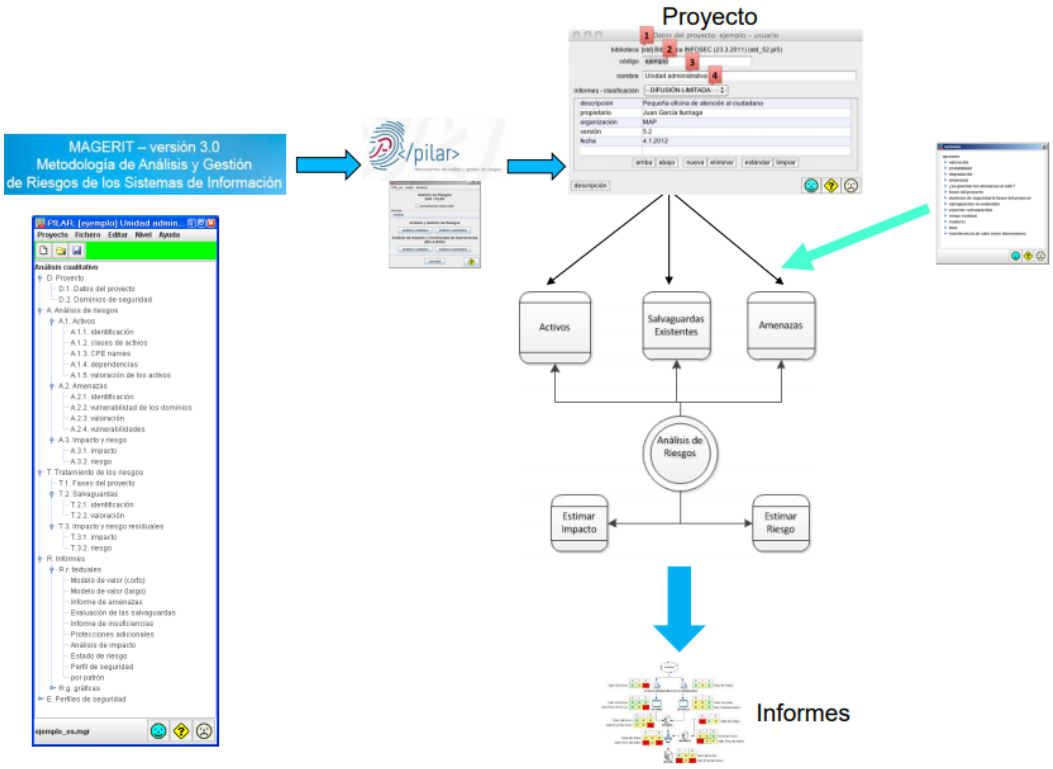


Figura 8 Estructura Pilar
Fuente: [18]

1.3.2.5 Norma ISO 31000

La Norma ISO 31000 proporciona los principios y guía exhaustivos para la para la gestión de riesgos, ayudando a las organizaciones en sus análisis y evaluación del riesgo, tanto si se trata de una entidad pública, privada o comunitaria; las recomendaciones de mejores prácticas de esta norma apoyan el mejoramiento de las técnicas de gestión y garantizando la seguridad propiamente dicha [19].

1.3.3 Métricas de recuperación

Con el fin de mantener la continuidad del negocio se establece un esquema que auxilia a la institución a recuperarse después de un desastre; tomando en cuenta que, un plan de continuidad del negocio, no es más que un mapa

que detalla cómo una institución puede continuar operando mientras dura la recuperación del desastre [20]. Para lo cual se hace referencia a las métricas de recuperación RPO y RTO.

- RTO Tiempo de recuperación objetivo: “Es el tiempo en el que el proceso del negocio debe estar restaurado después de un incidente grave, con el fin de evitar consecuencias inaceptables derivados de una para en la continuidad del negocio” [21].
- RPO Punto de recuperación objetivo: “Es la edad (tiempo que tiene un respaldo) de los archivos que se deben recuperar de almacenamiento de copia de seguridad para las operaciones tras un incidente grave” [21].

Así, el RPO es el tiempo máximo determinado entre una copia de seguridad con el objeto de mantener la continuidad de los servicios; mientras, que el RTO es el tiempo que tomará volver a la operatividad de acuerdo a los niveles de servicio pactados [21].

1.4 Respaldos

Otro aspecto importante ligada con el Plan de contingencia, es el respaldo de la información, éste puede ser interno o externo.

Figura 9 Respaldos
Elaborado por: Autor

1.4.1 Respaldo interno

El respaldo interno tiene como objetivo resolver contingencias leves que no necesiten el desplazamiento externo de donde están situados los elementos informáticos afectados [22].

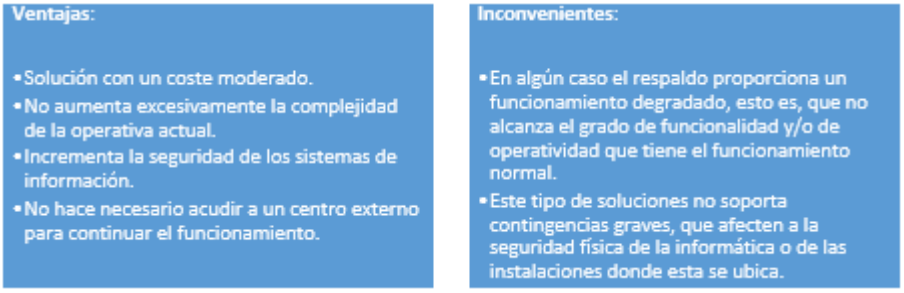


Figura 10 Ventajas e inconvenientes del respaldo interno.
Fuente: [22]

1.4.2 Respaldo externo

El respaldo externo tiene como objetivo resolver contingencias graves que si necesitan el desplazamiento externo a sitios diferentes a los habituales, aplican cuando la gravedad de la contingencia impide que las soluciones de respaldo interno se pueden aplicar [22].

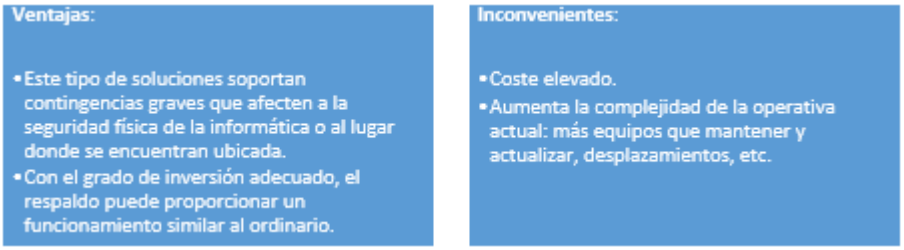


Figura 11 Ventajas e inconvenientes del respaldo interno.
Fuente: [22]**.**

1.5 Estado del Arte

Son algunos los trabajos realizados, ya sea a nivel regional o nacional, que guardan relación sobre el tema en cuestión, algunos se enfocan en el análisis

del riesgo, otros en cambio, presentan un manual o plan de contingencia de los activos y/o sistemas informáticos.

El primero se titula "Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar", desarrollado por De Freitas, Vidalina, éste tiene como objetivo el proponer estrategias que minimicen la ocurrencia de posibles amenazas a las están sometidos los activos de información que de la Dirección de Servicios Telemáticos de la Universidad Simón Bolívar (Caracas-Venezuela), basándose en los aspectos de seguridad física presentados en la Norma ISO-27001:2007; una vez efectuado el análisis y evaluación del riesgo, se propuso tratar o mitigar los riesgos encontrados en los siguientes activos de información: Servidores de correo y de Internet, demás Servidores empleados, Página Web y Servidores Intranet [8].

El segundo trabajo considerado se titula "Propuesta de un manual de contingencia informático para la U. T. C.", cuyos autores son: Claudio, Blanca & Chicaiza, Narcisa, tiene como objetivo proponer un plan de basado en el análisis de los riesgos a los cuales están expuestos los equipos, sistemas de informáticos y datos contenidos en los varios medios de almacenamiento, y así, reducir las vulnerabilidades y procedimientos a seguir en caso de algún incidente; finalmente los autores recomiendan redistribuir el equipo informático de acuerdo a las necesidades de las dependencias, proveer de una topología de la red de comunicaciones actualizada, establecer programas de capacitación tecnológica para el personal técnico y usuarios y planificar cronogramas de actualización tecnológica, entre otras [1].

Asimismo, se toma en consideración el trabajo titulado "Diseño de un plan de contingencias del TICs para la Empresa Eléctrica Centrosur" presentado por Granda, Andrea, cuyo fin es proporcionar una solución estructurada que permita mantener operativas las funciones esenciales cuando una contingencia afecte la infraestructura TI, para lograrlo se determinan acciones preventivas que reducen el grado de vulnerabilidad y exposición al riesgo, así como se dimensiona el riesgo potencial y la toma de decisiones ante fallas; además, exhorta a tomar conciencia de que los siniestros.) pueden realmente

ocurrir, y se debe tomar con gran responsabilidad un plan de contingencia, dada la importancia que se otorga a la Seguridad Institucional, y en un futuro la propuesta de un plan de continuidad [23].

Finalmente, el cuarto trabajo considerado se denomina “Plan de contingencia de los equipos y sistemas informáticos en el Gobierno Autónomo Descentralizado Municipal del cantón Junín”, que tiene como meta el elaborar un plan de contingencia para proteger los equipos y sistemas informáticos, con el fin de precautelar la información, y los componentes físicos y lógicos; las conclusiones y/o recomendaciones generadas en dicho documento, puntualizan que al contar con esta herramienta le permitirá recuperarse ante las fallas o siniestros ocasionados por factores internos o externos, además, indica que es necesario invertir en seguridad informática , destinando recursos económicos para salvaguardar la información, ya que en caso de no hacerlo corre riesgo de que se materialice alguna amenaza [22].

1.6 Conclusiones Capítulo I

Los planes de contingencia para servicios informáticos se centran en el desarrollo de actividades que eviten o minimicen el impacto de una contingencia, y permitan recuperar los servicios informáticos y/o tecnológicos dañados por algún contingente; para este caso se considerarán los lineamientos de las Normas ISO 27001, 27002, 27005 y 31000, además, la metodología MAGERIT para el análisis del riesgo, así como la herramienta PILAR, que servirán de apoyo para la gestión y tratamiento de los riesgos como tales.

CAPÍTULO II. PROPUESTA

2.1 Diagnóstico del problema

2.1.1 Generalidades

La Junta administradora de agua potable Pilacoto (JAAP Pilacoto), entidad avalada por la Secretaria del Agua (SENAGUA), se localiza en la provincia de Cotopaxi, cantón Latacunga, parroquia Guaytacama, barrio del mismo nombre, actualmente está bajo la administración de su presidente, Luis Javier Casa, tiene como actividad principal la ejecución de programas o/o sistemas de suministro de agua, y cuenta con un total de 756 socios.

A continuación, se presenta el organigrama estructural de la JAAP Pilacoto:

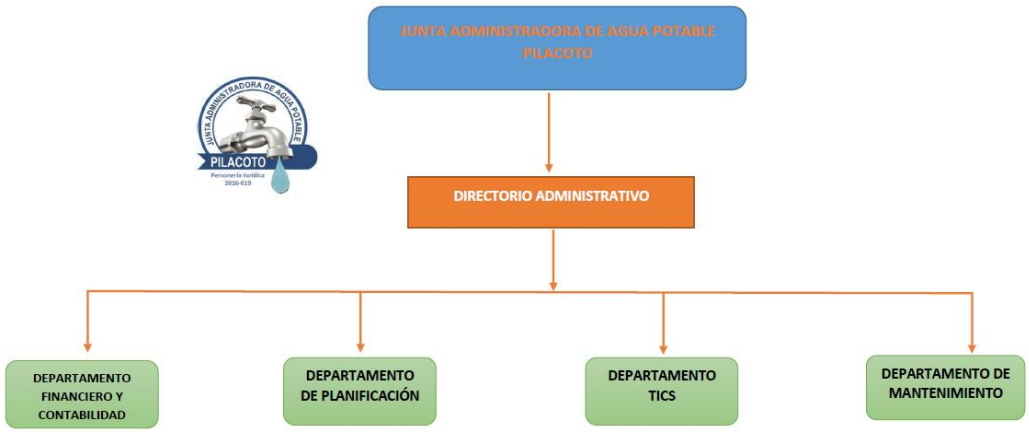


Figura 12 Organigrama JAAP Pilacoto
Fuente: [24]

Específicamente, la JAAP Pilacoto está compuesta por las siguientes personas:

NOMBRE	CARGO
GUALPA CASA BLANCA JEANETH	RECAUDADORA MATRIZ
GUAITA QUILUMBA SEGUNDO DANIEL	OPERADOR MATRIZ
SILVA VASQUEZ MIGUEL ANGEL	SISTEMAS CIS.
CEVALLOS LOZADA DAMIAN ANDRES	CONTADOR
GUALPA CASA BLANCA JEANETH	RECAUDADORA SAN SEBASTIAN
GUALPA CASA BLANCA JEANETH	RECAUDADORA SAN PEDRO
GUAITA QUILUMBA SEGUNDO DANIEL	OPERADOR SAN SEBASTIAN
GUAITA QUILUMBA SEGUNDO DANIEL	OPERADOR SAN PEDRO

Figura 13 Estructura Departamento TICS
Fuente: [24]

2.1.2 Activos

Tabla 1 Activos de Hardware

HARDWARE	
Cantidad	Descripción
1	Equipo de amplificación (2 parlantes, 1 mini consola y 2 trípodes)
3	Micrófono
1	Teléfono
1	Calculadora eléctrica
1	Cámara
2	Celular
1	Reloj biométrico
1	Proyector
1	Kit de cámaras de seguridad (4 cámaras)
1	GPS
12	**Regulador de voltaje modelo**
1	**Módem (Internet)**
12	**Computadora (incluida 1 que hace de Servidor)**
3	**Impresora**
3	**Switch**

Elaborado por: Autor

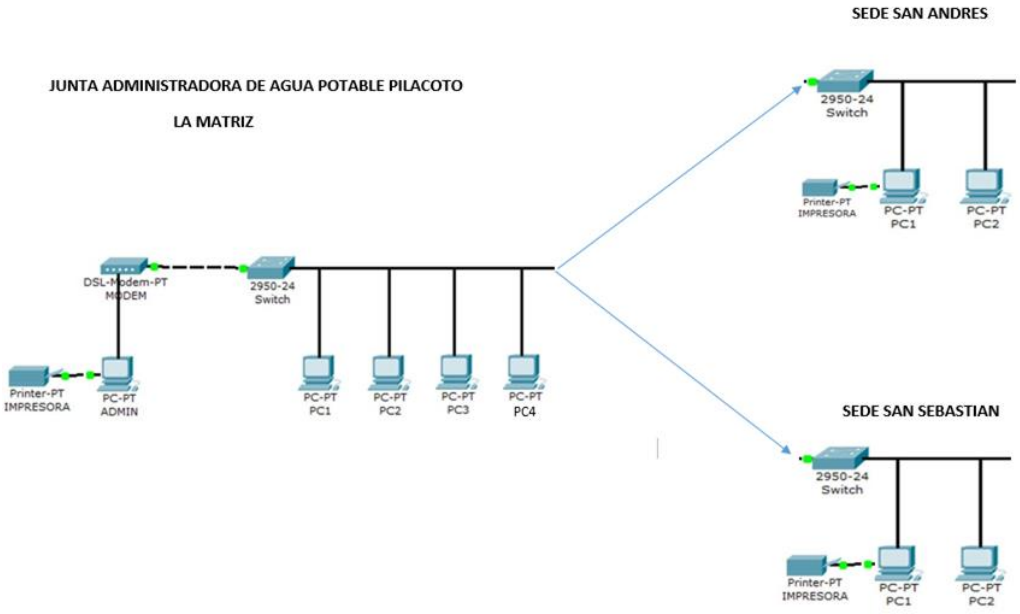


Figura 14 Red JAAP Pilacoto
Elaborado por: Autor

Tabla 2 Activos de Software

SOFTWARE	
Cantidad	Descripción
1	Programa de contabilidad SIBACF
9	Programas de Ofimática

Elaborado por: Autor

Tabla 3 Seguridad informática

SEGURIDAD INFORMÁTICA	
Cantidad	Descripción
12	Claves de usuarios
1	Respaldo en disco duro

Elaborado por: Autor

Cabe indicar que la JAAP Pilacoto carece de:

- Otros programas, a excepción de los programas regulares de ofimática.
- Correo institucional.
- Y, sobre todo de políticas, lineamientos, procesos y/o manuales de toda índole, incluidos los relacionados al riesgo como tal.

2.1.3 Situación actual

Tal y como se indica en el epígrafe anterior, la Junta de Pilacoto, no posee mecanismos de control de los sistemas de información, y lamentablemente no cuentan un estudio sobre el impacto en caso de desastres, ataques o incidentes, más aún considerando que se encuentran ubicados en una zona de riesgo del Volcán Cotopaxi, y que, debido a la falta de seguridades, en cualquier momento pueden verse afectados por algún ataque cibernético; debido a lo cual es imprescindible la gestión de riesgos y a la vez la propuesta de un plan de continuidad para los sistemas informáticos empleados en la JAAP Pilacoto.

Por tal razón, en un principio en base a la fundamentación teórica y metodológica de Magerit, se ejecuta un análisis de riesgos en la herramienta Pilar, que permitan determinar en base a los activos más importante determinar lo puntos críticos más sobresalientes en la seguridad de la

información para la Junta Administradora de Agua Potable de Pilacoto, y de igual manera los controles de seguridad de la información más críticos, en base a los cuales se presentará el plan de contingencia más acoplado a la realidad de la Junta y que permita palear cualquier desastre que se presente.

2.2 Métodos específicos de la especialidad a emplear en la investigación

Con respecto a los métodos específicos a emplear en la investigación, éstos se dividen en tres componentes, tal y como se muestra en la figura.

Figura 15 Métodos específicos
Elaborado por: Autor

El primero se centra en el uso de la metodología Magerit para el análisis y/o gestión de riesgos propiamente dicha; el segundo es relativo a la validación de la propuesta mediante el método de campo, usando la técnica de la encuesta, aplicada a través de dos cuestionarios, uno para empleados y otro para los usuarios; y el tercero relacionado con la ejecución de la auditoría informática, igualmente aplicando el método de campo, pero esta vez usando la técnica de la entrevista, gracias a un cuestionario semiestructurado, aplicado al Presidente de la Junta, pero especialmente al encargado de Tics de la misma.

2.3 Diseño experimental y/o método de criterio de experto para validar la propuesta

El criterio o juicio de expertos tiene como objetivo el encontrar un consenso entre la opinión de un conjunto de expertos sobre un tema en particular. Uno de los métodos para aplicarlo es el Método Delphi, el cual consiste en el envío de cuestionarios a expertos con información del proyecto, a quienes se les requiere que determinen una puntuación a cada afirmación mostrada.

Para esto, se emplea el método Delphi, el cual se centra básicamente en las siguientes fases:

- Formulación del problema: En esta fase se define con precisión el área de investigación, para así determinar con acierto el perfil de los expertos requeridos y las preguntas a realizar.
- Elección de expertos: Se selecciona los expertos por su amplio conocimiento en el campo correspondiente, particularidad que garantizará la seguridad de la validación.
- Elaboración y lanzamiento del cuestionario: El cuestionario se elabora de tal manera que facilite a los expertos su análisis, quienes podrán responder de modo que los datos puedan ser cuantificados.
- Desarrollo práctico y explotación de resultados: Se remite el cuestionario por correo electrónico a los expertos, el mismo que a más de contener una breve la descripción del método Delphi, presenta cuestionamientos que permitan determinar si existe consenso y, por ende, si es factible y viable implantar la metodología, la herramienta y el plan de contingencia propuesto para el análisis y manejo de riesgos en la JAAP Pilacoto y su prevención.

2.4 Descripción metodológica de la valoración económica, tecnológica, operacional, y medioambiental de la propuesta

Entre los factores de impactos que se consideran en cada una de las valoraciones correspondientes, tienen como eje principal la filosofía institucional, así como las normas, políticas y procedimientos internos que son aplicados en la JAAP Pilacoto, además sus miembros han demostrado una clara predisposición para su la implantación, tanto de la sugerencia de gestión del riesgo por medio de la herramienta Pilar, así como de la aplicación de las políticas de recuperación y el plan de contingencia a proponer.

Específicamente respecto a los factores a tomar en cuenta para la valoración económica, por un lado, se deberán considerar por un lado los costos de los recursos informáticos que actualmente posee la JAAP Pilacoto, tanto en su matriz como en sus dos sedes, y por el otro, los costos o mejor llamado el presupuesto de la propuesta a realizar.

Por el momento, en relación a los factores relacionados con el impacto tecnológico y operativo, los cuales para este caso van de la mano, corresponden con las capacidades del capital humano para el uso de la herramienta Pilar, e igualmente para la puesta en marcha de las políticas y de ser el caso el plan en caso de materialización de una amenaza, ya sea física, virtual o natural, ya que se contaría con el software y hardware necesario para su implantación; por esta razón, es importante la capacitación por parte del Autor del presente trabajo al Encargado de Tics de la Junta en mención, para que sea capaz de mantener un entorno informático operativo en caso de desastre.

En último lugar, sobre los factores referentes al impacto medioambiental, en este caso, debido al tema desarrollado, éste no implica ningún tipo de afectación en tal sentido, por lo que simplemente no se consideran ningún elemento de impacto.

2.5 Propuesta (Gestión, Políticas y Plan de contingencia)

2.5.1 Gestión de riesgos (ISO 27001 & 31000 - MAGERIT - PILAR)

Para el análisis y gestión de riesgos se toma como base la metodología MAGERIT, la cual se apoya en la herramienta PILAR, que permite realizarlos de forma eficiente y eficaz.

En tal sentido, para realizar el análisis de riesgos se plantean el desarrollo de las siguientes etapas:

- Etapa 1: Determinar los activos más importantes para la JAAP Pilacoto
- Etapa 2: Determinar las amenazas a las que están expuestos dichos activos
- Etapa 4: Evaluar el impacto de la materialización dichas amenazas
- Etapa 3: Evaluar el riesgo según la probabilidad de ocurrencia de la amenaza.

Así, para iniciar se determina los activos más importantes, los cuales serán ingresados en la herramienta Pilar para proceder con el análisis correspondiente. Cabe mencionar que todos los activos están en el mismo dominio de seguridad (default) en Pilar, por lo que los requisitos de seguridad son los máximos en cada dimensión de seguridad.

Tabla 4 Activos

Activos	Software	Sistemas de información	SIBACF (Contabilidad)
	Hardware	Servidor	1 PC Admin
		Estaciones de trabajo	2 PC Sedes
		Switch	3
		Módem	1
	Infraestructura	Instalaciones	Matriz y 2 Sedes
	Datos	Respaldos BDD, Documentos, Registros	

Elaborado por: Autor

Cabe destacar que, Pilar automáticamente aplica un perfil de ataque y elabora un mapa de riesgos; además aplica un perfil de seguridad; en base a esto, se obtuvo los siguientes resultados:

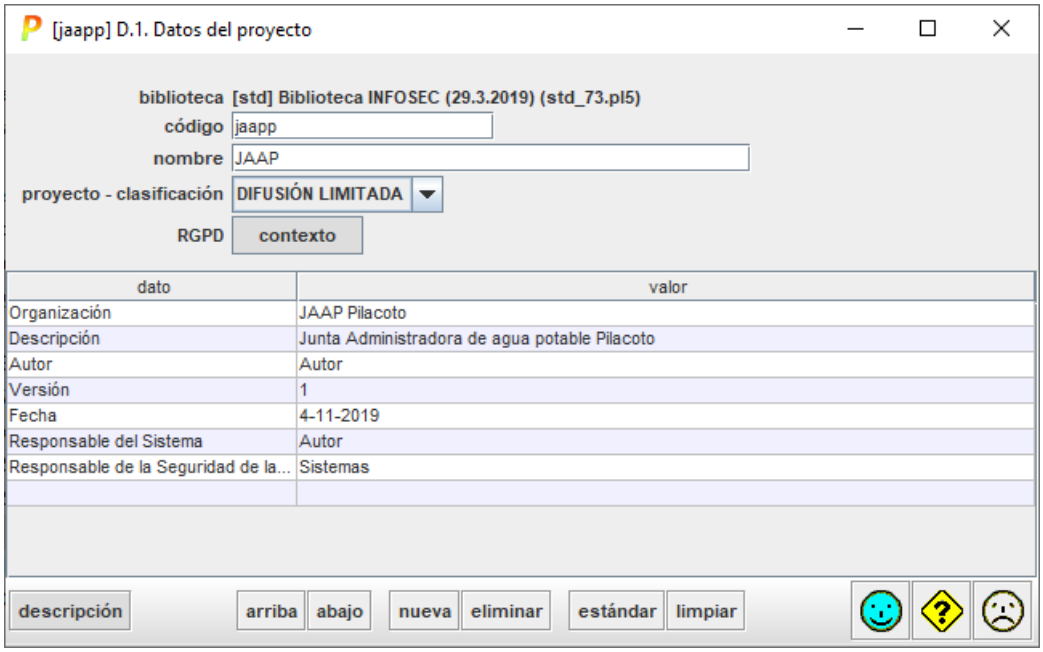


Figura 16 Datos del proyecto
Fuente: [25]
Elaborado por: Autor

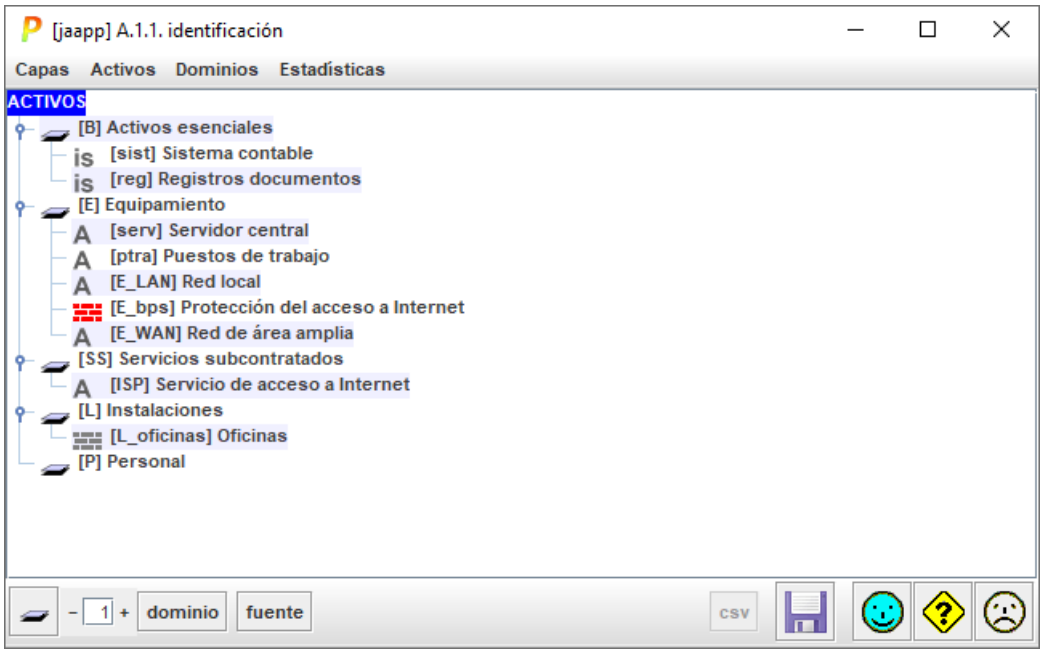


Figura 17 Identificación de activos
Fuente: [25]
Elaborado por: Autor

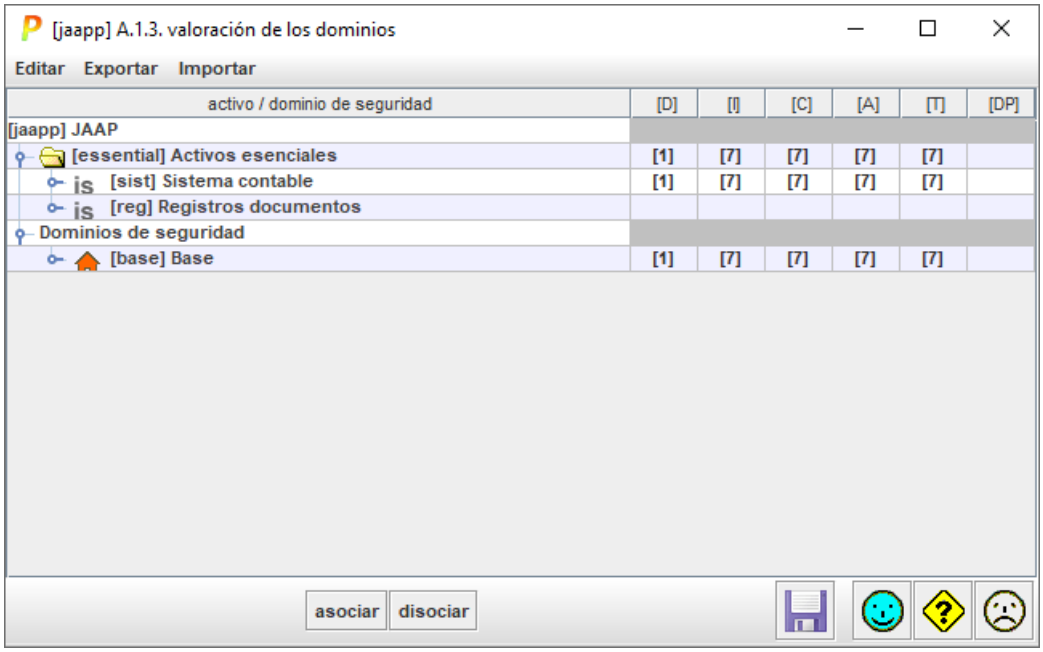


Figura 18 Valoración de dominios
Fuente: [25]
Elaborado por: Autor

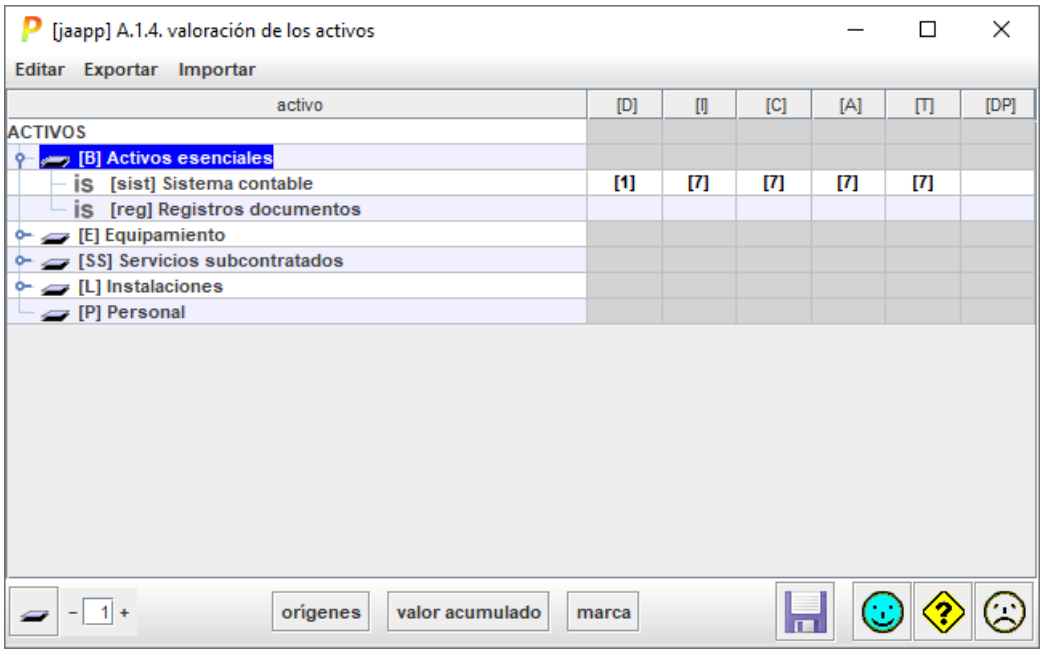


Figura 19 Valoración de activos esenciales
Fuente: [25]
Elaborado por: Autor

Considerando tabla valoración manejada por MAGERIT la cual se adjunta a continuación, el sistema contable se encasilla en un daño importante y los registros (documentos administrativos), en daño grave.

Tabla 5 Escala de valoración de activos

Valoración		
10	extremo	daño extremadamente grave
9	muy alto	daño muy grande
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor

Elaborado por: Autor

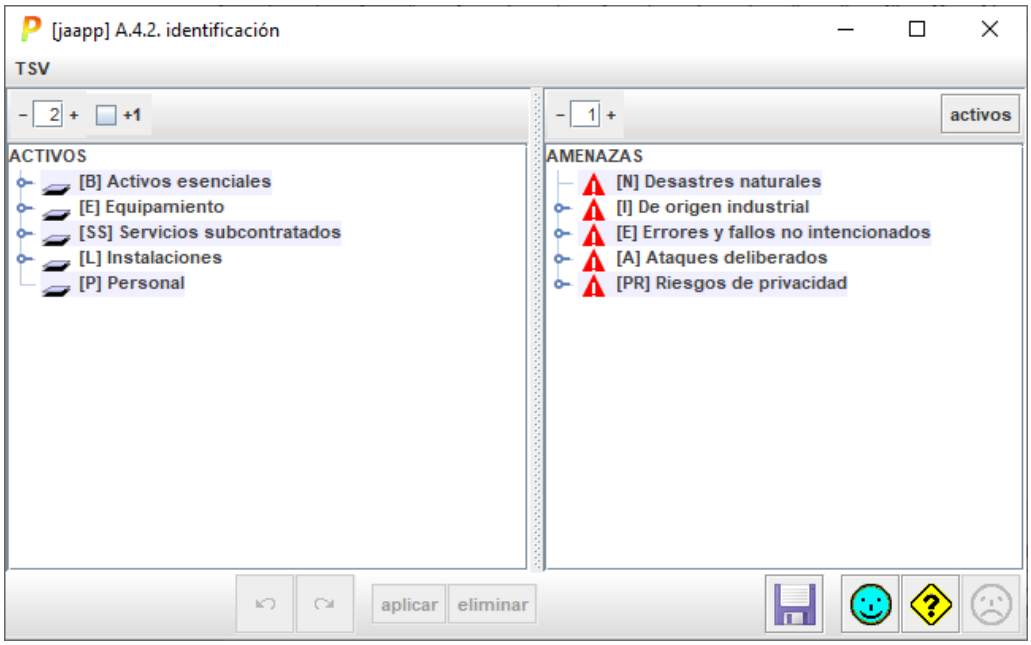


Figura 20 Identificación de amenazas (default)
Fuente: [25]
Elaborado por: Autor

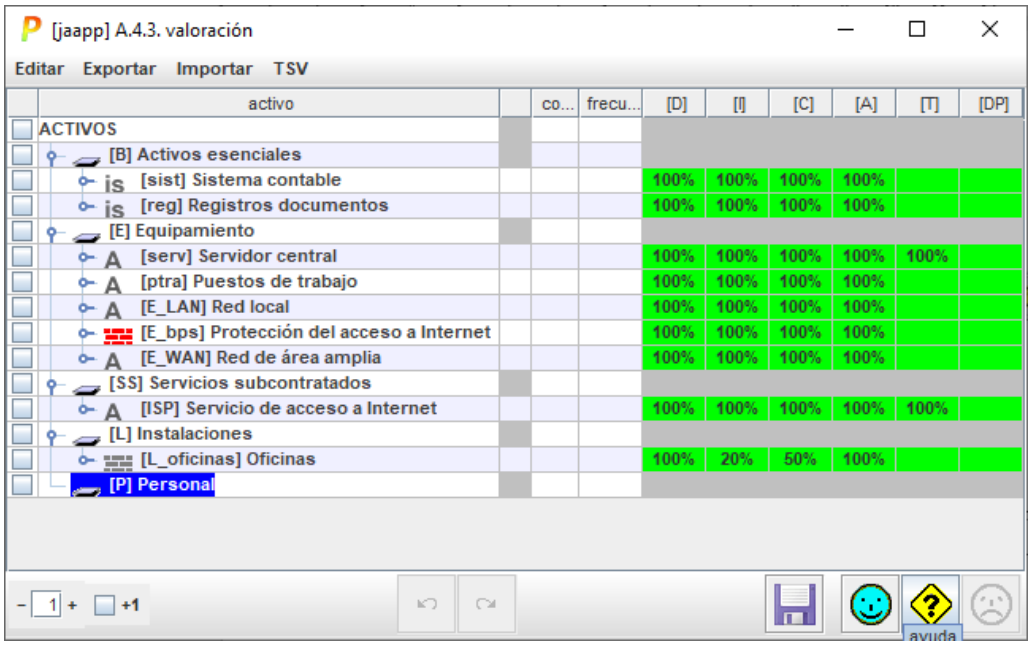


Figura 21 Valoración de amenazas
Fuente: [25]

Elaborado por: Autor

Para la valoración de las amenazas se consideran los siguientes criterios: disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y privacidad.

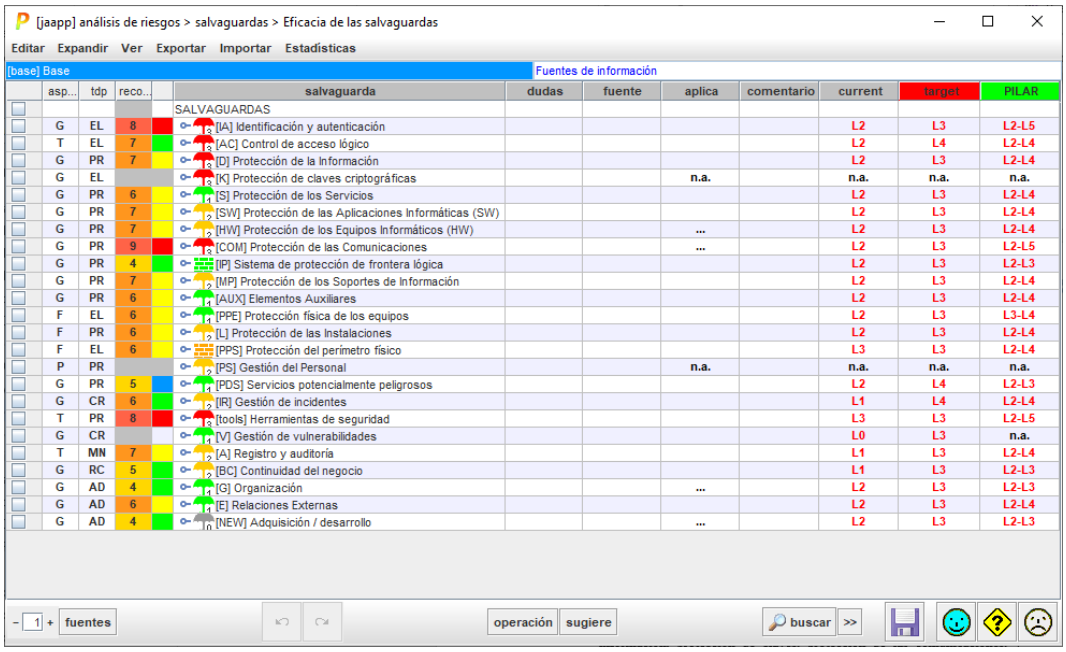


Figura 22 Valoración de la seguridad de la información
Fuente: [25]
Elaborado por: Autor

Contemplando que para la eficacia de las salvaguardas se considera la siguiente escala:

Tabla 6 Escala de valoración de efectividad

Valoración de la Efectividad	
L0	0%
L1	10%
L2	50%
L3	90%
L4	95%
L5	100%

Elaborado por: Autor

Se deprende que, los puntos críticos en la seguridad de la información son: identificación y autenticación, protección de las comunicaciones, y herramientas de seguridad.

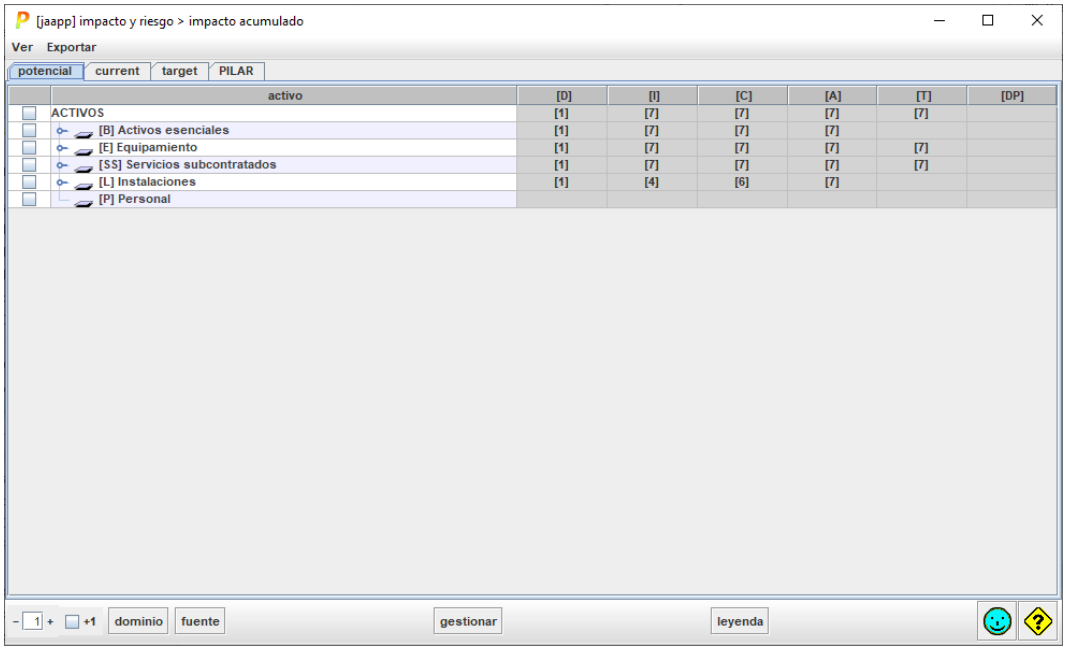


Figura 23 Impacto acumulado desde el punto de vista técnico
Fuente: [25]
Elaborado por: Autor

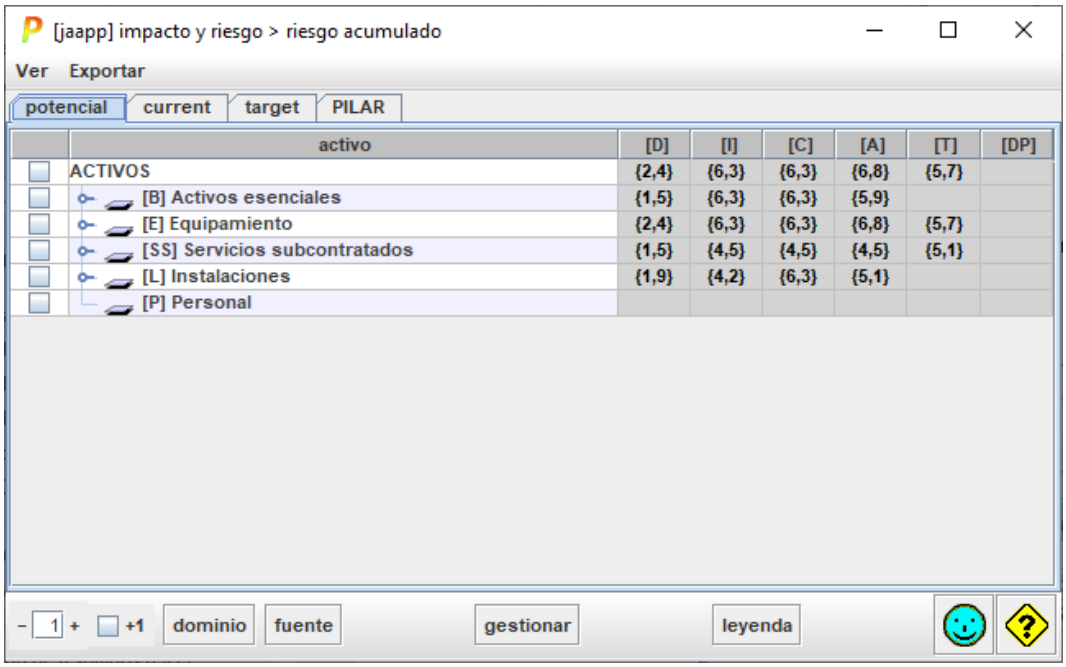


Figura 24 Riesgo acumulado desde el punto de vista técnico
Fuente: [25]
Elaborado por: Autor

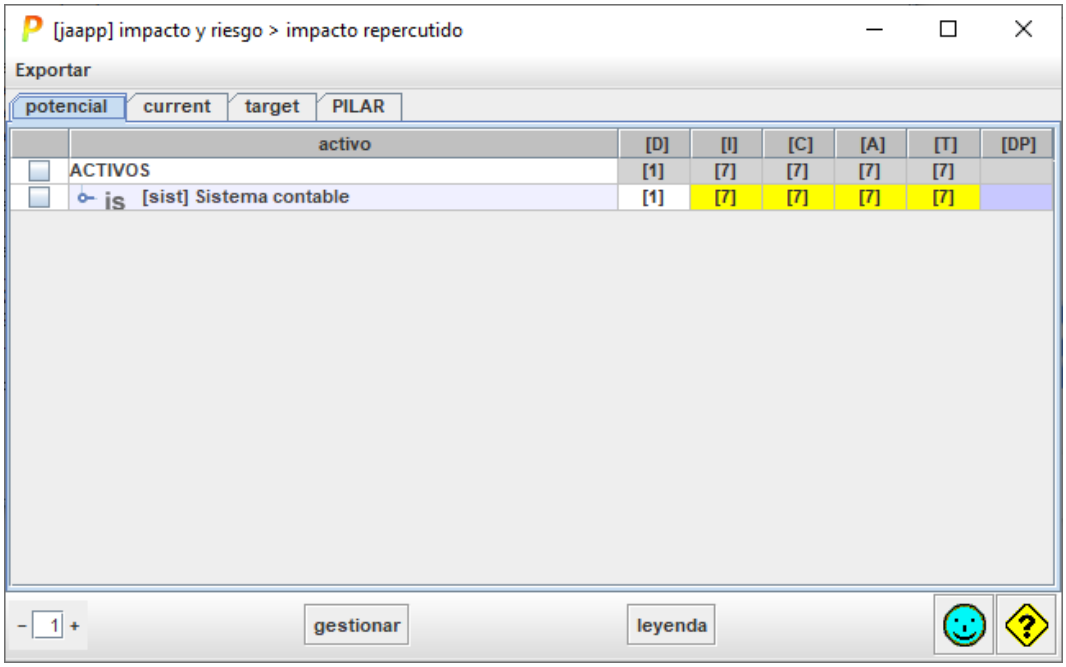


Figura 25 Impacto repercutido desde el punto de vista del negocio
Fuente: [25]
Elaborado por: Autor

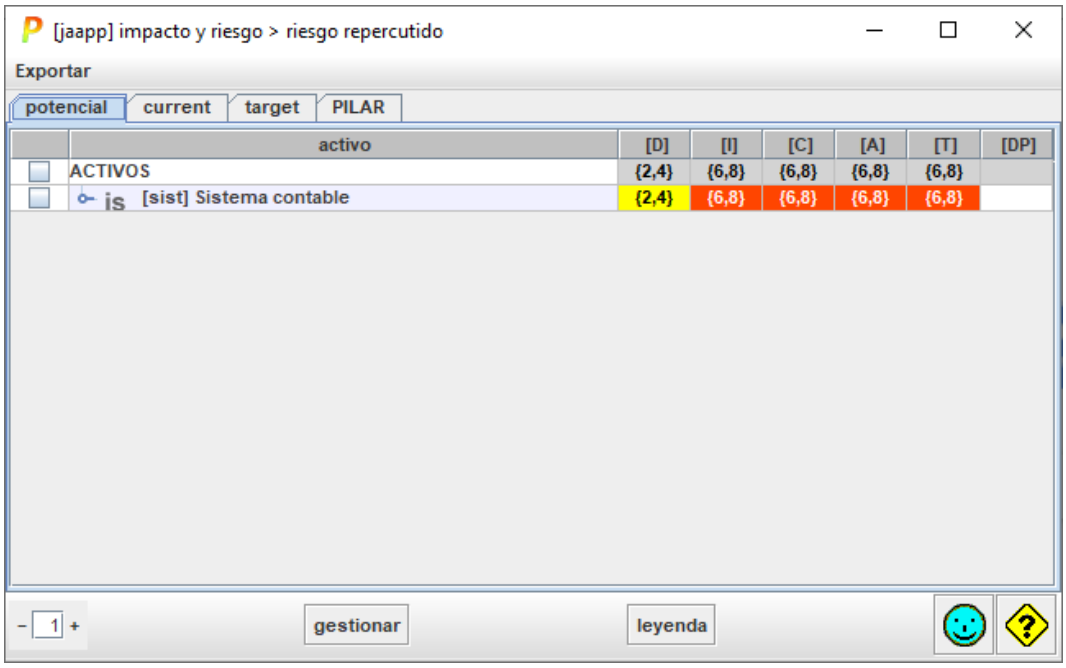


Figura 26 Riesgo repercutido desde el punto de vista del negocio
Fuente: [25]
Elaborado por: Autor

La madurez evaluada respecto al riesgo, el cual como se aprecia actualmente es intermedio, está por encima del riesgo sin salvaguardas, pero por debajo del nivel óptimo, una vez aplicado el plan de contingencia respectivo.

Finalmente, se presenta la valoración para los controles de seguridad de la información, como se observa los más críticos son: organización interna de la seguridad de la información, manipulación de los soportes, gestión de archivos de usuario, responsabilidades de usuario, protección contra su software malicioso, copias de seguridad, registros y supervisión, control del software en exploración, y gestión de la seguridad de redes.

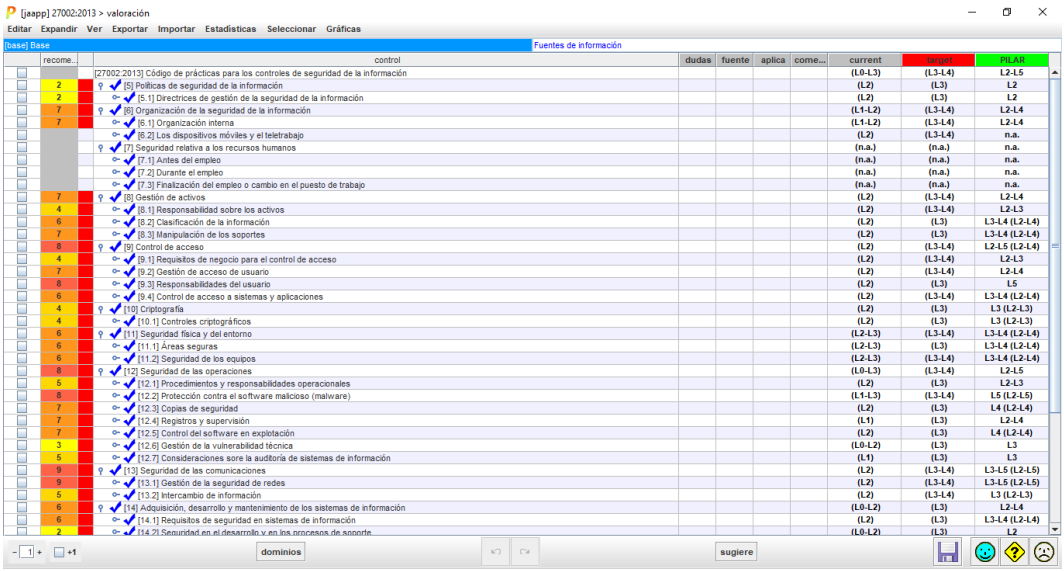


Figura 27 Valoración para los controles de seguridad de la información 1
Fuente: [25]
Elaborado por: Autor

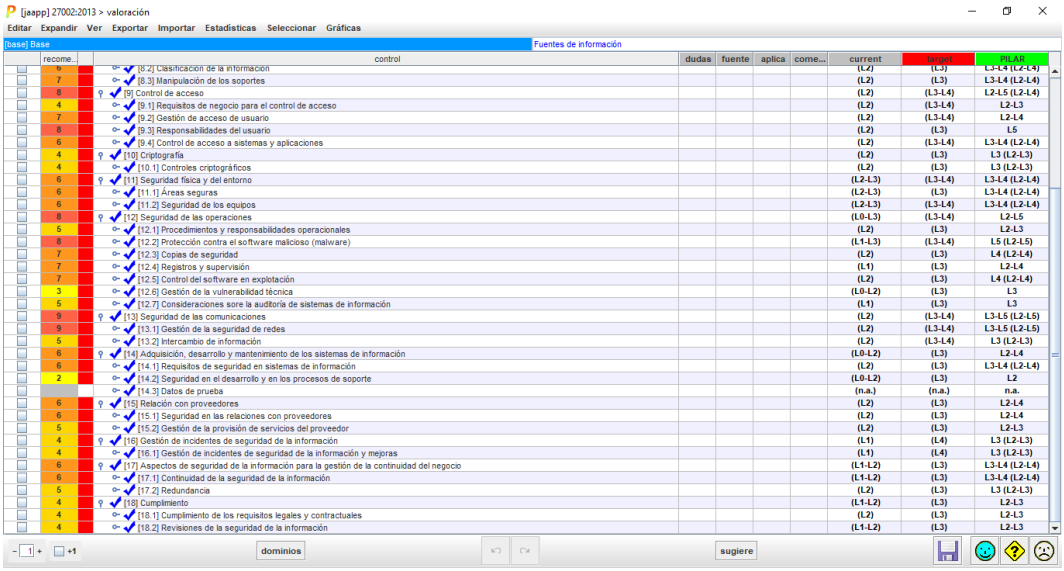


Figura 28 Valoración para los controles de seguridad de la información 2
Fuente: [25]
Elaborado por: Autor

2.5.2 Gestión de respaldos (ISO 27001)

Actividades a considerar:

- Identificar la información de la que se va a realizar backups.
- Seleccionar medios adecuados para guardar los backups.
- Mantener respaldos en medios físicos y virtuales que serán manejados solo por el encargado de Sistemas CIS.
- Los medios físicos deberán ser guardados en una caja de seguridad.
- Verificar el estado óptimo de backups.
- Elaborar un inventario de los respaldos de información, y mantenerlo actualizado, con apoyo de una bitácora de respaldos.
- Realizar backups diarios de información sensible en un disco duro externo
- Realizar backups semanales de otro tipo de información en un disco duro externo
- Realizar un backup mensual de toda la información en la nube
- Realizar revisiones de los backups antiguos y eliminar los que tienen más de 3 meses de antigüedad.

2.5.3 Políticas y estrategias de recuperación por factores naturales y tecnológicos -físicos y virtuales-) (ISO 27002 &31000)

Teniendo en cuenta los resultados arrojados por la herramienta PILAR, las políticas y estrategias deben estar focalizadas en los siguientes aspectos: organización interna de la seguridad de la información, manipulación de los soportes, áreas seguras, protección contra su software malicioso, copias de seguridad, control del software en exploración, y gestión de la seguridad de redes.

A continuación, se enuncian los lineamientos a tomar en cuenta:

- Organización interna de la seguridad de la información
    - Formalizar procedimientos de operación (Manuales)

    - Normalizar la gestión de cambios
    - Restringir el acceso al área de trabajo y a los equipos informáticos, mediante claves de seguridad.
- Manipulación de los soportes (comunicaciones y operaciones)
    - Realizar mantenimientos preventivos y correctivos a los equipos informáticos, incluido el servidor y la red, con una periocidad de mínimo 3 meses
    - Proporcionar la capacidad adecuada a los equipos informáticos para la realización adecuada de las operaciones.
    - De ser necesario, adquirir equipos nuevos o actualizar los existentes.
- Áreas seguras
    - Implementar un sistema de control de acceso a las oficinas de la Junta
    - Implementar un sistema contra incendios
    - Contar con un sistema de vigilancia que permita monitorear e identificar posibles sospechosos que deseen atentar con la integridad del personal, los equipos, y la infraestructura
    - Contratar seguros para los equipos informáticos
    - Crear alianzas estratégicas con otras entidades en ubicaciones diferentes, para que, en caso de un siniestro mayor, continuar con las operaciones de la JAAP Pilacoto en dicha ubicación.
- Protección contra su software malicioso
    - Combinar medidas tecnológicas (firewall, antivirus, antimalware, etc.), con medidas educativas (concienciación y formación sobre las medidas tecnológicas y buenas prácticas de prevención)
    - Realizar revisiones periódicas del contenido de los equipos, además de programas y/o de datos de los registros y del sistema contable y así identificar archivos no aprobados o alteraciones no autorizadas

- Prohibir la instalación de programas sin el respectivo permiso del responsable de Sistemas CIS.

- Copias de seguridad
  - Formalizar y normalizar los procedimientos de respaldo
- Control del software en exploración
  - Instalar sistemas en producción, no en pruebas
- Gestión de la seguridad de redes
  - Aplicar los controles esenciales para salvaguardar la integridad y confidencialidad de los datos mediante la red local o inalámbrica
  - El cableado, la red eléctrica y de telecomunicaciones deben estar ocultos, para evitar daños por manipulación.
  - Solo el personal autorizado puede manipular algún componente de la red, lo mismo se aplica para cualquier mantenimiento que se realice.

2.5.4 Roles y responsabilidades

Debido a que la JAAP Pilacoto es una entidad que maneja un bajo volumen de información y que cuenta con el personal estrictamente necesario para su operación, el responsable de socializar y ejecutar el presente plan será la persona encargada de Sistemas CIS.

2.5.5 Plan de contingencia (Manual de procedimientos)

2.5.5.1 Objetivo

Permitir la reanudación de las operaciones de la Junta Administradora de agua Pilacoto, específicamente de su sistema informático, luego de presentarse una contingencia o siniestro.

2.5.5.2 Alcance

Abarca el procedimiento de reanudación para los equipos informáticos y el sistema contable actualmente manejado, mediante la ejecución de procedimientos concretos en caso de interrupción de operaciones, debido a la materialización de amenazas informáticas y/o físicas, tanto en la matriz, en sus dos extensiones.

2.5.5.3 Normas y metodología usadas

- ISO 27001:2013
- ISO 27002:2013
- ISO/ 27005:2018
- ISO 31000:2018
- Metodología Magerit

2.5.5.4 Responsables

- Presidente de la Junta: Responsable de la aprobación y socialización del plan de contingencia, así como de proveer los recursos necesarios para ejecutarlo
- Personal de Sistemas: Responsable de la ejecución de acciones pre preventivas, así como de las correctivas, en caso de una contingencia en los sistemas informáticos.

2.5.5.5 Plan previo a la recuperación

Una vez materializado el siniestro o la contingencia que afectó a los sistemas informáticos y/o a las instalaciones en las que estos se encuentran, en primera instancia se debe evaluar el título daño ocasionado a los activos esenciales. Posteriormente se debe determinar si estos son recuperables considerando tanto el hardware como el software de los mismos, si se determina su recuperación pequeños ajustes se debe proceder con el plan de recuperación como tal, pero si por el contrario no son recuperables, en primera instancia se debe recurrir por un lado a los acreedores para obtener equipo informático nuevo y la nueva instalación del sistema contable y posteriormente ejecutar el plan de recuperación y básicamente se centra en la configuración de éstos y la subida de los respaldos respectivos.

2.5.5.6 Plan de respaldo

Se deben seguir las acciones propuestas en el apartado gestión de respaldo, así como las políticas y estrategias de recuperación concernientes a los respaldos como tales.

2.5.5.7 Plan de recuperación

1. Evaluar si la oficina es segura para la reanudación de las actividades.
2. Determinar las pérdidas físicas y lógicas de los equipos e información.
3. Proceder con la respectiva configuración de los equipos, en caso de ser necesario.
4. Realizar el inmediato restablecimiento de los respaldos de información.
5. Efectuar la restauración de la base de datos, sistema de información respaldada.

6. Notificar al personal de la Junta sobre el estado de los equipos e información y el procedimiento realizado.
7. Ejecutar la notificación a los usuarios en el momento de que los sistemas informáticos se puedan volver a utilizar.

Tal y como se mencionó anteriormente, en caso de que un desastre o daño mayor afecte no sólo los sistemas informáticos, sino también las instalaciones de la Junta y haga inhabitable este lugar, se deberá inmediatamente proceder con la compra de nuevos equipos, así como el contacto con proveedores para lograr reanudar operaciones lo más pronto posible en un nuevo lugar destinado por el Presidente de la entidad.

2.5.5.8 Plan posterior a la recuperación

Una vez lograda la puesta en marcha de los activos y los sistemas informáticos y de comunicación, el responsable del sistema deberá generar un informe de lo ocurrido y de las acciones ejecutadas para la recuperación de los mismos; dicho informe deberá ser aprobado por el Presidente de la Junta.

Posteriormente, deberá ser socializado en una reunión que involucre tanto a todo el personal que trabaja tanto en la Matriz con sus dos extensiones, para así no solo dar a conocer de lo ejecutado, sino también, generar una retroalimentación que permita validar y mejorar el plan de contingencia como tal.

Seguidamente, se revisarán los manuales de procesos, las políticas y estrategias que como medida preventiva debían ser implementadas y ajustarlos a la nueva realidad de la Junta.

2.6 Conclusiones Capítulo II

La implementación del plan consistirá en la ejecución de las recomendaciones y los procedimientos establecidos en el análisis de riesgos que conjuntamente con las políticas y estrategias apropiadas, minimizarán el impacto de las amenazas y por ende el riesgo propiamente dicho, identificado en el análisis correspondiente.

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 (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.

También se debe indicar que, la propuesta planteada, puede sin ningún inconveniente ser aplicada en las demás Juntas Administradoras de Agua potable.

La metodología a aplicar, la cual básicamente consta de la metodología técnica, que se usará en el análisis de riesgos, y la que se empleará para la validación propuesta, abarcan por un lado el método Magerit, y por el otro el método de campo con aplicación de encuestas y entrevistas, permitirán determinar si la propuesta en cuestión es viable para aplicarla en la Junta administradora de agua Pilacoto.

CAPÍTULO III. APLICACIÓN Y/O VALIDACIÓN DE LA PROPUESTA

3.1 Resultados del diagnóstico del problema realizado

Es relevante mencionar, al igual que se lo hizo en el capítulo anterior, la JAAP Pilacoto solo maneja un sistema informático, claro está a más de los programas ofimáticos empleados tanto en su matriz como en sus sedes, dicho programa, es el **programa contable SIBACF**, que es usado para contabilidad como para la facturación y el SRI, el cual se consideró como activo vital en el análisis realizado en la herramienta Pilar.

Sobre la **Auditoría informática** realizada por el Autor a la JAAP Pilacoto, cabe mencionar que se siguieron los siguientes pasos:

1. Primero se realizó una visita a la Junta administradora de agua potable Pilacoto, con el fin de pedir autorización a los miembros de esta institución para llevar a cabo la auditoría al Departamento de Tics que se encuentra en el JAAP.
2. Se realizó una plática informal en donde se obtuvo datos sobre las condiciones en la que se encuentra el Departamento de Tics y su infraestructura.
3. Se realizó una entrevista formal al presidente de la Junta y al encargado del área de TICS, para ello fueron utilizadas las preguntas necesarias de auditoría que involucraron los siguientes aspectos:
   a) Incidentes anteriores
   b) Infraestructura
   c) Evaluación del entorno

d) Mobiliario y equipo
e) Hardware
f) Software
g) Seguridad física

De esto, se obtuvieron los siguientes resultados:

Incidentes que sucedieron en el JAAP en el aspecto tecnológico:

- Pérdida de software y hardware en los periodos 2009-2010
- Pérdidas de los aparatos electrónicos como discos externos donde contenían información administrativa y tecnológica del JAAP
- Pérdida de información de la base de datos contable JAAP
- Manipulación de registros informáticos en la base de datos contable del JAAP
- No registro de las compras de los aparatos tecnológicos para el departamento de TICS como Switch, Cables de Red, Discos duros etc.

Infraestructura: Según lo manifestado por el encargado de Tics, no tienen una buena infraestructura, debido a que en el año 2015 sufrieron grandes daños tecnológicos por la emanación de la ceniza del volcán Cotopaxi, incluso pérdida de servidores, computadoras averiadas, instalaciones de red en mal estado, y la no ventilación del cuarto de Tics.

Evaluación del entorno: Se supo que todos estos aspectos son muy incómodos dentro del entorno, ya que es una institución muy pequeña para los Departamentos como TICS, Administrativos, Contabilidad, Recursos Humanos y Atención al Cliente, y no cuentan con las normas necesarias para un buen funcionamiento de esta institución.

Mobiliario y Equipo: Si es adecuado el equipo de cómputo para el manejo administrativo y de Tics, pero no existen repuestos para el mantenimiento y/o reemplazo del equipo, y aunque existen lugares específicos para aparatos electrónicos, guardar papelería y herramientas (bodega), la misma no está adecuada para cada uno de los departamentos. Igualmente, no disponen de licencias de seguridad las máquinas de la institución, los sistemas operativos

tampoco tienen licencias actualizadas, y se evidenció que los usuarios no tienen contraseñas. En relación a los CPU, el teclado y más, son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida, y éstos no cuentan con un inventario de aparatos electrónicos y hay pérdida de cables de poder, pérdida de ratones, teclados, flash memories; además los aparatos electrónicos no cuentan con un soporte adecuado para el manejo ideal de estos. También se encontraron varias dificultades como equipos sin renovación de garantía, sin mantenimiento adecuado en el tiempo establecido, equipos que están utilizando sin fines a la necesidad de la institución. Respecto al licenciamiento y la facturación del software, estos están caducados, se tuvo, además, la instalación innecesaria de programas, igualmente carecen de programas esenciales para el manejo de la página web y sus componentes, tampoco hay actualización del software del servidor central y del programa contable de la institución.

Seguridad: En general, no existe una vigilancia exhaustiva que permite salvaguardar los recursos tecnológicos como las instalaciones, ni controles preventivos y de riesgo. Otro de los problemas en la institución es que no cuenta con un personal adecuado para la administración de la red de datos, existe personal de sistemas, pero no un administrador de red que opere los servicios que están configurados en ella. También se ha detectado que los empleados de la red tienen el mismo nivel de acceso a la información y a los servicios, y se han ocasionado problemas tales como: caídas frecuentes del servicio de internet, el sistema operativo de red no está actualizado, los dispositivos de red están obsoletos y en general no existe mantenimiento sobre la red de datos de la institución. Tampoco existen políticas y procedimientos de seguridad o sistemas de control informático que ayuden a mitigar las vulnerabilidades y amenazas que se podrían presentar. Otros aspectos en cuanto a la seguridad de la información que no se presentan en la institución son es que no existe reguardo de la seguridad de los activos de información, políticas sobre los controles de acceso a los sistemas de información, ni tampoco una gestión ante incidentes en la seguridad de la información y gestión de la seguridad en la red.

Respaldos: Uno de los aspectos más importantes que se encontró es que semanalmente se guarda información de los servidores en un medio de almacenamiento como un disco externo.

De esta manera, el problema identificado inicialmente relacionado con el tema de este estudio, se centra en la falta de mecanismos de control de los sistemas de información que ayuden a determinar el impacto en caso de desastres, ataques o incidentes, lo que no permite gestionar la prevención y la recuperación de los servicios informáticos y/o tecnológicos en caso de ocurrencia.

Por esta razón, primeramente, se procedió a gestionar los riesgos y el impacto de los mismos, determinando que los puntos críticos más sobresalientes en la seguridad de la información para la Junta Administradora de Agua Potable de Pilacoto abarcan la identificación y autenticación, la protección de las comunicaciones, y las herramientas de seguridad; de forma general, el riesgo se evalúa como intermedio.

Asimismo, respecto a los controles de seguridad de la información más críticos se identificaron: la organización interna de la seguridad de la información, la manipulación de los soportes, gestión de archivos de usuario, las responsabilidades de usuario, la protección contra un software malicioso, las copias de seguridad, los registros y supervisión, el control del software en exploración, y la gestión de la seguridad de redes.

De esta manera, y considerando lo antes mencionado, se procedió a realizar la propuesta de un plan de contingencia que permita la reanudación de las operaciones del sistema informático de la Junta, después de presentarse una contingencia o siniestro.

3.2 Resultados de los métodos específicos de la especialidad empleado en la investigación

Sobre la metodología Magerit que se aplica directamente en la herramienta Pilar con la cual se gestionó el riesgo para la Junta Administradora de Agua Potable de Pilacoto, cabe mencionar que de una manera sistemática y relativamente sencilla, permite evaluar los riesgos y/o amenazas a las que está expuesta la Junta, lo que permitió determinar el escenario actual, así como el ideal, en base a lo cual se determinó el plan de contingencia (manual de procedimientos) a aplicar para optimizar dicha situación.

Respecto a la investigación in situ, así como la aplicación de la encuesta para validar la propuesta, se pudo evidenciar la realidad en la que la Junta se desenvuelve, lo que sirvió para proponer un plan de contingencia de acuerdo no solo a sus necesidades, sino a su realidad, lo que garantiza su aplicabilidad; y seguramente, es lo que persuadió tanto a empleados como a usuarios, quienes creen que lo desarrollado servirá positivamente para la Junta y la preservación de la información sensible de la misma.

3.2.1 Análisis e interpretación de encuestas a empleados

Los resultados de la encuesta aplicada a los empleados de la Junta Administradora de Agua Potable de Pilacoto en la Parroquia de Guaytacama se muestran a continuación:

Pregunta 1.- ¿Cree Usted que mediante el software PILAR en el plan de contingencia, la información del JAAP este más segura?

Tabla 7 Pregunta 1 – Encuesta empleados

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	23	92%

NO	2	8%
TOTAL	25	100%

Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

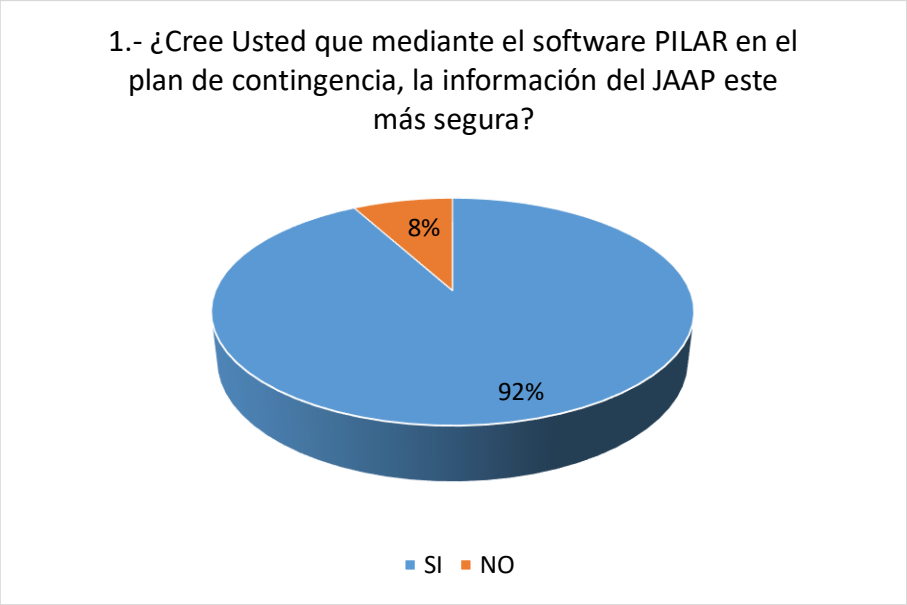


Figura 29 Pregunta 1 – Encuesta empleados
Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Del total de los encuestados, el 92% de los empleados opinan que la información del JAAP estará más segura con el uso del software PILAR, y tan solo el 8% opinan que no es necesario el software.

Pregunta 2.- ¿Con el software PILAR dentro del plan de contingencia, cree usted que el JAAP esté preparado para estos tipos de desastres tecnológicos y naturales?

Tabla 8 Pregunta 2 – Encuesta empleados

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	22	88%
NO	3	12%
TOTAL	25	100%

Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

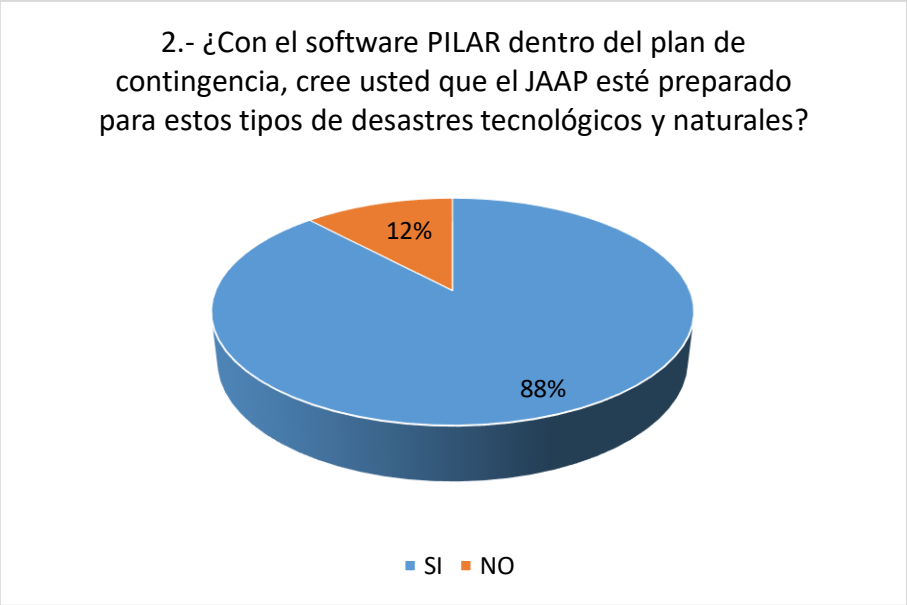


Figura 30 Pregunta 2 – Encuesta empleados
Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

EL 88% de los empleados opinan que el plan de contingencia con el software PILAR le permitirá al JAAP estar preparado para estos tipos de desastres tecnológicos y naturales, el 12% opinan que no es necesario el uso de PILAR en el plan de contingencia.

Pregunta 3.- ¿Usted recomendaría que el software sea utilizado dentro de un plan de contingencia informático en otras Juntas administradoras de Agua Potable, que estén en zonas de riego?

Tabla 9 Pregunta 3 – Encuesta empleados

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	17	68%
NO	8	32%
TOTAL	25	100%

Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

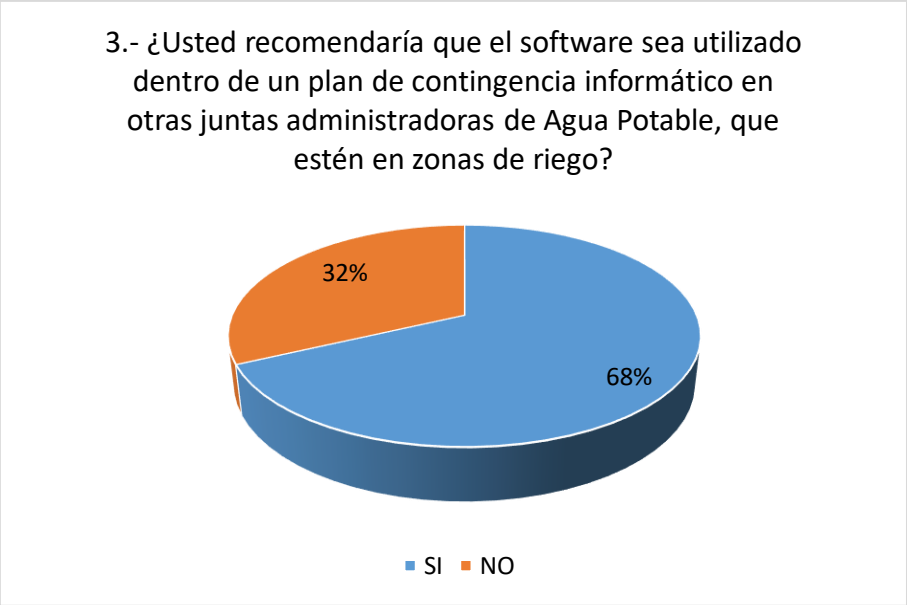


Figura 31 Pregunta 3 – Encuesta empleados
Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Del 100% de los empleados consultados, el 68% de los éstos recomendarían que el software sea utilizado dentro de un plan de contingencia informático en otras Juntas administradoras de Agua Potable, que estén en zonas de riego; el 32% en cambio, opinan que el software no lo harían.

Pregunta 4.- ¿Mediante la demostración del software PILAR, cree usted que esta herramienta tecnológica es amigable e intuitiva para los empleados del JAAP?

Tabla 10 Pregunta 4 – Encuesta empleados

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	19	76%
NO	6	24%
TOTAL	25	100%

Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

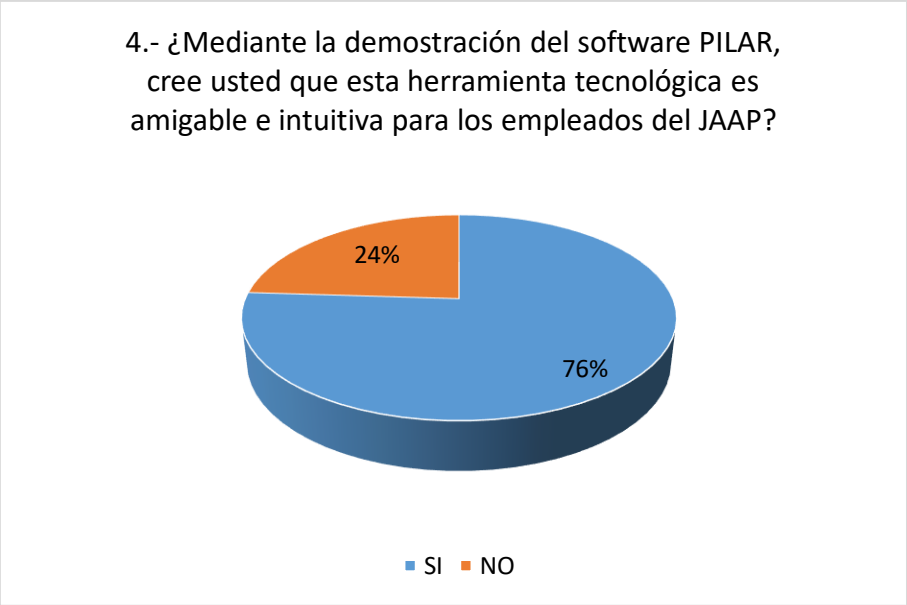


Figura 32 Pregunta 4 – Encuesta empleados
Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Luego de la demostración del software PILAR, el 79% de los empleados de la JAAP cree que esta herramienta tecnológica es amigable e intuitiva, mientras que el 24% opinan que no lo es.

Pregunta 5.- ¿Después de la exposición del software PILAR, usted está satisfecho con los resultados esperados de dicha herramienta?

Tabla 11 Pregunta 5 – Encuesta empleados

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	24	96%
NO	1	4%
TOTAL	25	100%

Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

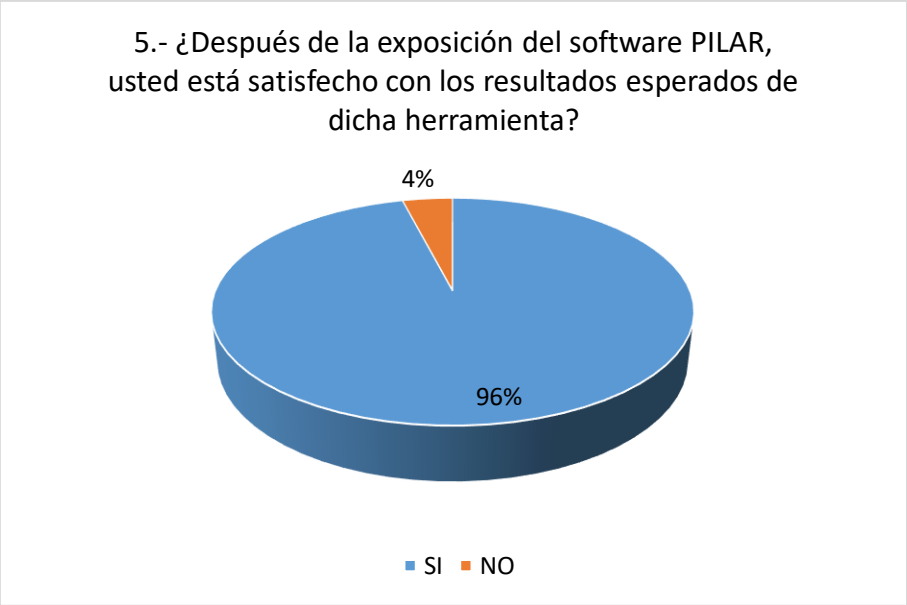


Figura 33 Pregunta 5 – Encuesta empleados
Fuente: Empleados de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Después de la exposición del software PILAR, EL 96% de todos los encuestados usted está satisfecho con los resultados esperados de dicha herramienta, opinando que ayudará en la administración del JAAP; el 4% restante opina que no está satisfecho por lo que no será útil para la administración.

3.2.2 Análisis e interpretación de resultados de encuestas a usuarios

Los resultados de la encuesta aplicada a los moradores de la Junta Administradora de Agua Potable de Pilacoto en la Parroquia de Guaytacama, quienes son los usuarios de la misma, se exponen enseguida:

Pregunta 1: ¿Sabe usted que vive en un sector que es zona de riesgo?

Tabla 12 Pregunta 1 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	49	49%
NO	51	51%

TOTAL	100	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

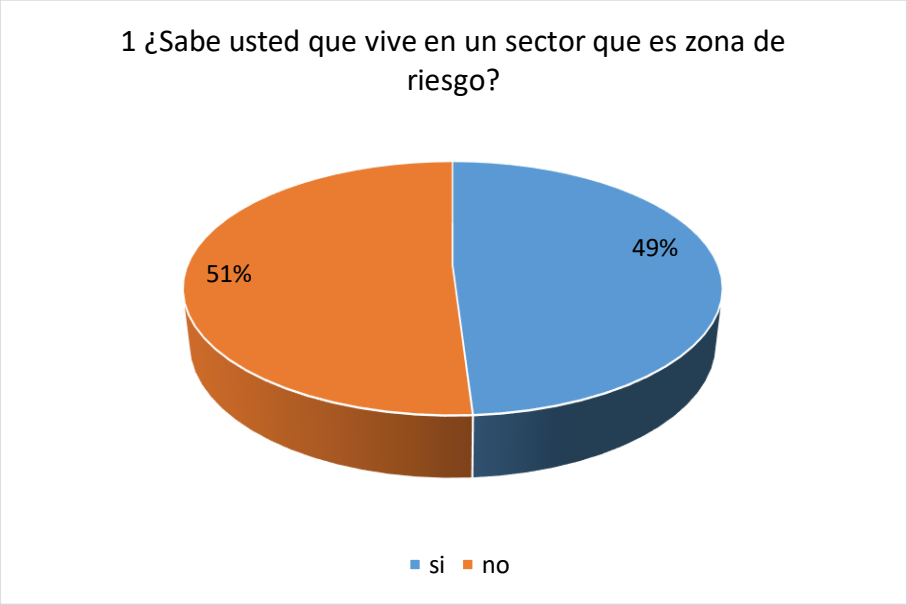


Figura 34 Pregunta 1 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Del total de los encuestados, el 49% está consciente que están viviendo en una zona de riego; en cambio el 51% indica que no viven en un sector riesgoso.

Pregunta 2: ¿Conoce usted la infraestructura física de la Junta administradora de agua Potable Pilacoto?

Tabla 13 Pregunta 2 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,64	64%
NO	0,36	36%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

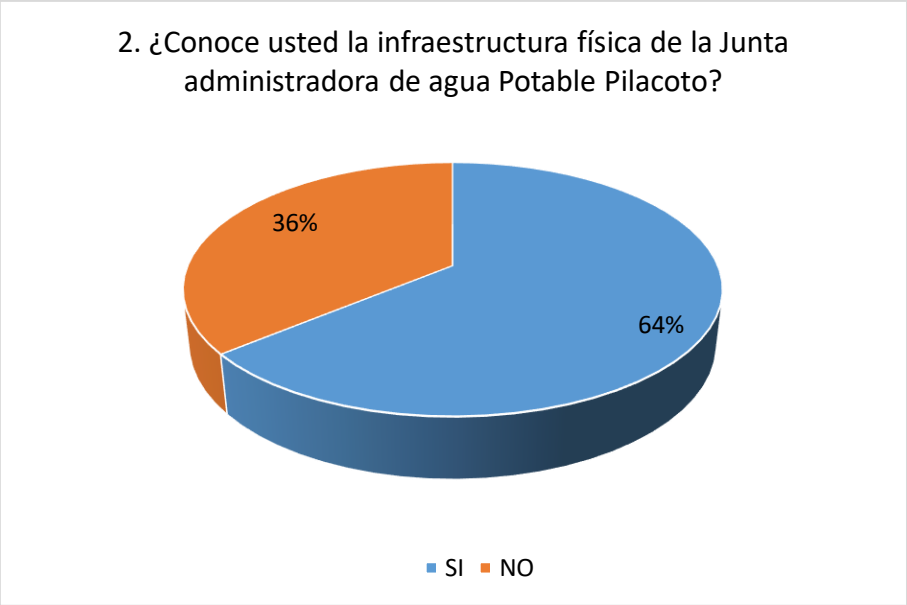


Figura 35 Pregunta 2 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

El 64% de los usuarios de la JAAPP si conocen la infraestructura física de la Junta, pero el 36% indica que no la conocen.

Pregunta 3: ¿Cree usted que la Junta administradora de agua potable está preparada para afrontar un desastre tecnológico y natural?

Tabla 14 Pregunta 3 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,4	40%
NO	0,6	60%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

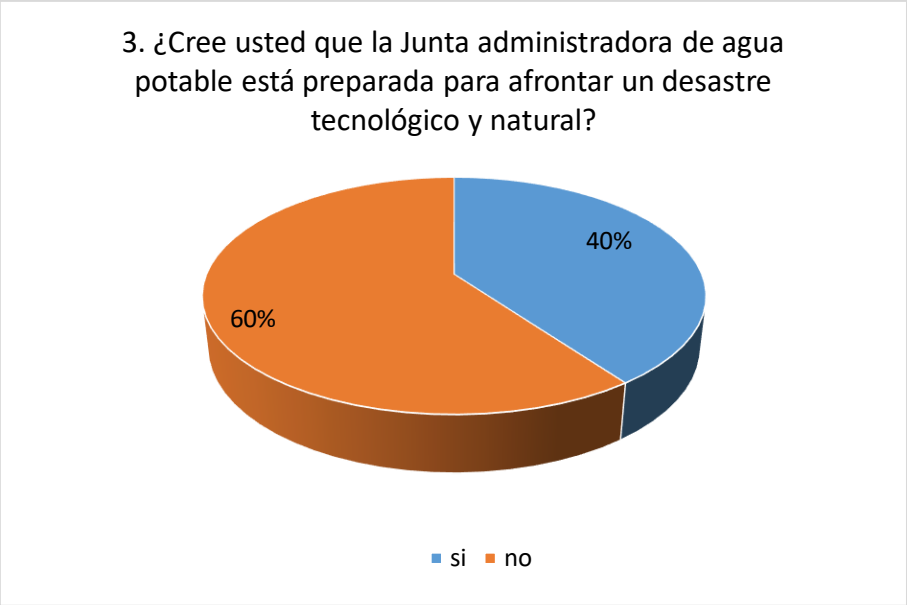


Figura 36 Pregunta 3 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Asimismo, respecto a la capacidad de afrontar un desastre tecnológico y natural, el 40% de los usuarios piensan que la Junta si está preparada; mientras que el 60% indica que no está preparada la Junta para afrontar una eventualidad de este tipo.

Pregunta 4: ¿Conoce usted teléfono de emergencia en caso de desastres tecnológicos y naturales?

Tabla 15 Pregunta 4 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,43	43%
NO	0,57	57%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

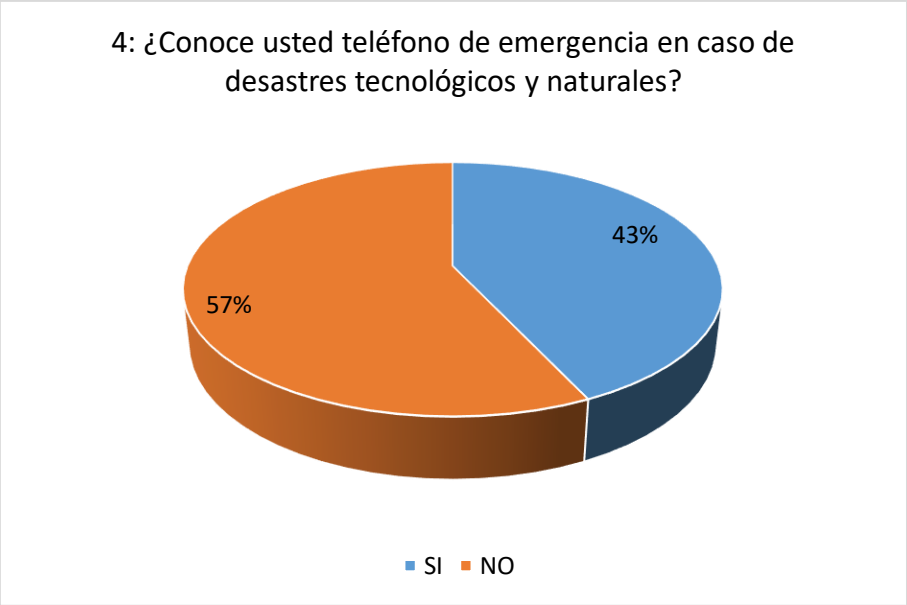


Figura 37 Pregunta 4 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

El 43% de los usuarios de la JAAPP si conocen el teléfono de emergencia en caso de desastres tecnológicos y naturales; en cambio el 57% indica que lo desconocen.

Pregunta 5: ¿Sabe cómo actuar después de un desastre tecnológico y desastres naturales?

Tabla 16 Pregunta 5 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,44	44%
NO	0,56	56%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

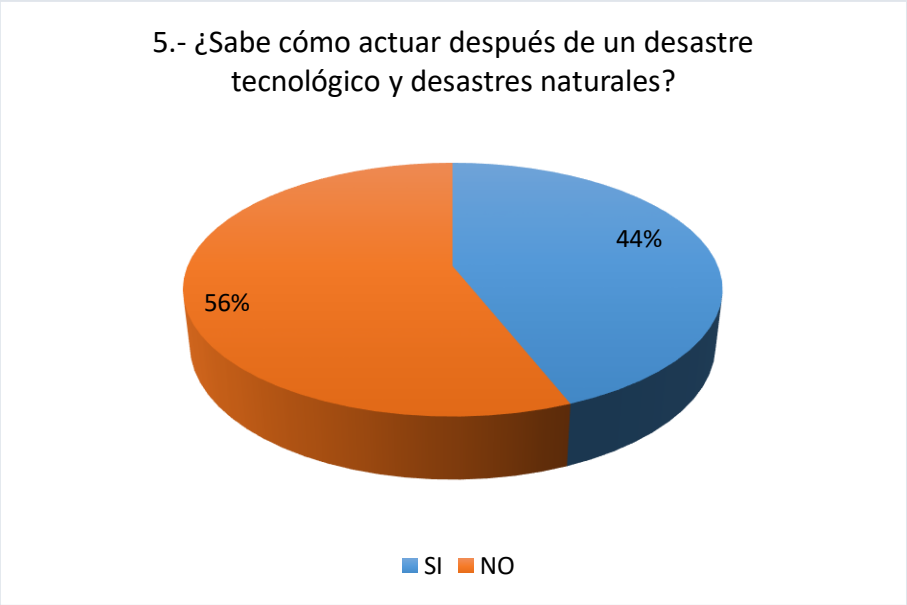


Figura 38 Pregunta 5 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

En relación a cómo actuar después de un desastre Tecnológico y desastres naturales, el 44% de los usuarios indica que si sabe que debe hacer, y el 56% indica que no.

Pregunta 6: ¿Conoce el modo de almacenamiento de información de la JAAPP en caso de un desastre Tecnológico y natural?

Tabla 17 Pregunta 6 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,32	32%
NO	0,68	68%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

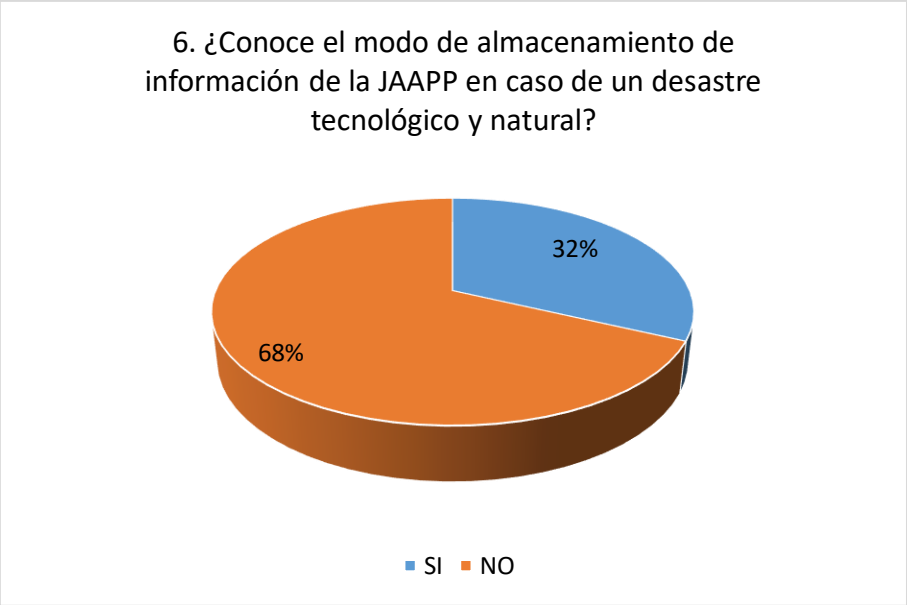


Figura 39 Pregunta 6 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Del 100% de los encuestados, el 68% menciona que no conoce el modo de almacenamiento de información del JAAPP en caso de un desastre tecnológico y natural; el 32% restante lo desconoce.

Pregunta 7: ¿Sabe usted que es un plan de contingencia?

Tabla 18 Pregunta 7 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,5	50%
NO	0,5	50%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Figura 40 Figura 41 Pregunta 7 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

El 50% de los usuarios del JAAPP si conocen que es un plan de contingencia, en cambio el 50% indica que no tiene conocimiento sobre el tema.

Pregunta 8: ¿Estarías de Acuerdo que se elabore un plan de contingencia para la Junta Administradora de agua potable Pilacoto para posibles desastres Tecnológicos y Naturales?

Tabla 19 Pregunta 8 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,8	80%
NO	0,2	20%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

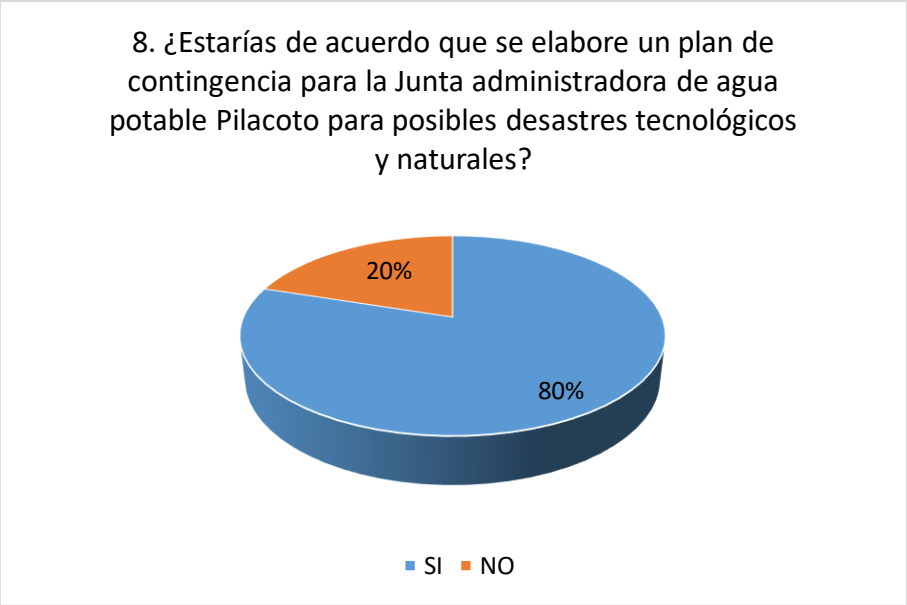


Figura 42 Pregunta 8 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

En lo referente a la elaboración de un plan de contingencia para la JAAPP para posibles desastre tecnológicos y naturales, un abrumador 80% indica que si están de acuerdo, y tan solo el 20% menciona que no.

Pregunta 9: ¿Mediante la elaboración del plan de contingencia cree usted que estaríamos preparados para posibles desastres tecnológicos y naturales?

Tabla 20 Pregunta 9 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,79	79%
NO	0,21	21%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

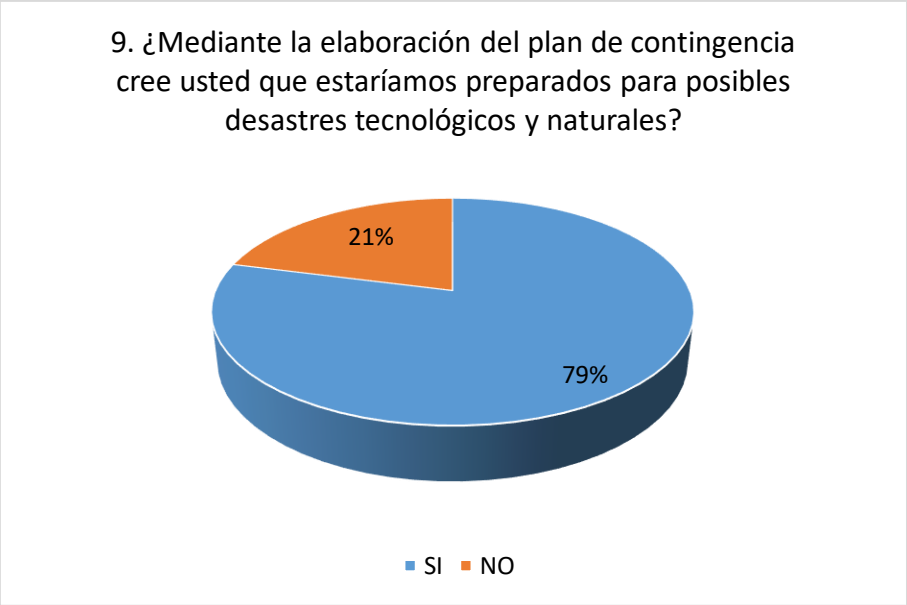


Figura 43 Pregunta 9 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Del total de los usuarios, el 79% señala que si estaría la JAAPP preparada para posibles desastres tecnológicos mediante el plan de contingencia; en cambio el 21% indica que no.

Pregunta 10: ¿Estarías de acuerdo que después de la elaboración del Plan de Contingencia se dé a conocer a todos los usuarios del JAAP?

Tabla 21 Pregunta 10 – Encuesta usuarios

ESCALA VALORATIVA	FRECUENCIA	PORCENTAJE
SI	0,92	92%
NO	0,08	8%
TOTAL	1	100%

Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

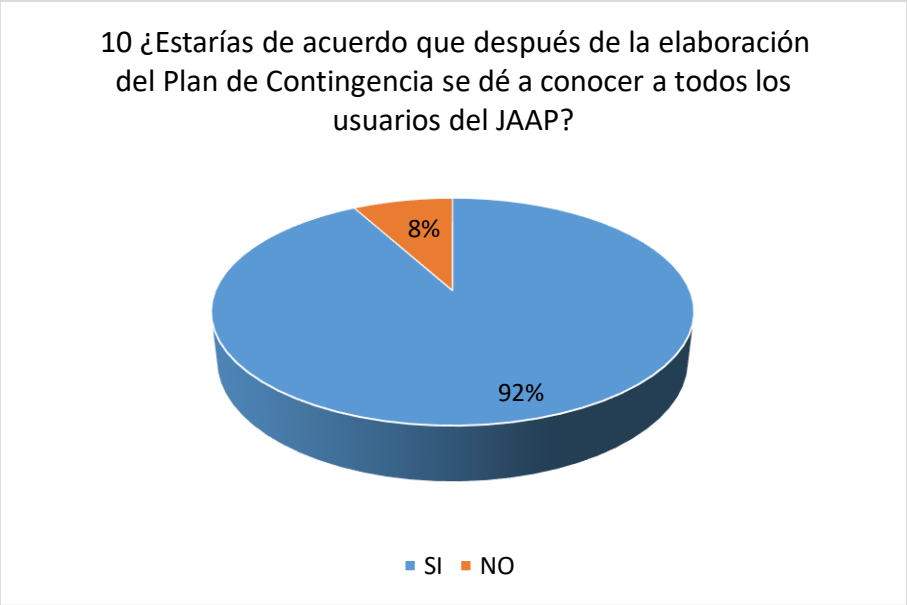


Figura 44 Pregunta 10 – Encuesta usuarios
Fuente: Usuarios de la JAAP de Pilacoto en la Parroquia de Guaytacama.
Elaborado por: Autor

Finalmente, el 92% de encuestados si estarían de acuerdo que después de la elaboración del plan de contingencia se dé a conocer a los usuarios del JAAPP, en cambio el 8% indica que no estarían de acuerdo.

3.3 Resultado del método de criterio de experto que demuestren la validación de la propuesta

Con el propósito de validar la factibilidad de la propuesta, se procedió a aplicar una encuesta a 3 profesionales en el área de conocimiento de Sistemas/Redes y 2 profesionales en el área de conocimiento Seguridad y Prevención de Riesgos Laborales, los mismos que cuentan con amplia experiencia en las respectivas áreas de conocimiento. Cabe mencionar que, los expertos poseen títulos de cuarto nivel en el área respectiva a la elaboración de planes de contingencia en la Universidad de las Fuerzas Armadas ESPE Matriz y Sede Latacunga, cuya experiencia que va desde 5 hasta 15 años, quienes respondieron una encuesta según el campo de dominio; es decir, relacionada con la elaboración del plan de contingencia para los

sistemas informáticos, y la seguridad con los profesionales del área de seguridad y prevención de riesgos.

Tabla 22 Expertos Sistemas/Redes

NOMBRE	TÍTULO	TRABAJO ACTUAL	EXPERIENCIA	TRAYECTORIA	CORREO	TELF.
Paulina Tatiana Mayorga Soria	Msc. Redes y Telecomunicaciones Msc. E-Learning y Redes Sociales	Jefe de la Unidad de Tecnologías de la Información y las Comunicaciones ESPE	22 años Utics- Espe	22 años	ptmayorga@espe.edu.ec	0982443019
Luis Gonzalo Borja Almeida	Msc. Redes de Información y Conectividad	Docente Tiempo Completo ESPE - Carrera de Software, Finanzas y Auditoria, Hotelería y Turismo	11 Años Utc, 4 Espe, varias empresas Tecno papel, Parmalat, Nabisco	20 años	lgborja2@espe.edu.ec	0998390674
Cristian Santiago Viteri Arias	Msc. Tics y Competencias digitales	Departamento de Tics Novacero	7 años	10 años	csviteri@nova.ec	0983306482

Elaborado por: Autor

Tabla 23 Expertos Seguridad y Prevención de riesgos

NOMBRE	TITULO	TRABAJO ACTUAL	EXPERIENCIA	TRAYECTORIA	CORREO	TELF.
Galo Roberto Saavedra Acosta	Msc. Seguridad y Prevención de Riesgos Laborales	Director de Carrera de Seguridad y Prevención de Riesgos Laborales	16 años 4 años Espe. Latacunga	20 años	grsaavedra@espe.edu.ec	0983107769
Marco Antonio Gavilánez Lagla	Msc. Sistemas Integrados de Gestión	Docente Tiempo Completo ESPE - Carrera de Seguridad y Prevención de Riesgos Laborales	4 años Espe,	10 años	magavilanez@espe.edu.ec	0984301842

Elaborado por: Autor

Las respuestas a estas interrogantes fueron recabadas mediante dos cuestionarios plan de contingencia y manejo de la metodología Magerit y Herramienta Pilar con 5 preguntas para expertos en seguridad y prevención de riesgos laborales y con 5 preguntas para los profesionales en sistemas y seguridad y riesgos laborales, en una escala descendente de 5 hasta 1, donde 5 – Excelente, 4 – Muy Bien, 3 – Bien, 2 – Regular, 1 – Insuficiente.

3.3.1 Análisis de resultados del juicio de expertos en el área de Sistemas y Redes

Tabla 24 Resultados de los expertos en Sistemas

PROFESIONALES	MEDIA ARITMÉTICA $\bar{x}$	MODA $\hat{x}$
Sistemas		
Profesional 1	5	5
Profesional 2	4,5	4 y 5
Profesional 3	4,3	4

Fuente: Criterio de expertos
Elaborado por: Autor

El primer experto da una valoración de 5 en todos los aspectos obteniendo una media aritmética de 5 y una moda de 5. Es decir que el usuario valora la propuesta como excelente el manejo de la metodología y la herramienta.

El experto dos da como resultados una media aritmética de 4,5 y una moda de 4 y 5, es decir que el usuario valora la propuesta entre muy buena con una tendencia a excelente el manejo de la metodología y la herramienta.

El tercer experto valora de la siguiente manera entre 4 a 5, lo que nos da una media aritmética de 4,33 y una moda de 4. Es decir que califica la propuesta entre muy buena a excelente el manejo de la metodología y la herramienta.

En la actualidad, se hace indispensable el uso de herramientas tecnológicas que ayuden al ser humano, por ende y a juicio de profesionales se puede destacar que se encuentran de acuerdo con el tema propuesto, su desarrollo y aplicación, además de considerarlo como un indicador de ayuda para la elaboración del plan de contingencia para los sistemas informáticos de la Junta Administradora de Agua Potable Pilacoto.

3.3.2 Análisis de resultados del juicio de expertos en el área de Seguridad ocupacional y Riesgos Laborales

Tabla 25 **Resultados de la Valoración a través del criterio de expertos**

PROFESIONALES	MEDIA ARITMÉTICA $\bar{x}$	MODA $\hat{x}$
Seguridad ocupacional y Riesgos Laborales		
Profesional 1	4,5	4 y 5
Profesional 2	4,67	5

Fuente: Criterio de expertos
Elaborado por: Autor

El primer experto valora de la siguiente manera entre 4 a 5, lo que da como resultado de la media aritmética 4,5 y una moda de 4 a 5, es decir que el usuario valora la propuesta como muy buena con mira a excelente, manejo de la metodología.

El experto dos indica que su valoración va desde 4 a 5, con una media aritmética de 4,67 y una moda de 5, es decir que el usuario considera como excelente la propuesta, manejo de la metodología.

3.3.3 Valoración de los criterios de los Profesionales de Sistemas de Información

Tabla 26 **Valoración de los criterios de los profesionales de Sistemas**

PROFESIONALES	Argumentación propuesta $\bar{x}$	Metodología y Herramienta $\bar{x}$	Lógica de la aplicación $\bar{x}$	Importancia $\bar{x}$	Facilidad $\bar{x}$	Valoración Integral $\bar{x}$
Sistemas	4,6	4,3	4,6	5	4,6	4,3

Fuente: Criterio de expertos
Elaborado por: Autor

En relación a la argumentación de la propuesta de la metodología, los expertos valoraron con una media aritmética de 4,6. Es decir que los profesionales califican que existe una buena argumentación en la propuesta.

En lo referente a la herramienta, los profesionales calificaron con una media aritmética de 4,3; es decir, la califican con una buena herramienta de manejo para el plan de contingencia

Para la lógica de la aplicación de la propuesta, los profesionales valoraron con una media aritmética de 4,6; es decir, que de manera consensuada creen que la propuesta tiene una buena lógica interna.

En cuanto a la importancia de la metodología y herramienta propuesta tecnológica, la media aritmética es de 5, es decir que todos los usuarios coinciden en la importancia de poner en marcha este tipo de metodología y herramienta en el JAAP.

En lo que tiene que ver a la facilidad de la implementación, los expertos dan una valoración de 4,6; de manera que, el criterio consensuado aporta evidencias que permiten sustentar que la propuesta presenta facilidad de uso para los usuarios.

Con relación a la Valoración Integral, los expertos coinciden en darle una valoración de 4,3; de manera que, existe el criterio consensuado, del aporte afirmativo de la propuesta.

3.3.4 Valoración de los criterios de los Profesionales de Seguridad Ocupacional y Riesgos Laborales

Tabla 27 Valoración de los criterios de los profesionales de Seguridad Ocupacional y Riesgos Laborales

PROFESIONALES	**Argumentación propuesta** $\bar{x}$	**Metodología y Herramienta** $\bar{x}$	**Lógica de la aplicación** $\bar{x}$	**Importancia** $\bar{x}$	**Facilidad** $\bar{x}$	**Valoración Integral** $\bar{x}$
Seguridad Ocupacional y Riesgos Laborales	4,6	4,3	4,6	4,3	4,6	4,3

Fuente: Criterio de expertos
Elaborado por: Autor

En cuanto a la argumentación de la propuesta del plan de contingencia para los sistemas informáticos, los usuarios valoraron con una media aritmética de 4,6. Es decir que los profesionales mencionan que existe buena argumentación en la propuesta.

En lo referente a estructura y diseño de la aplicación de la propuesta, los profesionales califican con una media aritmética de 4,3; es decir que la califican con una buena Metodología y Herramienta.

Con relación a la lógica de la aplicación de la propuesta, los profesionales valoran con una media aritmética de 4,6; es decir que, de manera consensuada, aportan evidencias de que la propuesta tiene buena lógica interna.

En cuanto a la importancia de la aplicación propuesta, la media aritmética es de 4,3; es decir, todos los usuarios coinciden en la importancia de poner en marcha este plan de contingencia

En lo que tiene que ver a la facilidad de la implementación, los usuarios dan una valoración de 4,6; de manera que, el criterio consensuado aporta evidencias que permite sustentar que la propuesta tiene facilidad de uso.

Con relación a la Valoración Integral de la aplicación propuesta, los usuarios coinciden en darle una valoración de 4,3; de manera que, el criterio consensuado aporta de manera afirmativa en el desarrollo de la propuesta.

En general, tanto los profesionales de Sistemas, como los de Seguridad y Riesgos Laborales, coinciden sobre la importancia de proporcionar que el plan de contingencia permita dar un cambio en cuanto a mejorar su manejo, a través del estudio realizado.

3.4 Resultados de la valoración económica, tecnológica, operacional y ambiental

Debido a que el presente trabajo de titulación se centra en plantear una propuesta metodológica y tecnológica, más no en la implementación de la misma, únicamente se analiza la valoración (en sus diferentes aspectos) de forma general, tanto para el plan previo a la recuperación, el de respaldo, el de recuperación, como el plan posterior a la recuperación.

En tal sentido, respecto a los recursos humanos, éstos se centran en el Presidente de la Junta y el personal de Sistemas de la misma, quienes tienen claramente sus roles en el plan de contingencia como tal; sobre los recursos materiales, sobresalen los medios físicos para backups, así como los medios digitales para el mismo fin. Asimismo, se deben considerar los gastos en caso de un incidente que imposibilite el uso de la logística y equipos actualmente empleados.

El presupuesto respectivo para la ejecución del plan de contingencia será obviamente, responsabilidad de la Junta Administradora de Agua Pilacoto, que debido a la gran aceptación que han expresado las autoridades sobre esta propuesta, se tiene por sentado la asignación económica correspondiente.

A continuación, se detalla el presupuesto correspondiente al escenario preventivo:

Tabla 28 Presupuesto Escenario preventivo

Herramienta	Análisis	Versión Estándar	Licencia anual	$1.500
Respaldos	Medios físicos	Caja de seguridad	1	$250
	Medios virtuales	Amazon S3 (1 Tb)	0,0450/Gb/mes * 1000 Gb (1Tb tamaño promedio del respaldo) $45 mensuales $540 anuales	$540
			Total	$2.290

Elaborado por: Autor

Igualmente, dicha predisposición, influye en la factibilidad tecnología y operacional ya que, al disponer del apoyo total, en especial del Presidente de

la Junta, no se espera tener ningún limitante al respecto, por lo que se garantiza la implantación de este contingente y por ende la operatividad en caso de ser necesaria su activación.

Finalmente, sobre la factibilidad medioambiental, cabe resaltar que este proyecto no causa impacto alguno al ambiente, únicamente se deberá considerar la repercusión propia de la amenaza/incidente, en el caso de que sea natural, que se pueda generar.

3.5 Discusión de la aplicación y/o validación de la propuesta

3.5.1 Discusión general

El contar con un plan de contingencia para los sistemas informáticos de la Junta Administradora de agua potable Pilacoto, permitirá a su administración y a sus miembros, por un lado, minimizar los riesgos latentes, al aplicar políticas y estrategias que eviten la materialización de las amenazas a las que están puestos, y por el otro, conocer el procedimiento a ejecutar en caso de que algún siniestro llegara suceder, y así reanudar la operatividad normal y oportuna de los servicios prestados por dicha entidad.

Las políticas y estrategias planteadas se apegan no sólo a las necesidades de la Junta Pilacoto, sino a su realidad, palpada en la observación in situ realizada; en este sentido, es importante indicar que, los lineamientos deberán ser implantados en un tiempo no mayor a los tres meses, apoyándose en el uso de los recursos propios de la entidad como tal.

Es fundamental que, el responsable de Sistemas CIS en coordinación con la administración, trabaje en la pronta y efectiva ejecución del plan presentado, ya que conjuntamente con la socialización y concienciación de los miembros de la junta y la Junta de Pilacoto de manejar un Plan de contingencia, se logrará mitigar las insuficiencias identificadas.

La mejor forma de estar seguro de que el plan de contingencia presentado es conveniente para la Junta Pilacoto es, primeramente, con la ejecución de las políticas presentadas, y posteriormente con los respectivos simulacros de siniestros tecnológicos y/o naturales, es realizar diversas pruebas, que permitan recolectar información fehaciente, que consentirán aplicar los correctivos necesarios para el efectivo funcionamiento de dicho plan.

Es válido resaltar de que la implementación de este plan de contingencia en la Junta administradora de agua potable no sólo servirá para los clientes internos como tales (administrativos y empleados), sino también a los clientes externos, que en este caso son los socios (usuarios) que posee la Junta, ya que al socializar esta implementación se espera crear mayor confianza en ellos, mejorando a la vez, la imagen de la Junta como una entidad comprometida comunidad al garantizar la dignidad de sus servicios informáticos.

3.5.2 Relación Costo/Beneficio

Finalmente, se presenta la Relación C/B, mediante la cual se espera determinar la factibilidad o no de la implantación de la propuesta, tanto de la gestión de riesgos propiamente dicha, como del plan de contingencia preventivo.

Tabla 29 Costos Activos informáticos

Activos informáticos				
Tipo	**Cantidad**	**Descripción**	**Valor unitario**	**Valor total**
Hardware	12	Regulador de voltaje modelo	$20	$240
	1	Módem (Internet)	$30	$30
	12	Computadora (incluida 1 que hace de Servidor)	$450	$5400
	3	Impresora	$150	$450
	3	Switch	$40	$120
Redes	3	Matriz y dos Sedes		$1200
Software	1	Programa de contabilidad SIBACF		$2500
Respaldo	1	Respaldo en disco duro		$150
			Total	**$10.090**

Fuente: Criterio de expertos
Elaborado por: Autor

En este caso, la relación costo/beneficio se calcula dividiendo los costos de la propuesta (presupuesto), para los costos de los activos informáticos (beneficio que se obtendrá, al resguardarlos con el plan de contingencia) si dicha relación es menor que 0, el índice es negativo, y la propuesta deberá rechazarse, si por el contrario es mayor que 0, el índice es positivo, y deberá aceptarse.

$$Relación\ C/B = \frac{Presupuesto}{Activos\ informáticos}$$

$$Relación\ C/B = \frac{2.290}{10.090}$$

$$Relación\ C/B = 0{,}23$$

3.6 Conclusiones del capítulo III

La Auditoría informática realizada a la Junta de Pilacoto, a pesar de algunos aspectos positivos, en su mayoría se identificaron algunos problemas e inconvenientes relacionados principalmente con el ambiente adecuado, mantenimiento de equipos, actualización de software, manejo de licencias, aplicación controles, y en esencia gestión de la seguridad de la información, evidenciándose la precaria situación, respecto a la ineficiente gestión del riesgo y la inexistencia procedimientos de recuperación ante la materialización de eventuales amenazas.

La validación de la propuesta con la ayuda de las encuestas tanto a empleados como a usuarios de la JAAP Pilacoto, así como las encuestas realizadas a los expertos son positivas, ya que aprecian y convergen en como el plan de contingencia puede ayudar a la Junta y a preservar su información y operatividad en caso de desastres tecnológicos y/o naturales.

De la misma manera, las distintas validaciones adicionales dan resultados provechosos, lo que reafirma la utilidad que la presente propuesta tiene para

la Junta administradora de agua potable Pilacoto, sus empleados y los usuarios de la misma; por esta razón, se recomienda su pronta implantación.

Con respecto al presupuesto relacionado con el escenario preventivo, este asciende a $2.290 anuales, mientras que el valor de los activos informáticos es de $10.090 , dando como resultado una relación Costo/Beneficio de 0,23, la cual al ser mayor a 0 ratifica que la propuesta es factible de realizarse en la JAAP Pilacoto.

CONCLUSIONES Y RECOMENDACIONES

Los planes de contingencia para servicios informáticos se centran en el desarrollo de actividades que eviten o minimicen el impacto de una contingencia, y permitan recuperar los servicios informáticos y/o tecnológicos dañados por algún contingente.

Para este caso se consideran los lineamientos de las Normas ISO 27001, 27002, 27005 y 31000, además la metodología MAGERIT para el análisis del riesgo, así como la herramienta PILAR, que sirven de apoyo para la gestión y tratamiento de los riesgos como tales.

La implementación del plan consistirá en la ejecución de las recomendaciones y los procedimientos establecidos en el análisis de riesgos que conjuntamente con las políticas y estrategias apropiadas, minimizarán el impacto de las amenazas y por ende el riesgo propiamente dicho, identificado en el análisis correspondiente.

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 (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.

También se debe indicar que, la propuesta planteada, puede sin ningún inconveniente ser aplicada en las demás Juntas administradoras de agua potable.

La metodología a aplicar, la cual básicamente consta de la metodología técnica, que se usará en el análisis de riesgos, y la que se empleará para la validación propuesta, abarcan por un lado el método Magerit, y por el otro el método de campo con aplicación de encuestas y entrevistas, permitirán determinar si la propuesta en cuestión es viable para aplicarla en la Junta administradora de agua Pilacoto.

La auditoría informática realizada a la Junta de Pilacoto, a pesar de algunos aspectos positivos, en su mayoría se identificaron algunos problemas e inconvenientes relacionados principalmente con el ambiente adecuado, mantenimiento de equipos, actualización de software, manejo de licencias, aplicación controles, y en esencia gestión de la seguridad de la información, evidenciándose la precaria situación, respecto a la ineficiente gestión del riesgo y la inexistencia procedimientos de recuperación ante la materialización de eventuales amenazas.

La validación de la propuesta con la ayuda de las encuestas tanto a empleados como a usuarios de la JAAP Pilacoto, así como las encuestas realizadas a los expertos son positivas, ya que aprecian y convergen en como el plan de contingencia puede ayudar a la Junta y a preservar su información y operatividad en caso de desastres tecnológicos y/o naturales.

De la misma manera, las distintas validaciones adicionales dan resultados provechosos, lo que reafirma la utilidad que la presente propuesta tiene para la Junta administradora de agua potable Pilacoto, sus empleados y los usuarios de la misma; por esta razón, se recomienda su pronta implantación.

Con respecto al presupuesto relacionado con el escenario preventivo, este asciende a $2.290 anuales, mientras que el valor de los activos informáticos es de $10.090 , dando como resultado una relación Costo/Beneficio de 0,23, la cual al ser mayor a 0 ratifica que la propuesta es factible de realizarse en la JAAP Pilacoto.

En base a lo anteriormente mencionado, se recomienda la pronta implantación tanto para la gestión del riesgo, como el plan de respaldos, y el de contingencia que abarca diferentes estrategias antes, durante y después de un incidente, cuyo objetivo fundamental es salvaguardar la información manejada por el sistema contable de la Junta administradora de agua potable Pilacoto.

También, se recomienda que, al ser la propuesta planteada, sin ningún inconveniente, aplicable en las demás Juntas administradoras de agua potable, se considere su pronta implantación en dichas instituciones.

BIBLIOGRAFÍA

[1] B. Claudio y N. Chicaiza, «Propuesta de un manual de contingencia informático para la U. T. C.,» Universidad Técnica de Cotopaxi, Ecuador, 2003.

[2] R. Lara, «Plan de contingenica informático para el conjunto de bodegas Parkenor,» Universidad de Fuerzas Armadas - ESPE , 2010.

[3] DPAE - Dirección de Prevención y Atención de Emergencias, «Guía para la elaboración de plan de emergencia y contingencia,» 2009. [En línea]. Available: http://www.ridsso.com/documentos/muro/15998_1481829766_5852ed8673dc4.pdf. [Último acceso: 15 Agosto 2019].

[4] LOPD, «Contingencia y continuidad para su negocio - Planes de contingencia y continuidad basados en un SGSI,» 2018. [En línea]. Available: https://ayudaleyprotecciondatos.es/2018/03/19/contingencia-continuidad-negocio/. [Último acceso: 28 Noviembre 2019].

[5] R. Sejzer, «El Círculo de Deming (Shewhart): Ciclo PDCA,» 2016. [En línea]. Available: http://ctcalidad.blogspot.com/2016/06/el-circulo-de-deming-shewhart-ciclo-pdca.html. [Último acceso: 28 Octubre 2019].

[6] J. Bernal, «Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua,» 2013. [En línea]. Available: https://www.pdcahome.com/5202/ciclo-pdca/. [Último acceso: 30 Septiembre 2019].

[7] D. Ortega, «Calidad en las TIC,» 2011. [En línea]. Available: http://calidadtic.blogspot.com/2011/01/como-hacer-un-plan-de-contingencia.html. [Último acceso: 22 09 2019].

[8] V. De Freitas, «Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar,» *Enlace,* vol. 6, nº 1, 2009.

[9] L. Sena y S. Tenzer, «Introducción a riesgo informático,» 2004. [En línea]. Available: http://www.interaktiv.cl/blog/wp-

content/uploads/2011/08/Introduccion_al_riesgo_informatico.pdf. [Último acceso: 28 Septiembre 2019].

[10] SNGR, «Gestión de riesgos,» 2012. [En línea]. Available: https://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf. [Último acceso: 28 Octubre 2019].

[11] G. Ramírez y E. Álvarez, «Auditorías a la gestión de las tecnologías y sistemas de información,» *Indata,* vol. 6, nº 1, 2003.

[12] Gestión Integral TA, «Gestión de riesgo en EPM,» 2012. [En línea]. Available: https://arango-arango.blogspot.com/2012/05/gestion-de-riesgo-en-epm.html. [Último acceso: 28 Octubre 2019].

[13] Arrizabalagauriarte Consulting, «Documentos para la gestión de riesgos,» 2019. [En línea]. Available: https://arrizabalagauriarte.com/documentos-la-gestion-riesgos/. [Último acceso: 28 Octubre 2019].

[14] C. Pablos, V. Izquierdo y J. López, Dirección y gestión de los sistemas de información en la empresa, España: ESIC, 2006.

[15] J. Calle, Reingeniería y seguridad en el ciberespacio, España: Díaz de Santos, 1996.

[16] ISACA, «Isaca Lanza Risk It Framework para ayudar a organizaciones a equilibrar los riesgos con los beneficios,» 2019. [En línea]. Available: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Launches-Risk-IT-Framework-to-Help-Organizations-Balance-Risk-with-Profit-Spanish.aspx. [Último acceso: 28 Octubre 2019].

[17] Ministerio de Hacienda y Administraciones Públicas, «MAGERIT – versión 3.0,» 2019. [En línea]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Último acceso: 28 Octubre 2019].

[18] R. Barzanallana, «Guía Pilar,» 2019. [En línea]. Available: https://www.um.es/docencia/barzana/GESESI/GuiaPilar.pdf. [Último acceso: 30 Noviembre 2019].

[19] BSI, «Norma ISO 31000 - Gestión de Riesgos,» 2019. [En línea]. Available: https://www.bsigroup.com/es-ES/ISO-31000-Gestion-de-Riesgos/. [Último acceso: 02 Octubre 2019].

[20] Revista Datacenter, «¿RTO vs RPO?,» 12 Diciembre 2013.

[21] L. Montenegro, «Elaboración de un plan de contingencia para sistemas informáticos – Caso de estudio Ministerio de justicia, derechos humanos y cultos,» Pontificia Universidad Católica del Ecuador, Ecuador, 2016.

[22] R. Palacios y J. Quiroz, «Plan de contingencia de los equipos y sistemas informáticos en el Gobierno autónomo descentralizado municipal del cantón Junín,» Escuela Superior Politécnica Agropecuaria de Manabí, Ecuador, 2013.

[23] A. Granda, «Diseño de un plan de contingencias del TICs para la Empresa Eléctrica Centrosur,» Universidad de Cuenca, Ecuador, 2011.

[24] JAAP Pilacoto, *Información Institucional*, Ecuador: La Institución, 2019.

[25] Pilar - Autor , *Proyecto JAAPP*, Ecuador: La Herramienta & el Autor, 2019.

ANEXOS

Anexo 1: Análisis de riesgos

Análisis de Riesgos

[jaapp] JAAP

18.11.2019

1 Introducción

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

Datos del sistema sujeto a análisis:

Código: jaapp
Nombre: JAAP

Descripción:

Datos administrativos:

- Organización: JAAP Pilacoto
- Descripción: Junta Administradora de agua potable Pilacoto
- Autor: Autor
- Versión: 1
- Fecha: 4-11-2019
- Responsable del Sistema: Autor
- Responsable de la Seguridad de la Información: Sistemas

1. Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [V] Valor (ej. vidas humanas, patromonio corporativo, etc.)
- [DP] Datos personales

2 Dominios de seguridad

dominios de seguridad
- [base] Base

1. Agravantes y atenuantes

[base] Base

2. Valoración de los activos

capa: [B] Activos esenciales

Activos esenciales

activo	
[sist] Sistema contable	[1](1)

(1) [1] 1 día < RTO < 5 días
(2) [7] de elevado valor comercial

3. Valoración de los dominios

dominio de seguridad	
[base] Base	[1]

3 Riesgo acumulado

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

amenaza
: presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella

D – dimensión
: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto
: se muestra el máximo impacto causado por esta amenaza en algún activo del sistema

R – riesgo
: se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

[potencial]
[base] Base

amenaza
[A.11] Acceso no autorizado
[A.56] Retirada de objetos (a través del perímetro físico)
[A.3] Manipulación de los registros de actividad (log)
[A.15] Modificación de la información
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso

[current] situación actual
[base] Base

amenaza
[A.11] Acceso no autorizado
[A.3] Manipulación de los registros de actividad (log)
[A.5] Suplantación de la identidad
[A.13] Repudio (negación de actuaciones)
[A.6] Abuso de privilegios de acceso
[A.15] Modificación de la información

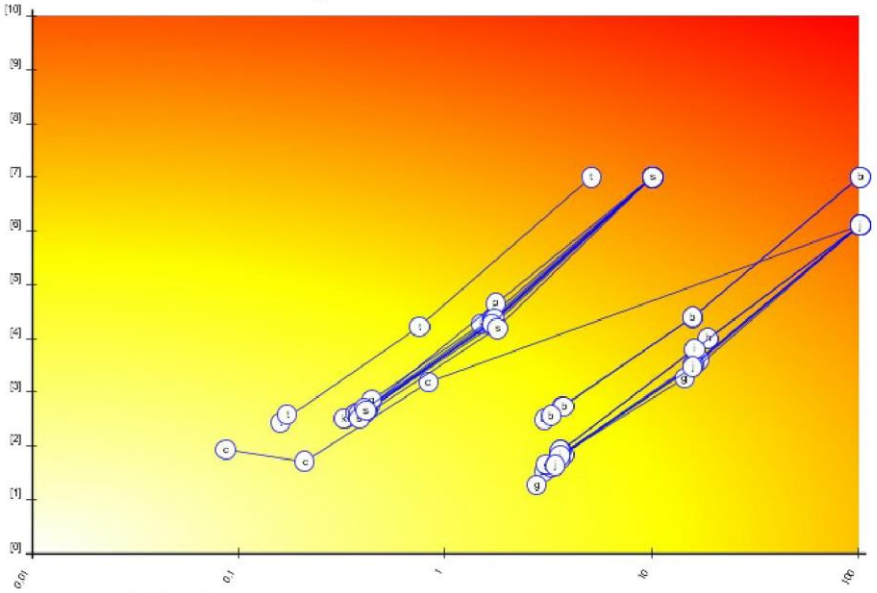
[target] situación objetivo
[base] Base

amenaza
[A.11] Acceso no autorizado
[A.3] Manipulación de los registros de actividad (log)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.15] Modificación de la información
[A.25] Robo de equipos
[A.13] Repudio (negación de actuaciones)

[PILAR] recomendación
[base] Base

amenaza
[A.11] Acceso no autorizado
[A.3] Manipulación de los registros de actividad (log)
[A.6] Abuso de privilegios de acceso
[A.5] Suplantación de la identidad
[A.15] Modificación de la información
[A.25] Robo de equipos
[A.13] Repudio (negación de actuaciones)

1. Evolución del riesgo



- a. A: E_LAN * A.11
- b. A: serv * A.11
- c. C: L_oficinas * A.56
- d. C: E_LAN * A.11
- e. I: serv * A.3
- f. C: serv * A.11
- g. C: sist * A.11
- h. I: reg * A.3
- i. C: reg * A.11
- j. C: ptra * A.11
- k. I: serv * A.15
- l. A: serv * A.5
- m. A: E_WAN * A.5
- n. A: E_bps * A.5
- o. A: E_LAN * A.5
- p. A: reg * A.5
- q. A: serv * A.6
- r. A: ptra * A.5
- s. A: sist * A.5
- t. I: ptra * A.15

4 Riesgo repercutido

Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

activo
presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

amenaza
presenta la amenaza dentro del catálogo de PILAR.

D – dimensión
se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto
se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

R – riesgo
se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

[potencial]
[base] Base

activo
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable

[current] situación actual
[base] Base

activo
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable
[sist] Sistema contable

[target] situación objetivo
[base] Base

activo
[sist] Sistema contable
[sist] Sistema contable

[PILAR] recomendación
[base] Base

activo
[sist] Sistema contable
[sist] Sistema contable

5 Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] Base
- Activos esenciales
  - [B] Activos esenciales
    - [sist] Sistema contable
    - [reg] Registros documentos
- activos
  - [E] Equipamiento
    - [serv] Servidor central
    - [ptra] Puestos de trabajo
    - [E_LAN] Red local
    - [E_bps] Protección del acceso a Internet
    - [E_WAN] Red de área amplia
  - [SS] Servicios subcontratados
    - [ISP] Servicio de acceso a Internet
  - [L] Instalaciones
    - [L_oficinas] Oficinas

1. Descripción

Detalle de los activos identificados en el sistema de información.

dominio de seguridad: [base] Base

[sist] Sistema contable

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información
  - [essential.info.biz] datos de interés para el negocio
  - [essential.info.adm] datos de interés para la administración pública
  - [essential.info.vr] datos vitales (registros de la organización)
  - [essential.service] servicio
  - [essential.service.operations] operaciones
  - [essential.service.financial] financieros
  - [essential.service.programme] programas
  - [essential.bp] proceso de negocio
- [D] Datos / Información
  - [D.files] ficheros de datos
  - [D.backup] copias de respaldo
  - [D.int] datos de gestión interna
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)

[reg] Registros documentos
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información
  - [essential.info.biz] datos de interés para el negocio
  - [essential.info.vr] datos vitales (registros de la organización)
  - [essential.service] servicio
  - [essential.service.operations] operaciones
  - [essential.service.financial] financieros
  - [essential.service.administrative] administrativos
  - [essential.bp] proceso de negocio
- [D] Datos / Información
  - [D.files] ficheros de datos
  - [D.conf] datos de configuración
  - [D.int] datos de gestión interna
  - [D.password] credenciales (ej. contraseñas)
  - [D.acl] datos de control de acceso
  - [D.log] registro de actividad (log)
  - [D.exe] código ejecutable
- [Media] Soportes de información
  - [Media.electronic] electrónicos

[serv] Servidor central
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.files] ficheros de datos
  - [D.backup] copias de respaldo
  - [D.conf] datos de configuración
  - [D.int] datos de gestión interna
  - [D.password] credenciales (ej. contraseñas)
  - [D.acl] datos de control de acceso
  - [D.log] registro de actividad (log)
- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.www] world wide web
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.www] servidor de presentación
  - [SW.std.app] servidor de aplicaciones
  - [SW.std.directory] servidor de directorio
  - [SW.std.file] servidor de ficheros
  - [SW.std.office] ofimática
  - [SW.std.os] sistema operativo

- [HW] Equipamiento informático (hardware)
  - [HW.mid] equipos medios
- [COM] Redes de comunicaciones
  - [COM.LAN] red local
  - [COM.WAN] red de área amplia
- [Media] Soportes de información
  - [Media.electronic] electrónicos
  - [Media.electronic.disk] discos

[ptra] Puestos de trabajo

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.files] ficheros de datos
  - [D.conf] datos de configuración
  - [D.int] datos de gestión interna
- [S] Servicios
  - [S.client] somos clientes de ...
  - [S.client.www] navegación web
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.browser] navegador web
  - [SW.std.office] ofimática
  - [SW.std.os] sistema operativo
  - [SW.sec] herramientas de seguridad
  - [SW.sec.av] anti virus
- [HW] Equipamiento informático (hardware)
  - [HW.pc] informática personal
  - [HW.peripheral] periféricos
  - [HW.peripheral.print] medios de impresión
- [Media] Soportes de información
  - [Media.electronic] electrónicos
  - [Media.electronic.disk] discos
  - [Media.electronic.usb] memorias USB

[E_LAN] Red local

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.backup] copias de respaldo
  - [D.conf] datos de configuración
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.os] sistema operativo
- [HW] Equipamiento informático (hardware)
  - [HW.network] soporte de la red

- [HW.network.switch] conmutador
- [HW.network.router] encaminador
- [COM] Redes de comunicaciones
  - [COM.LAN] red local

[E_bps] Protección del acceso a Internet

Dominio de seguridad

[base] Base

Clases de activos

- [arch] Arquitectura del sistema
  - [arch.ip] sistema de protección de frontera lógica
- [D] Datos / Información
  - [D.conf] datos de configuración
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.os] sistema operativo
- [HW] Equipamiento informático (hardware)
  - [HW.network] soporte de la red
  - [HW.network.router] encaminador

[E_WAN] Red de área amplia

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.conf] datos de configuración
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.os] sistema operativo
- [HW] Equipamiento informático (hardware)
  - [HW.network] soporte de la red
  - [HW.network.switch] conmutador
- [COM] Redes de comunicaciones
  - [COM.WAN] red de área amplia

[ISP] Servicio de acceso a Internet

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.3rd] contratado a terceros
  - [S.3rd.ISP] Proveedor de acceso a Internet
  - [S.3rd.comms] transporte / comunicaciones

[L_oficinas] Oficinas

Dominio de seguridad

[base] Base

Clases de activos

- [arch] Arquitectura del sistema
  - [arch.pps] sistema de protección física del perímetro
- [COM] Redes de comunicaciones
  - [COM.LAN] red local
  - [COM.WAN] red de área amplia
- [AUX] Equipamiento auxiliar
  - [AUX.cabling] cableado de datos
- [L] Instalaciones
  - [L.local] cuarto

Anexo 2: Declaración de aplicabilidad ISO 27000

Declaración de Aplicabilidad - ISO/IEC 27002:2013

[jaapp] JAAP

18.11.2019

1 Introducción

Código: jaapp
Nombre: JAAP

Descripción:

Datos administrativos:

- Organización: JAAP Pilacoto
- Descripción: Junta Administradora de agua potable Pilacoto
- Autor: Autor
- Versión: 1
- Fecha: 4-11-2019
- Responsable del Sistema: Autor
- Responsable de la Seguridad de la Información: Sistemas

2 Dominios de seguridad

[base] Base

3 Valoración de los activos

capa: [B] Activos esenciales

Activos esenciales

activo	
[sist] Sistema contable	[1](1)

(1) [1] 1 día < RTO < 5 días
(2) [7] de elevado valor comercial

4 Controles

1. *[5] Políticas de seguridad*

dominio: [base] Base

control
[5] Políticas de seguridad de la información
[5.1] Directrices de gestión de la seguridad de la información
[5.1.1] Políticas para la seguridad de la información
[5.1.2] Revisión de las políticas para la seguridad de la información

2. *[6] Organización de la seguridad de la información*

dominio: [base] Base

control
[6] Organización de la seguridad de la información
[6.1] Organización interna
[6.1.1] Roles y responsabilidades en seguridad de la información
[6.1.2] Separación de tareas
[6.1.3] Contacto con las autoridades
[6.1.4] Contacto con grupos de interés especial
[6.1.5] Seguridad de la información en la gestión de proyectos
[6.2] Los dispositivos móviles y el teletrabajo
[6.2.1] Política de dispositivos móviles
[6.2.2] Teletrabajo

3. *[7] Seguridad relativa a los recursos humanos*

dominio: [base] Base

control
[7] Seguridad relativa a los recursos humanos
[7.1] Antes del empleo
[7.1.1] Investigación de antecedentes
[7.1.2] Términos y condiciones del empleo
[7.2] Durante el empleo
[7.2.1] Responsabilidades de gestión
[7.2.2] Concienciación, educación y capacitación en seguridad de la información
[7.2.3] Proceso disciplinario
[7.3] Finalización del empleo o cambio en el puesto de trabajo
[7.3.1] Responsabilidades ante la finalización o cambio

4. [8] Gestión de activos

dominio: [base] Base

control
[8] Gestión de activos
[8.1] Responsabilidad sobre los activos
[8.1.1] Inventario de activos
[8.1.2] Propiedad de los activos
[8.1.3] Uso aceptable de los activos
[8.1.4] Devolución de activos
[8.2] Clasificación de la información
[8.2.1] Clasificación de la información
[8.2.2] Etiquetado de la información
[8.2.3] Manipulado de la información
[8.3] Manipulación de los soportes
[8.3.1] Gestión de soportes extraíbles
[8.3.2] Eliminación de soportes
[8.3.3] Soportes físicos en tránsito

5. [9] Control de acceso

dominio: [base] Base

control
[9] Control de acceso
[9.1] Requisitos de negocio para el control de acceso
[9.1.1] Política de control de acceso
[9.1.2] Acceso a las redes y a los servicios de red
[9.2] Gestión de acceso de usuario
[9.2.1] Registro y baja de usuario
[9.2.2] Provision de acceso de usuario
[9.2.3] Gestión de privilegios de acceso
[9.2.4] Gestión de la información secreta de autenticación de los usuarios
[9.2.5] Revisión de los derechos de acceso de usuario
[9.2.6] Retirada o reasignación de los derechos de acceso
[9.3] Responsabilidades del usuario
[9.3.1] Uso de la información secreta de autenticación
[9.4] Control de acceso a sistemas y aplicaciones
[9.4.1] Restricción del acceso a la información
[9.4.2] Procedimientos seguros de inicio de sesión

[9.4.3] Sistema de gestión de contraseñas
[9.4.4] Uso de utilidades con privilegios del sistema
[9.4.5] Control de acceso al código fuente de los programas

6. *[10] Criptografía*

dominio: [base] Base

control
[10] Criptografía
[10.1] Controles criptográficos
[10.1.1] Política de uso de los controles criptográficos
[10.1.2] Gestión de claves

7. *[11] Seguridad física y del entorno*

dominio: [base] Base

control
[11] Seguridad física y del entorno
[11.1] Áreas seguras
[11.1.1] Perímetro de seguridad física
[11.1.2] Controles físicos de entrada
[11.1.3] Seguridad de oficinas, despachos y recursos
[11.1.4] Protección contra las amenazas externas y ambientales
[11.1.5] El trabajo en áreas seguras
[11.1.6] Áreas de carga y descarga
[11.2] Seguridad de los equipos
[11.2.1] Emplazamiento y protección de equipos
[11.2.2] Instalaciones de suministro
[11.2.3] Seguridad del cableado
[11.2.4] Mantenimiento de los equipos
[11.2.5] Retirada de materiales propiedad de la empresa
[11.2.6] Seguridad de los equipos fuera de las instalaciones
[11.2.7] Reutilización o eliminación segura de equipos
[11.2.8] Equipo de usuario desatendido
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia

8. [12] Seguridad de las operaciones

dominio: [base] Base

control
[12] Seguridad de las operaciones
[12.1] Procedimientos y responsabilidades operacionales
[12.1.1] Documentación de los procedimientos de operación
[12.1.2] Gestión de cambios
[12.1.3] Gestión de capacidades
[12.1.4] Separación de los recursos de desarrollo, prueba y operación
[12.2] Protección contra el software malicioso (malware)
[12.2.1] Controles contra el código malicioso
[12.3] Copias de seguridad
[12.3.1] Copias de seguridad de la información
[12.4] Registros y supervisión
[12.4.1] Registro de eventos
[12.4.2] Protección de la información de registro
[12.4.3] Registros de administración y operación
[12.4.4] Sincronización del reloj
[12.5] Control del software en explotación
[12.5.1] Instalación del software en explotación
[12.6] Gestión de la vulnerabilidad técnica
[12.6.1] Gestión de las vulnerabilidades técnicas
[12.6.2] Restricción en la instalación de software
[12.7] Consideraciones sore la auditoría de sistemas de información
[12.7.1] Controles de auditoría de sistemas de información

9. [13] Seguridad de las comunicaciones

dominio: [base] Base

control
[13] Seguridad de las comunicaciones
[13.1] Gestión de la seguridad de redes
[13.1.1] Controles de red
[13.1.2] Seguridad de los servicios de red
[13.1.3] Segregación en redes
[13.2] Intercambio de información
[13.2.1] Políticas y procedimientos de intercambio de información
[13.2.2] Acuerdos de intercambio de información
[13.2.3] Mensajería electrónica
[13.2.4] Acuerdos de confidencialidad o no revelación

10. [14] Adquisición, desarrollo y mantenimiento de sistemas de información

dominio: [base] Base

control
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[14.1] Requisitos de seguridad en sistemas de información
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas
[14.1.3] Protección de las transacciones de servicios de aplicaciones
[14.2] Seguridad en el desarrollo y en los procesos de soporte
[14.2.1] Política de desarrollo seguro
[14.2.2] Procedimiento de control de cambios en sistemas
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
[14.2.4] Restricciones a los cambios en los paquetes de software
[14.2.5] Principios de ingeniería de sistemas seguros
[14.2.6] Entorno de desarrollo seguro
[14.2.7] Externalización del desarrollo de software
[14.2.8] Pruebas funcionales de seguridad de sistemas
[14.2.9] Pruebas de aceptación de sistemas
[14.3] Datos de prueba
[14.3.1] Protección de los datos de prueba

11. [15] Relación con proveedores

dominio: [base] Base

control
[15] Relación con proveedores
[15.1] Seguridad en las relaciones con proveedores
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores
[15.1.2] Requisitos de seguridad en contratos con terceros
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones
[15.2] Gestión de la provisión de servicios del proveedor
[15.2.1] Control y revisión de la provisión de servicios del proveedor
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor

12. [16] Gestión de incidentes de seguridad de la información

dominio: [base] Base

control
[16] Gestión de incidentes de seguridad de la información
[16.1] Gestión de incidentes de seguridad de la información y mejoras
[16.1.1] Responsabilidades y procedimientos
[16.1.2] Notificación de eventos de seguridad de la información
[16.1.3] Notificación de puntos débiles de la seguridad
[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información
[16.1.5] Respuesta a incidentes de seguridad de la información
[16.1.6] Aprendizaje de los incidentes de seguridad de la información
[16.1.7] Recopilación de evidencias

13. [17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio

dominio: [base] Base

control
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio
[17.1] Continuidad de la seguridad de la información
[17.1.1] Planificación de la continuidad de la seguridad de la información
[17.1.2] Implementar la continuidad de la seguridad de la información
[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información
[17.2] Redundancia
[17.2.1] Disponibilidad de los recursos de tratamiento de la información

14. [18] Cumplimiento

dominio: [base] Base

control
[18] Cumplimiento
[18.1] Cumplimiento de los requisitos legales y contractuales
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales
[18.1.2] Derechos de propiedad intelectual (DPI)
[18.1.3] Protección de los registros de la organización
[18.1.4] Protección y privacidad de la información de carácter personal
[18.1.5] Regulación de los controles criptográficos
[18.2] Revisiones de la seguridad de la información

[18.2.1] Revisión independiente de la seguridad de la información
[18.2.2] Cumplimiento de las políticas y normas de seguridad
[18.2.3] Comprobación del cumplimiento técnico

Anexo 3: Cumplimiento ISO 27000

Cumplimiento ISO/IEC 27002:2013

[jaapp] JAAP

18.11.2019

1 Introducción

Código: jaapp
Nombre: JAAP

Descripción:

Datos administrativos:

- Organización: JAAP Pilacoto
- Descripción: Junta Administradora de agua potable Pilacoto
- Autor: Autor
- Versión: 1
- Fecha: 4-11-2019
- Responsable del Sistema: Autor
- Responsable de la Seguridad de la Información: Sistemas

2 Dominios de seguridad

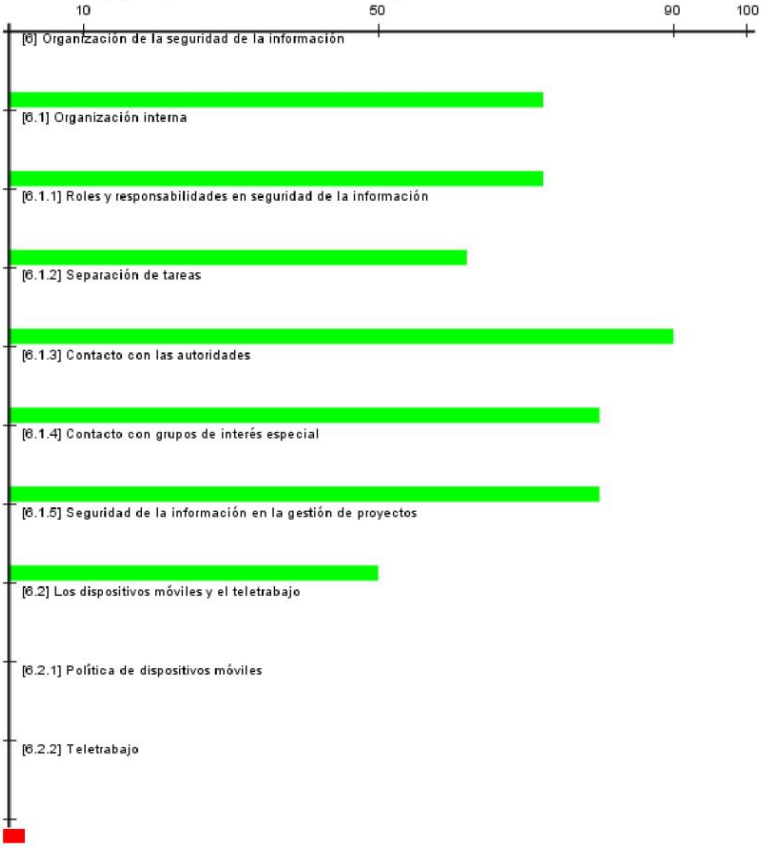
[base] Base

3 Controles

1. Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

3. [6] Organización de la seguridad de la información



[current] situación actual

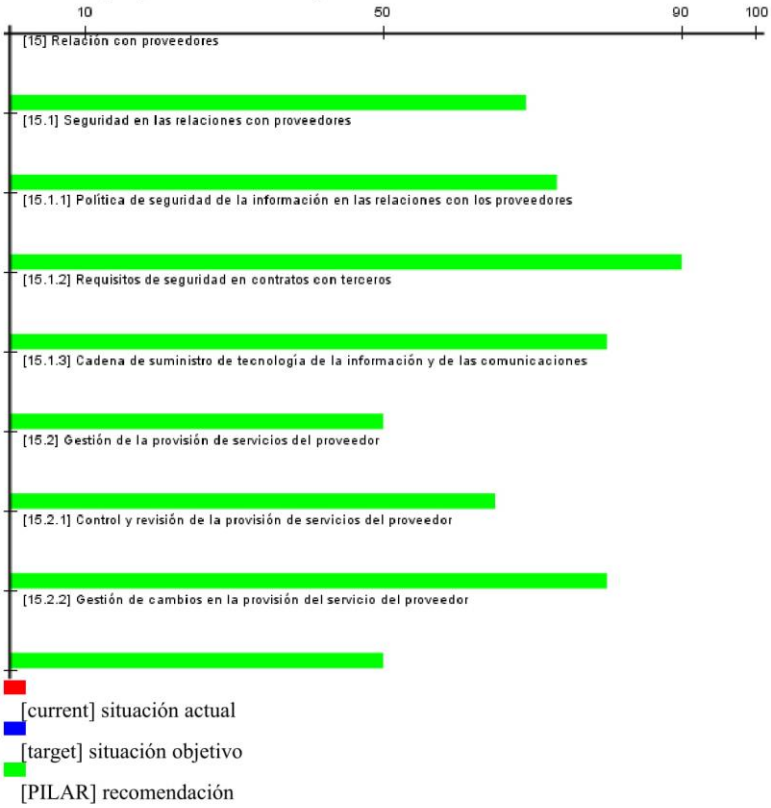
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[6] Organización de la seguridad de la información
[6.1] Organización interna
[6.1.1] Roles y responsabilidades en seguridad de la información
[6.1.2] Separación de tareas
[6.1.3] Contacto con las autoridades

12. [15] Relación con proveedores



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[15] Relación con proveedores
[15.1] Seguridad en las relaciones con proveedores
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores
[15.1.2] Requisitos de seguridad en contratos con terceros
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones
[15.2] Gestión de la provisión de servicios del proveedor
[15.2.1] Control y revisión de la provisión de servicios del proveedor
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[14.1] Requisitos de seguridad en sistemas de información
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas
[14.1.3] Protección de las transacciones de servicios de aplicaciones
[14.2] Seguridad en el desarrollo y en los procesos de soporte
[14.2.1] Política de desarrollo seguro
[14.2.2] Procedimiento de control de cambios en sistemas
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
[14.2.4] Restricciones a los cambios en los paquetes de software
[14.2.5] Principios de ingeniería de sistemas seguros
[14.2.6] Entorno de desarrollo seguro
[14.2.7] Externalización del desarrollo de software
[14.2.8] Pruebas funcionales de seguridad de sistemas
[14.2.9] Pruebas de aceptación de sistemas
[14.3] Datos de prueba
[14.3.1] Protección de los datos de prueba


10
50
90
100
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[14.1] Requisitos de seguridad en sistemas de información
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas
[14.1.3] Protección de las transacciones de servicios de aplicaciones
[14.2] Seguridad en el desarrollo y en los procesos de soporte
[14.2.1] Política de desarrollo seguro
[14.2.2] Procedimiento de control de cambios en sistemas
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
[14.2.4] Restricciones a los cambios en los paquetes de software
[14.2.5] Principios de ingeniería de sistemas seguros
[14.2.6] Entorno de desarrollo seguro
[14.2.7] Externalización del desarrollo de software
[14.2.8] Pruebas funcionales de seguridad de sistemas
[14.2.9] Pruebas de aceptación de sistemas
[14.3] Datos de prueba

11. [14] Adquisición, desarrollo y mantenimiento de sistemas de información

[13.2] Intercambio de información
[13.2.1] Políticas y procedimientos de intercambio de información
[13.2.2] Acuerdos de intercambio de información
[13.2.3] Mensajería electrónica
[13.2.4] Acuerdos de confidencialidad o no revelación

10.[13] Seguridad de las comunicaciones

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[13] Seguridad de las comunicaciones
[13.1] Gestión de la seguridad de redes
[13.1.1] Controles de red
[13.1.2] Seguridad de los servicios de red
[13.1.3] Segregación en redes

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[12] Seguridad de las operaciones
[12.1] Procedimientos y responsabilidades operacionales
[12.1.1] Documentación de los procedimientos de operación
[12.1.2] Gestión de cambios
[12.1.3] Gestión de capacidades
[12.1.4] Separación de los recursos de desarrollo, prueba y operación
[12.2] Protección contra el software malicioso (malware)
[12.2.1] Controles contra el código malicioso
[12.3] Copias de seguridad
[12.3.1] Copias de seguridad de la información
[12.4] Registros y supervisión
[12.4.1] Registro de eventos
[12.4.2] Protección de la información de registro
[12.4.3] Registros de administración y operación
[12.4.4] Sincronización del reloj
[12.5] Control del software en explotación
[12.5.1] Instalación del software en explotación
[12.6] Gestión de la vulnerabilidad técnica
[12.6.1] Gestión de las vulnerabilidades técnicas
[12.6.2] Restricción en la instalación de software
[12.7] Consideraciones sore la auditoría de sistemas de información
[12.7.1] Controles de auditoría de sistemas de información


10
50
90
100
[12] Seguridad de las operaciones
[12.1] Procedimientos y responsabilidades operacionales
[12.1.1] Documentación de los procedimientos de operación
[12.1.2] Gestión de cambios
[12.1.3] Gestión de capacidades
[12.1.4] Separación de los recursos de desarrollo, prueba y operación
[12.2] Protección contra el software malicioso (malware)
[12.2.1] Controles contra el código malicioso
[12.3] Copias de seguridad
[12.3.1] Copias de seguridad de la información
[12.4] Registros y supervisión
[12.4.1] Registro de eventos
[12.4.2] Protección de la información de registro
[12.4.3] Registros de administración y operación
[12.4.4] Sincronización del reloj
[12.5] Control del software en explotación

9. [12] Seguridad de las operaciones

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[11] Seguridad física y del entorno
[11.1] Áreas seguras
[11.1.1] Perímetro de seguridad física
[11.1.2] Controles físicos de entrada
[11.1.3] Seguridad de oficinas, despachos y recursos
[11.1.4] Protección contra las amenazas externas y ambientales
[11.1.5] El trabajo en áreas seguras
[11.1.6] Áreas de carga y descarga
[11.2] Seguridad de los equipos
[11.2.1] Emplazamiento y protección de equipos
[11.2.2] Instalaciones de suministro
[11.2.3] Seguridad del cableado
[11.2.4] Mantenimiento de los equipos
[11.2.5] Retirada de materiales propiedad de la empresa
[11.2.6] Seguridad de los equipos fuera de las instalaciones
[11.2.7] Reutilización o eliminación segura de equipos
[11.2.8] Equipo de usuario desatendido
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia


10
50
90
100
[11] Seguridad física y del entorno
[11.1] Áreas seguras
[11.1.1] Perímetro de seguridad física
[11.1.2] Controles físicos de entrada
[11.1.3] Seguridad de oficinas, despachos y recursos
[11.1.4] Protección contra las amenazas externas y ambientales
[11.1.5] El trabajo en áreas seguras
[11.1.6] Áreas de carga y descarga
[11.2] Seguridad de los equipos
[11.2.1] Emplazamiento y protección de equipos
[11.2.2] Instalaciones de suministro
[11.2.3] Seguridad del cableado
[11.2.4] Mantenimiento de los equipos
[11.2.5] Retirada de materiales propiedad de la empresa
[11.2.6] Seguridad de los equipos fuera de las instalaciones
[11.2.7] Reutilización o eliminación segura de equipos

8. [11] Seguridad física y del entorno

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[10] Criptografía
[10.1] Controles criptográficos
[10.1.1] Política de uso de los controles criptográficos
[10.1.2] Gestión de claves

[current] situación actual

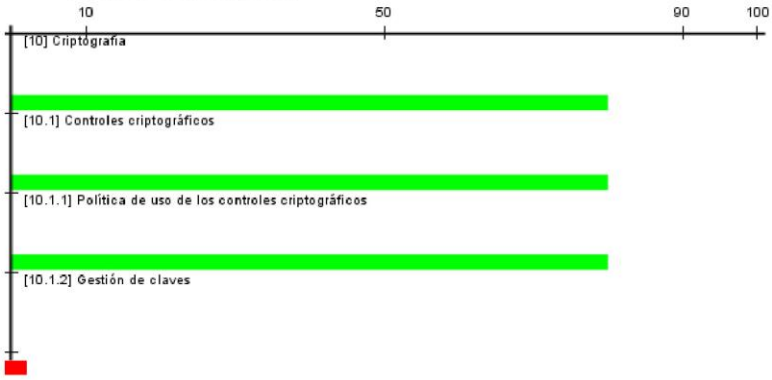
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[9] Control de acceso
[9.1] Requisitos de negocio para el control de acceso
[9.1.1] Política de control de acceso
[9.1.2] Acceso a las redes y a los servicios de red
[9.2] Gestión de acceso de usuario
[9.2.1] Registro y baja de usuario
[9.2.2] Provision de acceso de usuario
[9.2.3] Gestión de privilegios de acceso
[9.2.4] Gestión de la información secreta de autenticación de los usuarios
[9.2.5] Revisión de los derechos de acceso de usuario
[9.2.6] Retirada o reasignación de los derechos de acceso
[9.3] Responsabilidades del usuario
[9.3.1] Uso de la información secreta de autenticación
[9.4] Control de acceso a sistemas y aplicaciones
[9.4.1] Restricción del acceso a la información
[9.4.2] Procedimientos seguros de inicio de sesión
[9.4.3] Sistema de gestión de contraseñas
[9.4.4] Uso de utilidades con privilegios del sistema
[9.4.5] Control de acceso al código fuente de los programas

7. *[10] Criptografía*




10
50
90
100
[9] Control de acceso
[9.1] Requisitos de negocio para el control de acceso
[9.1.1] Política de control de acceso
[9.1.2] Acceso a las redes y a los servicios de red
[9.2] Gestión de acceso de usuario
[9.2.1] Registro y baja de usuario
[9.2.2] Provision de acceso de usuario
[9.2.3] Gestión de privilegios de acceso
[9.2.4] Gestión de la información secreta de autenticación de los usuarios
[9.2.5] Revisión de los derechos de acceso de usuario
[9.2.6] Retirada o reasignación de los derechos de acceso
[9.3] Responsabilidades del usuario
[9.3.1] Uso de la información secreta de autenticación
[9.4] Control de acceso a sistemas y aplicaciones
[9.4.1] Restricción del acceso a la información
[9.4.2] Procedimientos seguros de inicio de sesión

6. [9] Control de acceso

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[8] Gestión de activos
[8.1] Responsabilidad sobre los activos
[8.1.1] Inventario de activos
[8.1.2] Propiedad de los activos
[8.1.3] Uso aceptable de los activos
[8.1.4] Devolución de activos
[8.2] Clasificación de la información
[8.2.1] Clasificación de la información
[8.2.2] Etiquetado de la información
[8.2.3] Manipulado de la información
[8.3] Manipulación de los soportes
[8.3.1] Gestión de soportes extraíbles
[8.3.2] Eliminación de soportes
[8.3.3] Soportes físicos en tránsito

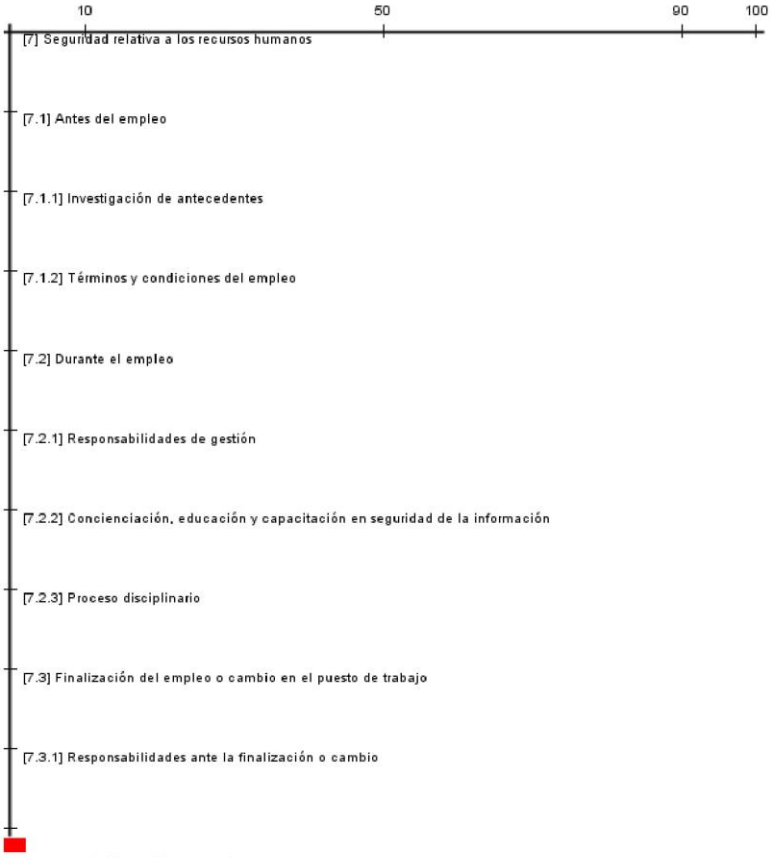
5. [8] Gestión de activos

dominio: [base] Base

control
[7] Seguridad relativa a los recursos humanos
[7.1] Antes del empleo
[7.1.1] Investigación de antecedentes
[7.1.2] Términos y condiciones del empleo
[7.2] Durante el empleo
[7.2.1] Responsabilidades de gestión
[7.2.2] Concienciación, educación y capacitación en seguridad de la información
[7.2.3] Proceso disciplinario
[7.3] Finalización del empleo o cambio en el puesto de trabajo
[7.3.1] Responsabilidades ante la finalización o cambio

[6.1.4] Contacto con grupos de interés especial
[6.1.5] Seguridad de la información en la gestión de proyectos
[6.2] Los dispositivos móviles y el teletrabajo
[6.2.1] Política de dispositivos móviles
[6.2.2] Teletrabajo

4. [7] Seguridad relativa a los recursos humanos

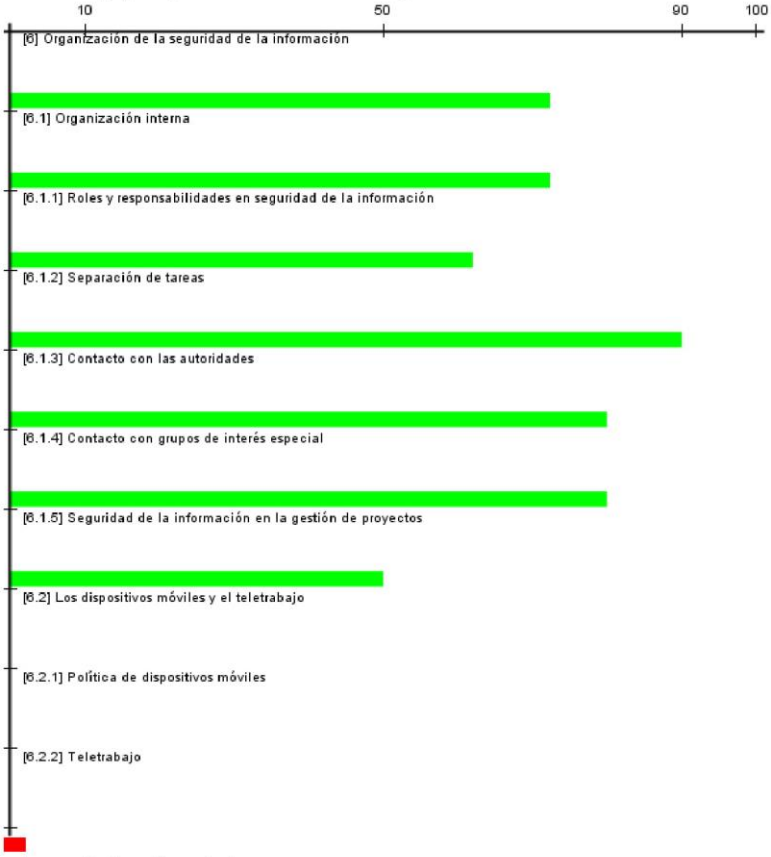


[current] situación actual

[target] situación objetivo

[PILAR] recomendación

3. [6] Organización de la seguridad de la información



[current] situación actual

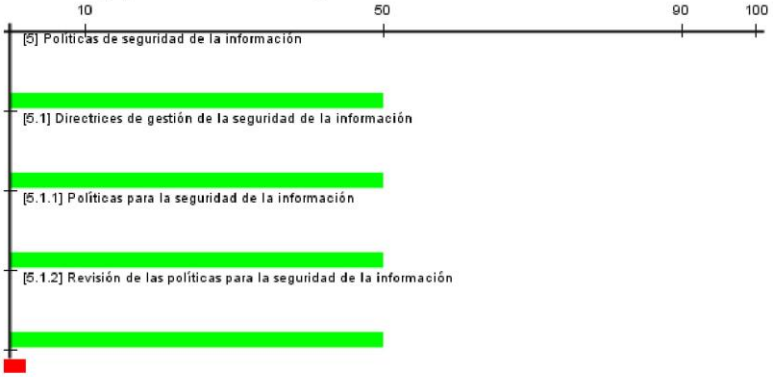
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[6] Organización de la seguridad de la información
[6.1] Organización interna
[6.1.1] Roles y responsabilidades en seguridad de la información
[6.1.2] Separación de tareas
[6.1.3] Contacto con las autoridades

2. [5] Políticas de seguridad



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[5] Políticas de seguridad de la información
[5.1] Directrices de gestión de la seguridad de la información
[5.1.1] Políticas para la seguridad de la información
[5.1.2] Revisión de las políticas para la seguridad de la información

Cumplimiento ISO/IEC 27002:2013

[jaapp] JAAP

18.11.2019

1 Introducción

Código: jaapp
Nombre: JAAP

Descripción:

Datos administrativos:

- Organización: JAAP Pilacoto
- Descripción: Junta Administradora de agua potable Pilacoto
- Autor: Autor
- Versión: 1
- Fecha: 4-11-2019
- Responsable del Sistema: Autor
- Responsable de la Seguridad de la Información: Sistemas

2 Dominios de seguridad

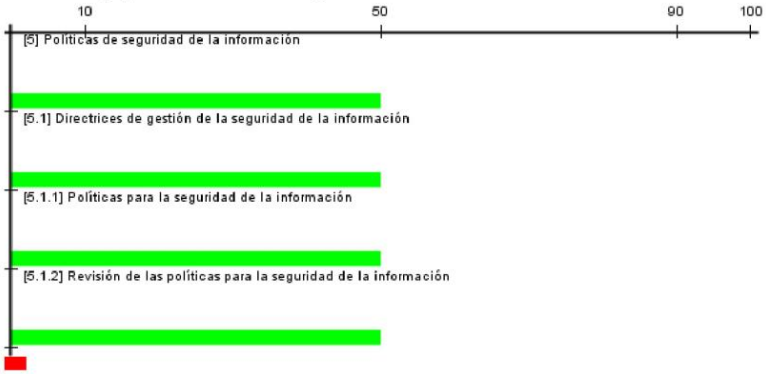
[base] Base

3 Controles

1. Niveles de madurez

- L0 - inexistente
- L1 - inicial / ad hoc
- L2 - reproducible, pero intuitivo
- L3 - proceso definido
- L4 - gestionado y medible
- L5 - optimizado

2. [5] Políticas de seguridad



[current] situación actual

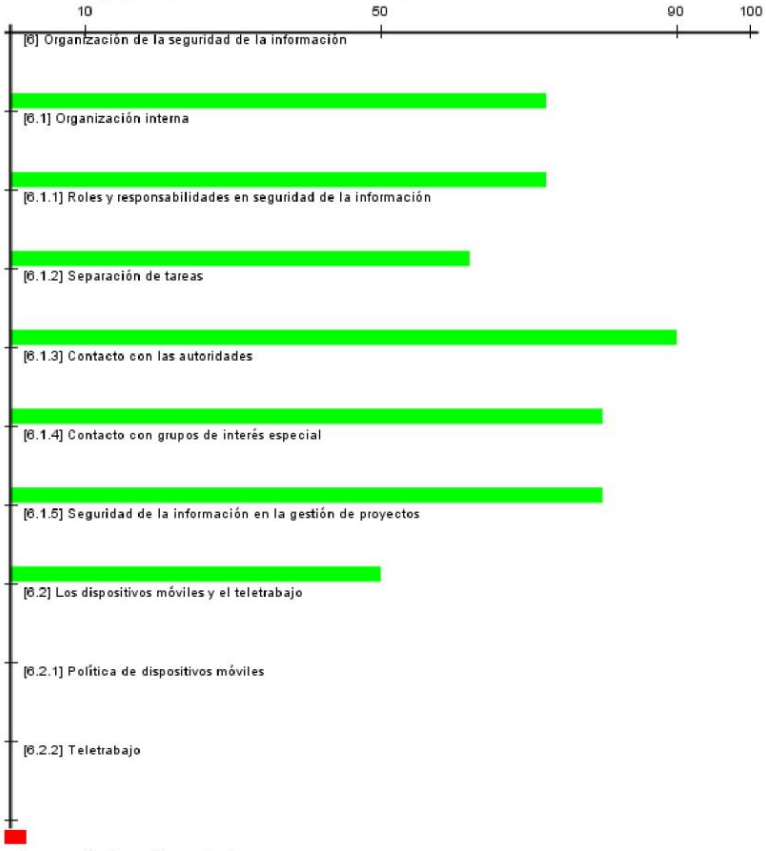
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[5] Políticas de seguridad de la información
[5.1] Directrices de gestión de la seguridad de la información
[5.1.1] Políticas para la seguridad de la información
[5.1.2] Revisión de las políticas para la seguridad de la información

3. [6] Organización de la seguridad de la información



[current] situación actual

[target] situación objetivo

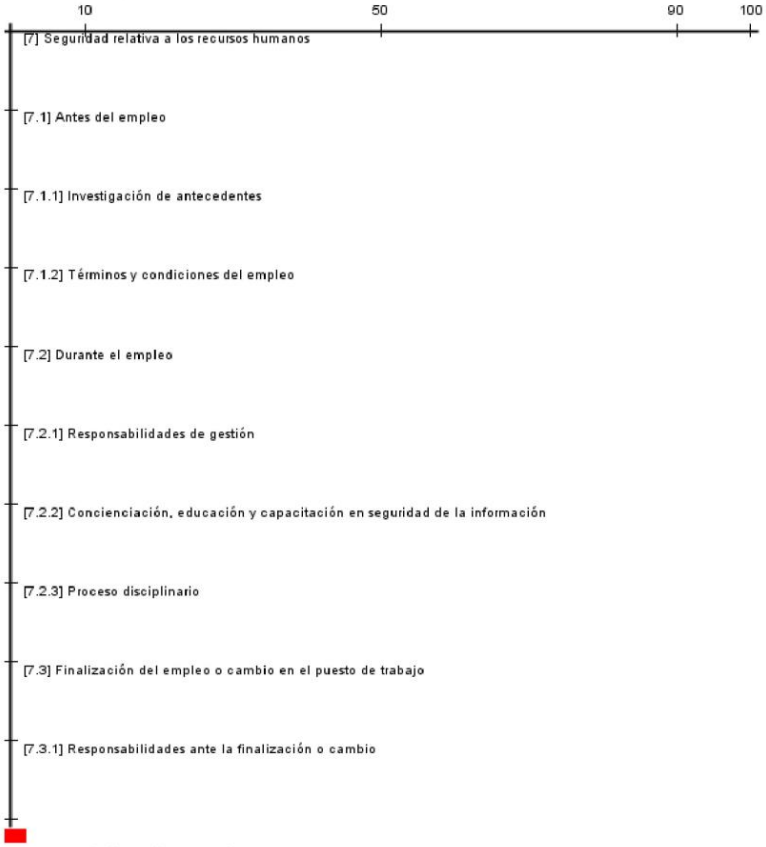
[PILAR] recomendación

dominio: [base] Base

control
[6] Organización de la seguridad de la información
[6.1] Organización interna
[6.1.1] Roles y responsabilidades en seguridad de la información
[6.1.2] Separación de tareas
[6.1.3] Contacto con las autoridades

[6.1.4] Contacto con grupos de interés especial
[6.1.5] Seguridad de la información en la gestión de proyectos
[6.2] Los dispositivos móviles y el teletrabajo
[6.2.1] Política de dispositivos móviles
[6.2.2] Teletrabajo

4. [7] Seguridad relativa a los recursos humanos



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[7] Seguridad relativa a los recursos humanos
[7.1] Antes del empleo
[7.1.1] Investigación de antecedentes
[7.1.2] Términos y condiciones del empleo
[7.2] Durante el empleo
[7.2.1] Responsabilidades de gestión
[7.2.2] Concienciación, educación y capacitación en seguridad de la información
[7.2.3] Proceso disciplinario
[7.3] Finalización del empleo o cambio en el puesto de trabajo
[7.3.1] Responsabilidades ante la finalización o cambio

5. [8] Gestión de activos

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[8] Gestión de activos
[8.1] Responsabilidad sobre los activos
[8.1.1] Inventario de activos
[8.1.2] Propiedad de los activos
[8.1.3] Uso aceptable de los activos
[8.1.4] Devolución de activos
[8.2] Clasificación de la información
[8.2.1] Clasificación de la información
[8.2.2] Etiquetado de la información
[8.2.3] Manipulado de la información
[8.3] Manipulación de los soportes
[8.3.1] Gestión de soportes extraíbles
[8.3.2] Eliminación de soportes
[8.3.3] Soportes físicos en tránsito

6. [9] Control de acceso


10
50
90
100
[9] Control de acceso
[9.1] Requisitos de negocio para el control de acceso
[9.1.1] Política de control de acceso
[9.1.2] Acceso a las redes y a los servicios de red
[9.2] Gestión de acceso de usuario
[9.2.1] Registro y baja de usuario
[9.2.2] Provisión de acceso de usuario
[9.2.3] Gestión de privilegios de acceso
[9.2.4] Gestión de la información secreta de autenticación de los usuarios
[9.2.5] Revisión de los derechos de acceso de usuario
[9.2.6] Retirada o reasignación de los derechos de acceso
[9.3] Responsabilidades del usuario
[9.3.1] Uso de la información secreta de autenticación
[9.4] Control de acceso a sistemas y aplicaciones
[9.4.1] Restricción del acceso a la información
[9.4.2] Procedimientos seguros de inicio de sesión

[current] situación actual

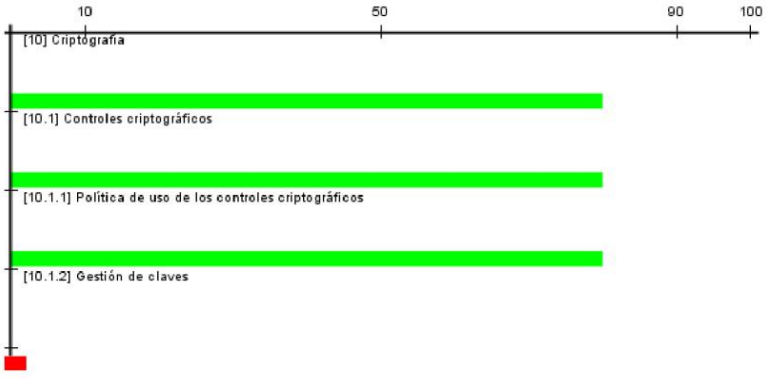
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[9] Control de acceso
[9.1] Requisitos de negocio para el control de acceso
[9.1.1] Política de control de acceso
[9.1.2] Acceso a las redes y a los servicios de red
[9.2] Gestión de acceso de usuario
[9.2.1] Registro y baja de usuario
[9.2.2] Provision de acceso de usuario
[9.2.3] Gestión de privilegios de acceso
[9.2.4] Gestión de la información secreta de autenticación de los usuarios
[9.2.5] Revisión de los derechos de acceso de usuario
[9.2.6] Retirada o reasignación de los derechos de acceso
[9.3] Responsabilidades del usuario
[9.3.1] Uso de la información secreta de autenticación
[9.4] Control de acceso a sistemas y aplicaciones
[9.4.1] Restricción del acceso a la información
[9.4.2] Procedimientos seguros de inicio de sesión
[9.4.3] Sistema de gestión de contraseñas
[9.4.4] Uso de utilidades con privilegios del sistema
[9.4.5] Control de acceso al código fuente de los programas

7. [10] Criptografía



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[10] Criptografía
[10.1] Controles criptográficos
[10.1.1] Política de uso de los controles criptográficos
[10.1.2] Gestión de claves

8. [11] Seguridad física y del entorno


10
50
90
100
[11] Seguridad física y del entorno
[11.1] Áreas seguras
[11.1.1] Perímetro de seguridad física
[11.1.2] Controles físicos de entrada
[11.1.3] Seguridad de oficinas, despachos y recursos
[11.1.4] Protección contra las amenazas externas y ambientales
[11.1.5] El trabajo en áreas seguras
[11.1.6] Áreas de carga y descarga
[11.2] Seguridad de los equipos
[11.2.1] Emplazamiento y protección de equipos
[11.2.2] Instalaciones de suministro
[11.2.3] Seguridad del cableado
[11.2.4] Mantenimiento de los equipos
[11.2.5] Retirada de materiales propiedad de la empresa
[11.2.6] Seguridad de los equipos fuera de las instalaciones
[11.2.7] Reutilización o eliminación segura de equipos

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[11] Seguridad física y del entorno
[11.1] Áreas seguras
[11.1.1] Perímetro de seguridad física
[11.1.2] Controles físicos de entrada
[11.1.3] Seguridad de oficinas, despachos y recursos
[11.1.4] Protección contra las amenazas externas y ambientales
[11.1.5] El trabajo en áreas seguras
[11.1.6] Áreas de carga y descarga
[11.2] Seguridad de los equipos
[11.2.1] Emplazamiento y protección de equipos
[11.2.2] Instalaciones de suministro
[11.2.3] Seguridad del cableado
[11.2.4] Mantenimiento de los equipos
[11.2.5] Retirada de materiales propiedad de la empresa
[11.2.6] Seguridad de los equipos fuera de las instalaciones
[11.2.7] Reutilización o eliminación segura de equipos
[11.2.8] Equipo de usuario desatendido
[11.2.9] Política de puesto de trabajo despejado y pantalla limpia

9. [12] Seguridad de las operaciones


10
50
90
100
[12] Seguridad de las operaciones
[12.1] Procedimientos y responsabilidades operacionales
[12.1.1] Documentación de los procedimientos de operación
[12.1.2] Gestión de cambios
[12.1.3] Gestión de capacidades
[12.1.4] Separación de los recursos de desarrollo, prueba y operación
[12.2] Protección contra el software malicioso (malware)
[12.2.1] Controles contra el código malicioso
[12.3] Copias de seguridad
[12.3.1] Copias de seguridad de la información
[12.4] Registros y supervisión
[12.4.1] Registro de eventos
[12.4.2] Protección de la información de registro
[12.4.3] Registros de administración y operación
[12.4.4] Sincronización del reloj
[12.5] Control del software en explotación

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[12] Seguridad de las operaciones
[12.1] Procedimientos y responsabilidades operacionales
[12.1.1] Documentación de los procedimientos de operación
[12.1.2] Gestión de cambios
[12.1.3] Gestión de capacidades
[12.1.4] Separación de los recursos de desarrollo, prueba y operación
[12.2] Protección contra el software malicioso (malware)
[12.2.1] Controles contra el código malicioso
[12.3] Copias de seguridad
[12.3.1] Copias de seguridad de la información
[12.4] Registros y supervisión
[12.4.1] Registro de eventos
[12.4.2] Protección de la información de registro
[12.4.3] Registros de administración y operación
[12.4.4] Sincronización del reloj
[12.5] Control del software en explotación
[12.5.1] Instalación del software en explotación
[12.6] Gestión de la vulnerabilidad técnica
[12.6.1] Gestión de las vulnerabilidades técnicas
[12.6.2] Restricción en la instalación de software
[12.7] Consideraciones sore la auditoría de sistemas de información
[12.7.1] Controles de auditoría de sistemas de información

10.[13] Seguridad de las comunicaciones

[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[13] Seguridad de las comunicaciones
[13.1] Gestión de la seguridad de redes
[13.1.1] Controles de red
[13.1.2] Seguridad de los servicios de red
[13.1.3] Segregación en redes

[13.2] Intercambio de información
[13.2.1] Políticas y procedimientos de intercambio de información
[13.2.2] Acuerdos de intercambio de información
[13.2.3] Mensajería electrónica
[13.2.4] Acuerdos de confidencialidad o no revelación

11. [14] Adquisición, desarrollo y mantenimiento de sistemas de información


10
50
90
100
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[14.1] Requisitos de seguridad en sistemas de información
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas
[14.1.3] Protección de las transacciones de servicios de aplicaciones
[14.2] Seguridad en el desarrollo y en los procesos de soporte
[14.2.1] Política de desarrollo seguro
[14.2.2] Procedimiento de control de cambios en sistemas
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
[14.2.4] Restricciones a los cambios en los paquetes de software
[14.2.5] Principios de ingeniería de sistemas seguros
[14.2.6] Entorno de desarrollo seguro
[14.2.7] Externalización del desarrollo de software
[14.2.8] Pruebas funcionales de seguridad de sistemas
[14.2.9] Pruebas de aceptación de sistemas
[14.3] Datos de prueba

[current] situación actual

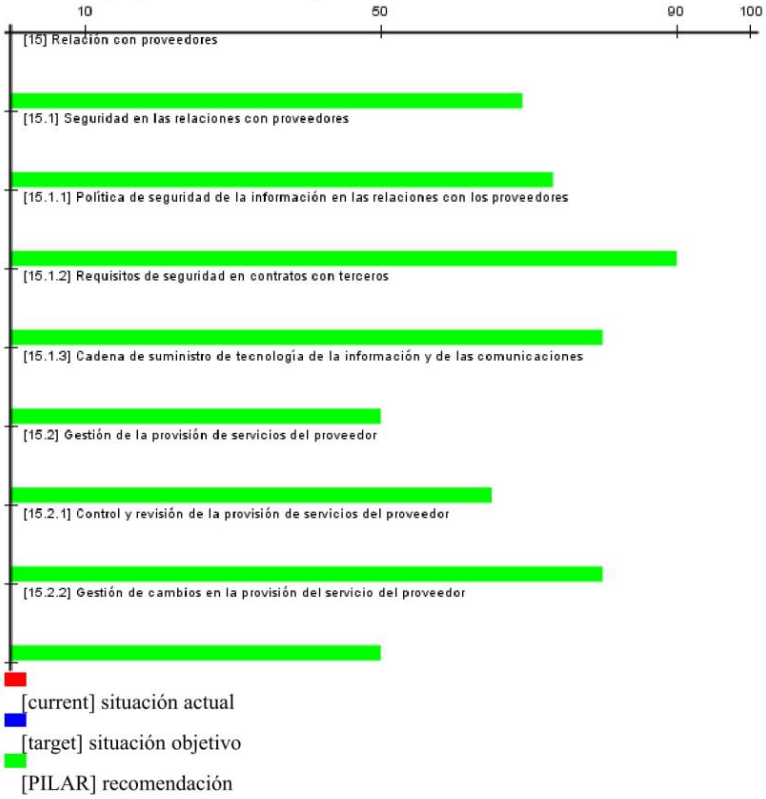
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[14] Adquisición, desarrollo y mantenimiento de los sistemas de información
[14.1] Requisitos de seguridad en sistemas de información
[14.1.1] Análisis de requisitos y especificaciones de seguridad de la información
[14.1.2] Asegurar los servicios de aplicaciones en redes públicas
[14.1.3] Protección de las transacciones de servicios de aplicaciones
[14.2] Seguridad en el desarrollo y en los procesos de soporte
[14.2.1] Política de desarrollo seguro
[14.2.2] Procedimiento de control de cambios en sistemas
[14.2.3] Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
[14.2.4] Restricciones a los cambios en los paquetes de software
[14.2.5] Principios de ingeniería de sistemas seguros
[14.2.6] Entorno de desarrollo seguro
[14.2.7] Externalización del desarrollo de software
[14.2.8] Pruebas funcionales de seguridad de sistemas
[14.2.9] Pruebas de aceptación de sistemas
[14.3] Datos de prueba
[14.3.1] Protección de los datos de prueba

12.[15] Relación con proveedores



[current] situación actual

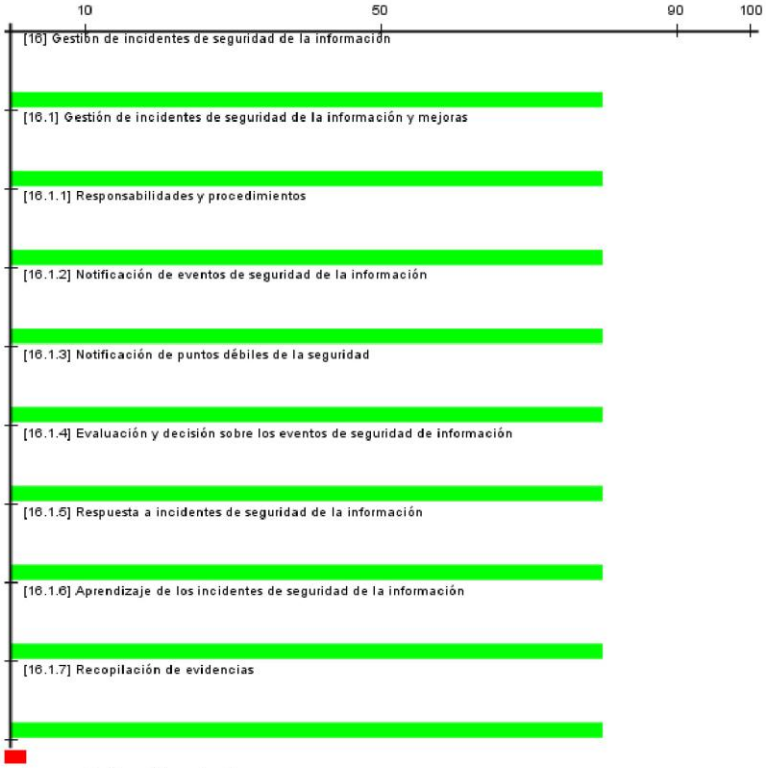
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[15] Relación con proveedores
[15.1] Seguridad en las relaciones con proveedores
[15.1.1] Política de seguridad de la información en las relaciones con los proveedores
[15.1.2] Requisitos de seguridad en contratos con terceros
[15.1.3] Cadena de suministro de tecnología de la información y de las comunicaciones
[15.2] Gestión de la provisión de servicios del proveedor
[15.2.1] Control y revisión de la provisión de servicios del proveedor
[15.2.2] Gestión de cambios en la provisión del servicio del proveedor

13. [16] Gestión de incidentes de seguridad de la información



[current] situación actual

[target] situación objetivo

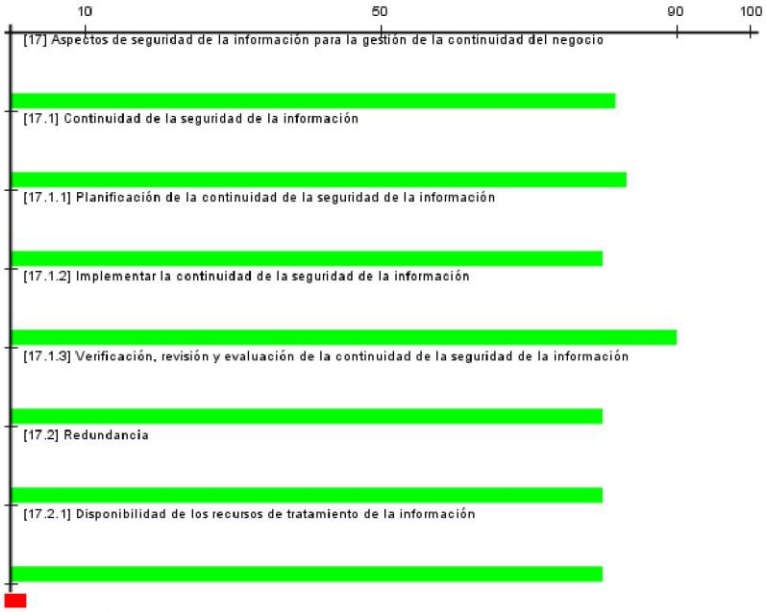
[PILAR] recomendación

dominio: [base] Base

control
[16] Gestión de incidentes de seguridad de la información
[16.1] Gestión de incidentes de seguridad de la información y mejoras
[16.1.1] Responsabilidades y procedimientos
[16.1.2] Notificación de eventos de seguridad de la información
[16.1.3] Notificación de puntos débiles de la seguridad

[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información
[16.1.5] Respuesta a incidentes de seguridad de la información
[16.1.6] Aprendizaje de los incidentes de seguridad de la información
[16.1.7] Recopilación de evidencias

14.[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio
[17.1] Continuidad de la seguridad de la información
[17.1.1] Planificación de la continuidad de la seguridad de la información
[17.1.2] Implementar la continuidad de la seguridad de la información

[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información
[17.2] Redundancia
[17.2.1] Disponibilidad de los recursos de tratamiento de la información

15.[18] Cumplimiento

[current] situación actual

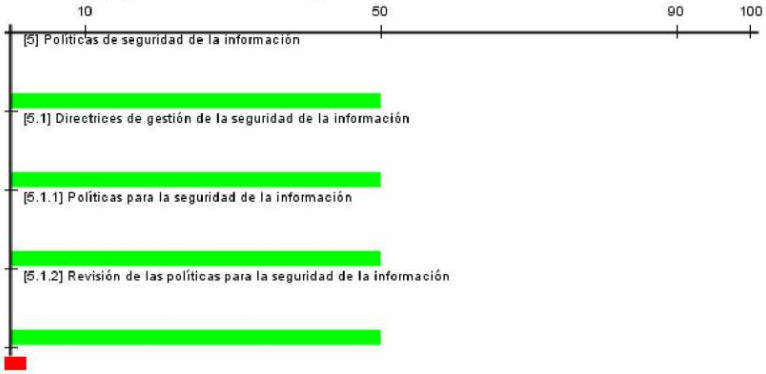
[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[18] Cumplimiento
[18.1] Cumplimiento de los requisitos legales y contractuales
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales
[18.1.2] Derechos de propiedad intelectual (DPI)
[18.1.3] Protección de los registros de la organización
[18.1.4] Protección y privacidad de la información de carácter personal
[18.1.5] Regulación de los controles criptográficos
[18.2] Revisiones de la seguridad de la información
[18.2.1] Revisión independiente de la seguridad de la información
[18.2.2] Cumplimiento de las políticas y normas de seguridad
[18.2.3] Comprobación del cumplimiento técnico

2. [5] Políticas de seguridad



[current] situación actual

[target] situación objetivo

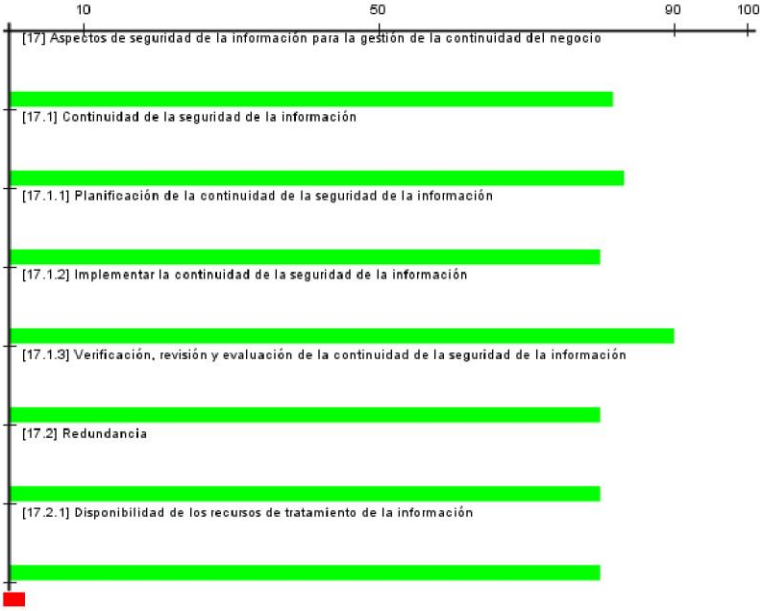
[PILAR] recomendación

dominio: [base] Base

control
[5] Políticas de seguridad de la información
[5.1] Directrices de gestión de la seguridad de la información
[5.1.1] Políticas para la seguridad de la información
[5.1.2] Revisión de las políticas para la seguridad de la información

[16.1.4] Evaluación y decisión sobre los eventos de seguridad de información
[16.1.5] Respuesta a incidentes de seguridad de la información
[16.1.6] Aprendizaje de los incidentes de seguridad de la información
[16.1.7] Recopilación de evidencias

14.[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio



[current] situación actual

[target] situación objetivo

[PILAR] recomendación

dominio: [base] Base

control
[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio
[17.1] Continuidad de la seguridad de la información
[17.1.1] Planificación de la continuidad de la seguridad de la información
[17.1.2] Implementar la continuidad de la seguridad de la información

[17.1.3] Verificación, revisión y evaluación de la continuidad de la seguridad de la información
[17.2] Redundancia
[17.2.1] Disponibilidad de los recursos de tratamiento de la información

15.[18] Cumplimiento

[PILAR] recomendación

dominio: [base] Base

control
[18] Cumplimiento
[18.1] Cumplimiento de los requisitos legales y contractuales
[18.1.1] Identificación de la legislación aplicable y de los requisitos contractuales
[18.1.2] Derechos de propiedad intelectual (DPI)
[18.1.3] Protección de los registros de la organización
[18.1.4] Protección y privacidad de la información de carácter personal
[18.1.5] Regulación de los controles criptográficos
[18.2] Revisiones de la seguridad de la información
[18.2.1] Revisión independiente de la seguridad de la información
[18.2.2] Cumplimiento de las políticas y normas de seguridad
[18.2.3] Comprobación del cumplimiento técnico

Anexo 4: Formato de encuestas

UNIVERSIDAD TÉCNICA DE COTOPAXI
DIRECCIÓN DE POSGRADO
MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO:" ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO."

ENCUESTA A EMPLEADOS

La siguiente encueta va dirigido a los empleados de la Junta Administradora de Agua Potable Pilacoto

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa.

1.- ¿Cree usted que mediante el software PILAR en el plan de contingencia, la información del JAAP este más segura?

SI ☐ NO ☐

2.- ¿Con el software PILAR dentro del plan de contingencia, cree usted que el JAAP esté preparado para estos tipos de desastres tecnológicos y naturales?

SI ☐ NO ☐

3.- ¿Usted recomendaría que el software sea utilizado dentro de un plan de contingencia informático en otras Juntas administradoras de Agua Potable, que estén en zonas de riego?

SI ☐ NO ☐

4.- ¿Mediante la demostración del software PILAR, cree usted que esta herramienta tecnológica es amigable e intuitiva para los empleados del JAAP?

SI ☐ NO ☐

5.- ¿Después de la exposición del software PILAR, usted está satisfecho con los resultados esperados de dicha herramienta?

SI	NO
☐	☐

UNIVERSIDAD TÉCNICA DE COTOPAXI
DIRECCIÓN DE POSGRADO
MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: "ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO."

ENCUESTA A USUARIOS

La siguiente Encueta va dirigido a los usuarios de la Junta Administradora de Agua Potable Pilacoto

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa.

1.- ¿Sabe usted que vive en un sector que es zona de riesgo?

SI ☐ NO ☐

2.- ¿Conoce usted la infraestructura física de la Junta administradora de agua Potable Pilacoto?

SI ☐ NO ☐

3.- ¿Cree usted que la Junta administradora de agua potable está preparada para afrontar un desastre tecnológico y natural?

SI ☐ NO ☐

4.- ¿Conoce usted teléfono de emergencia en caso de desastres tecnológicos y naturales?

SI ☐ NO ☐

5.- ¿Sabe cómo actuar después de un desastre tecnológico y desastres naturales?

SI ☐ NO ☐

6.- ¿Conoces el modo de almacenamiento de información de la JAAPP en caso de un desastre tecnológico y natural?

SI ☐ NO ☐

7.- ¿Sabe usted que es un plan de contingencia?

SI ☐ NO ☐

8.- ¿Estarías de Acuerdo que se elabore un plan de contingencia para la Junta Administradora de agua potable Pilacoto para posibles desastres tecnológicos y Naturales?

SI ☐ NO ☐

9.- ¿Mediante la elaboración del plan de contingencia cree usted que estaríamos preparados para posibles desastres tecnológicos y naturales?

SI ☐ NO ☐

10.- ¿Estarías de acuerdo que después de la elaboración del Plan de Contingencia se dé a conocer a todos los usuarios del JAAP?

SI ☐ NO ☐

UNIVERSIDAD TÉCNICA DE COTOPAXI
DIRECCIÓN DE POSGRADO
MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO:" ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO."

Estimado Profesional Ud. Ha sido seleccionado mediante su conocimiento y trayectoria en laboral sobre la "ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA LOS SISTEMAS INFORMÁTICOS DE LAS JUNTAS ADMINISTRADORAS DE AGUA POTABLE DE LA PARROQUIA DE GUAYTACAMA - CASO DE ESTUDIO JUNTA ADMINISTRADORA DE AGUA POTABLE PILACOTO."

Datos del Profesional

Nombre:

Título de tercer /Cuarto Nivel:

Cargo que Desempeña:

Años de Experiencia en el área:

Instructivo:

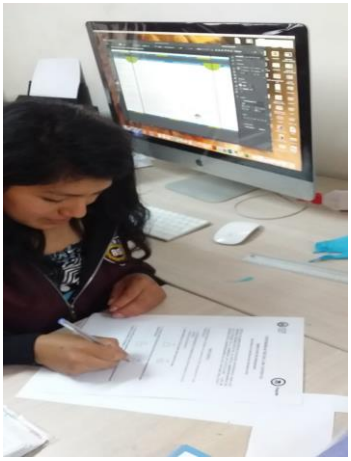
Es una escala descendente de 5 hasta 1, donde 5 – Excelente, 4 – Muy Bien, 3 – Bien, 2 – Regular, 1 – Insuficiente.

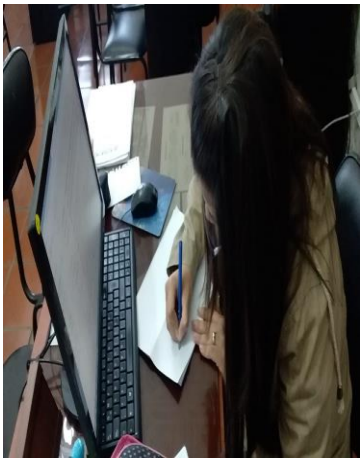
Metodología Magerit y Herramienta Pilar		**1**	**2**	**3**	**4**	**5**
1	Contamos con profesionales que tienen experiencia en la elaboración de un plan de contingencia					
2	Cree usted la metodología Magerit y el software es fundamental para un plan de contingencia					
3	El usuario verificar los reporte del software de la manera más sencilla y eficaz					
4	La metodología y el software son más compatibles para los respaldos de información					

5	Después de la exposición de la metodología y el software PILAR, usted recomendaría la utilización de dicha metodología y herramienta					

Seguridad y Prevención de Riesgos		**1**	**2**	**3**	**4**	**5**
1	Contamos con profesionales que tienen experiencia en la elaboración de un plan de contingencia bajo normas de seguridad					
2	Cree usted la metodología Magerit utiliza los estándares internacionales para un plan de contingencia					
3	Cree usted que las normas de seguridad son esenciales para un desastre natural y tecnológico					
4	Usted recomendaría que utilicen la metodología Magerit en otras Juntas administradoras de Agua Potable, que estén en zonas de riego.					
5	Después de la exposición de la metodología y el software PILAR, usted recomendaría la utilización de dicha metodología y herramienta					

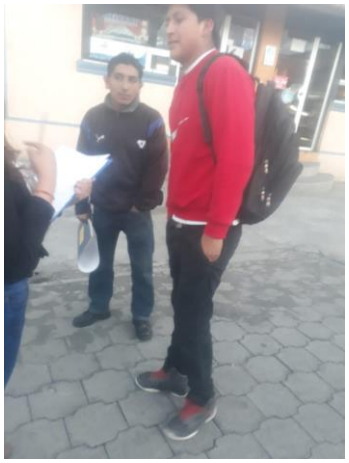
Anexo 5: Aplicación de encuestas a empleados





Anexo 6: Aplicación de encuestas a usuarios



Anexo 7: Cotización PILAR

EAR / PILAR

EAR / PILAR
adquisición

Las herramientas EAR son propiedad de

A.L.H. J. Mañas S.L.

La aplicación puede descargarse libremente:

- uso libre para consultar análisis de riesgos realizados en soporte fichero (.mgr) (modo "**read only**")
- para generar nuevos análisis de riesgos se requiere una licencia comercial
- para utilizar PILAR sobre base de datos se requiere una licencia comercial extendida.

Coste

herramienta	precio
μPILAR	250 €
PILAR Basic	500 €
PILAR Estándar	1.500 €
PILAR Estándar + BBDD	2.000 €
RMAT	3.000 €

Incluyendo:

1. garantía frente a defectos por 1 año
2. derecho a todas las actualizaciones dentro de la misma versión (por ejemplo, de 5.x a 5.y)

Puede ver una comparativa de las diferentes versiones de PILAR:

compara_es.pdf

Nuevas versiones

Servicio de mantenimiento. Por una tarifa anual del 15% del precio de venta, se dispondrá de las nuevas versiones. (por ejemplo, de 5.x a 6.y).

Alternativamente, si no ha contratado el servicio de mantenimiento, para saltar de una versión a la siguiente, se facturará un 15% del precio de la nueva versión.

Adquisición

Solicitud de licencia comercial

Información

info@pilar-tools.com

Los organismos de la Administración Pública deben dirigirse al Centro Criptológico Nacional:

ccn@cni.es

Anexo 8: Cotización almacenamiento en la nube

Tomando en cuenta que, los precios de Amazon Web Services AWS son similares a las tarifas de los servicios de servicios básicos, ya que solo se paga por lo que consume, y una vez que cancela el servicio, no se aplican costos adicionales, se seleccionó Amazon Simple Storage Services (S3) para guardar los respaldos en línea de la JAAP que en promedio tienen un tamaño de 1Tb (1000 Gb)