UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

DISEÑO DE UNA METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES PARA EL MINISTERIO DE EDUCACIÓN

PRESENTADO POR:

ADA PATRICIA LOVO ZELAYA

KEVIN JAIME RIVERA FLORES

ADÁN MAURICIO ROMERO LÓPEZ

PARA OPTAR AL TÍTULO DE:

INGENIERO DE SISTEMAS INFORMÁTICOS

CIUDAD UNIVERSITARIA, DICIEMBRE DE 2009

UNIVERSIDAD DE EL SALVADOR

RECTOR

MSc. RUFINO ANTONIO QUEZADA SÁNCHEZ

SECRETARIO GENERAL

LIC. DOUGLAS VLADIMIR ALFARO CHÁVEZ

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO

ING. MARIO ROBERTO NIETO LOVO

SECRETARIO

ING. OSCAR EDUARDO MARROQUÍN HERNÁNDEZ

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

DIRECTOR

ING. CARLOS ERNESTO GARCÍA GARCÍA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO DE SISTEMAS INFORMÁTICOS

Título

DISEÑO DE UNA METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES PARA EL MINISTERIO DE EDUCACIÓN

Presentado por

ADA PATRICIA LOVO ZELAYA

KEVIN JAIME RIVERA FLORES

ADÁN MAURICIO ROMERO LÓPEZ

Trabajo de Graduación Aprobado por:

Docente Director

Ing. Pedro Eliseo Peñate Hernández

San Salvador, diciembre de 2009

Trabajo de Graduación Aprobado por:

Docente Director

Ing. Pedro Eliseo Peñate Hernández

A Dios, por tener fe; aunque debía haber sido al revés.

Ada Lovo

A Dios, mi más grande amigo el que siempre ha estado conmigo y nunca me fallo

Kevin Rivera

A Dios Todopoderoso por ser la luz, la guía y por darme la inteligencia y sabiduría necesaria en este camino que llevé.

Adán Romero

Agradecimientos

Reconocemos la importante colaboración del Ing. Max Fernando Mirón en la ejecución de este proyecto, así como del Ing. Pedro Eliseo Peñate, por su asesoría académica, la cual ha sido fundamental para el éxito del Trabajo de Graduación.

Ada, Kevin y Adán.

Agradezco de todo corazón a:

Señor Todopoderoso: Por haberme permitido llegar hasta este momento y bendecirme continuamente; por escucharme y responderme; por acompañarme cada día de mi vida incluso desde antes de tejerme en el vientre de mi madre.

Mis padres: Por el amor y apoyo incondicional que me han manifestado; por estar ahí para mí. Los amo y reconozco sus innumerables esfuerzos y sacrificios. ¡¡¡Infinitamente gracias!!!

Mis hermanas y hermano: Por su amor fraternal para conmigo, por su ayuda y por hacerme partícipe en sus proyectos y sueños a pesar del tiempo que no hemos estado juntos.

Familiares: Por tenerme presente en sus oraciones; por la confianza demostrada y por todas las atenciones que me han prodigado.

Maestros: Aquellos que me hicieron ver que el conocimiento de las ciencias tiene sentido solamente si se aplica en la creación de una sociedad más humana.

Amistades: Por sus muestras de cariño y palabras de aliento. Por su presencia, incluso desde la distancia.

Todos y todas: Quienes de una u otra manera me han apoyado a lo largo de este camino, y cuyos nombres no alcanzaría a mencionar. En mi corazón guardo sus muestras de afecto y simpatía. Bendiciones para ustedes.

Ada Lovo

AGRADEZCO A:

A Dios todopoderoso por haberme permito avanzar y perseverar en este arduo camino que lleva a la culminación de la carrera, por haberme brindado la sabiduría, la inteligencia y paciencia para tomar las mejores decisiones. Gracias por siempre estar conmigo y protegerme en los momentos difíciles por darme la fuerza interior para seguir y nunca claudicar.

A mis padres Carlos Jaime Rivera y Reina Armida Flores por darme todo en esta vida, por apoyarme en lo moral y lo económico a lo largo de la carrera y darme valor para enfrentar los conflictos. Gracias por estar siempre creyendo en mí y brindarme siempre su amor.

A mi Hermano Geovanny Moisés por estar compartiendo mis sueños, apoyándome y haciendo que me esfuerce más en busca de mi carrera.

A mi familia que me ha dado todo su apoyo, su ayuda en los momentos que los necesite y por estar siempre animándome hasta la conclusión de mi carrera.

A mis Amigos que han estado dándome sus palabras de afecto y de fuerza para que nunca me rindiera y su ayuda cuando la necesite.

Gracias a todas las demás personas que de alguna u otra forma estuvieron conmigo, que me dieron sus consejos, su guía, su amistad y su amor, gracias de todo corazón.

Kevin Jaime Rivera

AGRADEZCO

A Dios Todopoderoso porque me ha permitido lograr esta meta más en mi vida y me ha fortalecido con su Divina Presencia , por darme la inteligencia y sabiduría necesaria en este camino que llevé y como siempre lo ha hecho en todo momento y lugar. Por todas las bendiciones y el amor que siempre me han dado fuerzas para seguir adelante a pesar de las dificultades.

A mis padres Juan Romero y Magdalena López por sus oraciones, esfuerzo y dedicación y por haberme apoyado en todo momento de mi vida en especial para obtener este logro, gracias por darme ánimo en los momentos más difíciles de mi carrera. Este triunfo es para ustedes.

A mi hermana Magdalena Isabel Romero por la confianza, el apoyo y el amor que siempre me has tenido, gracias por tus consejos y el soporte e inspiración que significaste durante toda mi carrera. Este triunfo te lo dedico especialmente a ti ya que sin tu apoyo, paciencia y comprensión no lo hubiera logrado Nenita te quiero mucho y que Dios te bendiga y te conceda la paz y felicidad en tu hogar.

A mis hermanas y hermanos Elia, Dina, Nuria, Elvira, Juan y Eduardo, por la compañía que siempre me han brindado, por todo su apoyo, su comprensión y el amor que siempre me han tenido. Ustedes son las personas que más quiero y este logro también es de ustedes.

A mis abuelos Simeón López y Lidia Tobar por ser dos personas maravillosas y un gran ejemplo a seguir, gracias abuelitos por todos los consejos que me han brindado a lo largo de mi vida.

A mi abuelito Sotero Romero (Q.D.D.G), Elmer Bladimir Romero (Q.D.D.G) y Ana Judith Romero (Q.D.D.G), siempre estarán presentes en mi corazón porque sé que desde el cielo me están mirando y están orgullosos de mí.

A toda mi familia y amigos que con sus palabras alimentaban mis ganas de seguir adelante, porque siempre creyeron en mí y por el afecto que siempre recibí de esas personas especiales.

A la familia Cardona Rodríguez que siempre me apoyaron y me dieron ánimos para seguir adelante en este proyecto hasta la culminación del mismo.

A mis compañeros de Tesis por ser magníficas personas, por brindarme toda su amistad, gracias por ser mi apoyo y permitirme ser el suyo en todo el desarrollo de este proyecto y por acompañarme en este último paso de nuestras carreras.

A todas las personas que de alguna u otra forma colaboraron para que esta meta llegara a su final, hago extensivo mi más sincero agradecimiento.

Adán Mauricio Romero López

INDICE

INTRODUCCIÓN.

Un riesgo se define como la probabilidad de que un suceso no planeado afecte negativamente el desarrollo o ejecución de una actividad. Los riesgos existen en todas las circunstancias, y aunque algunas veces su materialización no acarrea una consecuencia trascendentemente desastrosa, en otros casos conlleva a grandes pérdidas y/o frustraciones de importantes proyectos. Con el afán de minimizar el impacto cuando un riesgo se materializa, o en el mejor de los casos, de reducirlo o mitigarlo, surge la Administración de Riesgos.

Por otra parte, las Tecnologías de Información y Comunicaciones (TIC), han evolucionado y se han vuelto indispensables para la vida de las personas, quienes las han implementado en sus organizaciones con el fin de incrementar la productividad en las mismas. Sin embargo, estas tecnologías son altamente susceptibles a verse afectadas por diferentes tipos de riesgos que al materializarse afectan a los servicios que soportan.

Ante esta situación, el Ministerio de Educación de la República de El Salvador (MINED, por sus siglas), a través de la Dirección de Informática, con la participación directa de la Gerencia de Normas y Calidad, entidad responsable de la Administración de los Riesgos de estas tecnologías, pretenden encontrar la forma de administrar los riesgos de las TIC y es con el afán de satisfacer esta necesidad que surge la idea de diseñar una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones que permita ser aplicada en referido Ministerio.

El proyecto inicia con el desarrollo de un Diagnóstico sobre la utilización de Metodologías de Administración de Riesgos de TIC desde un enfoque externo e interno. En el enfoque externo se presentan el plan de tabulación y el respectivo análisis de datos que se obtuvieron de la investigación en las instituciones gubernamentales y autónomas generando información de gran relevancia en la utilización de mecanismos de administración de riesgos de TIC, a la vez que dieron a conocer las debilidades más frecuentes que padecen las instituciones en este respecto. En el enfoque interno se presenta la información recopilada por medio de la observación y entrevistas realizadas en el Ministerio de Educación.

Este Diagnóstico constituye una herramienta metodológica utilizada para recabar valiosos insumos que permitieran una visión más amplia al momento de determinar el problema, así como de identificar los requerimientos que permitieran diseñar una propuesta de solución eficaz.

Como resultado, surge MARMINED: una alternativa que ofrece una solución efectiva y ordenada al problema de la Gestión de Riesgos de TIC en el Ministerio de Educación, agrupando esfuerzos conjuntos de las diferentes Gerencias de la Dirección de Informática, bajo la coordinación de la Gerencia de Normas y Calidad .

MARMINED se acompaña de un prototipo de software funcional que facilita su utilización mediante la automatización de determinadas tareas. MARMINED es una aplicación web que ha sido construida adoptando el Modelo de Prototipado como Ciclo de Vida de Desarrollo de Software mediante el Diseño y la Programación Orientada a Objetos.

Finalmente, se presenta la Documentación respectiva que servirá de guía a los diferentes tipos de usuarios para la correcta implementación, mantenimiento, consulta y utilización de MARMINED.

OBJETIVOS.

Objetivo General.

- Diseñar una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación con el fin de identificar, analizar, evaluar y mitigar los diferentes tipos de riesgos que pueden influir o afectar los objetivos que persigue dicho ministerio al usar las Tecnologías de Información y Comunicaciones**.**

Objetivos Específicos.

- Investigar la utilización de metodologías de Administración de Riesgos existentes orientados a las Tecnologías de Información y Comunicaciones.
- Realizar un diagnóstico de la situación actual en la utilización de las metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones en el MINED.
- Extraer y analizar los requerimientos para el diseño de la Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones en el MINED.
- Diseñar la Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para ser aplicadas en el MINED.
- Elaborar un prototipo de software como parte de la Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para ser implementado en el MINED.

JUSTIFICACIÓN DEL PROYECTO.

El Ministerio de Educación, en su afán de poder satisfacer las necesidades que sus usuarios demandan, ha tenido a bien incrementar su activo mediante la adquisición de Tecnologías de Información y Comunicaciones desde el año 2004 hasta la fecha.

La inversión en TIC ha ido en aumento hasta que hoy en día suma $ 3.5 millones, una cantidad nada despreciable, considerando sobre todo que tal adquisición ha surgido proveniente de las arcas del Estado salvadoreño.

El Ministerio de Educación paga anualmente una póliza de $ 20,000.00[1] en concepto de seguro por daños al equipo de TIC, pero dicho seguro no cubre más de $ 200,000.00, es decir, solo un 5.71% del valor de la inversión.

Dado este contexto, es sumamente importante contar con un mecanismo de seguridad que minimice el riesgo de daños y/o fallos en el equipo y en los diferentes sistemas que tienen en ejecución.

Por otra parte, el MINED tiene presupuestado $ 1,320,000.00 para la solvencia de problemas relacionados solamente con la infraestructura de red, si a eso sumamos el monto de las acciones a realizar para solucionar los otros problemas de TIC que más afectan el desarrollo de las actividades, por la cantidad de procesos dependientes y por el impacto que producen[2], sumando también el tratamiento y solución de los otros fallos, se tiene un aproximado de $ 600,000.00, es decir, casi $ 2,000,000.00 que pueden ser invertidos de diferente manera si se contara con una Metodología de Administración de Riesgos de TIC que disminuya el monto de estos gastos.

La Metodología que se propone pretende reducir esos gastos por un costo que representa el 1%[3] del valor del activo a proteger, en otras palabras, la Metodología propuesta ofrece importantes beneficios frente a un costo de desarrollo relativamente bajo.

---

[1] Datos proporcionados por la Dirección de Informática del MINED.

[2] Ver Anexo 1A en el que se presenta el detalle de los Criterios de Medición de Riesgo. El Anexo 1B muestra que el servicio con mayor porcentaje de criticidad es el de fallos en la Infraestructura de Red.

[3] Cálculo obtenido aplicando regla de 3, *porcentaje del valor de la metodología respecto del activo a proteger* = costo de la metodología propuesta por 100% entre el valor del activo a proteger.

IMPORTANCIA DEL PROYECTO.

Una vez implementada la Metodología para la Administración de Riesgos de Tecnologías de Información y Comunicaciones, ofrecerá una efectiva gestión de los riesgos que se presentan actualmente respecto de las tecnologías de información y comunicaciones que se utilizan en el Ministerio de Educación.

Alrededor de 2,600 usuarios administrativos se beneficiarán con el uso de la Metodología, ya que se reducirá la materialización de las amenazas de fallos de las tecnologías de información significativamente. Es importante destacar que existen también beneficiarios indirectos, los cuales suman aproximadamente 32,000 docentes y 250,000 estudiantes de educación media en centros públicos; 90,000 estudiantes en centros privados, que forman parte del sistema educativo nacional y que utilizan diferentes servicios de sistemas de información del MINED quienes se ven afectados cuando estos sistemas colapsan por una causa determinada; se interrumpen actividades, se generan atrasos en la ejecución de los diferentes programas de estudio, y otras tantas repercusiones que entorpecen el cumplimiento de las metas trazadas; tal es el caso de la Gerencia de Tecnologías Educativas, quienes administran sistemas de información desde Internet contando con alrededor de 372,000[4] usuarios a nivel nacional; al implementar la Metodología propuesta, mediante la Gerencia de Normas y Calidad, se podrán reducir las probabilidades de ocurrencia de fallos de las TIC.

Por otra parte, vale mencionar que se ha presupuestado una importante cantidad de recurso público para ser destinado al rubro de las tecnologías de información para el Ministerio de Educación; dicho monto asciende a $ 2, 000,000.00 para el presente año[5]. Hasta principios de 2009, la inversión realizada desde 2004 en el rubro de TIC totalizaba $ 3, 500,000.00[6], lo cual enfatiza la importancia de cuidar dicho activo, dándole el mejor uso posible y minimizando los riesgos que le provocaran un decrecimiento en su vida útil, así como también garantizando el máximo desempeño de las mismas con el propósito de cumplir con la misión del Ministerio de Educación, con la eficiencia y eficacia que de esta importante Institución Pública se demande.

[4] Datos proporcionados por la Dirección de Informática del MINED.
[5] Este monto todavía no ha sido invertido. Datos proporcionados por la Dirección de Informática del MINED.
[6] Datos proporcionados por la Dirección de Informática del MINED.

ALCANCES DEL PROYECTO.

- La propuesta de solución será diseñada de manera que cumpla con los requerimientos exclusivos de la Gerencia de Normas y Calidad de la Dirección de Informática del MINED orientadas a la administración de riesgos de TIC, por lo que no se ha contemplado las responsabilidades de otras unidades organizativas de dicha Institución.

- El proyecto está dirigido al Ministerio de Educación y de manera general a todas las instituciones que cuenten con una infraestructura de TIC similar a la de referido Ministerio que deseen reducir las amenazas de fallos en las TIC mediante una administración de riesgos eficiente y efectiva.

- El proyecto que aquí se presenta parte del desarrollo de un Diagnóstico de la situación actual respecto de la utilización de metodologías de administración de riesgos de TIC en el Ministerio de Educación, como institución de referencia, así como también en otras instituciones gubernamentales fortaleciendo de esta manera el aporte social que la propuesta de Metodología de Administración de Riesgos de TIC ofrece a los usuarios directos e indirectos del Ministerio de Educación.

- La Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones se acompaña de un prototipo de software.

FORMULACIÓN DEL PROBLEMA.

Planteamiento del problema

La Gerencia de Normas y Calidad, entidad que depende de la Dirección de Informática del Ministerio de Educación es la encargada de mantener un estricto control de las normas y calidad de las tecnologías de información y comunicaciones que se podrían incumplir en el área administrativa de dicho Ministerio.

Actualmente no se ha adoptado un procedimiento que facilite la administración de los riesgos, lo que conlleva a que la potencialidad de ocurrencia de estos riesgos se materialice, convirtiéndose en amenazas puntuales que repercuten en las operaciones de las diferentes instituciones que utilicen tecnologías de información y comunicaciones. La Figura 1 muestra el Planteamiento del Problema de forma gráfica.

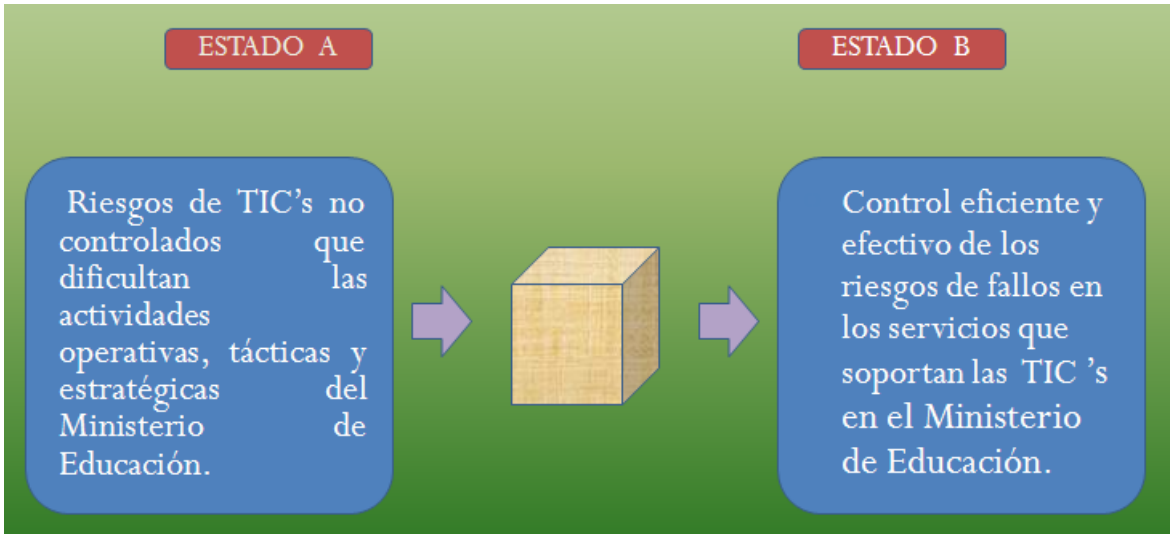


Figura 1. Planteamiento del problema.

Análisis del Problema

Entrada: Riesgos de Tecnologías de Información no controlados que dificultan las actividades operativas, tácticas y estratégicas del Ministerio de Educación.

Variables de Entrada:

- Registro de fallos de las Tecnologías de Información en la Dirección de Informática del Ministerio de Educación.
- Registro de gastos ocasionados por reparación de fallos de Tecnologías de Información en la Dirección de Informática del Ministerio de Educación.
- Categorización de Riesgos de las Tecnologías de Información, así como su impacto en el desarrollo de actividades.
- Otras metodologías para la Administración de Riesgos.
- Lineamientos impuestos por la Corte de Cuentas de la República acerca de la Administración de Riesgos en entidades gubernamentales.
- Información de estándares o normas a seguir.

Salida: Control eficiente y efectivo de los riesgos de fallos en los servicios que soportan las TIC en el Ministerio de Educación.

- Metodología para la Administración de Riesgos de Tecnologías de Información.
- Prototipo funcional de la propuesta de Metodología para Administración de Riesgos de Tecnologías de Información.

Restricciones:

- El proyecto debe ser terminado en un período menor o igual a 8 meses.

Criterios:

- Facilidad de aplicación de la Metodología propuesta.
- Metodología sencilla y práctica.
- Efectividad en Reducción de Riesgos hasta en un 76%.

Uso:

- En todas las direcciones del Ministerio de Educación, bajo la responsabilidad de la Dirección de Informática a través de la Gerencia de Normas y Calidad.

CAPITULO I: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL.

A. OBJETIVOS DEL DIAGNÓSTICO.

Objetivo General.

- Diagnosticar la situación actual respecto a la utilización de metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones en las instituciones gubernamentales de manera que se identifiquen la calidad de los servicios, la frecuencia de fallos de TIC y los procedimientos actuales para llevar a cabo dicha administración.

Objetivos Específicos.

- Definir el tamaño de la muestra de las instituciones gubernamentales a visitar.

- Establecer el contexto de las instituciones gubernamentales con respecto a la utilización de metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones para determinar las oportunidades y amenazas a las que se enfrentan estas instituciones en materia de administración de riesgos de TIC.

- Determinar la situación de adopción y aprovechamiento de la utilización de metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones en las instituciones gubernamentales a fin de identificar las fortalezas y debilidades que estas instituciones pueden obtener al administrar riesgos de TIC.

- Analizar la Situación Externa de las instituciones gubernamentales y la situación interna del MINED en la administración de riesgos de TIC para determinar los puntos claves que debe contener una metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones.

B. FORMULACIÓN DE HIPÓTESIS.[7]

1. Hipótesis general.

Se formula la hipótesis general, siendo ésta la respuesta tentativa al problema de estudio; se presenta una hipótesis nula, que nos servirá para aceptar o rechazar la variable que sea definido como independiente (causa) y como la manipulación afecta la variable dependiente (efecto), además se enuncian hipótesis auxiliares las cuales dando respuesta a cada una de ellas nos permitirá aceptar o rechazar la general que es el centro de la investigación.

- "La utilización de una metodología de administración de riesgos de tecnologías de información y comunicaciones en las instituciones gubernamentales, favorecerá alrededor de un 76% a la disminución de los riesgos de ocurrencia de fallos de los servicios soportados por estas tecnologías".

2. Hipótesis nula.

La formulación de esta hipótesis indica que la información a obtener es contraria a la hipótesis general, con esta hipótesis se pretende negar la variable independiente, es decir, la causa identificada como origen del problema es extraña, por lo tanto debe rechazarse como tal.

- "La utilización de una metodología de administración de riesgos de tecnologías de información y comunicaciones en las instituciones gubernamentales no favorecerá en lo absoluto a la disminución de los riesgos de ocurrencia de fallos de los servicios soportados por estas tecnologías".

3. Hipótesis alternativa.

- "La falta de controles sobre los riesgos en las instituciones gubernamentales influyen en un 80% en la ocurrencia de fallos en las TIC".

[7] Ver apartado Referencia Bibliográfica I: Libros Literal 2.

4. Operacionalización de las variables de estudio.

a. Conceptualización de las hipótesis y variables de estudio.

- Instituciones gubernamentales y autónomas: Entidades que son parte del gobierno y que dependen administrativa y económicamente del aparato estatal.
- Utilización de una metodología de administración de riesgos de TIC: Variable independiente a medir en el diagnóstico.
- Disminución de los riesgos: Variable dependiente de la variable a medir.

b. Clasificación de la variable de acuerdo a su aspecto de estudio.

El aspecto de estudio al cual se enfocará nuestro trabajo es en el área administrativa.

c. Determinación de variables generales.

Se determinó que la variable general es: Metodología de administración de riesgos de TIC.

La relación entre las variables independiente y dependiente es una relación de proporción inversamente proporcional, debido a que "a mayor porcentaje de utilización de una metodología de administración de riesgos de TIC en las instituciones gubernamentales existe una disminución de los riesgos de TIC".

d. Matriz de Indicadores.

En la Tabla 1 se muestra la Matriz de Indicadores conteniendo la variable general, sus dimensiones y los indicadores para cada dimensión dentro de las instituciones.

Variable General	Dimensiones	Indicadores
Metodología de administración de riesgos de TIC.	**Procedimentales**	Manuales de procedimientos Normas utilizadas Personal encargado Beneficios prestados por el uso de la metodología
	Servicios	Fallos de servicios de TIC Beneficios de TIC Productividad Eficiencia y efectividad de servicios de TIC Soporte a los servicios de TIC
	Económicos	Costos por fallos de TIC Inversión en TIC Bitácora de gastos por fallos

Tabla 1. Matriz de Indicadores.

E. OPERACIONES METODOLÓGICAS. [8]

1. Definición del tipo de estudio.

El diagnóstico de la utilización de metodologías de administración de riesgos de TIC constituye un estudio **descriptivo.**

Los estudios descriptivos están dirigidos a determinar cómo es, cómo está la situación de las variables o estudios en una población, la presencia o ausencia de algo, la frecuencia con que ocurre un fenómeno. Estas investigaciones brindan bases cognoscitivas para otros estudios, para posibles hipótesis a comprobar o rechazar.

2. Delimitación de la investigación.

La delimitación de la investigación es un proceso que implica, bajar de los niveles abstractos, a los más concretos y operativos en la investigación.

El estudio contará con dos enfoques uno externo y otro interno. Para el enfoque externo se ha delimitado la zona metropolitana y alrededores como región de estudio, ya que es en referido lugar donde se concentran la mayor cantidad de instituciones gubernamentales y autónomas que cuentan con una mayor infraestructura tecnológica. El enfoque interno se realizará en el Ministerio de Educación.

3. Determinación de la población y muestra.

Una muestra es una reunión de unidades de estudios que forman una parte representativa de la porción o parte representativa de la población o universo.

Algunas de las ventajas que ofrece la investigación a través del muestreo son:

i. Permite que el estudio se realice en menor tiempo
ii. Los costos de estudiar todos los elementos de una población son elevados.
iii. Puede existir una imposibilidad física de verificar todos los elementos.
iv. Posibilita profundizar en las variables.
v. Permite tener mayor control de las variables a estudiar.

Para éste caso, se ha optado por un diseño muestral ¨por conglomerado¨ el cual consiste en escoger grupos de unidades de estudio llamadas conglomerados, los cuales son escogidos

[8] Ver apartado Referencia Bibliográfica I: Libros Literal 2.

al azar. Éstos pueden ser subdivisiones geográficas tales como departamentos, municipios, cantones; o bien instituciones como escuelas, etc. Una vez seleccionadas las áreas, las unidades de estudio elementales de las cuales se ha de capturar el dato deseado, se eligen aleatoriamente, siguiendo un diseño simple.[9]

En la determinación del tamaño de la muestra, al saber de la existencia de las 290 instituciones en El Salvador por medio de una visita de campo a la Corte de Cuentas de la República se aplica el diseño muestral por conglomerado para delimitar la zona geográfica, ya que nos permite reducir el costo en una investigación de una población dispersa, por lo que el resultado nos deja con un universo de 42 instituciones, lo cual obedece a la delimitación geográfica definida previamente. Sin embargo, también se combinó con el diseño muestral dirigido en el que se justifica a visitar a aquellas instituciones que representan y poseen el conocimiento para proporcionar la información que el estudio necesita y que con la aleatoriedad no se lograría cumplir.

Se utilizará la fórmula que obtiene el tamaño de la muestra a partir de la proporción de éxito y es la siguiente:

$$n = \frac{NZ^2P(1-P)}{(N-1)(LE)^2 + Z^2P(1-P)}$$

Donde:

Z: Nivel de confianza.

N: Tamaño de universo.

LE: Error máximo tolerable.

P: Probabilidad de éxito.

Aplicando en el nivel de confianza para una investigación de carácter tecnológico según el libro de Estadística Aplicada a los Negocios y Economía[10] es de 90 % de nivel de confianza por lo que el valor de Z resulta ser de 1.64 y LE es igual 0.1 entonces sustituyendo en la fórmula anterior.

Z= 1.64.

[9] Tomado de *¨Así se investiga, Pasos para hacer una investigación¨*, de E. Zacarías Ortez. Ver Referencia Bibliográfica I: Libros Literal 3.

[10] Ver apartado Referencia Bibliográfica I: Libros Literal 4.

N= 42

LE= 0.1

P= 0.5

Entonces el resultado es:

n = 26.09 ~ 27 instituciones.

Al calcular el valor de la muestra aplicando la fórmula anterior da como resultado 26.09, por lo que se aproximó a 27.

4. Selección de técnicas e instrumentos de investigación.

En esta sección se determinarán los instrumentos a utilizar para recolectar y registrar la información.

a. Encuesta: En el enfoque externo se realizará una encuesta telefónica en las instituciones que se determinaron en la muestra con el fin de conocer si en dichas instituciones se utiliza algún mecanismo de administración de riesgos de TIC. Posteriormente, se utilizará un cuestionario conteniendo una serie de preguntas elaboradas cuidadosamente sobre los hechos y aspectos que interesan a la administración de riesgos de TIC.

b. Entrevista: En el enfoque interno se utilizarán una entrevista no estructurada en la cual se van formulando conforme el entrevistado va respondiendo a las situaciones planteadas.

c. Observación: Se realizará un registro visual de la forma de administrar los riesgos de TIC en el Ministerio de Educación, clasificando los hechos pertinentes de acuerdo con un esquema previsto, basados en los objetivos planteados y en la determinación de las unidades de observación y los aspectos a registrar.

5. Plan de Tabulación y Análisis de Datos.

a. Tabulación de datos

En el plan de tabulación de datos se representará los resultados obtenidos como producto de la recopilación de datos utilizando las técnicas e instrumentos de investigación. Dichos resultados se representarán en tablas donde se podrá observar cada variable, su correspondiente dominio, así como su frecuencia.

Posteriormente, se presentará tablas las cuales contendrán los resultados obtenidos.

Finalmente, se presentarán gráficos estadísticos que obedecen a la tabulación de las

variables y que facilitan el análisis de los datos. En la Tabla 2 se muestra un ejemplo de la tabulación de datos que se utilizará.

Variable: Utilización de metodologías de administración de riesgos de TIC.	Sí	No
Indicadores	…..	…..
SUMA		

Tabla 2. Ejemplo de Tabulación de datos.

b. Análisis de datos.

Encuesta telefónica

Objetivo de la encuesta:

Verificar la utilización de una metodología, mecanismo o procedimiento destinado a la administración de riesgos de tecnologías de información y comunicaciones (TIC) en las instituciones públicas y autónomas que forman parte de la muestra de la investigación.

Se busca obtener el porcentaje de instituciones que utilizan metodologías de administración de riesgos de TIC. Esta pregunta se realizará mediante una encuesta telefónica para filtrar aquellas instituciones que sí utilizan metodologías de administración de riesgos de TIC, en las cuales se centrará especial atención.

Encuesta escrita[11]

Objetivo de la encuesta:

Conocer la situación actual de la utilización de metodologías de administración de riesgos de tecnologías de información y comunicaciones (TIC) en instituciones públicas y autónomas que pertenecen a la zona metropolitana y alrededores de San Salvador y que cuentan con un mecanismo de administración de riesgos de TIC.

Parte I

Procedimientos actuales.

En esta parte se busca obtener información sobre la utilización de las metodologías de administración de riesgos de TIC, saber si la institución está aplicando de manera adecuada el concepto de metodología y cuáles beneficios le está aportando a la institución.

[11] Ver Anexo 2. Encuesta dirigida a personal de Informática.

1. Se pretende obtener información acerca del conocimiento general sobre metodologías de administración de riesgos de TIC por parte del personal informático de las instituciones.

2. Se busca obtener información acerca de la unidad organizativa que administra los riesgos de TIC en las instituciones.

3. Se pretende conocer la frecuencia en el uso de procedimientos, normas, políticas o métodos actuales para administrar los riesgos de TIC en las instituciones.

4. Se busca información cualitativa acerca de los beneficios aportados por los mecanismos empleados para administrar los riesgos de TIC.

5. Se pretende conocer el grado de eficiencia de las TIC en base a una adecuada administración de riesgos de las mismas.

6. Se pretende conocer si las instituciones cuentan con planes de contingencia en caso de fallos de TIC.

Parte II

Calidad de servicios.

La información que se recabará en esta sección es relevante en el sentido que se verificarán las partes sensibles de las TIC, los problemas más comunes y la frecuencia en las ocurrencias de éstos.

7. Se desea encontrar el porcentaje de instituciones que cuentan con una bitácora o registro de frecuencia de fallos en las TIC.

8. Se obtendrá el número aproximado de sistemas que se administran en las instituciones.

9. Obtener el número aproximado de equipos que se administran en las instituciones.

10. Encontrar el número aproximado de usuarios de los equipos utilizados en las instituciones.

11. Se busca obtener la evaluación de la calidad de servicios prestados por las TIC en las instituciones.

12. Obtener información del tiempo aproximado de fallos en los servicios prestados por las TIC en las instituciones.

13. Obtener los porcentajes de los servicios de TIC que presentan fallos más frecuentes en las instituciones.

14. Obtener los porcentajes de las causas más frecuentes de fallos de TIC en las instituciones.

15. Establecer el orden de los rubros de las TIC que presentan fallos más frecuentes en las instituciones.

16. Obtener el orden de importancia de los rubros de las TIC para las instituciones.

Parte III

Aspecto económico.

El siguiente apartado se centra en obtener información respecto de los beneficios económicos que aportan las diferentes metodologías de administración de riesgos en las instituciones. De la misma manera, se pretende obtener valores aproximados de los costos de los diversos rubros de TIC que afectan a dichas instituciones.

17. Se espera conocer si la institución encuestada lleva una bitácora donde se registren los costos o gastos en que se han incurrido por los fallos de TIC. A raíz de esta interrogante se preguntará por un aproximado anual de estos gastos.

18. Es importante para el objeto de estudio conocer las tendencias en las inversiones de los rubros de TIC en los últimos años.

19. Se espera adquirir conocimiento concerniente al porcentaje de gastos por fallos en los diferentes rubros de TIC en los últimos años.

F. TABULACIÓN Y ANÁLISIS DE DATOS.

1. Enfoque Externo

a. Análisis e Interpretación de Datos.

i. Encuesta Telefónica.

Alternativas	Sí	No
Frecuencias	27	0
Total	27	

Tabla 3. Tabulación de resultados de encuesta telefónica.

En el siguiente gráfico se representa la muestra tomada en la investigación respecto a la aplicación de un mecanismo o método orientado a la administración de riesgos de TIC en las instituciones.

Gráfica 1. Resultados encuesta telefónica.

Todas las instituciones que fueron encuestadas telefónicamente han adoptado algún *mecanismo*[12] para administrar los riesgos de TIC, lo cual garantiza que la muestra tomada para realizar el enfoque externo del diagnóstico mostrará información relevante sobre la utilización de algunos tipos de metodologías de administración de riesgos de TIC. Se puede inferir que existe una alta tendencia a utilizar algún mecanismo orientado a administrar los riesgos de TIC en las instituciones.

[12] La palabra *mecanismo* se usa para referirse a una forma general de instrumento adoptado por las instituciones encuestadas para administrar los riesgos de TIC.

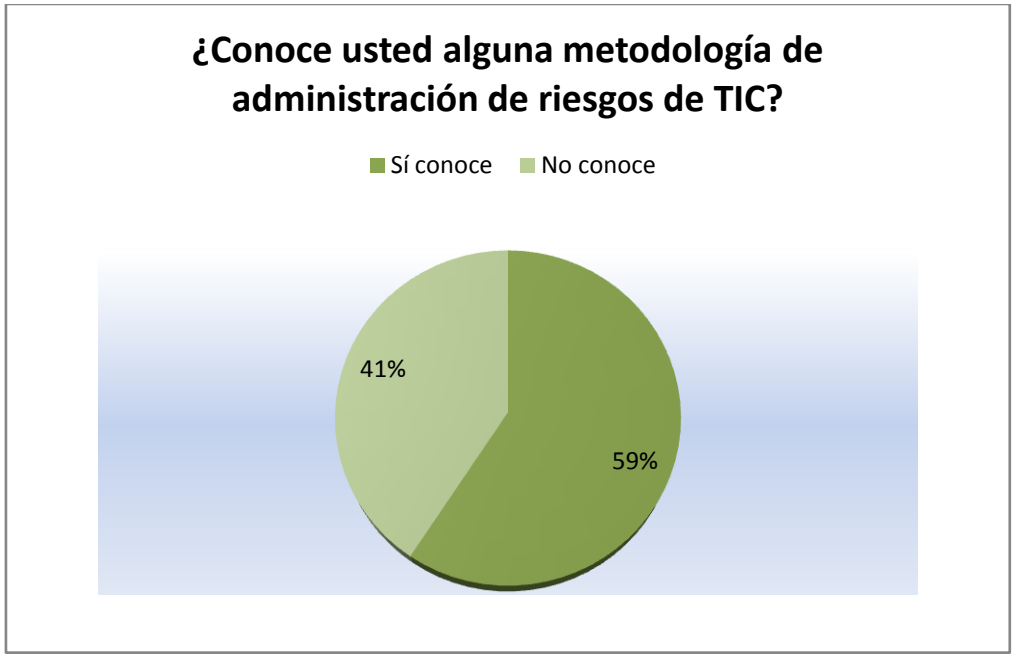
ii. Encuesta escrita.

A continuación se presentan los resultados de la encuesta realizada en las instituciones públicas y autónomas acerca de la utilización de metodologías de administración de riesgos de TIC.

Pregunta 1. **¿Conoce usted alguna metodología de administración de riesgos de TIC?**

Alternativas	Sí	No
Frecuencia	16	11
SUMA	27	

Tabla 4. Tabulación de resultados de la pregunta 1.



Gráfica 2. Conocimiento sobre la existencia de metodologías de administración de riesgos de TIC.

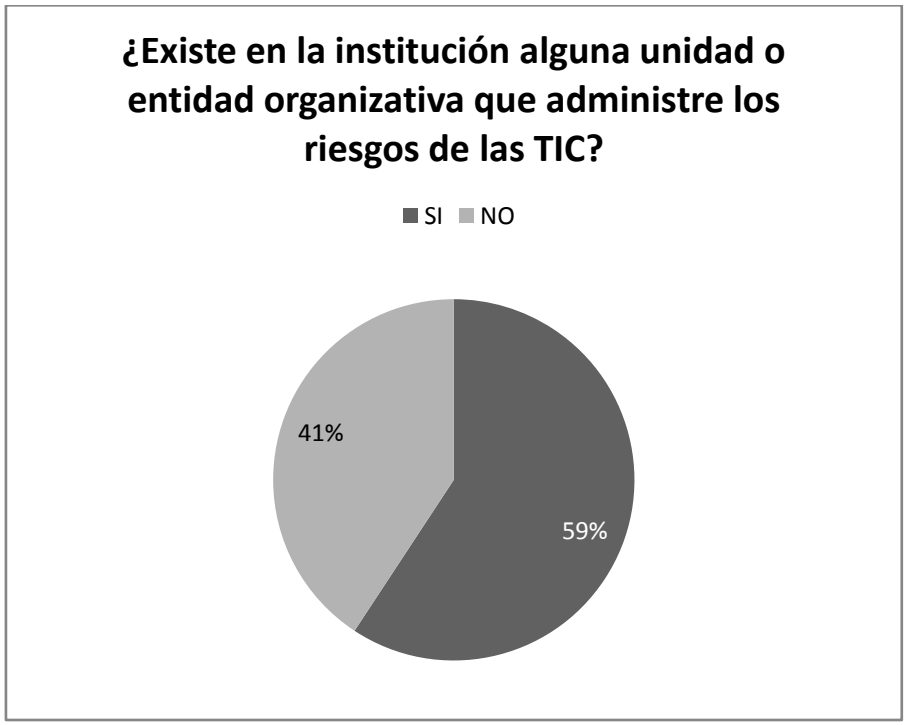
Más de la mitad de las instituciones encuestadas manifestaron conocer alguna metodología de administración de riesgos de TIC; sin embargo, al preguntarles sobre los nombres de estas metodologías, solamente el 22% mencionaron metodologías conocidas tales como Magerit, COBIT, CRAMM, ITIL, Administración de riesgos MISP, Método cualitativo/cuantitativo BSI; el 15% toman por metodologías las políticas institucionales, normas y planes de contingencia mientras que el 22% restante no mencionaron un nombre específico por cuestiones de seguridad. Se concluye que existe una evidente confusión entre

lo que entienden por metodologías de administración de riesgos de TIC y el resto de mecanismos orientados a ese fin y que en definitiva, no hay una comprensión a fondo de ellas que incite a las instituciones a utilizarlas para poder proteger sus activos de TIC.

Pregunta 2. **¿Existe en la institución alguna unidad o entidad organizativa que administre los riesgos de las TIC?**

Alternativas	Sí	No
Frecuencia	16	11
SUMA	27	

Tabla 5 . Tabulación de resultados de la pregunta 2.



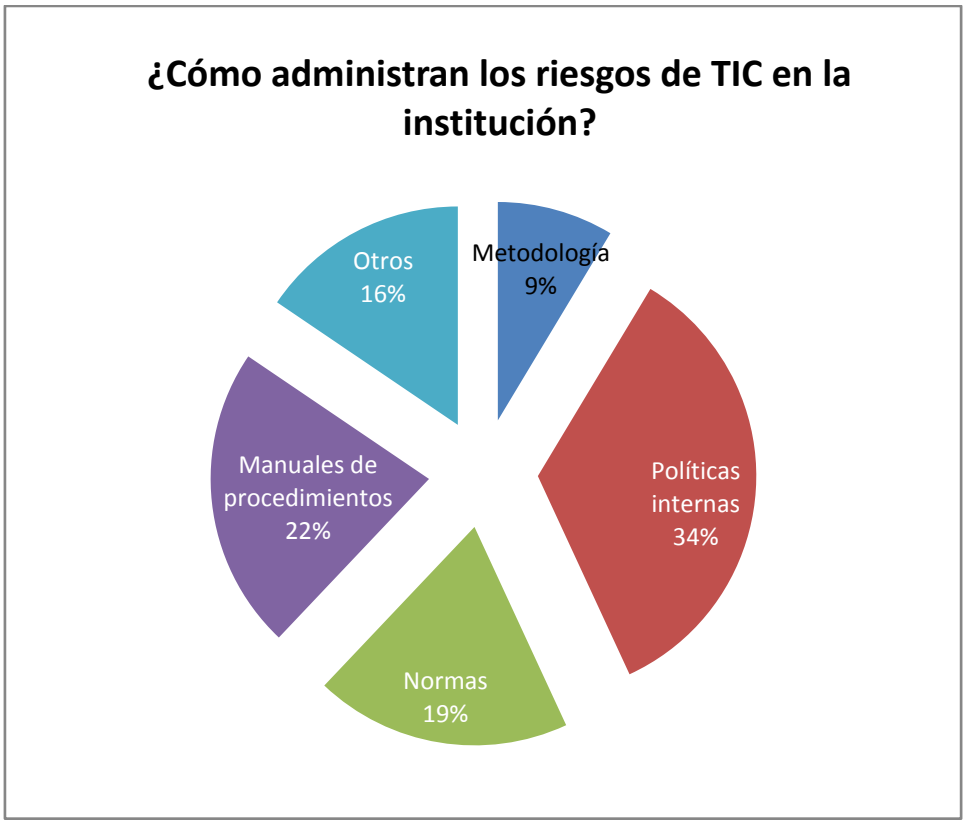
Gráfica 3. Porcentaje de instituciones que cuentan con una entidad organizativa donde se administren los riesgos de TIC.

Al igual que en la Pregunta 2 en más de la mitad de las instituciones encuestadas existe una unidad especializada encargada de la administración de los riesgos de TIC, lo cual es congruente y nos demuestra que si en las instituciones existe el conocimiento de administración de riesgos de TIC también se opta por crear una unidad especializada para este fin y que en la mayoría de los casos forma parte de la Unidad Informática. Este gráfico es representativo de la reciente importancia que las instituciones le están proporcionando al rubro de la administración de riesgos de TIC.

Pregunta 3. **¿Cómo administran los riesgos de TIC en la institución?**

Mecanismos	Metodología	Políticas internas	Normas	Manuales de procedimientos	Otros
Frecuencia	5	20	11	13	9

Tabla 6. Tabulación de resultados de la pregunta 3.



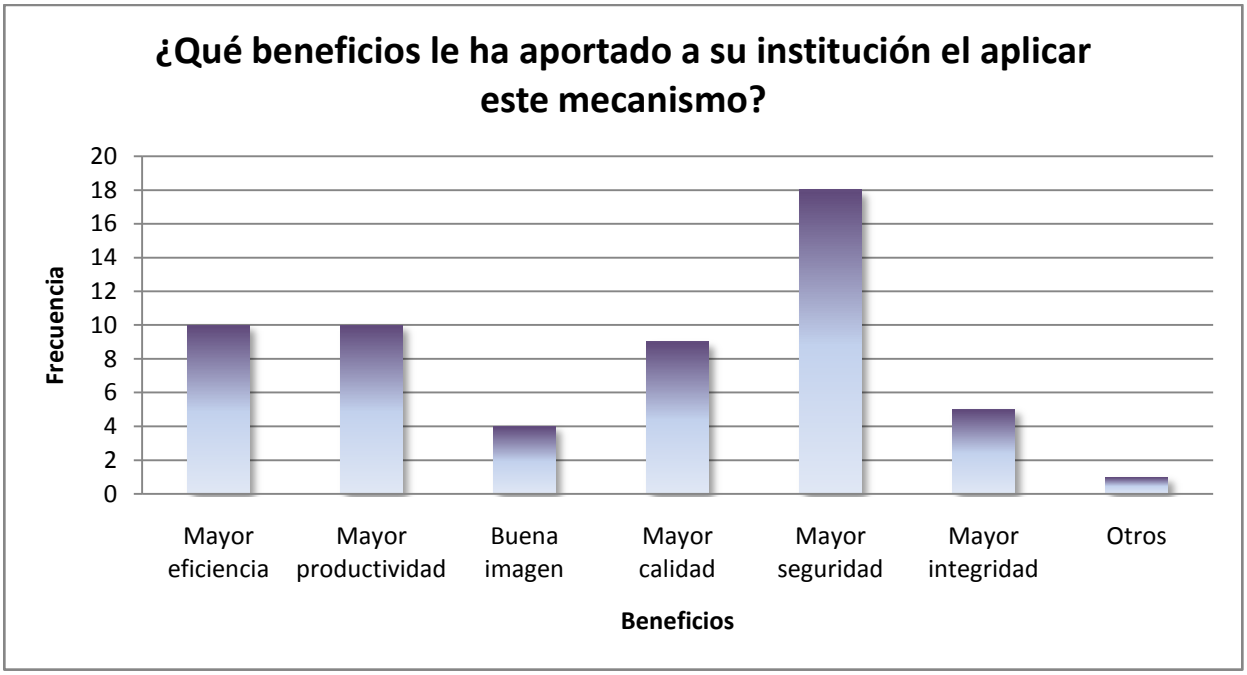
Gráfica 4. Mecanismos para administrar los riesgos en las instituciones.

En las instituciones encuestadas, los riesgos de TIC se administran mayoritariamente mediante políticas internas, seguidos por manuales de procedimientos, normas, y otras formas de administrar riesgos tales como planes de contingencia, toma de decisiones, procedimientos, dejando en último lugar el uso de metodologías. Existe una marcada tendencia a establecer en las políticas internas institucionales las directrices o procedimientos respecto a la administración de los riesgos de TIC, esto podría deberse a ahorros en inversiones por metodologías o a que no han encontrado una metodología que se adecúe de la mejor manera a sus necesidades de administración de riesgos de TIC.

Pregunta 4. **¿Qué beneficios le ha aportado a su institución el aplicar este mecanismo?**

Alternativas	Mayor eficiencia	Mayor productividad	Buena imagen	Mayor calidad	Mayor seguridad	Mayor integridad	Otros
Frecuencia	10	10	4	9	18	5	1

Tabla 7. Tabulación de resultados de pregunta 4.



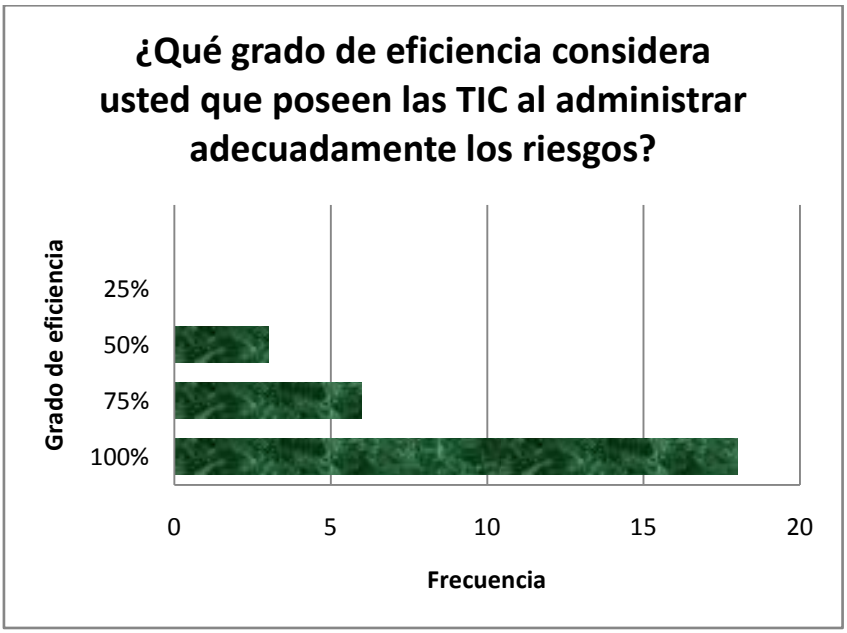
Gráfica 5. Beneficios de la utilización de una metodología de administración de riesgos de TIC.

Los beneficios de aplicar algún mecanismo de administración de riesgos de TIC tienen una tendencia muy marcada a mejorar la seguridad, es decir, una disminución en la probabilidad de ocurrencia de fallos, sin embargo en la investigación se comprobó que sólo las instituciones que utilizaban una metodología de administración de riesgos de TIC (9%) poseían un índice elevado de beneficios por dicho uso, dando también como resultado que las TIC poseían un mejor control de sus riesgos. Esto nos lleva a la conclusión de que al aplicar una metodología de administración de riesgos conlleva a tener una mejora en los beneficios y un mejor control de los riesgos de las TIC.

Pregunta 5. **¿Qué grado de eficiencia considera usted que poseen las TIC al administrar adecuadamente los riesgos?**

Alternativas	100%	75%	50%	25%
Frecuencia	18	6	3	0
SUMA	27			

Tabla 8. Tabulación de resultados de la pregunta 5.



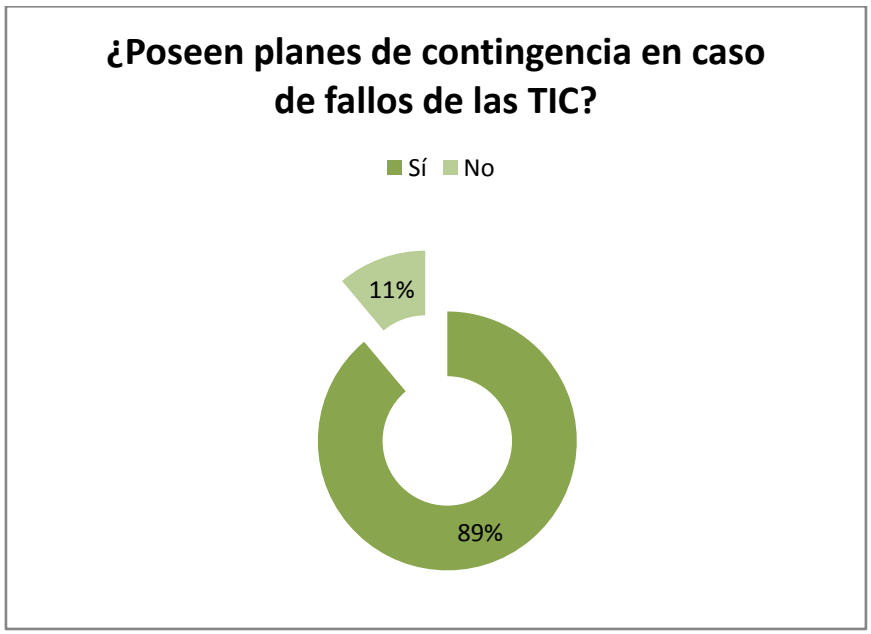
Gráfica 6. Opinión sobre el grado de eficiencia de las TIC al administrar los riesgos.

La mayoría de las instituciones encuestadas consideran que si se emplea una adecuada administración de riesgos de TIC, el grado de eficiencia de las mismas es óptimo, mientras que sólo una minoría no comparte ésta opinión posiblemente se deba a que como se mencionó en la Pregunta 1 en algunas instituciones no hay una comprensión a fondo de ellas y debido a esto no perciben la eficiencia y calidad que brindan las TIC en sus procesos de negocios.

Pregunta 6. **¿Poseen planes de contingencia en caso de fallos de las TIC?**

Alternativas	Sí	No
Frecuencia	24	3
SUMA	27	

Tabla 9. Tabulación de resultados de la pregunta 6.



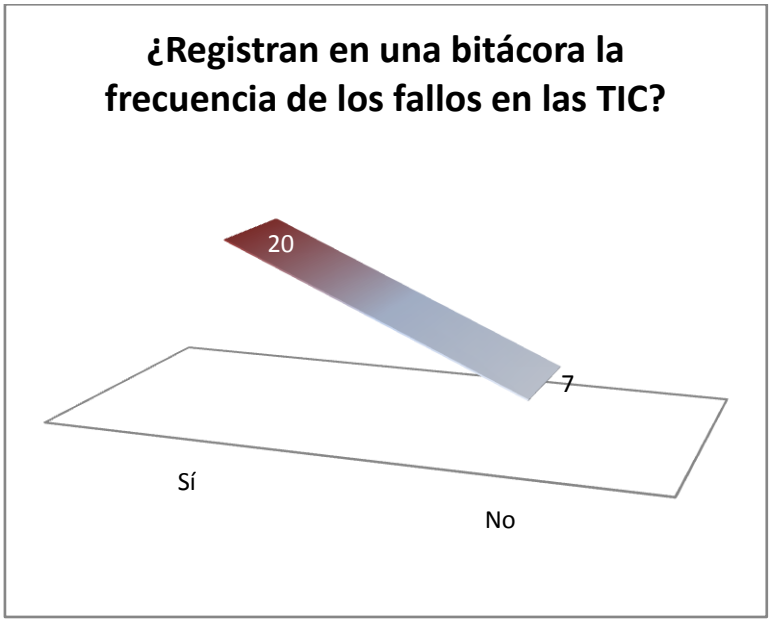
Gráfica 7. Existencia de planes de contingencia ante fallos de las TIC.

La mayoría de las instituciones encuestadas han diseñado planes de contingencia a poner en práctica en caso de materialización de amenazas, mientras que sólo en una pequeña parte no se han elaborado. Destaca el hecho que las instituciones están considerablemente preparadas en su mayoría para afrontar amenazas mediante la puesta en práctica de medidas contingenciales previamente diseñadas para los diferentes casos específicos de fallos en las TIC, esto demuestra la importancia que se la da a este rubro en los últimos años ya que consideran a las TIC como activo muy valioso y que se debe proteger.

Pregunta 7. **¿Registran en una bitácora la frecuencia de los fallos en las TIC?**

Alternativas	Sí	No
Frecuencia	20	7
SUMA	27	

Tabla 10. Tabulación de resultados de la pregunta 7.



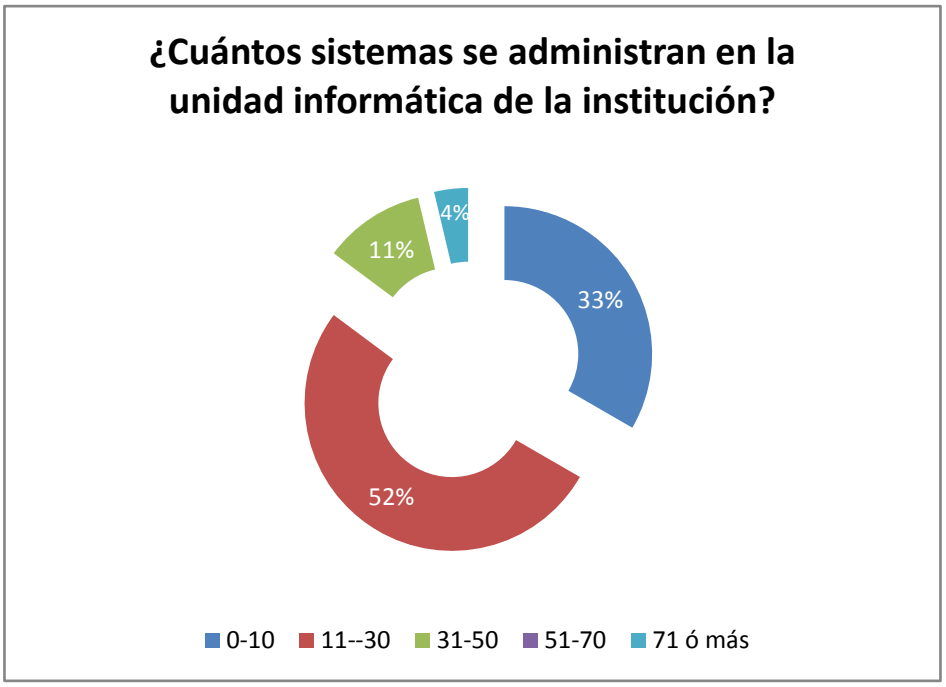
Gráfica 8. Instituciones que cuentan con una bitácora para registrar la frecuencia de fallos en las TIC.

20 instituciones de la muestra cuentan con un registro de la frecuencia de fallos en las TIC, el cual es utilizado con propósitos encaminados a la solvencia de dichos problemas. Se observó que las instituciones consideran este registro de fallos muy importante ya que ofrece muchas utilidades potenciales a los responsables de la gestión de los riesgos de TIC en la institución tales como tomar decisiones para contrarrestar esos fallos dependiendo de la frecuencia e impacto de los mismos, medidas más efectivas y oportunas cuando estos fallos se materializan ya que se posee una bitácora del procedimiento a seguir en situaciones similares.

Pregunta 8. **¿Cuántos sistemas se administran en la unidad informática de la institución?**

Cantidad de sistemas informáticos	0-10	11-30	31-50	51-70	71 ó más
Frecuencia	9	14	3	0	1

Tabla 11. Tabulación de resultados de la pregunta 8.



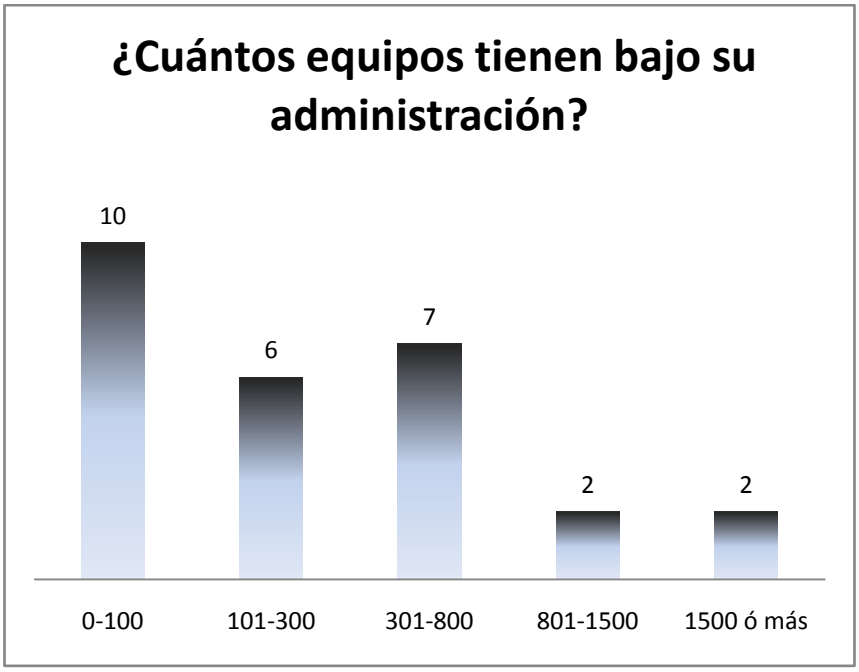
Gráfica 9. Porcentaje de cantidad de sistemas administrados en las instituciones.

La mitad de las instituciones encuestadas administra entre 11 y 30 sistemas, una tercera parte administra entre 0 y 10 sistemas y sólo una minoría administra más de 31 sistemas. Este dato es relevante para conocer la magnitud de infraestructura tecnológica con que cuentan la mayoría de instituciones gubernamentales y autónomas y se comprobó que sólo una minoría de las instituciones que utilizan una metodología de administración de riesgos de TIC son las que poseen la mayor cantidad de sistemas operando, lo que conlleva a concluir que a mayor cantidad de sistemas en operación es necesaria una metodología formal de administración de riesgos de TIC.

Pregunta 9. **¿Cuántos equipos tienen bajo su administración?**

Cantidad de equipos	0-100	101-300	301-800	801-1500	1500 ó más
Frecuencia	10	6	7	2	2

Tabla 12. Tabulación de resultados de la pregunta 9.



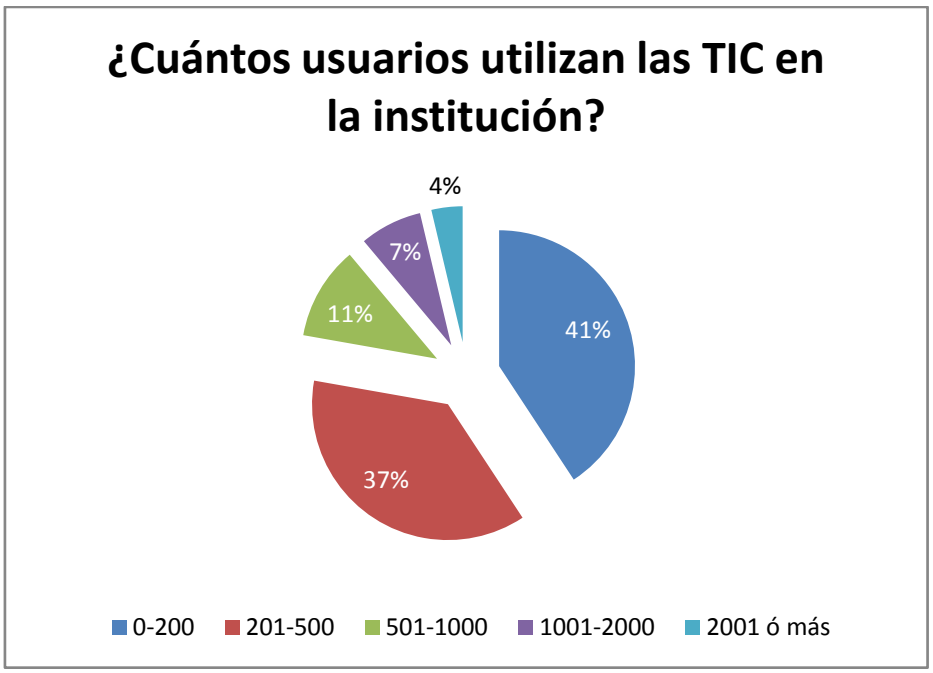
Gráfica 10. Cantidad de equipos que se administran en las instituciones encuestadas.

Esta pregunta es congruente con la anterior ya que solo una minoría de las instituciones encuestadas administra más de 801 equipos informáticos y donde se comprobó que sólo esta minoría de instituciones son las que utilizan una metodología de administración de riesgos de TIC, lo que conlleva a concluir que a mayor cantidad de equipos informáticos administrados por una institución es necesaria una metodología formal de administración de riesgos de TIC, ya que son más los activos a proteger y por ende existen más puntos de vulnerabilidad a los cuales puede estar expuesta la institución.

Pregunta 10. **¿Cuántos usuarios utilizan las TIC en la institución?**

Cantidad de usuarios	0-200	201-500	501-1000	1001-2000	2001 ó más
Frecuencia	11	10	3	2	1

Tabla 13. Tabulación de resultados de la pregunta 10.



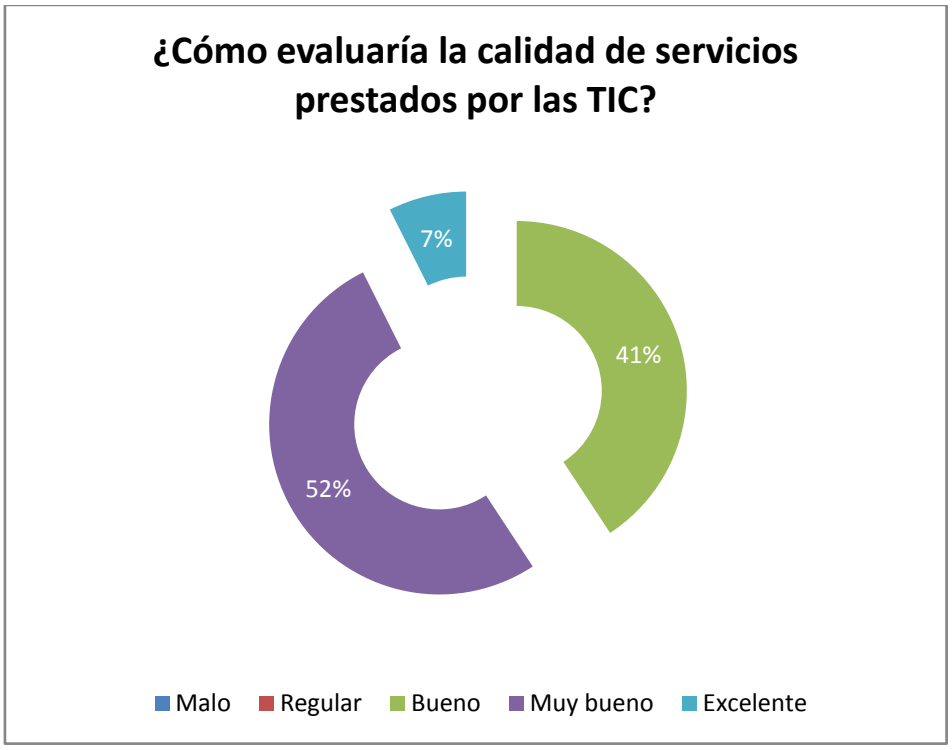
Gráfica 11. Porcentaje de la cantidad de usuarios de las TIC en las instituciones.

Esta pregunta guarda relación con las preguntas 8 y 9 ya que se observó la tendencia a que solo una minoría utilizaba una gran cantidad de sistemas y equipos informáticos de las instituciones encuestadas y como se mencionó anteriormente sólo esta minoría de instituciones son las que utilizan una metodología de administración de riesgos de TIC, lo que conlleva a concluir que a mayor cantidad de usuarios que utilizan las TIC en una institución es necesaria una metodología formal de administración de riesgos de TIC, ya que existen más puntos de vulnerabilidad a los cuales puede estar expuesta la institución y donde es necesario poseer un mayor control de las personas que hacen uso de dichas TIC.

Pregunta 11. **¿Cómo evaluaría la calidad de servicios prestados por las TIC?**

Alternativas	Malo	Regular	Bueno	Muy bueno	Excelente
Frecuencia	0	0	11	14	2

Tabla 14. Tabulación de resultados de la pregunta 11.



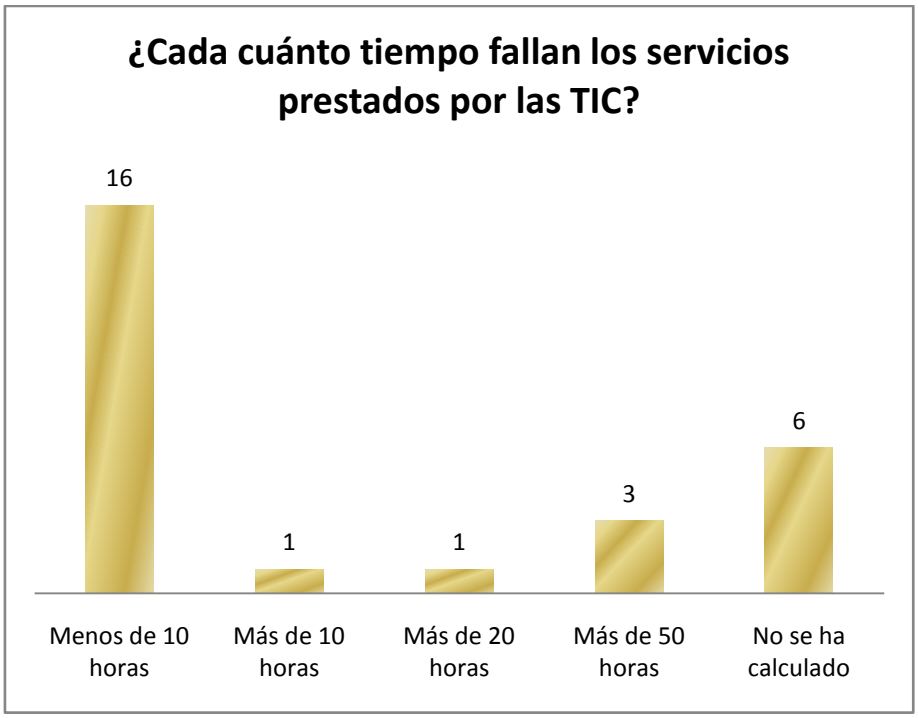
Gráfica 12. Evaluación de la calidad de los servicios soportados por las TIC.

Un poco más de la mitad de los encuestados opinan que la calidad de los servicios prestados por las TIC es *Muy buena.* Solamente una minoría considera que la calidad de los servicios prestados por las TIC es *Excelente.* Tanto los administradores como los usuarios de TIC de las instituciones encuestadas tienen expectativas que la administración de riesgos de TIC pueda mejorar considerablemente, esto se debe a la recurrencia de los fallos en los servicios soportados por el conjunto de TIC. También se observa la relación de esta pregunta con la Pregunta 3 donde sólo una minoría (9%) de estas instituciones utilizan una metodología formal de administración de riesgos de TIC y por ende son las instituciones que aprovechan al máximo los servicios brindados por las TIC ya que poseen mejores controles de riesgos.

Pregunta 12 **¿Cada cuánto tiempo fallan los servicios prestados por las TIC?**

Alternativas	Menos de 10 horas	Más de 10 horas	Más de 20 horas	Más de 50 horas	No se ha calculado
Frecuencia	16	1	1	3	6

Tabla 15. Tabulación de resultados de la pregunta 12.



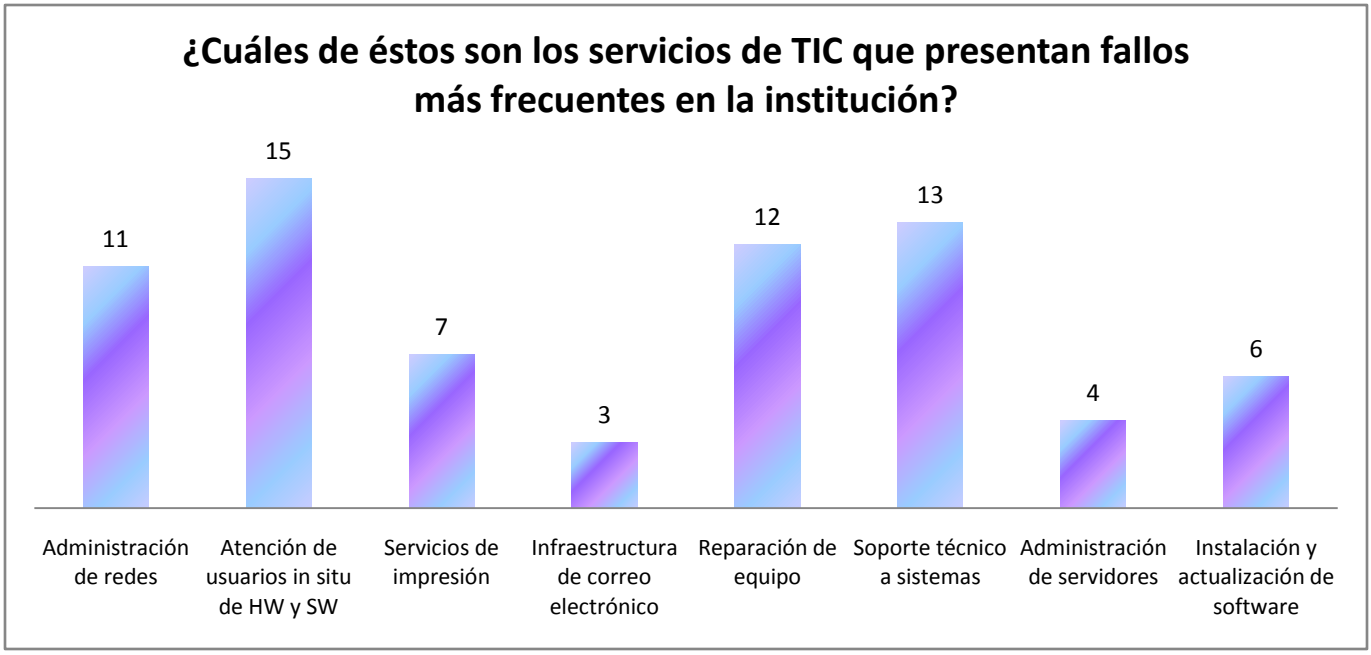
Gráfica 13. Tiempo entre fallos de los servicios de TIC.

Las mayoría de las instituciones encuestadas logran controlar sus fallos en períodos de tiempo relativamente cortos, (menos de 10 horas), sin embargo, este lapso de tiempo no es para nada despreciable, considerando la cantidad de procesos dependientes de dichos fallos. Las instituciones se han propuesto no solamente aumentar la robustez en los servicios de TIC, sino también percibir una disminución en la frecuencia de la ocurrencia de los mismos. Se concluye que al aumentar las TIC como es la tendencia en la actualidad los fallos también deben de aumentar pero si las instituciones están mejor preparadas con una adecuada administración de riesgos de TIC los intervalos de tiempo de fallos se deberían controlar en menor tiempo al que actualmente se controlan en las instituciones gubernamentales.

Pregunta 13. **¿Cuáles de éstos son los servicios de TIC que presentan fallos más frecuentes en la institución?**

Servicios de TIC	Frecuencia
Administración de redes	11
Atención de usuarios in situ de HW y SW	15
Servicios de impresión	7
Infraestructura de correo electrónico	3
Reparación de equipo	12
Soporte técnico a sistemas	13
Administración de servidores	4
Instalación y actualización de software	6

Tabla 16. Tabulación de resultados de la pregunta 13.



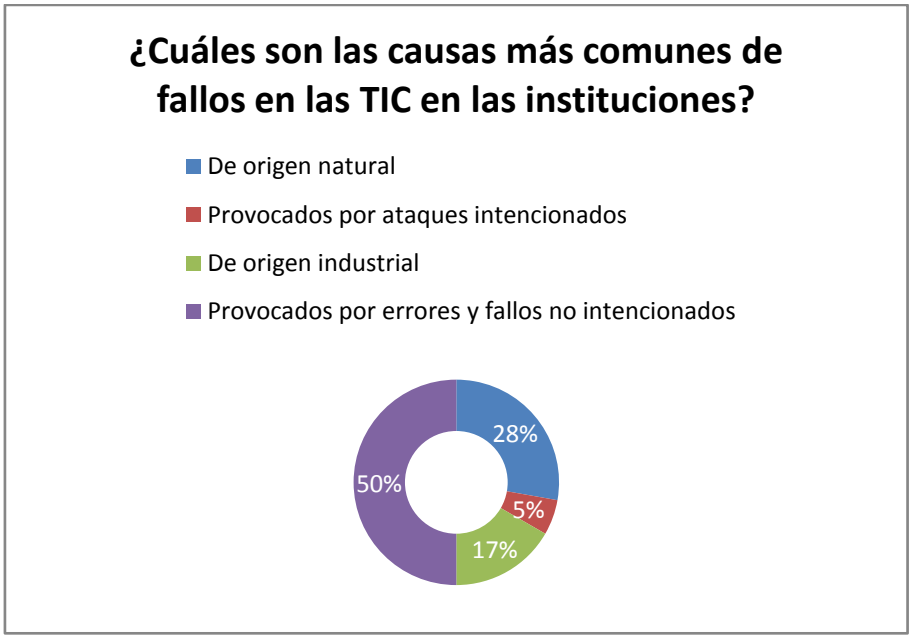
Gráfica 14. Frecuencia de los fallos de los servicios de TIC más comunes.

Se puede visualizar la tendencia a la Atención de usuarios in situ como el servicio de TIC que presenta fallos más frecuentes con respecto a los otros servicios de TIC en las instituciones encuestadas, esto se debe según comentarios de personal de la unidad de informática a la falta de capacitación técnica de usuarios frente a la prevención de errores comunes que provocan fallos recurrentes que van a parar a la larga cola de demandas que tiene la unidad de soporte técnico a usuarios y que dicho sea de paso la cantidad de usuarios supera con creces la cantidad de personal encargado de brindar el soporte técnico a los usuarios .

Pregunta 14. **¿Cuáles son las causas más comunes de fallos en las TIC en las instituciones?**

Alternativas	De origen natural	Provocados por ataques intencionados	De origen industrial	Provocados por errores y fallos no intencionados
Frecuencia	10	2	6	18

Tabla 17. Tabulación de resultados de la pregunta 14.



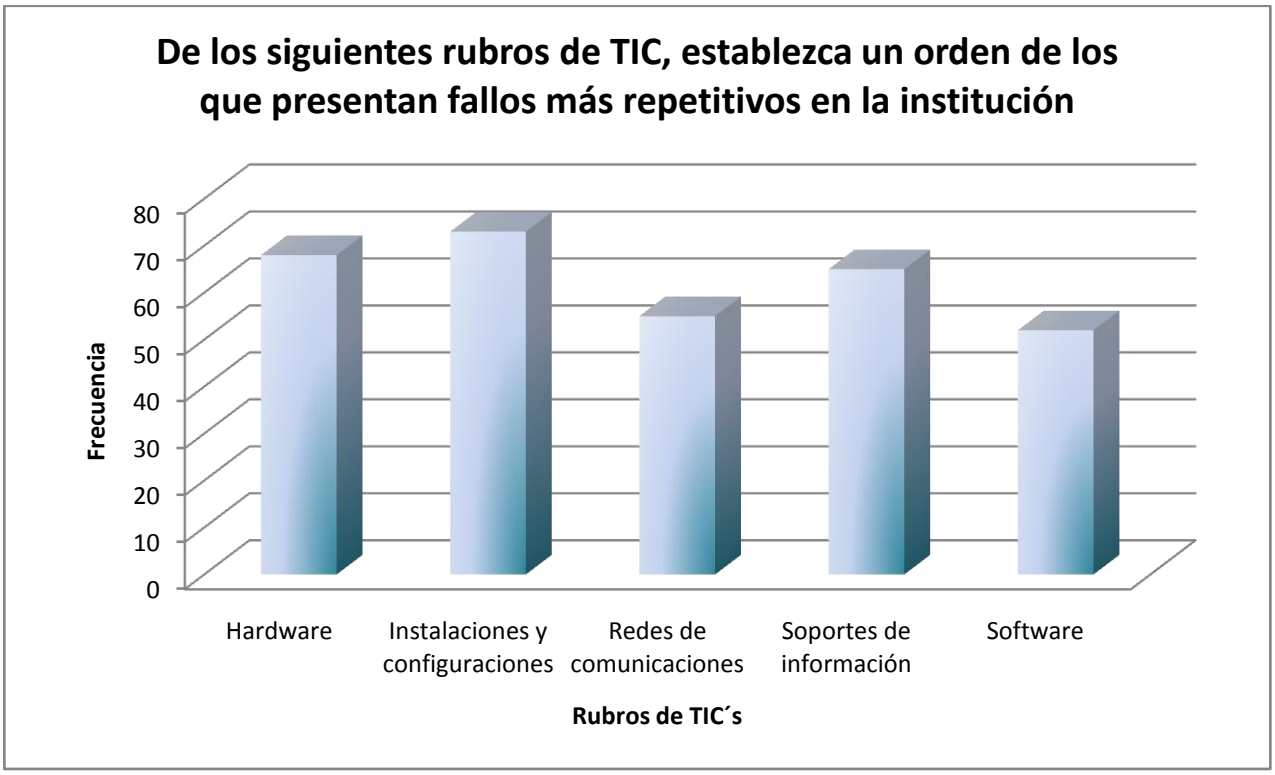
Gráfica 15. Causas más comunes de fallos en las TIC en las instituciones.

La mitad de las instituciones encuestadas considera la causa más común de fallo en las TIC los provocados por errores y fallos no intencionados, sólo una minoría consideraba los fallos provocados por ataques intencionados como una causa común debido a que sí manifestaron sufrir ese tipo de amenazas. En concordancia con el Gráfico 14, en éste se corrobora que la tendencia en las causas de fallos en las TIC son *provocados por errores y fallos no intencionados,* lo que se traduce en una notable deficiencia en la capacitación que la unidad informática ofrece a los diferentes usuarios de las TIC o en ocasiones también se debe a que aunque los usuarios conocen las normativas del uso de los equipos no siempre están conscientes de que pueden haber fallos por alguna mala utilización de parte de ellos, por lo que se debe instaurar una forma de concientizar a los usuarios que las TIC son una parte fundamental en el proceso del negocio de la institución.

Pregunta 15. **De los siguientes rubros de TIC, establezca un orden de los que presentan fallos más repetitivos en la institución**

Puntuación	F	*1	F	*2	F	*3	F	*4	F	*5	Total
Hardware	8	8	4	8	4	12	0	0	8	40	68
Instalaciones y configuraciones	4	4	4	8	0	0	9	36	5	25	73
Redes de comunicaciones	7	7	6	12	6	18	2	8	2	10	55
Soportes de información	4	4	5	10	5	15	4	16	4	20	70
Software	8	8	4	8	8	24	3	12	0	0	52

Tabla 18. Tabulación de resultados de la pregunta 15.



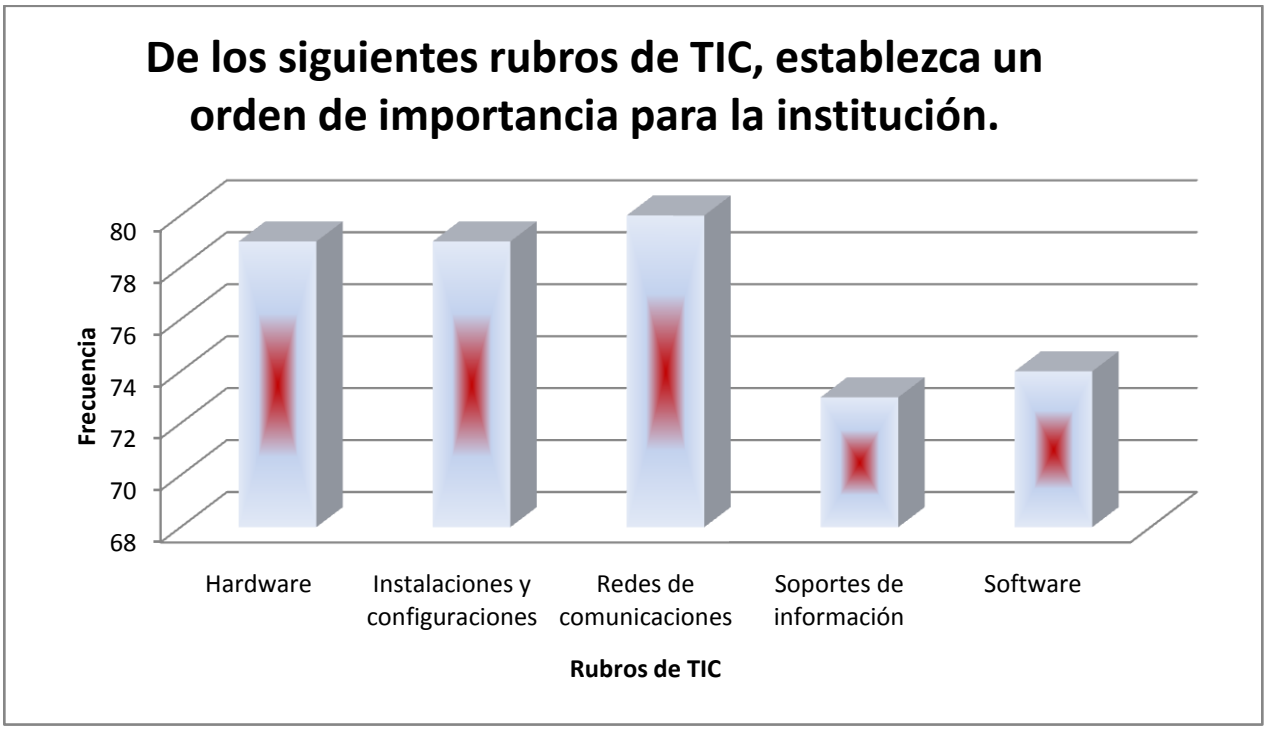
Gráfica 16. Orden ascendente de los rubros de TIC que presentan fallos más repetitivos.

Según las instituciones encuestadas, las instalaciones y configuraciones son el rubro de TIC que presenta fallos más repetitivos. Los problemas originados en las instalaciones y configuraciones normalmente son una consecuencia de la mala disposición del cableado, así como de la poca protección de los medios de transmisión, también se debe a que las instalaciones y configuraciones en algunas ocasiones se realizan por personal no capacitado para dicha tarea, pero cuando se da una buena administración de este rubro el software no tiene mayores inconvenientes por lo que resulta ser el rubro que menos fallos presenta.

Pregunta 16. **De los siguientes rubros de TIC, establezca un orden de importancia para la institución.**

Puntuación	F	*1	F	*2	F	*3	F	*4	F	*5	Total
Hardware	5	5	3	6	7	21	3	12	7	35	79
Instalaciones y configuraciones	3	3	5	10	5	15	9	36	3	15	79
Redes de comunicaciones	3	3	4	8	8	24	5	20	5	25	80
Soportes de información	8	8	2	4	4	12	6	24	5	25	73
Software	3	3	7	14	7	21	4	16	4	20	74

Tabla 19. Tabulación de resultados de la pregunta 16.



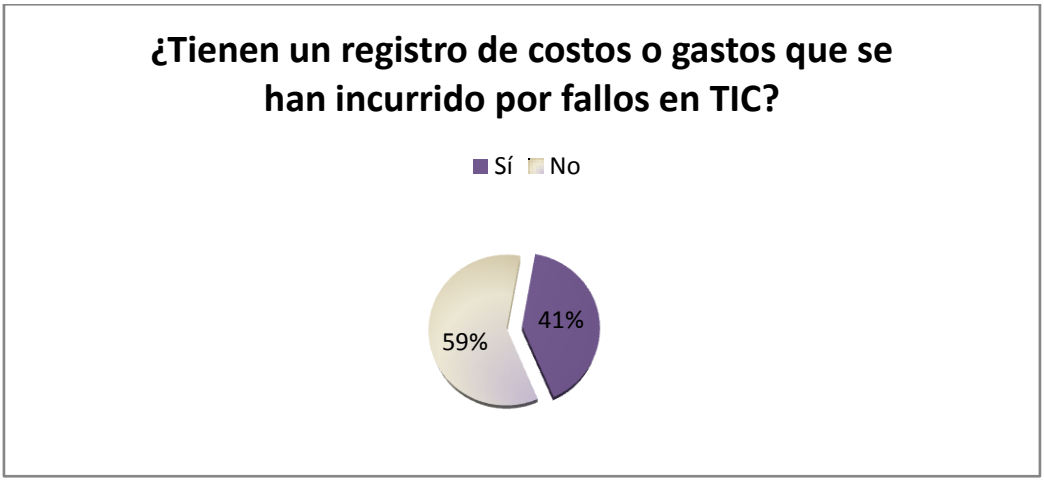
Gráfica 17. Orden ascendente de la importancia de los rubros de TIC en las instituciones.

Para las instituciones encuestadas las redes de comunicaciones son el rubro calificado como *más importante*, debido a que es altamente imprescindible en los procesos de negocio. Esto demuestra que consideran que las TIC sino tienen una buena comunicación no servirían para ayudar a las altas esferas administrativas en las decisiones para mejorar el rendimiento, calidad de los servicios y productos que ofrecen, debido a que una información que llegue tarde o alterada puede causar daños o atrasos en la productividad y eficiencia de las instituciones.

Pregunta 17. **¿Tienen un registro de costos o gastos que se han incurrido por fallos en TIC?**

Alternativas	Sí	No
Frecuencia	11	16
SUMA	27	

Tabla 20. Tabulación de resultados de la pregunta 17.



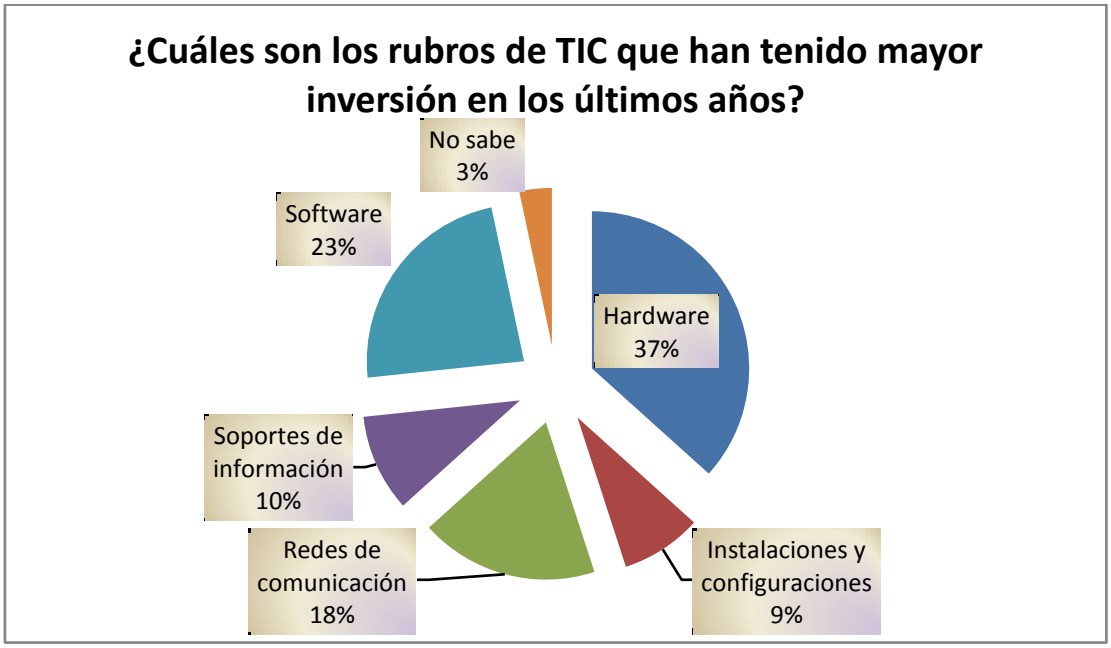
Gráfica 18. Porcentaje de las instituciones que tienen un registro de los gastos por fallos en las TIC.

En más de la mitad de las instituciones encuestadas se lleva un registro de los gastos por fallos en las TIC; aunque son las unidades informáticas las que generan estos gastos en algunas instituciones expresaron que los gastos no siempre eran constantes y que en ocasiones no eran predecibles. En las instituciones donde proporcionaron el monto al que ascendían dichos gastos, éstos oscilaban entre $2,000.00 y $1,000.00 anuales, aunque dichos valores podrían variar enormemente ya que en la gran mayoría de los casos no se proporcionó este valor por cuestiones de confidencialidad. Esta información refleja que en las instituciones donde no se lleva dicho registro de gastos por fallos en las TIC no se tiene conciencia de la gran importancia que tiene el poder conocer con certeza estos gastos y que seguramente se podrían disminuir al poseer una adecuada administración de riesgos de TIC.

Pregunta 18. **¿Cuáles son los rubros de TIC que han tenido mayor inversión en los últimos años?**

Rubros de TIC	Frecuencia
Hardware	22
Instalaciones y configuraciones	5
Redes de comunicación	11
Soportes de información	6
Software	14
No sabe	2

Tabla 21. Tabulación de resultados de la pregunta 18.



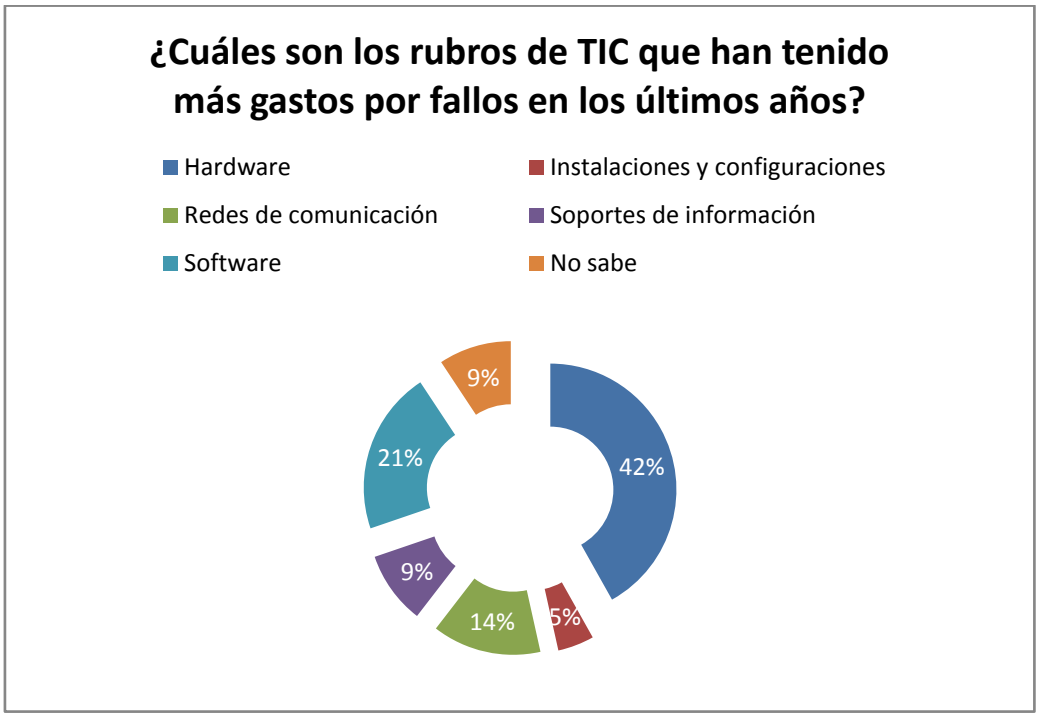
Gráfica 19. Rubros de TIC que han tenido mayor inversión en los últimos años.

La tendencia de las instituciones encuestadas al momento de invertir demostró que es la de tener mejores tecnologías de información y comunicaciones o actualizarse por lo que el rubro que más destaca es el hardware, pero también para poder hacer uso de este e instalarlo en su respectiva área se comprobó que se invirtió en el software, por lo que estos rubros son los que más han crecido en los últimos años en las instituciones y que siguen en crecimiento en la actualidad, esto puede deberse también a la mayor carga de transacciones que se realizan diariamente o que los equipos informáticos que poseen ya se encuentran obsoletos.

Pregunta 19. **¿Cuáles son los rubros de TIC que han tenido más gastos por fallos en los últimos años?**

Rubros de TIC	Frecuencia
Hardware	18
Instalaciones y configuraciones	2
Redes de comunicación	6
Soportes de información	4
Software	9
No sabe	4

Tabla 22. Tabulación de resultados de la pregunta 19.



Gráfica 20. Rubros de TIC que han generado más gastos por fallos en los últimos años.

La mayor parte de los gastos en las instituciones es causado por los fallos en el hardware, siendo el rubro más representativo; es importante destacar que ese dato es coherente con la Gráfica 19, donde el hardware también ocupa el 1er lugar en inversiones de TIC. Los gastos por las instalaciones y configuraciones se encuentran el último lugar, contrastando con los resultados mostrados en la Gráfica 16 donde se establece que dicho rubro es el que presenta fallos más repetitivos, por lo que se puede inferir que a pesar de ser los más repetitivos, son los menos costosos para las instituciones. Esta información refleja que los rubros en que más se invierte son también los rubros en que más se gasta por fallos, por lo que queda comprobado que para una institución los activos que se adquieren deben

tener algún mecanismo para protegerlos y evitar que sigan produciendo gastos, situación que no se está atendiendo efectivamente, según la información recopilada.

b. Comprobación de Hipótesis.

En el trabajo de investigación la medición de los riesgos se refiere intrínsecamente a la parte de procedimientos en la que se consigue la información cualitativa de los beneficios obtenidos de aplicar un mecanismo de administración de riesgos de TIC, y del grado de eficiencia que han logrado con la aplicación de una adecuada administración de riesgos.

A pesar de que no se pregunte textualmente acerca de la disminución de riesgos, la información entre líneas que se obtiene se presta para interpretarla de la siguiente forma: que a una adecuada administración de riesgos éstos disminuyen considerablemente; sin embargo, en las instituciones en las que se aplica una metodología y que se tuvo acceso en la investigación se destaca que los beneficios eran mayores, que los fallos a los servicios prestados por las TIC eran menores y que los costos eran aceptables para la institución, por lo que se deduce que los riesgos disminuyen.

La información que se obtuvo de la investigación da como resultado que la seguridad es el beneficio que más aumenta junto a la efectividad y la productividad[13] y el mismo número de instituciones manifestaron que el grado de eficiencia es de 100%[14] por lo que al verificar en la parte de los factores críticos, no críticos y genéricos de la confiabilidad[15] en la que se dice que una metodología de administración de riesgos de TIC tendrá un 76% de confiabilidad, concluimos que:

Al tomar las 18 instituciones en el que el grado de eficiencia es de 100% y al obtener el porcentaje de entre todas las instituciones se dice que en un 67% de las empresas gubernamentales la aplicación de una metodología de administración de riesgos de las tecnologías de información y comunicaciones favorecerá alrededor de un 76% a la disminución de los riesgos de ocurrencia de fallos de los servicios soportados por las TIC. En el siguiente apartado se comprueba estadísticamente la hipótesis general.

[13] Ver pregunta 4 de la encuesta, Página 19.
[14] Ver pregunta 5 de la encuesta, Página 20.
[15] Ver Anexo 5.

i. Prueba estadística Chi-cuadrado.

Esta prueba de significación estadística nos permite encontrar relación o asociación entre dos variables de carácter cualitativo.

Chi-cuadrado sirve para determinar si los datos obtenidos de una muestra presentan variaciones estadísticamente significativas respecto de la hipótesis nula Ho. Cuando se formula la hipótesis general, simultáneamente se define la hipótesis nula, que niega la hipótesis general. De acuerdo a la hipótesis nula las variaciones en la variable independiente no tienen correspondencia con las variaciones que pudiere haber de la variable dependiente. Es decir, que existe "independencia estadística". Para la aplicación del Chi-cuadrado es necesario, antes realizar dos pasos. Por una parte, establecer el nivel de significación (α) con el cual se trabajará, y determinar los grados de libertad de la muestra. El nivel de significación es arbitrario y se fija de antemano, para este estudio se trabajará con el 5%. Los grados de libertad se establecen en función de la cantidad de celdas resultantes (cuatro para este caso), producto del cruce de dos variables.

Al aplicar la fórmula de Chi-cuadrado a los datos recolectados, los resultados se comparan con el valor de la tabla Chi-cuadrado. Si el resultado real es mayor que el resultado de la tabla entonces se rechaza la hipótesis nula Ho y se acepta la general, caso contrario se acepta la hipótesis nula.

Fórmula de Chi-cuadrado:

$$\mathbf{X^2 =} \sum \frac{(F0-Fe)^2}{Fe} \textbf{ (Ecuación 1)}$$

En donde:

X^2: valor del Chi-cuadrado.

F0: Valores observados o reales.

Fe: Valores esperados o teóricos.

Σ: Sumatoria de puntaje.

Fórmula para calcular valores esperados:

$$\mathbf{Fe=}\frac{(tf)(tc)}{total}\ \mathbf{(Ecuación\ 2)}$$

Donde:

tf: total de filas.

tc: total de columnas.

total: total global

En la Tabla 23 se presentan los valores obtenidos por medio de las encuestas, dichos valores se observaron para las variables definidas como independiente (Utilización de metodologías de administración de riesgos en las TIC) y dependiente (Disminución de riesgos).

Valores Obtenidos	Sí	No	Total
Utilización de metodologías de administración de riesgos de TIC	5	22	27
Disminución de riesgos	18	9	27
Total	23	31	54

Tabla 23. Valores obtenidos por medio de las encuestas.

Los valores esperados que se muestran en la Tabla 24 se obtuvieron de utilizar la ecuación 2.

Valores Esperados	Sí	No	Total
Utilización de metodologías de administración de riesgos de TIC	11.5	15.5	27
Disminución de riesgos	11.5	15.5	27
Total	23	31	54

Tabla 24. Valores esperados de las variables.

En la Tabla 25 se muestran los valores de aplicar la ecuación 1 para obtener el valor de Chi-cuadrado.

F0	Fe	F0-Fe	$(F0-Fe)^2$	$(F0-Fe)^2/Fe$
5	11.5	-6.5	42.25	3.673
22	15.5	6.5	42.25	2.726
18	11.5	6.5	42.25	3.673
9	15.5	-6.5	42.25	2.726
				$X^2= 12.798$

Tabla 25. Obtención del valor de Chi-cuadrado.

La obtención del valor de la tabla de Chi-cuadrado, se hizo mediante el siguiente procedimiento:

La tabla de Chi-cuadrado tiene dos entradas: Alfa (α) y los grados de libertad, el valor de Alfa hace referencia al nivel de confianza, para el caso en estudio es de 95%[16], el valor de alfa es de 0.05, lo cual corresponde al complemento porcentual de la confianza.

Los grados de libertad se refieren a la posibilidad que se tiene de establecer, en una distribución dada, valores arbitrarios sin modificar el marginal de dicha distribución. Es un estimador del número de categorías independientes en la prueba de independencia o experimento estadístico. La fórmula para calcular los grados de libertad es la siguiente:

Gl= (F-1) (C-1).

En donde: F= 2 (filas) y C= 2 (columnas)

Sustituyendo los valores en la fórmula nos queda que Gl=1 y e=5% (grado de significancia).

Dado que el valor de la tabla de Chi-cuadrado para un nivel de confianza del 95% es de (3.84) y el valor Chi-cuadrado de lo observado es de (12.798) se rechaza la hipótesis nula y se acepta la hipótesis general, por lo que se determina que la utilización de una metodología de administración de riesgos de TIC en las instituciones gubernamentales favorecerá en la disminución de los riesgos alrededor de un 76%?[17]

c. Resumen del Enfoque Externo.

Las unidades informáticas asumen la responsabilidad de la correcta administración de riesgos de TIC de las instituciones a las que pertenecen, para ese propósito en algunos casos asignan a un personal especializado, creando una sub dependencia; sin embargo, esto sucede en las unidades informáticas mejor organizadas, y no se ha observado en la muestra.

Aunque la totalidad de la muestra manifestó conocer algún tipo de mecanismo de administración de riesgos de TIC, solamente el 59% conoce sobre la existencia de *metodologías* diseñadas para ese propósito. Es importante destacar que aunque los profesionales informáticos tienen conocimiento sobre estas metodologías, no siempre se implementan en las diferentes instituciones.

Se pudo observar que en la actualidad el mecanismo más utilizado para administrar los riesgos de TIC está basado en las políticas internas particulares de cada administración institucional mostrando el 34% del total, los manuales de procedimientos son el segundo

[16] Ver apartado Referencia Bibliográfica I: Libros Literal 2.
[17] Ver apartado Formulación de Hipótesis en página 13.

instrumento más utilizado por las instituciones. Las metodologías son el instrumento menos aplicado para la administración de riesgos, contando solamente con el 9% del total. Sin embargo, vale mencionar que el 100% de las instituciones que aplican una metodología de administración de riesgos de TIC presentan un mayor grado de eficiencia en los servicios que soportan las TIC; además de incrementar la productividad y seguridad en dichos servicios.

Es importante notar que el 67% de las instituciones reconocen que la eficiencia de los servicios de las TIC es óptima cuando se realiza una adecuada administración de los riesgos a los que son susceptibles.

Casi el 90% de las instituciones cuentan con planes de contingencia, y en las que no cuentan, ya se han iniciado su respectiva construcción.

En la mayoría de instituciones (74%) se cuenta con una bitácora para registrar los fallos de las TIC, esto se hace con el propósito de tomar las medidas pertinentes para evitar las futuras fallas y/o tomar acciones contingenciales.

La moda observada en los resultados de la encuesta apunta a que en la mayoría de las instituciones se utilizan entre 0 y 100 equipos informáticos, y cuentan mayoritariamente con 200 usuarios.

Existe un contraste aparente cuando se observa en la Gráfica 12 que el 52% de los encuestados opinan que la calidad de los servicios prestados por las TIC es *Muy buena,* mientras que el 67% de los encuestados manifiestan que administrando eficientemente los riesgos se puede lograr un 100% de eficiencia en los servicios soportados por las TIC, según se muestra en la Gráfica 6**.** La diferencia radica en que el resto de encuestados evaluaron la eficiencia de los servicios soportados por las TIC con 50% y 75%, lo que se traduce en inconformidad con la calidad de dichos servicios.

A pesar que la duración de los fallos de los servicios de TIC dura menos de 10 horas, éstos repercuten de manera significativa en los procesos dependientes de ellos, generando un atraso en cadena que se percibe en la gran mayoría de las dependencias administrativas.

La atención de usuarios in situ de hardware y software destaca como el servicio más recurrente de TIC; por otra parte, las causas más comunes de fallos en las TIC son las provocadas por errores y fallos no intencionados.

Los rubros de TIC que presentan fallos más repetitivos en la institución son las instalaciones y configuraciones; los rubros que las instituciones consideran más importantes son las redes de comunicaciones.

Los rubros de TIC que presentan más gastos por fallos en los últimos años son el hardware y el software, formando el 63%, lo cual es coherente con la información presentada en la Gráfica 19**,** donde se puede apreciar que esos mismos rubros son los que presentan el mayor nivel de inversiones.

2. Enfoque Interno.

a. Resultados de la Observación y Entrevista realizada en el MINED.[18]

Actualmente en el MINED no se cuenta con una metodología de administración de riesgos de Tecnologías de Información y Comunicaciones (TIC), para poder administrar los riesgos de TIC según exigencia de la Corte de Cuentas de la República, la Gerencia de Normas y Calidad de la Dirección de Informática del MINED realiza anualmente las siguientes actividades:

- Registro que contiene la frecuencia de fallos, porcentaje de criticidad y el nivel de impacto de los servicios de TIC con sus respectivos nombres y gerencias a las que pertenecen.

- Registro que contiene una matriz o criterios de evaluación de riesgos, esto se realiza para cada unidad organizativa.

- Registro que contiene una matriz de acciones de mitigación de riesgos para cada unidad organizativa, aquí es donde se presupuestan las reparaciones para solventarlos.

A continuación se detallan cada uno de los elementos de las TIC identificadas en el MINED:

i. <u>Aplicaciones (software) y servicios.</u>

Se cuenta con 51 sistemas en funcionamiento y 20 en fase de construcción. Cada sistema posee una división de módulos: un modo público, para el cual no es necesario un usuario y contraseña para tener acceso a la información; y un módulo de servicio de acceso a sistemas, el cual se basa en una estructura de roles, mediante los cuales se crean usuarios que tienen acceso a la información dependiendo del grupo al que pertenecen. Quien crea los roles y los asigna a los diferentes tipos de usuarios es el administrador de sistemas.

[18] Ver Anexos 3 y 4. Entrevista y Guía de Observación para visita técnica al MINED.

Poseen sistemas en ambiente web, los cuales poseen dos URL, una URL pública, a la cual se puede accesar vía Internet y una URL privada, la cual está disponible a través de una intranet; ambas se conectan a la misma base de datos.

Se observó que la transferencia de archivos se realiza sin encriptar los datos; sin embargo, los roles, permisos, privilegios de los diferentes grupos sí se encuentran encriptados.

Todas sus bases de datos poseen un esquema relacional, es decir, entidad-relación.

Los sistemas están diseñados en 3 ó más capas, aunque también existen arquitecturas cliente-servidor.

Es importante mencionar que todas las aplicaciones de sistemas web se desarrollan por consultoras, a quienes se les proporciona los requerimientos de construcción, tales como plataforma Java, servidor web Tomcat, y Oracle en la base de datos.

A nivel institucional se utiliza el Antivirus McAffee versión 8.7.

El sistema operativo en las máquinas terminales es Microsoft Windows y va desde la versión 98 a la versión Vista. El sistema operativo de los servidores es Microsoft Windows 2003 Server SP2, y en algunos utilizan Red Hat Enterprise 4 Edition.

El servidor de correos utiliza el software Microsoft Server Exchange.

Poseen seguridad perimetral, filtro web y filtro SMTP.

La vulnerabilidad de los sistemas radica principalmente en la poca cultura informática que tienen algunos usuarios de los sistemas, en el sentido que no son cuidadosos de la importancia del acceso a dichos sistemas y en ocasiones comparten sin ninguna precaución los nombres de usuario y contraseñas. Hasta el momento no se han registrado casos de intromisión no autorizada a los diferentes sistemas y en el caso que hubiera, no se han diseñado planes de contingencia.

Existen alrededor de 71 servicios soportados por las TIC, de los cuales cinco tienen un alto impacto, pues entre ellos alcanzan 722 procesos críticos dependientes que componen el 67.29% del total. Los períodos de inactividad o suspensión de los servicios de TIC alcanzan un promedio de 12.9 horas de suspensión anualmente, afectando 1073 procesos críticos dependientes y a todos los usuarios de las mismas.

Servicios brindados por la Gerencia de Sistemas:

- Soporte a usuarios de Sistemas en Producción

Es la asistencia técnica a los sistemas informáticos que se utilizan en el nivel central, departamental y local. También la asistencia para los usuarios de sistemas con alcance a la comunidad escolar.

- Desarrollo de Sistemas.

Análisis, diseño y desarrollo de soluciones informáticas para automatizar los procesos institucionales que se requieran.

- Implementación de cambios y mejoras a los Sistemas

Es la implementación de mejoras o requerimientos en los procesos, ventanas, etc. para un sistema en particular.

Servicios brindados por la Gerencia de Infraestructura Tecnológica:

- Administración de Seguridad.

Son los servicios que prestan para proteger la infraestructura tecnológica del MINED (equipos de usuarios, redes, servidores, equipos de seguridad), y los accesos a dicha infraestructura por parte de todos los usuarios a través de los mecanismos de identificación correspondiente (usuarios y contraseña), segmentando los accesos a nivel de usuarios, servidores, y computadoras personales.

- Administración de Redes.

Son todas las actividades que se realizan para mantener funcionando las redes de computadoras del MINED (configuración, monitoreo, mantenimiento preventivo y correctivo) para brindar los servicios de usuario final (acceso a la red, correo electrónico, Internet, intranet y servicios de aplicación, enlaces con las oficinas descentralizadas y otras instituciones).

- Administración de Servidores.

Son las acciones que realizan los técnicos especialistas para poder mantener operando las computadoras centrales, en las cuales se ejecutan los servicios de bases de datos, correo electrónico, aplicaciones, Internet, intranet. Estas actividades son: Instalación, configuración,

mantenimiento, monitoreo, resolución de problemas, planificación de crecimiento de infraestructura.

- Administración de la infraestructura central de correo electrónico .

Son las actividades para proveer el servicio de correo electrónico (de autorización, creación, asignación de almacenamiento) interno e interinstitucional a los usuarios del MINED.

- Planificación de la Infraestructura Tecnológica.

Son las actividades de planeación realizadas según los lineamientos de la dirección, para proponer al comité estratégico de tecnologías de información, con el objeto de dimensionar las capacidades de procesamiento y almacenamiento de información del MINED. Además de la creación de las especificaciones técnicas para adquirir, administrar y asegurar la infraestructura institucional; utilizando las diferentes formas de financiamiento.

- Publicación Web.

Son las actividades realizadas para poder brindar los servicios de acceso a las páginas web del MINED desde el Internet, además del acceso a las aplicaciones que usan tecnología web (matrícula de media, censo, matrícula de básica, entre otros).

Servicios brindados por la Gerencia de Atención a Usuarios:

- Atención a usuarios in situ de hardware y software.

La Gerencia de Atención al Usuario del MINED recibe llamadas, reportes acerca de los incidentes de más de 1600 usuarios a nivel nacional, los cuáles requieren de una pronta y oportuna atención a las solicitudes de soporte técnico que se realizan (entre 40 y 50 en promedio diario) para garantizar un buen servicio.

- Reparación y mantenimiento de equipos de cómputo (correctivo, preventivo y gestión de garantías).

Consiste en proporcionar servicios de Mantenimiento a los equipos de los usuarios en coordinación con la empresa outsourcing a efecto de mantener la funcionalidad del hardware.

- Instalación y Actualización de programas en uso.

Cuando el software instalado no está adecuado a las necesidades del usuario, se instalan programas debidamente licenciados para uso del MINED, a efecto de que los usuarios tengan lo que necesitan para elaborar sus tareas diarias.

- Servicios de impresión.

Este servicio comprende la impresión y fotocopiado de documentos institucionales. La impresión se realiza por la asignación de impresores y una cuota de páginas mensual. El fotocopiado se realiza por la asignación de una cuota de páginas mensual, controlados a través de códigos de acceso a los equipos de fotocopiado. La administración de los costos de este servicio está bajo responsabilidad de la Gerencia de Logística.

Actividades que han impactado el servicio normal de esta gerencia:

- Esfuerzo técnico enfocado a la reconfiguración de colas de impresión por problemas de impresores dañados.
- Incorporación de técnicos adicionales a soporte.
- Trabajo de gestiones de actualización y revisión de antivirus en todos los equipos de los edificios A3 y A4. (Por problemas de virus).
- Inventario de hardware de todos los equipos del MINED Central.
- Revisión de todos los equipos del MINED Central para extraer inventario de hardware. Instalación de impresores Xerox en el MINED Central.
- Proyecto de evaluación de logros.
- Revisión de todos los equipos del MINED Central para extraer inventario de UPS.
- Reconfiguración de proxy de Internet al IP: 172.20.0.47 en 107 equipos, por problemas con el proxy 172.20.0.4.
- Nueva reconfiguración de proxy de Internet.

<u>Servicios brindados por la Gerencia de Normas y Calidad.</u>

- Revisión y documentación de Procedimientos y Políticas.

Revisión de los procedimientos actuales y su correspondiente documentación y codificación en base al marco de trabajo de la Dirección de Informática. Se realiza a demanda.

- Medición del Desempeño.

Revisión de los indicadores de desempeño definidos para los procesos de cada Gerencia. Puede realizarse a demanda o Trimestral.

- Auditorías de proceso y de sistemas.

Revisión de los controles dentro de los procesos y aplicaciones, con el objetivo de verificar la calidad de los servicios prestados. Se realiza a demanda.

- Determinación de la cantidad de procesos críticos dependientes.

Consiste en el cálculo de la cantidad de procesos críticos dependientes para cada uno de los servicios soportados por las TIC que son proporcionados por las diferentes Gerencias de la Dirección de Informática.

En la Tabla 26 se muestra un listado de la documentación de la Dirección de Informática.

Tipo de documento	Cantidad
Políticas	3
Normas	6
Manuales	8
Instructivos	11
Documentos	23
Formularios	50
Total	**101**

Tabla 26. Documentación de la Dirección de Informática.

ii. Equipos informáticos (hardware).

Se cuenta con una infraestructura de red que ha crecido en los últimos dos años hasta tener un centro de datos con 50 servidores divididos en 5 categorías las cuales son: servidores DNTE, servidores Infra-MINED, servidores de aplicación, servidores de prueba y servidores de contingencia, cada uno cuenta con 2 discos duros de 73GB que se encuentran en modalidad mirror raid1, una tarjeta RAM con capacidad mínima de 4GB y máxima de 32GB y con un procesador de capacidad mínima de 2.0Ghz a 2.9Ghz de capacidad máxima.

Las impresoras en un 93% pertenecen a una compañía que ofrece sus servicios de outsourcing y se encarga de darle el soporte técnico en caso de fallas.

Los routers, pasarelas, switchs, firewall, concentradores se encuentran en gabinetes 42o. Poseen varios puntos de acceso wireless en los niveles de las instalaciones para los diferentes tipos de usuarios. Existe un UPS para el cuarto de servidores el cual tiene una duración de 30 minutos y se activa después del primer respaldo que es una planta de diesel la cual dura alrededor de 5 horas.

Algunos servidores tienen garantía y en caso de fallo de alguna de sus partes éstas son sustituidas por el fabricante, los equipos por obsolescencia se depositan en una bodega.

Se tiene 800 equipos en los 4 edificios administrativos del MINED y 800 equipos distribuidos en las dependencias de los 14 departamentos del país. Todos estos activos vienen a sumar una inversión de $3, 500,000.00 a la fecha.

iii. Redes de comunicaciones.

La red telefónica o ADSL la brinda un proveedor externo con un ancho de banda de 1GB, con una topología en estrella híbrida, poseen switches de bordes en cada nivel de los 4 edificios, el backbone es de 100Mb de datos dedicados, los cuales se dividen en 2Mb para cada departamento, poseen una VPN interna que es utilizada por aproximadamente 20 personas, también poseen una intranet.

iv. Soportes de información.

Se realizan copias de respaldo (backups) diarias en cintas magnéticas de los correos, de las bases de datos, de la información institucional, de los portales y de los servicios de la Intranet las cuales duran 4 semanas. Se realizan copias de respaldo semanales de los correos y

del sistema de marcación biométrica las cuales duran 1 año, las copias de respaldo mensuales duran 5 años y las anuales no se borran.

Para ingresar a ciertas áreas restringidas se utilizan tarjetas inteligentes.

v. Equipamiento auxiliar.

El cuarto de servidores posee un aire acondicionado que mantiene su temperatura en 19^0 C, también posee sensores de humo y un sistema de gas que extrae el oxígeno en caso de incendios. Poseen una planta de diesel que mantiene el servicio de energía eléctrica por una duración de alrededor de 5 horas. También se cuenta con un sistema de alarmas que se activa por la noche 4 segundos después de un ingreso no autorizado.

vi. Instalaciones.

El MINED posee 4 edificios administrativos denominados A1, A2, A3, A4, el cuarto de servidores tiene una dimensión de $40m^2$ y se encuentra sobre una plataforma de 35cm. sobre el nivel del piso para protección del equipo contra inundaciones y dicho piso soporta hasta 3 toneladas, actualmente se está construyendo un edificio para montar un sistema de redundancia de servidores en caso de terremotos e inundaciones.

vii. Personal.

El MINED cuenta con alrededor de 1600 usuarios y personal administrativo que utilizan los servicios de TIC. La estructura organizativa del departamento de Informática está dividida en 5 instancias las cuales son:

- Dirección.
- Gerencia de Infraestructura Tecnológica
- Gerencia de Sistemas.
- Gerencia de Atención a Usuarios.
- Gerencia de Normas y Calidad.

b. Resumen del Enfoque Interno.

En el MINED la unidad informática encargada de administrar los riesgos de TIC es la Gerencia de Normas y Calidad aunque no cuentan con una metodología apropiada para tal propósito; lo que se realizan son registros anuales de la frecuencia de fallos, criterios de evaluación y mitigación de riesgos.

Según una encuesta realizada en el MINED sobre la calidad de los servicios de TIC, mostró un resultado con calificación de Bueno (7.6), debido a que algunos gerentes no estaban del todo conformes con los servicios brindados por las TIC de la institución.

En el MINED se considera necesaria la implementación de una metodología de administración de TIC ya que reconocen que la eficiencia de los servicios de las TIC sería óptima si se realiza una adecuada administración de los riesgos a los que son susceptibles.

Se cuenta con planes de contingencia pero según opiniones de personal de informática es necesario contar con un sitio de redundancia de información debido a la carga de procesos y distribución de la información.

Los registros de bitácoras por fallos se almacenan en archivos de hojas de cálculo que se clasifican por mes y año y también según el grado de impacto en el servicio normal de las TIC.

El equipo informático con que cuenta actualmente el MINED es de aproximadamente 1500 equipos informáticos y 50 servidores distribuidos en los 4 edificios administrativos y en las sedes departamentales, además los usuarios de dichos equipos se contabilizan en un aproximado de 1600.

A pesar que la duración de los fallos de los servicios de TIC en el MINED tiene una duración menor de 10 horas, en ocasiones éstos repercuten de manera significativa en los procesos dependientes de ellos, generando un atraso en cadena que se percibe en la gran mayoría de las dependencias administrativas. Sólo en los últimos 3 meses se contabilizan 3 fallas grandes pero que no han sobrepasado las 2 horas de duración y en ocasiones simplemente son pequeñas consultas de usuarios a soporte técnico.

La atención de usuarios in situ de hardware y software destaca como el servicio más recurrente de TIC, debido a la gran demanda y al escaso personal de soporte técnico para atender todos los casos diarios reportados por usuarios; por otra parte, las causas más comunes de fallos en las TIC son las provocadas por uso normal, degradación de equipos, de origen industrial e incidentes relacionados con hardware y problemas de red.

La infraestructura de red, servidores y los sistemas destacan como los rubros más importantes para el MINED debido a la inversión que se ha realizado en los últimos años.

Los rubros de TIC que presentan más gastos por fallos en los últimos años son el hardware, el software y la infraestructura de red.

La estructura organizativa del departamento de Informática está dividida en 5 instancias las cuales son: Dirección, Gerencia de Infraestructura Tecnológica, Gerencia de Sistemas, Gerencia de Atención a Usuarios y Gerencia de Normas y Calidad; cada una de estas instancias proporciona diferentes servicios a los usuarios del MINED.

La Dirección de Informática posee la documentación necesaria para poder administrar todo lo referente a su dirección, contando con 3 Políticas, 6 Normas, 8 Manuales, 11 Instructivos, 23 Documentos y 50 Formularios, totalizando 101 documentos.

G. MATRIZ DE CONGRUENCIA.

Diagnóstico de la utilización de metodologías de administración de riesgos en las tecnologías de información y comunicaciones.

Problemas	Objetivos del estudio	Hipótesis de la investigación	Métodos, técnicas, procedimientos e instrumentos.	Bosquejo del proyecto. Capitulación tentativa.
Conseguir administrar los riesgos de TIC según exigencia de la Corte de Cuentas de la República No se ha adoptado formalmente una metodología que facilite la administración de los riesgos, lo que conlleva a que la potencialidad de ocurrencia de estos riesgos se materialice. Riesgos de TIC, no controlados que dificultan las actividades operativas, tácticas y estratégicas.	General. Diagnosticar la situación actual en la utilización de metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones en las instituciones gubernamentales de manera que se identifiquen la calidad de los servicios, la frecuencia de fallos de TIC y los procedimientos actuales para llevar a cabo dicha administración.	General. La utilización de una metodología de administración de riesgos de tecnologías de información y comunicaciones en las instituciones gubernamentales, favorecerá alrededor de un 76% a la disminución de los riesgos de ocurrencia de fallos de los servicios soportados por estas tecnologías.	Tipo de investigación. Descriptiva. Métodos de investigación. Análisis. Síntesis. Técnicas para la recolección de datos Entrevista. Encuesta. Observación Instrumento de recolección de datos Cuestionario. Procedimiento Prueba de hipótesis	Capítulo I: Diagnóstico y Análisis de Requerimientos A. Objetivos del diagnóstico. B. Planteamiento del problema. C. Marco teórico. D. Formulación de hipótesis. E. Operaciones metodológicas. F. Tabulación y Análisis de datos G. Matriz de congruencia. H. Matriz FODA.

Problemas	Objetivos del estudio	Hipótesis de la investigación	Métodos, técnicas, procedimientos e instrumentos.	Bosquejo del proyecto. Capitulación tentativa.
	Específicos. Definir el tamaño de la muestra de las instituciones gubernamentales a visitar. Establecer el contexto de las instituciones gubernamentales con respecto a la utilización de metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones para determinar las oportunidades y amenazas a las que se enfrentan estas instituciones en materia de administración de riesgos de TIC.	Hipótesis nula. La utilización de una metodología de administración de riesgos de tecnologías de información y comunicaciones en las instituciones no favorecerá en lo absoluto la disminución de los riesgos de ocurrencia de fallos de los servicios soportados por estas tecnologías. Auxiliares. La falta de controles sobre los riesgos en las instituciones gubernamentales influye en un 80% en la ocurrencia de fallos en las TIC.		I. Diagnóstico de la situación actual de la utilización de metodologías de administración de riesgos de TIC.

Problemas	Objetivos del estudio	Hipótesis de la investigación	Métodos, técnicas, procedimientos e instrumentos.	Bosquejo del proyecto. Capitulación tentativa.
	Determinar la situación de adopción y aprovechamiento de la utilización de metodologías de Administración de Riesgos de Tecnologías de Información y Comunicaciones en las instituciones gubernamentales a fin de identificar las fortalezas y debilidades que estas instituciones pueden obtener al administrar riesgos de TIC. Analizar la situación externa de las instituciones gubernamentales y la situación interna del MINED en la administración de riesgos de TIC para determinar los puntos claves que debe contener una metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones.			

H. MATRIZ FODA.

Como complemento al diagnóstico realizado sobre la utilización de metodologías de administración de riesgos de tecnologías de información y comunicaciones en instituciones gubernamentales en la Tabla 27 se muestra el análisis FODA que considera las fortalezas, debilidades, oportunidades y amenazas de dichas instituciones.

Fortalezas	**Oportunidades**
• La existencia de una entidad responsable de la administración de riesgos de TIC. • Eficiencia y productividad mayor con el empleo de algún mecanismo. • Existencia de una bitácora de fallos. • Manejo de sistemas y equipos informáticos. • Administración de servidores. • Instalaciones y actualizaciones de software. • Buenas redes de comunicación. • Inversión en hardware y software.	• El conocimiento de metodologías de administración de riesgos de TIC. • Obtención de una mayor seguridad en las TIC. • La aplicación de algún mecanismo entre ellas las metodologías. • Defensas contra ataques intencionados. • Nuevos software o sistemas.
Debilidades	**Amenazas**
• Utilización de otras formas de administrar los riesgos que no son metodologías. • No existencia de un control de gastos por fallos. • Cantidad de usuarios demasiado grande. • El servicio de atención a usuarios in situ en Hw y Sw presenta fallos muy frecuentes. • Poca inversión en soportes de información.	• Los servicios no son considerados excelentes. • Los fallos en los servicios rondan la mayoría en alrededor de 10 horas. • La mala administración de redes. • De tipo natural. • Errores ocasionados por fallos no intencionados. • Los soportes de información que podrían desencadenar una contaminación viral masiva. • Gastos en hardware y software.

Tabla 27. Matriz FODA.

I. DIAGNÓSTICO DE LA UTILIZACIÓN DE METODOLOGÍAS DE ADMINISTRACIÓN DE RIESGOS DE TIC.

En base al enfoque externo realizado en las instituciones gubernamentales y autónomas se puede aseverar que la utilización de algún tipo de mecanismo orientado a la administración de riesgos de TIC tiene una importante influencia en la reducción de dichos riesgos a los que estas instituciones son susceptibles, así como en la cadena de procesos dependientes y en el impacto mismo de la materialización de amenazas.

A través del enfoque externo se logró identificar que las instituciones gubernamentales poseen diferentes infraestructuras tecnológicas que están íntimamente relacionadas en sus procesos de negocio, lo que las convierten en piezas indispensables en el engranaje de sus procesos operativos y administrativos. En lo que respecta la calidad de servicios se identificó que todas estas instituciones tienen una calificación de *Muy bueno*, que la frecuencia de los fallos es muy similar en casi todas las dependencias gubernamentales siendo de menos de 10 horas en la mayoría. De la misma manera, el estudio permitió conocer que los servicios que más fallos presentan son los de atención a usuarios in situ, acompañado de soporte técnico a sistemas y reparación de equipos, a esto también se le une que los ataques más comunes son los de errores y daños no intencionados.

Además, se conoció la forma en la que están siendo manejados los riesgos y se observó que el 74% de las instituciones aplica las políticas internas como mecanismo de administración de riesgos de TIC; sin embargo, en lo que respecta a la adopción de metodologías de administración de riesgos de TIC, se advirtió que la implementación de éstas conllevan ventajas importantes en relación a los otros mecanismos, entre estas ventajas sobresalen: el incremento notable de los beneficios, sobre todo la seguridad, productividad y calidad de los servicios soportados por las TIC.

Por otra parte, el enfoque interno del estudio orientado a conocer a fondo la situación actual del Ministerio de Educación en lo que respecta a la gestión de riesgos de las TIC arrojó importantes datos acerca de aspectos a considerar, entre los cuales destacan: la manera en la que se han estado administrando los riesgos de las TIC en el Ministerio de Educación hasta el día de hoy, las vulnerabilidades de las TIC que ameritan atención especial y los servicios que presentan los fallos más representativos. Se han observado vacíos en la

administración de riesgos de TIC que afectan de sobremanera el rendimiento de los servicios que soportan.

En vista de lo antes expuesto, y no dejando de lado el importante aporte argumentativo que ha resultado tanto de la investigación bibliográfica, como de la investigación de campo realizada en muchas instituciones que ya se han visto beneficiadas con las ventajas que ofrecen los diferentes mecanismos de administración de riesgos de TIC, de manera especial las Metodologías de Administración de Riesgos, ya que éstas se han diseñado (las metodologías preexistentes) con el fin único y particular de coadyuvar en la importante misión del personal administrador de riesgos de TIC, como lo es incrementar la productividad de las mismas, con el propósito de asegurarse que dichas TIC satisfagan las necesidades de información y comunicaciones para las que fueron adquiridas por las instituciones, y de manera especial, por el Ministerio de Educación.

A manera de resumen, se concluye que el Ministerio de Educación experimenta deficiencias en la administración de riesgos de TIC, la cual es producto de varios factores que han contribuido a ese estado, tales como la falta de un mecanismo ordenado, eficiente y diseñado para cubrir las necesidades particulares de dicha institución; de la misma manera, se ha percibido una falta de interés y/o prioridad en el área en cuestión, que ha predominado en los años anteriores y que oportunamente se está atendiendo en el presente.

El equipo de Trabajo de Graduación considera que, con el afán de proponer una solución eficiente y eficaz a los problemas de índole administrativa de la gestión de los riesgos de TIC, y obedeciendo a la necesidad urgente de mitigar el impacto de este inconveniente, tiene a bien sugerir, el diseño de una Metodología de Administración de Riesgos de TIC para el Ministerio de Educación; es decir, una metodología que satisfaga los requerimientos específicos de dicha institución en atención a procurar una máximo rendimiento en los servicios que soportan las TIC, así como a honrar la importante inversión que en este rubro se ha hecho en los últimos años.

CAPITULO II: ANÁLISIS DE REQUERIMIENTOS.

A. ANÁLISIS DEL PROBLEMA.

Enunciado del problema:

¿Cómo conseguir que el Ministerio de Educación controle eficiente y efectivamente los riesgos de fallos en los servicios que soportan las TIC con el fin que faciliten las actividades operativas, tácticas y estratégicas?

1. Determinación de las variables de entrada, salida y solución.

Variables de entrada	Limitaciones de entrada
Tipos de riesgos.	No existe.
Cantidad de TIC.	No existe.
Tipos de servicios.	No existe.
Mecanismos de administración de riesgos de TIC.	No existe.
Beneficios de los mecanismos de administración de riesgos de TIC.	No existe.
Registro de fallos de los servicios de TIC.	No existe.
Conocimiento básico de administración de riesgos de TIC.	No existe.

Tabla 28. Variables de entrada para el análisis del problema.

Variables de salida	Limitaciones de salida
Tipos de riesgos.	Riesgos a los que el MINED es susceptible.
Mecanismo de administración de riesgos de TIC.	Se debe especificar el mecanismo adecuado para la administración de riesgos de TIC del MINED.
Registro de fallos de los servicios de TIC.	Disminución en la cantidad de fallos del registro.
Beneficios de los mecanismos de administración de riesgos de TIC.	Incremento en los beneficios del mecanismo de administración de riesgos de TIC.
Conocimiento especializado sobre la aplicación de mecanismos de administración de riesgos de TIC.	El personal del MINED debe haber incrementado su nivel de conocimientos en la adopción y puesta en marcha de mecanismos orientados a administrar los riesgos de TIC.

Tabla 29. Variables de salida para el análisis del problema. Constituyen el resultado que se pretende alcanzar.

Variables de solución
• Método para determinar el tipo de mecanismo adecuado para administrar los riesgos de TIC.
• Método para determinar el enfoque del mecanismo de administración de riesgos de TIC.
• Método para determinar el porcentaje de efectividad de los mecanismos de administración de riesgos de TIC.

Tabla 30. Variables de solución para el análisis del problema.

a. Descripción de las variables de entrada.

- **Tipos de riesgos:** Se refiere a una tipificación de los riesgos de TIC. Se utilizará con el propósito de ordenar las diferentes secciones del mecanismo a diseñar.
- **Cantidad de TIC:** Es la cantidad de equipo de TI y TC que está inventariado en las oficinas centrales y dependencias departamentales del Ministerio de Educación.
- **Tipos de servicios:** Se refiere a los diferentes servicios que soportan las TIC.
- **Mecanismos de administración de riesgos de TIC:** Es el conjunto de mecanismos o instrumentos orientados a lograr una correcta administración de riesgos de TIC.
- **Beneficios de los mecanismos de administración de riesgos de TIC:** Es el conjunto de beneficios que ofrecen los diferentes mecanismos de administración de riesgos de TIC que fueron identificados por los usuarios en la fase de diagnóstico.
- **Registro de fallos de los servicios de TIC:** Es la bitácora de fallos de los servicios de TIC que se documenta en el Ministerio de Educación.
- **Conocimiento básico de administración de riesgos de TIC:** Se refiere al conocimiento básico con que debe contar el personal de informática del Ministerio de Educación.

b. Descripción de las variables de salida.

- **Tipos de riesgos:** Son el conjunto de riesgos de TIC que se podrían materializar en el Ministerio de Educación.
- **Mecanismo de administración de riesgos de TIC:** Es el mecanismo evaluado como más adecuado para ser implementado en el Ministerio de Educación, posterior a su selección y especificación.

- **Registro de fallos de los servicios de TIC:** Define y muestra un decremento en los fallos de los servicios soportados por las TIC en el Ministerio de Educación.
- **Beneficios de los mecanismos de administración de riesgos de TIC:** Representa un incremento en los beneficios que ofrece el mecanismo de administración de riesgos de TIC seleccionado.
- **Conocimiento especializado sobre la aplicación de mecanismos de administración de riesgos de TIC:** Se refiere a la capacitación técnica que debe tener el personal de informática del Ministerio de Educación a la hora de implementar el mecanismo de administración de riesgos de TIC especificado.

c. Descripción de las variables de solución.

- **Método para determinar el tipo de mecanismo adecuado para administrar los riesgos de TIC:** Es un procedimiento de elaboración propia que se utilizará con el propósito de evaluar y escoger el mecanismo más adecuado para posteriormente especificarlo, con el fin de mejorar el proceso de administración de riesgos de TIC en el Ministerio de Educación.
- **Método para determinar el enfoque del mecanismo de administración de riesgos de TIC:** Es un procedimiento de elaboración propia que se utilizará con el propósito de determinar la naturaleza del enfoque del mecanismo de administración de riesgos de TIC seleccionado, por ejemplo: *enfoque cualitativo, enfoque cuantitativo, enfoque mixto o híbrido,* entre otros.
- **Método para determinar el porcentaje de efectividad de los mecanismos de administración de riesgos de TIC:** Es un procedimiento de elaboración propia utilizado para determinar el grado de eficiencia y efectividad de las diferentes propuestas de mecanismos de administración de riesgos de TIC.

2. Restricciones.

La alternativa de solución deberá desarrollarse en el período comprendido entre febrero a noviembre de 2009.

3. Criterios que debe cumplir la solución.

Los criterios se han establecido en base a los requerimientos de los usuarios del Ministerio de Educación.

Criterios	Descripción
Sencillez	Se refiere a la facilidad de comprensión de la solución propuesta, mediante una redacción en lenguaje técnico y claro.
Aplicabilidad	Está orientado a que la solución propuesta sea fácilmente aplicable siguiendo las indicaciones correspondientes. Se refiere también a que debe ser ajustable al Ministerio de Educación.
Confiabilidad	Se refiere a la seguridad que al implementar la propuesta de solución se logrará el objetivo de minimizar significativamente los riesgos de TIC.
Efectividad	Se refiere a la capacidad de la solución para satisfacer las necesidades orientadas a la administración de riesgos de TIC en el Ministerio de Educación.
Costo mínimo	Se refiere a la inversión de recursos que será necesaria para la implementación de la solución seleccionada y especificada cumpliendo con los criterios antes mencionados.

Tabla 31. Criterios que debe cumplir la solución

4. Volumen.

Solución única que consiste en una propuesta de mecanismo orientado a administrar efectivamente los riesgos de las TIC en el Ministerio de Educación.

5. Uso.

La propuesta de solución se implementará en el Ministerio de Educación, a través de la Gerencia de Normas y Calidad. La solución deberá actualizarse cada cinco años, porque así lo establecen las políticas internas de dicha institución.

B. ANALISIS DE REQUERIMIENTOS.

1. Requerimientos Funcionales.

a. Requerimientos de Salida.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad

Nº	**Especificación**
1	**Reporte de Servicios de TIC.**
	La metodología proporcionará un listado de los servicios de TIC que brinda el MINED. Dicho informe deberá contener: Código, nombre y descripción del servicio de TIC. Nombre de la gerencia responsable, usuarios Procesos críticos dependientes, ubicación física, estado

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
2	**Reporte de Software.**
	La metodología proporcionará un listado de las aplicaciones informáticas que posee el MINED. Dicho informe deberá contener: Código, nombre y descripción de la aplicación informática. Nombre de la gerencia responsable, usuarios, ubicación física. Código de servicio que soporta, fecha de creación. Licencia, versión, estado.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
3	**Reporte de Hardware.**
	La metodología proporcionará un listado del Equipo Informático que soporta los diferentes servicios de TIC del MINED. Dicho informe deberá contener: Código y nombre del equipo. Responsable, usuarios, cantidad, ubicación física. Código de servicio que soporta Fecha de adquisición Características Tipo (Servidor ó Cliente) Estado

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
4	**Reporte de Tipos de Fuentes de Amenazas.**
	La metodología proporcionará un listado de amenazas a las que el MINED puede estar expuesto. Dicho informe deberá contener: Código y nombre de la amenaza. Tipo de origen o fuente de la amenaza. Motivación, acciones que materializarían la amenaza

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
5	**Reporte de vulnerabilidades.**
	La metodología proporcionará un listado de vulnerabilidades relacionadas a fuentes de amenazas identificadas en el MINED. Dicho informe deberá contener: Código y nombre de la vulnerabilidad. Código y fuente de la amenaza relacionada. Acciones que materializarían la amenaza

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
6	**Reporte de controles recomendados que garanticen el correcto funcionamiento de los servicios de TIC.**
	La metodología permitirá la recomendación de controles adecuados para garantizar los servicios de TIC en todas las unidades organizativas del MINED. Dicho informe deberá contener: Tipo de Origen, Código y nombre de fuente de amenaza. Código y nombre de vulnerabilidad, nivel del riesgo, magnitud de impacto, Listado de controles recomendados.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
7	**Reporte de Priorización de acciones.**
	La metodología proporcionará un informe con las acciones que se aplicarán prioritariamente a los servicios de TIC con niveles de riesgos altos ya que estos serán los que requerirán medidas de acción inmediatas para proteger los intereses del MINED de vulnerabilidades y amenazas. Dicho informe deberá contener: Código y nombre del servicio de TIC. Nivel del impacto del riesgo. Listado de controles recomendados.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad

Nº	**Especificación**
8	**Reporte de Plan de Acción.**
	La metodología proporcionará un informe del plan de acción que se seguirá en caso de una posible materialización de una amenaza perjudicando el correcto funcionamiento de los servicios de TIC del MINED. Dicho informe deberá contener: Código y nombre del plan de acción Código y nombre del servicio de TIC Código y nombre de la fuente de amenaza Probabilidad del riesgo, magnitud de impacto Nivel del impacto del riesgo Listado de controles recomendados Recursos necesarios para aplicar los controles Personal responsable Fecha de inicio y fin del plan de acción

b. Requerimientos de Entrada.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad

Nº	**Especificación**
1	**Administración de Servicios de TIC.**
	La metodología permitirá el registro y actualización de servicios de TIC brindados por el MINED. Los datos a registrar son: Código, nombre y descripción del servicio de TIC. Nombre de la gerencia responsable, usuarios Procesos críticos dependientes, ubicación física, estado

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
2	**Administración del Software.**
	La metodología permitirá el registro y actualización de las aplicaciones informáticas que posee el MINED. Los datos a registrar son: Código, nombre y descripción de la aplicación informática. Nombre de la gerencia responsable, usuarios, ubicación física. Código de servicio que soporta, fecha de creación. Licencia, versión, estado.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
3	**Administración del Hardware.**
	La metodología permitirá el registro y actualización del Equipo Informático que soporta los diferentes servicios de TIC. Los datos a registrar son: Código y nombre del equipo. Responsable, usuarios, cantidad, ubicación física. Servicio que soporta Fecha de adquisición Características Tipo (Servidor ó Cliente) Estado

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
4	**Administración de Tipos de Fuentes de Amenazas.**
	La metodología permitirá el registro y actualización de tipos de fuentes de amenazas a las que el MINED puede estar expuesto. Los datos a registrar son: Código y nombre de la amenaza. Tipo de origen o fuente de la amenaza. Motivación, acciones que materializarían la amenaza

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
5	**Administración de vulnerabilidades.**
	La metodología permitirá el registro y actualización de vulnerabilidades relacionadas a fuentes de amenazas identificadas en el MINED. Los datos a registrar son: Código y nombre de la vulnerabilidad. Código y fuente de la amenaza relacionada. Acciones que materializarían la amenaza

c. Requerimientos de Procesos.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
1	**Determinación del grado del ejercicio de la vulnerabilidad.**
	La metodología realizará un procedimiento para determinar el grado del ejercicio de la vulnerabilidad cuando una amenaza potencial se materialice valiéndose de una vulnerabilidad de las TIC. Para determinar dicho grado se deberán tener en cuenta los siguientes factores: Motivación y capacidad para materializar una amenaza. Naturaleza de la vulnerabilidad. Existencia y eficacia de los controles.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad
Nº	**Especificación**
2	**Determinación de la magnitud de impacto.**
	La metodología realizará un procedimiento para determinar la magnitud del impacto en las TIC cuando una amenaza se materialice. Para determinar la magnitud del impacto se deberá tener en cuenta la criticidad de cada uno de los servicios de TIC.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad

Nº	**Especificación**
3	**Determinación del nivel del impacto del riesgo.**
	La metodología realizará un procedimiento para determinar el nivel del impacto del riesgo en las TIC. Para determinar el nivel del impacto del riesgo se deberá tener en cuenta los valores de la probabilidad del riesgo y la magnitud del impacto.

d. Requerimientos de Seguridad.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación	
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores	**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón	**Gerencia:** Normas y Calidad

Nº	**Seguridad**	
1	**Manejo de errores**	La metodología deberá contemplar el manejo de errores en su uso y de alteración de información.
2	**Aplicación monousuaria.**	El prototipo de la aplicación de la metodología deberá estar diseñado para el Gerente de Normas y Calidad exclusivamente.

2. Requerimientos No Funcionales.

a. Requerimientos Generales.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación		
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores		**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón		**Gerencia:** Normas y Calidad
Nº	**Generales**	
1	**Idioma**	La metodología y su respectiva documentación serán desarrolladas en idioma español.
2	**Administración**	La metodología deberá ser administrada de manera centralizada por el jefe de la Gerencia de Normas y Calidad, así como su prototipo funcional.

b. Requerimientos de Documentación.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación		
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores		**Fecha:** 30/07/2009
Usuario: Ing. Max Mirón		**Gerencia:** Normas y Calidad
Nº	**Documentación**	
1	**Plan de Implementación**	La metodología contará con su respectivo plan de implementación
2	**Manual de Operación**	La metodología contará con su respectivo manual de Operación o Manual de Usuario (Prototipo de Software).

3. Requerimientos de Desarrollo.

a. Hardware para desarrollar la metodología

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación			
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores			**Fecha:** 30/07/2009
Nº	**Tipo**	**Características**	**Descripción**
1	Laptop1	Intel Celeron 1.60 GHz, Memoria RAM de 512MB, Unidad de DVD-ROM, Disco Duro de 40 GB, Fuente de alimentación HP 19V., Tarjeta Ethernet y Tarjeta de red inalámbrica.	Computadora para el desarrollo de la metodología
2	Laptop2	Dual Core 1.66 GHz, Memoria RAM de 2.5GB, Unidad de DVD-ROM, Disco Duro de 80 GB, Fuente de alimentación Dell 19.5V., Tarjeta Ethernet y Tarjeta de red inalámbrica.	Computadora para el desarrollo de la metodología
3	Laptop3	Dual Core 1.73 GHz, Memoria RAM de 1GB, Unidad de DVD-ROM, Disco Duro de 80 GB, Fuente de alimentación Acadapter 19V., Tarjeta Ethernet y Tarjeta de red inalámbrica.	Computadora para el desarrollo de la metodología
4	Switch	4 Puertos	Dispositivo electrónico de interconexión de redes de ordenadores
5	Cable UTP	Categoría 5	Cable de par trenzado utilizado como medio de comunicación en una red de ordenadores
6	Impresor	Canon IP1000	Periférico que permite producir una copia permanente de textos o gráficos de documentos almacenados en formato electrónico, en medios físicos normalmente en papel o transparencias.
7	Memoria USB	Capacidad de almacenamiento 1 GB	Pequeño dispositivo de almacenamiento de información

b. Software para desarrollar la metodología.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación			
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores			**Fecha:** 30/07/2009
Nº	**Tipo**	**Características**	**Descripción**
1	Sistema Operativo	Windows XP Profesional SP2	Programa que establece la comunicación entre las distintas partes del hardware y las aplicaciones
2	Herramientas de Ofimática	Microsoft Office 2007	Suite Ofimática que incluye los siguientes programas: Word (procesador de texto), Excel (hoja de cálculo), Access (base de datos) y PowerPoint (programa para presentaciones)
3	Lenguaje de Programación	Java	Java es un lenguaje de programación orientado a objetos que toma mucha de su sintaxis de C y C++.
4	Base de Datos	Oracle	Sistema de gestión de bases de datos relacionales.
5	Servidor Web	Tomcat	Funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation.
6	Antivirus	NOD32 3.0, AVG 8.5	Programa creado para prevenir o evitar la activación de virus en la PC.
7	Navegadores	Mozilla Firefox 3.0.11, Internet Explorer 8.0	Software que permite recuperar y visualizar documentos de hipertextos desde servidores web de todo el mundo a través de Internet
8	Utilitarios	Compresor de archivos WinRar 3.7	Programa compresor de archivos para ahorrar espacio en disco.

4. Requerimientos de Operación.

a. Hardware para la instalación/ejecución de la metodología.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación		
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores		**Fecha:** 30/07/2009
Nº	**Tipo**	**Características**
1	Computadora de Escritorio	**Características Mínimas:** Monitor 14 pulgadas VGA, Microprocesador Pentium II de 300Mhz, Memoria RAM de 128MB, Disco Duro de 20GB, Unidad de CD, Disquetera, Teclado, Mouse, Tarjeta de Red Ethernet. **Características Óptimas:** Monitor 14 pulgadas VGA, Microprocesador AMD de 2Ghz, Memoria RAM de 256MB, Disco Duro de 40GB, Lector de CD/DVD, Disquetera, Teclado, Mouse, Tarjeta de Red Ethernet, puertos USB.

b. Software para la instalación/ejecución de la metodología.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación		
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores		**Fecha:** 30/07/2009
Nº	**Tipo**	**Características**
1	Sistema Operativo	Windows 98 o superior.
2	Herramientas de Ofimática	Microsoft Office 2000 ó superior.
3	Lenguaje de Programación	Java
4	Base de Datos	Oracle
5	Servidor Web	Tomcat
6	Navegadores	Mozila Firefox 3.0.11

c. Definición del Marco Legal.

Diseño de una Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación		
Analistas: Ada Patricia Lovo Zelaya Adán Mauricio Romero López Kevin Jaime Rivera Flores		**Fecha:** 30/07/2009
Nº	**Definición del Marco Legal**	
1	Marco Legal	En el presente proyecto se respeta y se hace cumplir la ley de los derechos de autor cumpliendo con todas las prerrogativas que dicha ley establece, con la finalidad de evitar multas y demandas en el momento de implementar la metodología. Una vez diseñada la Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones para el Ministerio de Educación, la institución interesada deberá solicitar a la Escuela de Ingeniería de Sistemas Informáticos la Metodología con sus respectivos permisos de uso.

C. BÚSQUEDA DE POSIBLES SOLUCIONES.

En este apartado se procede a buscar las posibles soluciones que satisfagan las restricciones y criterios anteriormente expuestos.

Se realizó una investigación bibliográfica sobre metodologías de administración de riesgos de tecnologías de información y comunicaciones en las organizaciones.

Las alternativas de solución que más se apegan con las restricciones impuestas y las variables encontradas tanto en el diagnóstico como en el análisis de requerimientos para el MINED se presentan a continuación:

1. MAGERIT.

El CSAE (Consejo Superior de Administración Electrónica) ha elaborado y promueve la metodología Magerit como respuesta a la percepción de que la Administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la

información para la consecución de sus objetivos de servicio. La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

a. Objetivos que persigue esta metodología:

Directos:

i. Sensibilizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.

ii. Ofrecer un método sistemático para analizar tales riesgos.

iii. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

iv. Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda cada caso.

b. Fases de la Metodología.

Fase 1: Análisis de Riesgos.

Permite determinar qué tiene la Organización y estimar lo que podría pasar.

Elementos:

i. Activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con éste) que aportan valor a la Organización

ii. Amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización

iii. Salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen (tanto) daño.

Con estos elementos se puede estimar:

- El impacto: lo que podría pasar
- El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

Pasos que se realizan en esta fase:

Con el objeto de organizar el análisis, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean "potenciales": caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

Paso 1: Activos.

Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

Paso 2: Amenazas.

Determinar a qué amenazas están expuestos aquellos activos.

Paso 4: Determinación del Impacto.

Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

Paso 5: Determinación del Riesgo.

Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Paso 3: Salvaguardas.

Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo

Fase 2: Gestión de Riesgos.

Permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; el riesgo se reduce a un nivel residual que la Dirección asume. La gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

Pasos que se realizan en esta fase:

Paso 1. Interpretación de los valores de impacto y riesgo residuales.

Impacto y riesgo residual se toman como una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza

Mientras el valor residual sea más que despreciable, hay una cierta exposición.

El valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho. Los responsables de la toma de decisiones deben prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de Insuficiencias.

Paso 2. Selección de Salvaguardas.

Las amenazas se deben conjurar, por principio y mientras no se justifique lo contrario.

Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

i. Establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa

ii. Establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada

iii. Establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer

iv. Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas

v. Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto

No es necesario llevar a cabo todos los puntos anteriores para cada amenaza, por ello esta metodología propone cuatro tipos de salvaguardas:

- **Salvaguardas técnicas:** en aplicaciones, equipos y comunicaciones
- **Salvaguardas físicas:** protegiendo el entorno de trabajo de las personas y los equipos
- **Medidas de organización:** de prevención y gestión de las incidencias
- **Política de personal:** que, a fin de cuentas, es el eslabón imprescindible y más delicado: política de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

Paso 3. Pérdidas y ganancias.

No se puede invertir en salvaguardas más allá del valor de los propios activos a proteger.

Existen técnicas que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas, que pretenden reflejar cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%.

Paso 4. Actitud de la Dirección.

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable.

Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios.

2. COBIT.

El IT Governance Institute (ITGI por sus siglas en inglés) ha creado y diseñado COBIT que es una metodología que permite el desarrollo de políticas claras y de buenas prácticas para el control de TI (Tecnologías de Información) a través de las empresas.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución.

a. Criterios de control de la metodología.

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, COBIT define los siguientes siete criterios de información: La efectividad, la eficiencia, la confidencialidad, la integridad, la disponibilidad, el cumplimiento, la confiabilidad

b. Fases de la metodología.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI.

Fase 1. Planear y Organizar.

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que las TI puedan contribuir de la mejor manera al logro de los objetivos del negocio. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

Fase 2. Adquirir e Implementar.

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios afectarán las operaciones actuales del negocio?

Fase 3. Entregar y dar soporte.

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

Fase 4. Monitorear y Evaluar.

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?

• ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?

• ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

c. Objetivos de Control.

Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT.

El modelo de control consiste en comparar normas, estándares y objetivos institucionales con los procesos de TI basados en la información de control para poder actuar ó indicar acciones a seguir en un determinado momento.

3. ITIL.

ITIL son las siglas de una metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gubernativa de Comercio Británica (Office of Goverment Comerce). Las siglas de ITIL significan (Information Technology Infrastructure Library) o Librería de Infraestructura de Tecnologías de Información.

a. Objetivos de la metodología.

ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua.

Otra de las cosas que propone es que para cada actividad que se realice se debe de hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda la gente esté al tanto de los cambios y no se tome a nadie por sorpresa.

En la documentación se pone la fecha en la que se hace el cambio, una breve descripción de los cambios que se hicieron, quién fue la persona que hizo el cambio, así como quién es el que autorizó el cambio, para que así se lleve todo un seguimiento de lo que pasa en el entorno.

b. Fases de la metodología.

Fase 1. Manejo de Incidentes.

Su objetivo primordial es restablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, esto se hace con la finalidad de que se minimicen los efectos de la operación. Para este proceso se tiene un diagrama que en cada una de sus fases maneja cuatro pasos básicos que son: propiedad, monitoreo, manejo de secuencias y comunicación.

Fase 2. Manejo de problemas.

El objetivo de este proceso es prevenir y reducir al máximo los incidentes, y esto nos lleva a una reducción en el nivel de incidencia. Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

En este proceso lo que se busca es que se pueda tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo al problema.

El diagrama de este proceso es muy particular, ya que se maneja en dos fases: la primera está relacionada con lo que es el control del problema y la segunda es con el control del error.

Fase 3. Manejo de configuraciones.

Su objetivo es proveer con información real y actualizada de lo que se tiene configurado e instalado en cada sistema del cliente.

Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, entonces al cambiar una o varias de ellas se afecta el sistema en general, lo que hace que sea muy difícil de manipular. Aunque es lo más parecido a la realidad, porque nuestro entorno es dinámico y las decisiones de unos afectan a otros.

Fase 4. Manejo de cambios.

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de los cambios.

Primero se tiene un registro y clasificación del cambio a realizar, se pasa a la fase de monitoreo y planeación, si el rendimiento es satisfactorio se da la aprobación del cambio, y

en caso de que el rendimiento sea malo se pasa a la fase de reingeniería hasta que el proceso funcione adecuadamente, ya que se aprueban los cambios, se construyen prototipos o modelos en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las capacidades del sistema, ya que el proceso está probado se da la autorización e implementación; ya implementado se ve que no se hayan tenido desviaciones y se ajusta a las necesidades actuales que también se le considera como revisión post-implementación

Fase 5. Manejo de entregas.

Su objetivo es planear y controlar exitosamente la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real.

Este proceso tiene un diagrama que marca la transición que se da de acuerdo a los ambientes por los que se va dando la evolución del proyecto.

En el ambiente de desarrollo se tiene que hacer la liberación de las políticas, la liberación de la planeación, el diseño lógico de la infraestructura que se va a implementar y la adquisición de software y hardware están entre los ambientes de desarrollo y de pruebas controladas; luego se hace la construcción y liberación de las configuraciones (nivel lógico), se hacen las pruebas para establecer los acuerdos de aceptación; se da la aceptación total de versiones y de modelos, se arranca la planeación y finalmente las pruebas y comunicaciones; y en el ambiente se da la distribución e instalación.

En el proceso de entrega del servicio es el punto en el que el usuario hace uso del servicio y no sabe que detrás del servicio que está recibiendo hay un sin fin de actividades y de decisiones que se tuvieron que tomar para llegar a este punto.

4. MARMINED

MARMINED es la Metodología de Administración de Riesgos de TIC para el Ministerio de Educación que se pretende desarrollar por el grupo de trabajo en dicho Ministerio.

MARMINED es una metodología que pretende administrar los riesgos de TIC de una forma eficaz ya que considera la seguridad de las TIC como un componente importante en el éxito de una organización para que ésta pueda llevar a cabo su misión. Por lo tanto, el proceso de gestión de riesgos no debe ser tratado como una función técnica llevada a cabo por expertos de TIC sino como un elemento esencial de la función de gestión de la

organización. La metodología toma como base el hecho de que el riesgo es el impacto negativo neto del ejercicio de una vulnerabilidad, teniendo en cuenta la probabilidad y el impacto de la ocurrencia y que la gestión de riesgo constituye el proceso de identificación, evaluación y las medidas que se deben tomar para reducir el riesgo a un nivel aceptable.

a. Objetivos de la metodología.

i. Asegurar las TIC de la organización tanto de almacenamiento, procesamiento y de transmisión de información.

ii. Identificar, evaluar y mitigar los riesgos de TIC en la organización.

iii. Implementar planes de contingencias en caso de fallas de TIC en la organización

iv. Una administración que permita tomar decisiones de gestión de riesgo bien formadas y poder justificar gastos que forman parte de un presupuesto de TIC.

b. Fases de la metodología.

Fase 1. Configuración de Elementos de TIC.

En esta fase se caracterizarán los tipos de TIC que posee la organización. Dentro de los cuales se pueden mencionar los servicios de TIC, el software y hardware necesarios para los procesos de negocio diarios en la organización.

Fase 2. Evaluación de Riesgos.

En esta fase se determina el alcance de la amenaza potencial y los riesgos asociados de TIC. El resultado de este proceso ayuda a identificar los controles adecuados para reducir o eliminar los riesgos.

Para determinar la probabilidad de un futuro acontecimiento adverso, las amenazas a las TIC deben ser analizadas en relación con el potencial de las vulnerabilidades y los controles establecidos para ellas.

El impacto se refiere a la magnitud del daño que podría ser causado por una amenaza.

El nivel de impacto se rige por la sumatoria de los impactos potenciales y, a su vez produce un valor relativo para las TIC y los recursos afectados (por ejemplo, la criticidad y sensibilidad de los componentes de los sistemas y datos).

Esta fase abarca seis pasos que son:

Paso1: Identificación de Amenazas.

Paso2: Identificación de Vulnerabilidades.

Paso3: Determinación de Riesgos.

Paso4: Análisis de Impacto.

Paso5: Análisis de Riesgos.

Paso6: Recomendación de controles.

Paso7: Documentación.

Fase 3. Mitigación de Riesgos.

Mitigación de riesgos implica priorizar, evaluar y la aplicación de la reducción del riesgo de control recomendadas a partir de la evaluación de riesgos.

Dado que la eliminación de todo el riesgo suele ser poco práctico o casi imposible, es responsabilidad de los altos directivos y gerentes de negocios utilizar el menor costo aceptable y aplicar el enfoque más adecuado para disminuir los controles a un nivel de riesgo aceptable con un mínimo impacto negativo en los recursos de la organización y su misión.

Opciones de mitigación de riesgos:

- Reconocimiento de Riesgos. Para aceptar el riesgo potencial y que sigan operando las TIC o para poner en práctica controles para reducir el riesgo a un nivel aceptable.
- Prevención de riesgos. Para evitar el riesgo mediante la eliminación de la causa de riesgo y / o consecuencia (por ejemplo, renunciar a ciertas funciones del sistema o apagar el sistema cuando los riesgos son identificados).
- Limitación del riesgo. Para limitar el riesgo mediante la aplicación de los controles que reduzcan al mínimo los efectos adversos de una amenaza del ejercicio de una vulnerabilidad (por ejemplo, el uso de apoyo, prevención, controles de detección).
- Riesgo de Planificación. Para gestionar el riesgo mediante el desarrollo de un plan de mitigación de riesgo que prioriza, implementa y mantiene los controles.
- Investigación y Reconocimiento. Para reducir el riesgo de pérdida de reconocimiento de la vulnerabilidad o falla el control y la investigación para corregir la vulnerabilidad.

• Transferencia de riesgo. Para transferir el riesgo mediante el uso de otras opciones para compensar la pérdida, como la compra de seguros.

5. Evaluación de alternativas.

En la Tabla 32 se muestra los porcentajes de los requerimientos que cada alternativa de solución abarca para las especificaciones particulares del MINED, podemos observar que algunas alternativas cumplen con un porcentaje muy bajo de requerimientos para considerarse una alternativa de solución.

Requerimientos / Alternativas	HARDWARE	SOFTWARE	INSTALACIONES	PERSONAL
MAGERIT	50%	100%	50%	25%
COBIT	50%	50%	50%	50%
ITIL	50%	25%	50%	25%
MARMINED	100%	100%	85%	75%

Tabla 32. Evaluación de las alternativas de solución de acuerdo al porcentaje de cumplimiento de requerimientos del MINED.

D. FASE DE DECISIÓN.

En esa sección se procederá a seleccionar la alternativa que más se ajuste a los criterios de diseño expuestos en la sección de Análisis del Problema.

1. Codificación de las alternativas a evaluar.

No.	Nombre	Código
1	**MAGERIT**	Prop 01
2	**COBIT**	Prop 02
3	**ITIL**	Prop 03
4	**MARMINED**	Prop 04

Tabla 33. Codificación de las alternativas a evaluar.

2. Establecimiento y ponderación de los criterios de evaluación.

Criterios	Ponderación
Sencillez	15%
Confiabilidad	20%
Aplicabilidad	30%
Costo mínimo	10%
Efectividad	25%
Total	100%

Tabla 34. Ponderación de criterios que debe cumplir la solución.

3. Establecimiento y ponderación de áreas que debe cubrir la solución.

Áreas	Ponderación
Hardware	35%
Software	30%
Instalaciones	25%
Personal	10%
Total	100%

Tabla 35. Ponderación de áreas que debe cubrir la solución en base al análisis de requerimientos.

4. Escalas de calificación.

A continuación se presenta un cuadro con las escalas de calificación y sus respectivos conceptos o significados. La escala ha sido determinada de acuerdo a los niveles de aceptación que pudiera tener una alternativa de solución con respecto a los criterios a evaluar y a las áreas que cubrirá dicha solución.

Calificación	Concepto
1	No satisface el criterio en absoluto.
2	El criterio se cubre en una medida por debajo de la requerida.
3	El criterio se cumple en un 50%.
4	El criterio se cumple aceptablemente.
5	Satisface el criterio totalmente.

Tabla 36. Escalas de calificación.

5. Evaluación de alternativas de solución.

El grupo de trabajo ha asignado a cada alternativa de solución la calificación que considera pertinente, basándose en la investigación bibliográfica y en el análisis de requerimientos. En las Tablas 37 y 38 se muestran los resultados de la evaluación.

Criterios / Propuestas	**Sencillez 15%**		**Confiabilidad 20%**		**Aplicabilidad 30%**		**Costo Mínimo 10%**		**Efectividad 25%**		**Total**
	Nota	Total	Nota	Total	Nota	Total	Nota	Total	Nota	Total	
Prop 1	4	0.6	4	0.8	3	0.9	2	0.2	4	1	**3.5**
Prop 2	3	0.45	4	0.8	3	0.9	2	0.2	4	1	**2.3**
Prop 3	3	0.45	4	0.8	2	0.6	2	0.2	3	1	**2.0**
Prop 4	4	0.6	4	0.8	4	1.2	3	0.3	4	1	**3.9**

Tabla 37. Evaluación de alternativas de solución en base a los criterios que debe cumplir la solución.

Áreas / Propuestas	**Hardware 35%**		**Software 30%**		**Instalaciones 25%**		**Personal 10%**		**Total**
	Nota	Total	Nota	Total	Nota	Total	Nota	Total	
Prop 1	5	1.75	4	1.2	4	1.0	4	0.4	**4.4**
Prop 2	4	1.4	4	1.2	3	0.75	4	0.4	**3.8**
Prop 3	3	1.05	4	1.2	3	0.75	5	0.5	**3.5**
Prop 4	5	1.75	5	1.5	4	1.0	4	0.4	**4.6**

Tabla 38. Evaluación de alternativas de solución en base a las áreas que debe cubrir la solución.

A continuación se muestra en la Tabla 39 la calificación total de las dos evaluaciones de las Tablas 37 y 38 tomando en cuenta que cada evaluación constituye el 50% del total de la calificación para cada alternativa.

Propuestas	Evaluación 1	Evaluación 2	Total
Prop 1	**3.5**	**4.4**	**7.9**
Prop 2	**2.3**	**3.8**	**6.1**
Prop 3	**2.0**	**3.5**	**5.5**
Prop 4	**3.9**	**4.6**	**8.5**

Tabla 39. Calificación total de las alternativas de solución.

Al verificar los resultados obtenidos en la Tabla 39, se puede observar que la propuesta de solución mejor evaluada es la Prop 4 que es la alternativa MARMINED, este resultado es congruente con la evaluación que se realizó en la Tabla 32 en la página 85 de las alternativas de solución, donde también resulta ser la alternativa que posee los porcentajes más altos de cumplimiento de las especificaciones particulares del MINED, debido a esto se seleccionará como la alternativa de solución por haber logrado la máxima aceptación y calificación de los criterios de evaluación previamente establecidos y del análisis de requerimientos del MINED. La propuesta de solución seleccionada se especificará en la Etapa de Diseño de la Solución.

CAPITULO III: DISEÑO GENERAL.

A. INTRODUCCIÓN.

La Metodología de Administración de Riesgos de TIC[19] para el Ministerio de Educación[20] (MARMINED), nace con el propósito de ofrecer una gestión eficiente de los servicios soportados por las TIC en el Ministerio de Educación.

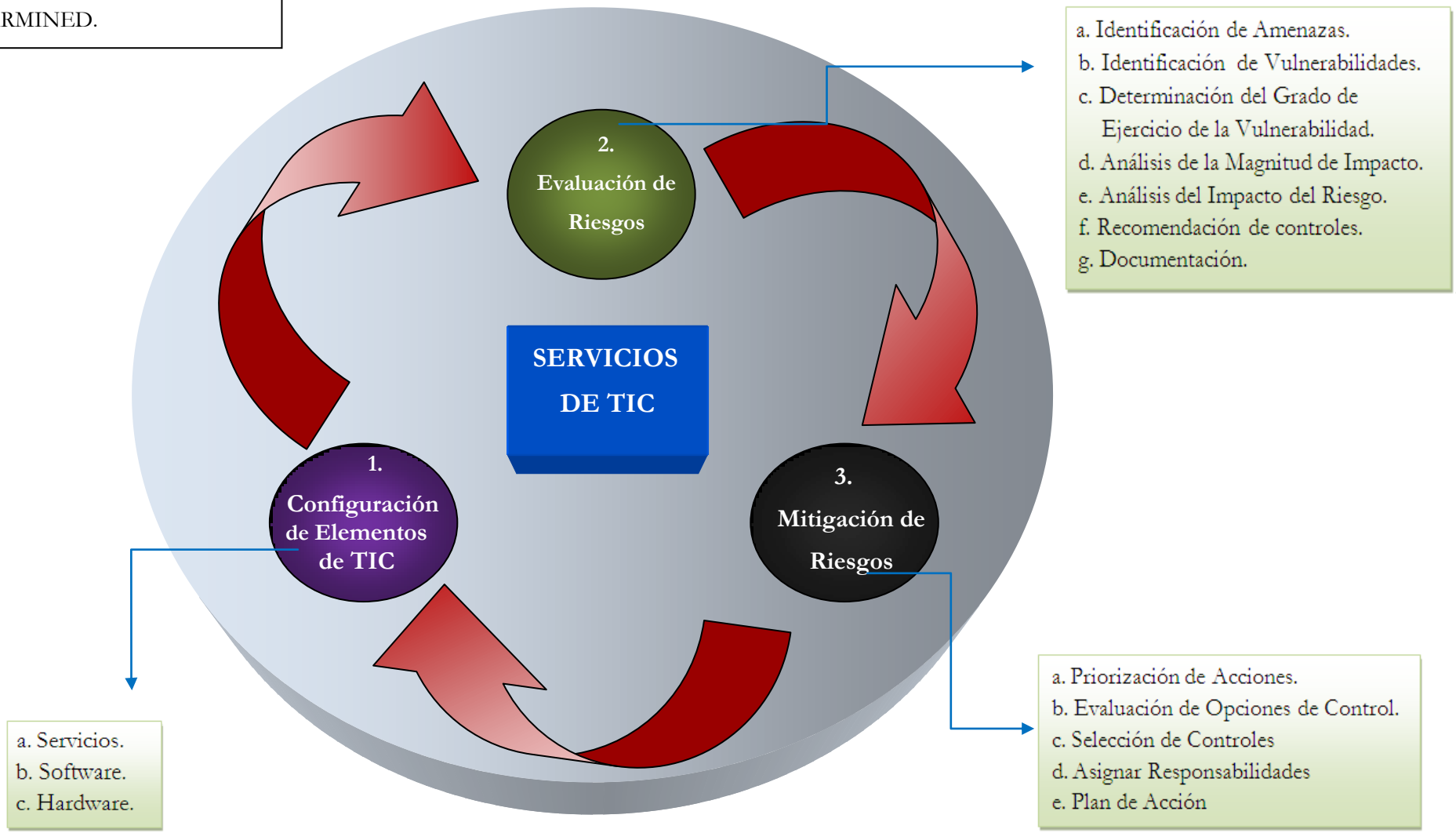
MARMINED es una excelente herramienta con la cual se podrían beneficiar numerosas instituciones estatales que atiendan las exigencias que dicta la Corte de Cuentas de la República, las cuales están establecidas en las Normas Técnicas de Control Interno.

En la siguiente página se muestra un bosquejo general de MARMINED (Figura 2) en el que destacan las fases en las que se divide la metodología. Se observa una estructura cíclica repetitiva, esto es debido a que la metodología se implementará cada dos años[21], registrando las diferentes amenazas y su relación con las vulnerabilidades; se sugerirán controles, se decidirá por los más adecuados según las posibilidades de la institución y se elaborará un plan de acción orientado a mitigar los riesgos identificados.

Cada una de las esferas de la Figura 2 representa una fase de MARMINED: la primera es la Configuración de los Elementos[22] de TIC; la segunda fase es la Evaluación de los Riesgos y la tercera es la Mitigación de los Riesgos; cada una de las cuales se explicará pertinentemente.

[19] Sigla usada para referirse a las Tecnologías de Información y Comunicaciones.
[20] En lo sucesivo se utilizará la sigla "MINED" para referirse al Ministerio de Educación.
[21] En la sección Generalidades se establece la frecuencia con que se implementará la metodología.
[22] La conceptualización de Configuración de Elementos de TIC se deberá interpretar como el registro de cualquier componente de TIC que necesite ser integrado por ser pieza fundamental en el engranaje de la administración de riesgos.

Figura 2. Esquema General de MARMINED.



B. OBJETIVO DE MARMINED.

Ofrecer una solución efectiva al problema de la gestión de riesgos de TIC en el Ministerio de Educación, de manera que se puedan administrar eficientemente cada uno de los elementos relacionados con los servicios que soportan las TIC, con el propósito de optimizar su rendimiento, así como de minimizar el grado de materialización de amenazas mediante el aprovechamiento de vulnerabilidades para que los beneficios que éstas tecnologías ofrecen pueda explotarse al máximo con la finalidad de brindar un servicio de calidad a sus usuarios.

C. GENERALIDADES.

Para la utilización de MARMINED debe existir un escenario que cuente con los siguientes elementos:

- La existencia de Tecnologías de Información y Comunicaciones (TIC) que brinden soportes a servicios en el MINED.
- La(s) persona(s) encargada de usar la metodología debe ser parte del personal de la Unidad Informática[23] del MINED.
- La(s) persona(s) que llenen los formularios deben poseer los conocimientos técnicos necesarios para obtener la información, es decir, los datos a ser utilizados por la metodología.
- Se debe corroborar la existencia de los servicios soportados por las TIC y clasificarlos de acuerdo al código según la gerencia del MINED a la que pertenezca el servicio.
- La Unidad Informática debe haber realizado las actividades pertinentes orientadas a obtener la cantidad de procesos críticos dependientes, ya sea para los servicios existentes como para los nuevos.
- La Unidad Informática debe de tener a disposición la información del equipo informático y de las aplicaciones informáticas con las que se cuenta.

[23] Se utiliza *Unidad Informática* para referirse a la Dirección Informática del Ministerio de Educación.

1. Acerca de los responsables del llenado de formularios.

El personal técnico que forma parte del equipo de trabajo de la Gerencia de Normas y Calidad, (la cual es una dependencia de la Unidad de Informática del MINED) serán los responsables del llenado de los formularios utilizados en las diferentes fases de MARMINED, junto a los especialistas de redes, de seguridad, de servidores y sistemas; es decir, un técnico de cada área y un técnico de calidad[24], quien verificará la validez de los datos introducidos de los servicios de TIC suministrados en los diferentes departamentos.

2. Acerca de la frecuencia de implementación de MARMINED.

MARMINED se implementará siguiendo las instrucciones de las políticas institucionales del MINED, las cuales establecen que la gestión de riesgos se deberá realizar cada dos años. Sin embargo para efectos de control y monitoreo interno, MARMINED se implementará una vez al año, sin estar sujetos a un determinado período.

3. Acerca de la cantidad y de la forma del llenado de formularios.

El llenado de los formularios utilizados en las diferentes fases de MARMINED se realizará atendiendo las indicaciones que en cada uno de ellos se encuentre y se procederá a un llenado manual.

La cantidad de formularios que se han de llenar obedece a la cantidad de TIC y a las posibles amenazas relacionadas a un servicio determinado.

[24] *Técnico de calidad:* persona que trabaja para la Gerencia de Normas y Calidad de la Unidad Informática del MINED.

D. DISEÑO DETALLADO.

1. FASE 1: "Configuración de Elementos de TIC".

Se consideran elementos de TIC los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente. En la Figura 3 se puede apreciar de forma gráfica los pasos a seguir en esta fase.

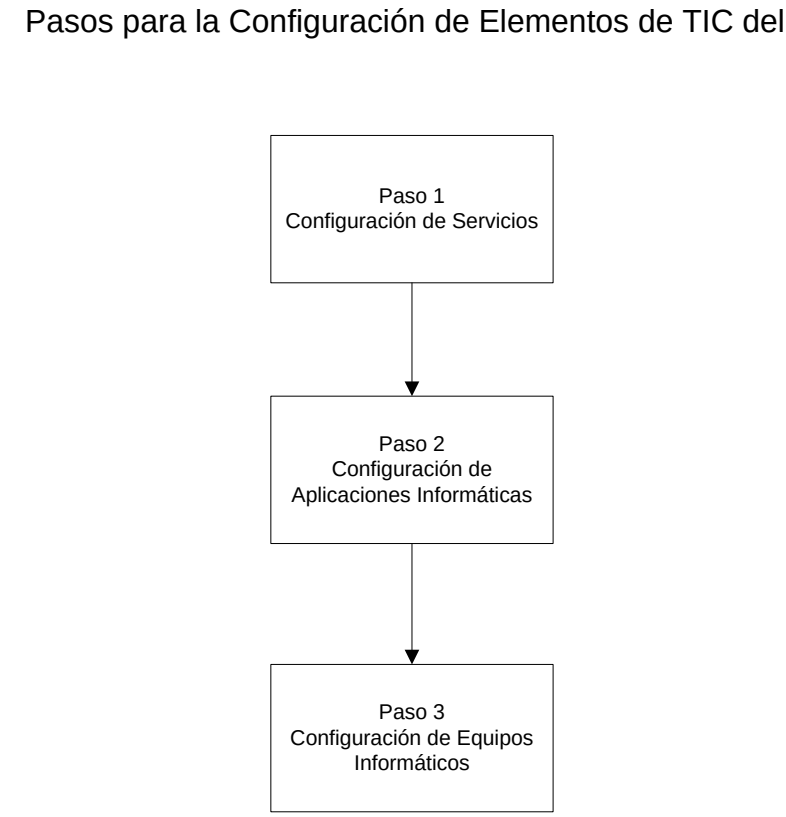


Figura 3: Pasos para la Configuración de Elementos de TIC del MINED**.**

En la configuración de elementos de TIC se pretende recabar información acerca de la infraestructura de TIC que posee el MINED para poder habilitar controles de monitoreo y mantenimiento de los recursos necesarios para brindar correctamente los servicios, el estado e historial de dichos elementos de TIC y las relaciones entre ellos. En base a lo anterior se presentan los Formularios de Tipos de Elementos de TIC que servirán para la configuración de los Servicios, Aplicaciones Informáticas y Equipos Informáticos, todo esto con el fin de establecer el alcance de la evaluación de riesgos y proporcionar información esencial para definir el escenario de los riesgos asociados a la institución.

Para poder identificar los elementos de TIC se necesita un profundo conocimiento del entorno en el cual se encuentran, ya que no todos los elementos tienen las mismas características; dependiendo del tipo de elemento, las amenazas y los controles serán diferentes, el elemento esencial es la información que maneja el sistema de información; o sea los datos. Y alrededor de estos datos se pueden identificar otros elementos relevantes tales como:

- **Los servicios** que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para gestionar dichos datos.
- **Las aplicaciones informáticas** (software) que permiten manejar los datos.
- **Los equipos informáticos** (hardware) que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

La configuración de elementos de TIC es una información documental de interés como un criterio de identificación de amenazas potenciales y controles apropiados a la naturaleza del elemento de TIC.

Los instrumentos a través de los cuales se configurarán los elementos de TIC del MINED son los Formularios 1, 2, 3a y 3b, determinando para cada uno un código, un nombre y otras características dependiendo del tipo de elemento de TIC.

a. Configuración de Servicios.

Los servicios son la función que satisfacen las necesidades de los usuarios (del servicio) del MINED. Para la prestación de un servicio se requieren una serie de medios. Estos servicios pueden ser servicios finales (prestados por la organización a terceros), instrumentales (donde los usuarios y los medios son propios), contratados (a otra organización que los proporciona con sus propios medios), de información, de comunicaciones y de seguridad de TIC.

A continuación se describe el procedimiento para la configuración de los servicios:

Paso 1: Completar el Formulario 1 [SER] que se muestra en la página siguiente, atendiendo cuidadosamente las indicaciones.

Paso 2: El código del servicio se escribirá dependiendo de la Gerencia responsable de la administración de dicho servicio; así por ejemplo, para el servicio Soporte Técnico a Sistemas, se tiene que corresponde a la Gerencia de Sistemas Informáticos, por lo que el código se escribirá así: GSI-001, donde GSI representa las iniciales del nombre de la Gerencia a la cual dicho servicio pertenece, seguido de un guión y su correspondiente número correlativo. Para las Gerencia de Infraestructura Tecnológica, Gerencia de Normas y Calidad, Gerencia de Atención a Usuarios In Situ se utilizarán GIT, GNC y GAU respectivamente.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"REGISTRO DE LOS SERVICIOS DE TIC"** **CÓDIGO: FOR-GNC-SER-009** **VERSIÓN: 1.0** **Página 1 de 1**	
[SER] Servicios	
Indicaciones: • En la Parte I complete los espacios en blanco con la información solicitada. • En la Parte II coloque un cheque (√) en la opción que más se adecúe al estado del servicio.	
Parte I	
Código: _____	**Nombre:** _____
Descripción: _____ _____	
Gerencia Responsable: _____	
Usuarios: _____ _____	
Procesos Críticos Dependientes: _____	
Ubicación Física: _____	
Parte II	
Estado: **( )** Activo	**( )** Inactivo

Formulario 1: Formulario de Configuración de Servicios del MINED.

b. Configuración de Aplicaciones Informáticas (Software).

Con múltiples denominaciones (programas, aplicaciones, sistemas y otros) este elemento se refiere a aquellas herramientas informáticas que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

A continuación se describe el procedimiento para la configuración de las aplicaciones informáticas (software):

Paso 1: Completar según las indicaciones el Formulario 2 [SW] que se muestra en la página siguiente. Atender cuidadosamente las indicaciones que en éste se presentan.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"REGISTRO DE SOFTWARE"** **CÓDIGO: FOR-GNC-SW-009** **VERSIÓN: 1.0** **Página 1 de 1**	
[SW] Aplicaciones Informáticas(software)	
Indicaciones: • En la Parte I complete los espacios en blanco con la información solicitada. • En la Parte II coloque un cheque (√) en la opción que más se adecúe al estado del software.	
Parte I	
Código: _____	**Nombre:** _____
Descripción: _____ _____	
Gerencia Responsable: _____	
Usuarios: _____ _____	
Ubicación Física: _____	
Código de servicio que soporta: _____	
Fecha de Creación: _____	
Licencia: _____	
Versión: _____	
Parte II	
Estado: **( )** Activo	**( )** Inactivo

Formulario 2: Formulario de Configuración de Aplicaciones Informáticas del MINED**.**

c. Configuración de Equipos Informáticos (Hardware).

Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta el MINED, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Se tipificarán 2 tipos de equipos informáticos con los que cuenta el MINED:

Equipos Servidores: Grandes equipos informáticos que almacenan y proporcionan enormes cantidades de información

Equipos Clientes: Estos equipos están clasificados en 3 categorías A, B y C definidos por rangos establecidos que dependen de sus características particulares.

A continuación se describe el procedimiento para la configuración de los equipos informáticos (hardware):

Paso 1: Completar según las indicaciones de los Formularios 3a y 3b [HW] que se presentan a continuación. Atender cuidadosamente las indicaciones que en éstos se presentan, porque el llenado difiere si se trata de un equipo servidor o uno del tipo cliente.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"REGISTRO DE HARDWARE"** **CÓDIGO: FOR-GNC-HW-009** **VERSIÓN: 1.0** **Página 1 de 2**
[HW] Equipos Informáticos (hardware)
Indicaciones: • En la Parte I complete los espacios en blanco con la información solicitada. • En la Parte II coloque un cheque (√) en la opción que más se adecúe al Tipo de Equipo Informático. • Si el Tipo de Equipo Informático es Servidor complete los espacios en blanco de la Parte IIa, si es equipo Cliente coloque un cheque (√) en la Parte IIb para seleccionar si el equipo es de Tipo A, B o C. • En la Parte III coloque un cheque (√) dependiendo el estado del Hardware.
Parte I
Código: _____ **Nombre:** _____
Gerencia Responsable: _____
Usuarios: _____ _____
Cantidad: _____
Ubicación Física: _____
Código de servicio que soporta: _____
Fecha de Adquisición: _____

Formulario 3a: Formulario de Configuración de Equipos Informáticos del MINED**.**

MINISTERIO DE EDUCACIÓN
DIRECCIÓN DE INFORMÁTICA
GERENCIA DE NORMAS Y CALIDAD

MARMINED
"REGISTRO DE HARDWARE"

CÓDIGO: FOR-GNC-HW-009
VERSIÓN: 1.0 **Página 2 de 2**

[HW] Equipos Informáticos (hardware)

Parte II

Tipo: Servidor **( )** Cliente **( )**

Parte IIa
Características:

Marca	Modelo	Disco Duro	Memoria RAM	Procesador

Parte IIb

Tipo A ( )

Componente\Rango	**Desde**	**Hasta**
Procesador	Pentium IV 2.0 Ghz	Core 2 Duo
Memoria RAM	2.5 GB	8GB
Disco Duro	80GB	1TB

Tipo B ( )

Componente\Rango	**Desde**	**Hasta**
Procesador	Pentium III 600Mhz	Pentium IV 1.9Ghz
Memoria RAM	256 MB	2.4 GB
Disco Duro	30 GB	79 GB

Tipo C ( )

Componente\Rango	**Desde**	**Hasta**
Procesador	Pentium I 200Ghz	Pentium III 599Mhz
Memoria RAM	64 MB	128 MB
Disco Duro	4 GB	29 GB

Parte III

Estado:
( ) Activo **( )** Inactivo

Formulario 3b: Formulario de Configuración de Equipos Informáticos del MINED.

2. FASE 2: "Evaluación de Riesgos".

Pasos para la Evaluación de Riesgos

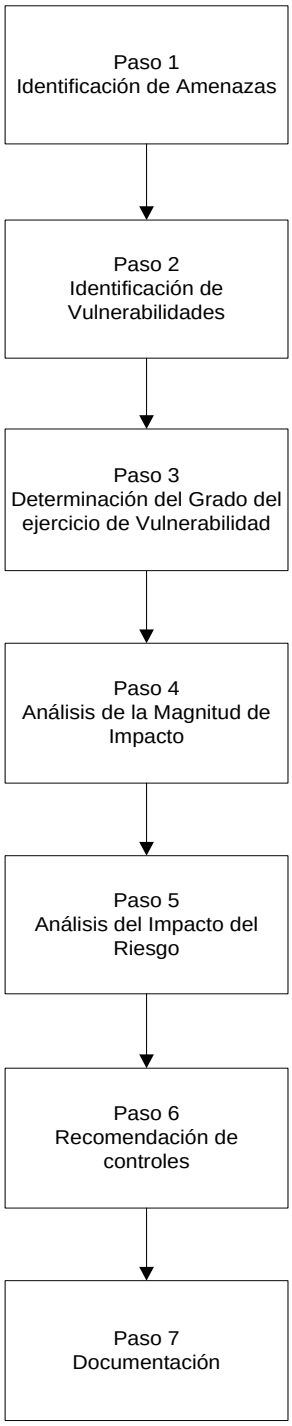


Figura 4. Pasos de la fase Evaluación de los Riesgos de TIC.

a. Identificación de amenazas.

Se entiende por amenaza el potencial que una fuente de amenaza se active accidental o intencionalmente, aprovechándose de una vulnerabilidad[25].

Los datos que se presentan a continuación han sido obtenidos mediante técnicas de investigación tales como la observación directa, entrevistas a los miembros responsables de la administración de riesgos de las TIC en el MINED.

La primera tarea al evaluar los riesgos de TIC consiste en identificar los tipos de fuentes de amenaza o tipos de origen, las fuentes mismas, así como las acciones que un atacante puede realizar para materializar una amenaza. En el siguiente apartado se muestran todos estos elementos que se identificaron previo al diseño de la metodología y que aquí se presentan para facilitar la identificación de las mismas. A continuación se describe el procedimiento para la identificación de amenazas:

Paso 1: Verificar en el Catálogo de tipos de fuente de amenaza o tipo de origen a cuál de los tipos pertenece la amenaza observada. El Catálogo se encuentra en el apartado **i** de esta sección.

Paso 2: Verificar en el Catálogo de fuente de amenaza si la fuente de amenaza que ha observado ya está identificada. Para facilitar la búsqueda, las fuentes de amenaza se listan según los tipos de origen al que pertenecen. El Catálogo se encuentra en el apartado **ii** de esta sección.

Paso 3: Si la amenaza observada no se encuentra en el Catálogo de fuente de amenaza, entonces se procederá a completar el Formulario 4 [IAM] mostrado en la siguiente página. El código de la fuente de amenaza se colocará respetando el tipo de origen al que pertenece, así por ejemplo, si se desea registrar una amenaza llamada *"Amenaza X"* que corresponde al tipo de fuente de amenaza "Riesgos Organizacionales", entonces se escribirá de la siguiente manera: FA-RO-02, donde FA-RO significa que es una Fuente de Amenaza del tipo de Riesgo Organizacional, y que su número correlativo es dos, debido a que en dicho catálogo ya se ha registrado el número uno para este misma fuente de amenaza.

[25] En la sección siguiente se tratará la vulnerabilidad.

MINISTERIO DE EDUCACIÓN
DIRECCIÓN DE INFORMÁTICA
GERENCIA DE NORMAS Y CALIDAD

MARMINED
"FORMULARIO PARA LA IDENTIFICACIÓN DE AMENAZAS"
CÓDIGO: FOR-GNC-IAM-009
VERSIÓN: 1.0 **Página 1 de 1**

[IAM] Formulario para la Identificación de Amenazas

Indicaciones:

- En la Parte I escriba un código para la amenaza a registrar.
- En la Parte II coloque un cheque en la opción que más se adecúe al tipo de origen de la amenaza a registrar.
- En la Parte III complete los espacios en blanco.

Parte I	*Parte II*
Código de fuente de amenaza: _____	**Tipo de origen:** **( )** [TFA-NA] Riesgos naturales. **( )** [TFA-FNI] Riesgos provocados por errores y/o fallos no intencionados. **( )** [TFA-FI] Riesgos provocados por errores y/o fallos intencionados. **( )** [TFA-FOI] Riesgos provocados por fallos de origen industrial. **( )** [TFA-RO] Riesgos organizacionales.

Parte III
Fuente de amenaza:
_____
_____

Motivación:
_____
_____
_____

Acciones que al realizarse materializarían la amenaza.
_____
_____
_____
_____

Formulario 4: Formulario para la Identificación de Amenazas.

i. Catálogo de los tipos de fuentes de amenaza o tipo de origen.

- *[TFA-NA] Riesgos naturales.*
- *[TFA-NI] Riesgos provocados por errores y/o fallos no intencionados.*
- *[TFA-FI] Riesgos provocados por errores y/o fallos intencionados.*
- *[TFA-IN] Riesgos provocados por fallos de origen industrial.*
- *[TFA-RO] Riesgos organizacionales.*

ii. Catálogo de la fuente de amenaza.

Una fuente de amenaza es la intención y el método orientados a aprovecharse de una vulnerabilidad; también se define como una situación y el método que puedan desencadenar una vulnerabilidad accidentalmente.

Las amenazas para las TIC en el MINED obedecen a diferentes fuentes de amenazas; de manera general, estas fuentes se pueden agrupar en:

- *[TFA-NA] Riesgos naturales: Acontecen de forma "independiente" a las actividades de los seres humanos.*
  - [FA-NA-01] Incendios.
  - [FA-NA-02] Inundaciones.
  - [FA-NA-03] Rayos.
  - [FA-NA-04] Tormentas eléctricas.
  - [FA-NA-05] Huracanes.
  - [FA-NA-06] Terremotos.

- *[TFA-NI] Riesgos provocados por errores y/o fallos no intencionados: Suceden por la utilización incorrecta del equipo de TIC por falta de capacitación a los usuarios de las mismas.*
  - [FA-NI-01] Introducción errónea de información en los diferentes servicios.
  - [FA-NI-02] Errores de configuración al momento de la instalación de software y redes de comunicaciones.
  - [FA-NI-03] Omisión por olvido de la actualización de los registros en las bases de datos, registros incompletos, registros incorrectos.
  - [FA-NI-04] Inconsistencia o inseguridad en la asignación de responsabilidades.
  - [FA-NI-05] Errores de configuración de cuentas por asignación de privilegios de acceso.
  - [FA-NI-06] Propagación involuntaria de virus, espías, troyanos, bombas lógicas, gusanos.

- [FA-NI-07] Entrega de información sensible a destinos incorrectos de forma involuntaria.
- [FA-NI-08] Borrado accidental de información.
- [FA-NI-09] Uso de software defectuoso.
- [FA-NI-10] Caída del sistema por insuficiencias de recursos.

❖ *[TFA-FI] <u>Riesgos provocados por errores y/o fallos intencionados:</u> Son fallos provocados con alevosía por parte de los usuarios con el fin de vulnerar la integridad del equipo de TIC.*

- [FA-FI-01] Manipulación de la configuración de los equipos de TIC.
- [FA-FI-02] Suplantación de identidad del usuario.
- [FA-FI-03] Abuso de privilegios de acceso.
- [FA-FI-04] Transmisión de software dañino.
- [FA-FI-05] Alteración en la ruta de la mensajería institucional.
- [FA-FI-06] Acceso no autorizado.
- [FA-FI-07] Análisis de tráfico.
- [FA-FI-08] Interceptación de información.
- [FA-FI-09] No aceptación de responsabilidades.
- [FA-FI-10] Introducción de información falsa, errónea o incompleta.
- [FA-FI-11] Degradación de la información.
- [FA-FI-12] Destrucción de la información.
- [FA-FI-13] Manipulación en la configuración del software.
- [FA-FI-14] Robo de equipos de TIC.
- [FA-FI-15] Ataque destructivo.
- [FA-FI-16] Extorsión a los usuarios de las TIC.
- [FA-FI-17] Ingeniería social.
- [FA-FI-18] Hacker.
- [FA-FI-19] Cracker.
- [FA-FI-20] Criminal informático.
- [FA-FI-21] Terroristas.
- [FA-FI-22] Empleados internos.

- *[TFA-IN] <u>Riesgos provocados por fuentes de amenazas de origen industrial:</u> Pueden ocurrir de forma accidental y son derivados de actividades humanas, están relacionadas con la composición química de ciertos materiales industriales así como también a la reacción a ciertos factores ambientales.*
  - [FA-IN-01] Incendio.
  - [FA-IN-02] Escapes, fugas o inundaciones de agua.
  - [FA-IN-03] Explosiones.
  - [FA-IN-04] Contaminación química.
  - [FA-IN-05] Sobrecarga y/o fluctuaciones eléctricas.
  - [FA-IN-06] Vibraciones, polvo, suciedad.
  - [FA-IN-07] Interferencia de radio y campos magnéticos.
  - [FA-IN-08] Defectos de fábrica del hardware.
  - [FA-IN-09] Fallos por corte en la alimentación eléctrica.
  - [FA-IN-10] Deficiencias en la aclimatación de los locales dispuestos para las TIC.
  - [FA-IN-11] Exceso de los márgenes de trabajo de las TIC. Fallos en los servicios de comunicaciones.
  - [FA-IN-12] Degradación de los soportes de almacenamiento de información.

- *[TFA-RO] <u>Riesgos organizacionales:</u> Son aquellos que afectan directa o indirectamente las funciones de una o más unidades organizativas, y que surgen a partir de lineamientos del nivel estratégico y/o medidas económicas que se adoptan estatalmente.*
  - [FA-RO-01] Falta de fondos para renovar licencias de software.

iii. Razones de iniciación de las acciones de amenaza.

Existen muchas posibles motivaciones que pueden llevar a un individuo o conjunto de ellos a materializar una amenaza, tales motivaciones obedecen a ciertos tipos de fuentes de amenaza y se manifiestan con acciones encaminadas a quebrantar la integridad de las TIC.

En la Tabla 40 se representan algunas fuentes de amenaza, las motivaciones que originan a tomar las acciones referidas:

Fuente de amenaza	Motivación	Acciones para materializar la amenaza
Hacker. Cracker.	• Ego. • Rebelión. • Desafío.	• Hacking. • Ingeniería Social. • Sistemas de intrusión, allanamientos. • Sistema de acceso no autorizado.
Criminal Informático.	• Destrucción de la información. • Revelación ilegal de información. • Ganancia monetaria. • Alteración no autorizada de datos.	• Delincuencia informática. • Acciones fraudulentas (suplantación de identidad, intercepción). • Soborno. • Spoofing. • Intrusión a los sistemas.
Terroristas.	• Chantaje. • Destrucción. • Explotación. • Venganza.	• Colocación de bombas. • Sistema de ataque (ejemplo: denegación de servicio, distribuido). • Sistemas de penetración. • Sistema de manipulación.
Empleados internos (con capacitación deficiente, descontentos, maliciosos, negligentes, deshonestos o despedidos).	• Curiosidad. • Ego. • Inteligencia. • Ganancia monetaria. • Venganza. • Errores no intencionados y omisiones (introducción de datos errónea, errores en la programación).	• Asalto a un empleado. • Chantaje. • Búsqueda de información confidencial. • Abuso del equipo de TIC. • Robo y fraude. • Soborno para obtener información confidencial. • Falsificación y daño de datos. • Intercepción. • Código malicioso (virus, troyanos, bombas lógicas). • Venta de información personal. • Sabotaje. • Intrusión.

Tabla 40. Motivación y acciones para materializar amenazas a las TIC.

b. Identificación de vulnerabilidades.

Vulnerabilidad es una falla o debilidad en el sistema, procedimientos de seguridad, diseño, ejecución o controles internos que puedan ser ejercidos accidentalmente o intencionalmente, provocando un fallo en la seguridad o una violación de las políticas de seguridad del sistema.

Los pasos a seguir para la identificación de vulnerabilidades son los siguientes:

Paso 1: Verificar en el Catálogo de vulnerabilidades si la vulnerabilidad observada ya se encuentra registrada, el catálogo se puede ver en el apartado **i** de esta misma sección.

Paso 2: Si la vulnerabilidad observada no se encuentra en el Catálogo de vulnerabilidades, entonces se procederá a completar el siguiente Formulario 5 [IVU] que se muestra a continuación. El código de vulnerabilidad se colocará de la siguiente manera: CV-0006, donde CV significa Código de Vulnerabilidad, y su número correlativo es seis.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"FORMULARIO PARA LA IDENTIFICACIÓN DE VULNERABILIDADES"** **CÓDIGO: FOR-GNC-IVU-009** **VERSIÓN: 1.0** **Página 1 de 1**
[IVU] Formulario para la Identificación de Vulnerabilidades
Indicaciones: • En la Parte I escriba un código para la vulnerabilidad a registrar. • En la Parte II coloque un cheque en la opción que más se adecúe al tipo de origen de la amenaza relacionada a la vulnerabilidad. • En la Parte III complete los espacios en blanco.
Parte I **Código de Vulnerabilidad:** _____
Parte II **Tipo de origen relacionado:** **( )** [TFA-NA] Riesgos naturales. **( )** [TFA-NI] Riesgos provocados por errores y/o fallos no intencionados. **( )** [TFA-FI] Riesgos provocados por errores y/o fallos intencionados. **( )** [TFA-IN] Riesgos provocados por fallos de origen industrial. **( )** [TFA-RO] Riesgos organizacionales.
Parte III **Vulnerabilidad:** _____ _____
Código de fuente de amenaza: _____ **Fuente de amenaza:** _____
Acciones que al realizarse materializarían la amenaza
_____

Formulario 5: Formulario para la Identificación de Vulnerabilidades.

A continuación se muestran las vulnerabilidades encontradas en la administración de riesgos de TIC en el MINED, junto con las posibles amenazas que podrían quebrantar la integridad de las TIC, así como de los servicios que soportan:

i. Catálogo de vulnerabilidades.

Código Vulnerabilidad	Vulnerabilidad	Fuente de amenaza	Acciones para materializar la amenaza
CV-0001	**En las diferentes oficinas administrativas se utilizan rociadores de agua para suprimir el fuego cuando los cobertores para proteger el equipo no están colocados.**	• Incendios. • Negligencia del personal.	Rociadores de agua que se activan al percibir humo mediante sus sensores.
CV-0002	**En el acceso al cuarto de servidores no se realiza una verificación de la caracterización física de las personas autorizadas para el ingreso.**	• Descuido en el uso y almacenamiento de la tarjeta de acceso al cuarto de servidores.	Robo de las tarjetas de acceso a los servidores, ingreso por suplantación de identidad. Sabotaje. Destrucción y/o robo de las cintas de respaldo.
CV-0003	**Los usuarios comparten sus nombres de inicio de sesión y contraseñas o las colocan en lugares visibles.**	• Poca cultura informática de algunos usuarios de los sistemas de informáticos.	Suplantación de identidad en el ingreso a sistemas informáticos. Modificación/borrado de datos.
CV-0004	**No existen sistemas de redundancia remota de la información contenida en los servidores y cintas de respaldo.**	• Terremotos. • Incendios. • Inundaciones.	Si un terremoto, incendio o inundación destruyera total o parcialmente uno o más cuartos de servidores, no habría manera de recuperar la información perdida.
CV-0005	**Existe muy poco personal en la Gerencia de Atención a Usuarios, de manera que no se da abasto a las demandas de los usuarios.**	• Falta de capacitación en el uso del software. • Fallos en el hardware. • Demanda de Soporte Técnico.	Problemas en el hardware por falta de mantenimiento. Errores en el software por falta de capacitación. Suspensión de la transmisión de datos por problemas en las redes de comunicaciones.

Tabla 41. Vulnerabilidades encontradas en el MINED y posibles acciones orientadas a materializar amenazas.

c. Determinación del Grado del Ejercicio de la Vulnerabilidad.

En esta sección se pretende evaluar el grado de materialización que una amenaza potencial puede tener valiéndose de una vulnerabilidad en la administración de riesgos de los servicios de TIC. Para realizar esta evaluación, es necesario tener en cuenta los siguientes factores:

i. Motivación y capacidad para materializar una amenaza.
ii. Naturaleza de la vulnerabilidad.
iii. Existencia y eficacia de los controles.

El grado de ejercicio de la vulnerabilidad mediante la materialización de una amenaza potencial puede ser catalogado como Alto, Medio o Bajo. En la siguiente tabla se describen los conceptos de dichos grados:

Grado del Ejercicio de la Vulnerabilidad	Definición
Alto	La fuente de amenaza es muy capaz y suficientemente motivada para materializarse. Los controles para evitar el ejercicio de la vulnerabilidad son ineficientes.
Medio	La fuente de amenaza está motivada y capaz pero se llevan controles que pueden obstaculizar el ejercicio de la vulnerabilidad con éxito.
Bajo	La fuente de amenaza carece de motivación y capacidad o se llevan a cabo controles que impiden y obstaculizan el ejercicio de la vulnerabilidad.

Tabla 42: Definición de los Grados del Ejercicio de la Vulnerabilidad.

Para determinar el grado de ejercicio de la vulnerabilidad que tiene una amenaza en particular, se seguirán los siguientes pasos:

Paso 1: Identificar la amenaza para la que se desea determinar el grado de ejercicio de la vulnerabilidad.

Paso 2: Completar los Formularios 6a y 6b [GEV][26] que se presentan en la siguiente página.

[26] En la Tabla 40 se resumen las motivaciones y las amenazas a las cuales están relacionadas. Se recomienda tomarlo como referencia.

MINISTERIO DE EDUCACIÓN
DIRECCIÓN DE INFORMÁTICA
GERENCIA DE NORMAS Y CALIDAD

MARMINED
"DETERMINACIÓN DEL GRADO DE EJERCICIO DE LA VULNERABILIDAD"
CÓDIGO: FOR-GNC-GEV-009
VERSIÓN: 1.0 **Página 1 de 2**

[GEV] Formulario para la Determinación del Grado del Ejercicio de la Vulnerabilidad.

Indicaciones:

- En la Parte I escriba el código de la amenaza de la cual se desea determinar el riesgo de ocurrencia.
- En la Parte II coloque un cheque (√) en la opción que más se adecúe al tipo de origen de la amenaza.
- En la Parte III marque con una (**X**) la opción que considere acertada teniendo en cuenta que las motivaciones de la 2 a la 15 corresponden al tipo de origen "Riesgos Provocados por errores y/o fallos intencionados".
- Para las secciones II, III colocar la puntuación en las casillas respectivas.
- En la Parte V coloque la suma de las puntuaciones en la casilla "Puntuación global" y seguidamente marque con un cheque (√) el grado del ejercicio de la vulnerabilidad correspondiente según la puntuación.

Parte I **Código de fuente de amenaza:**

Parte II.

Tipo de origen relacionado:

( ) [TFA-NA] Riesgos naturales.
( ) [TFA-NI] Riesgos Provocados por errores y/o fallos no intencionados.
( ) [TFA-FI] Riesgos Provocados por errores y/o fallos intencionados.
( ) [TFA-IN] Riesgos provocados por fallos de origen industrial.
( ) [TFA-RO] Riesgos organizacionales.

Puntuación de la Sección II: 1 .

Parte III

Motivación de la amenaza.

1. **( )** No se observa motivo desencadenante.
2. **( )** Ego.
3. **( )** Rebelión.
4. **( )** Desafío.
5. **( )** Destrucción de la información.
6. **( )** Revelación ilegal de información.
7. **( )** Ganancia monetaria.
8. **( )** Alteración no autorizada de datos.
9. **( )** Chantaje.
10. **( )** Destrucción.
11. **( )** Explotación.
12. **( )** Venganza.
13. **( )** Curiosidad.
14. **( )** Inteligencia.
15. **( )** Omisiones.
16. **( )** Otros, especifique:_____
_____

Puntuación de la Sección III:_____.

Formulario 6a: Formulario para Determinación del Grado del Ejercicio de la Vulnerabilidad.

MINISTERIO DE EDUCACIÓN
DIRECCIÓN DE INFORMÁTICA
GERENCIA DE NORMAS Y CALIDAD

MARMINED
"DETERMINACIÓN DEL GRADO DEL EJERCICIO DE LA VULNERABILIDAD"
CÓDIGO: FOR-GNC-GEV-009
VERSIÓN: 1.0 **Página 2 de 2**

[GEV] Formulario para la Determinación del Grado del Ejercicio de la Vulnerabilidad.

Parte IV

No.	Acerca de los controles.	Sí	No	Puntuación
1	¿Existen controles orientados a contrarrestar la amenaza?			
2	¿Son eficaces dichos controles?			

Parte V.

Puntuación global: _____

[] **Alto** (Puntuación global mayor o igual a 2).
[] **Medio** (Puntuación global mayor a 1 y menor a 2).
[] **Bajo** (Puntuación global igual a 1).

Formulario 6b: Formulario para Determinación del Grado del Ejercicio de la Vulnerabilidad.

Interpretación del formulario GEV.

A la sección II se le asignará un valor de 1, independientemente de la opción seleccionada. Esto es debido a que la amenaza debe corresponder a uno de los cinco tipos de origen.

Si en la sección III se ha marcado la opción "No se observa motivo desencadenante", se le asignará una puntuación de 0 (cero) a dicha sección del formulario. Si en caso contrario, hubiere 1 ó más opciones seleccionadas, se le asignará el valor de 1 a esa sección.

A la sección IV se le asignará el valor de 0.5 por cada opción marcada como "No". Si la respuesta a la primera pregunta fuera "No", entonces automáticamente se marcará la respuesta "No" para la pregunta 2, resultando una puntuación de 1 en referida sección. Si una o ambas respuestas fueran "Sí", se asignará el valor de 0.0 para cada una.

En la sección V, se sumarán las evaluaciones de las secciones II, III y IV, escribiéndose el total en el cuadro "Puntuación global", finalmente se colocará un cheque (√) en el cuadro en cuyo rango se encuentre la puntuación global resultante.

De manera que, si la nota de la evaluación total es 1.0, se dirá que esa amenaza tiene un grado de ejercicio de vulnerabilidad Bajo. Si la nota de evaluación total fuera mayor a 1.0 y menor a 2.0, se tendrá un grado de ejercicio de la vulnerabilidad Medio. Si la nota de la evaluación total fuera igual o mayor a 2.0 se tendrá un grado de ejercicio de vulnerabilidad Alto (1.0) para la amenaza evaluada.

d. Análisis de la Magnitud de Impacto.

Para la determinación del análisis de impacto, es importante tener en cuenta la criticidad[27] de cada uno de los servicios de TIC. La determinación de la cantidad de procesos críticos dependientes es una función de la Gerencia de Normas y Calidad.

En el análisis de impacto es importante considerar el concepto de seguridad de la información en la gestión de los recursos de TIC. Este concepto verifica que no se vulneren tres elementos fundamentales: integridad, disponibilidad y confidencialidad. El grado de criticidad de cada servicio se determina considerando dichos elementos. A continuación la descripción de los mismos:

Cualidad de la información	Descripción
Integridad	La integridad se refiere a la importancia que la información no sea modificada, sobre todo, la que tiene carácter confidencial o restringido. La integridad se pierde si se realizan cambios en los datos o sistemas de TIC, ya sea por actos intencionales o accidentales sin autorización expresa y documentada del responsable competente (el jefe de cada subdivisión de la Unidad de Informática). Si la pérdida o integridad de los datos no se corrige, se podría tener como resultado la inexactitud, fraude o decisiones erróneas.
Disponibilidad	Si un servicio prestado por las TIC catalogado de crítico según su impacto no se encuentra disponible, el MINED podría verse seriamente afectado en una disminución en la funcionalidad del conjunto de TIC así como de la eficacia operativa.
Confidencialidad	La confidencialidad de los datos es vulnerada cuando se divulgan sin autorización a personas no interesadas y en momentos inoportunos. El impacto de la divulgación no autorizada puede tener repercusiones graves como la pérdida de la confianza pública o acciones legales contra la institución.

Tabla 43: Cualidades de la seguridad de la información.

Para determinar el impacto de cada servicio, se seguirán los pasos que se describen a continuación:

[27] El concepto de criticidad está relacionado con la cantidad de procesos críticos dependientes de cada servicio de TIC.

Paso 1: Verificar la cantidad de procesos críticos dependientes que corresponden al servicio al que se le está haciendo el respectivo análisis de impacto. Esta cantidad se estableció en la 1ra. Fase de MARMINED en la Configuración de Servicios.

Paso 2: La Unidad de Informática del MINED ha establecido que la mayor cantidad de procesos críticos dependientes que se le puede asignar a un servicio es 233[28], de manera que por regla de tres simple se determinará el porcentaje de criticidad para cada servicio, así por ejemplo, se tiene que:

Servicio	Procesos críticos dependientes (Pcd)	Porcentaje de criticidad (% criticidad)
Administración de Redes	222	95%

Tabla 44: Ejemplo del cálculo del porcentaje de criticidad de un servicio.

Para determinar el porcentaje de criticidad que corresponde a 222 procesos críticos dependientes, se operará de la siguiente manera:

Pcd	% criticidad	X = 222*100/233
222	**X**	**X = 95.28 ≈ 95%**
233	100	**X = 95%**

Tabla 45: Determinación del porcentaje de criticidad de un servicio**.**

La magnitud de impacto se determina según el porcentaje de criticidad de la siguiente manera:

De 0% a 30.0%, el nivel del impacto se considera Bajo;

De 30.1% a 70.0%, el nivel del impacto se considera Moderado;

De 70.1% a 100.0%, el nivel del impacto se considera Alto.

Con el propósito de determinar con mayor puntualidad el análisis de impacto se recomienda registrar ordenadamente los gastos incurridos en el costo de la reparación de las TIC que presenten fallos, así como también definir el impacto que han tenido aspectos cualitativos tales como la insatisfacción de los usuarios internos y externos del resto de dependencias a las que la Unidad de Informática brinda sus servicios. Este análisis cualitativo deberá realizarse calificando cada uno de sus ítems según se describe en el cuadro siguiente:

[28] Esta cantidad total de procesos críticos dependientes está sujeto a actualizaciones que la Gerencia de Normas y Calidad realice pertinentemente en caso de un cambio considerable en los procesos de negocio relacionados con los servicios de TIC.

Magnitud del Impacto	Definición
Alto	La materialización de la amenaza puede: 1. Resultar muy costoso en la pérdida de principales recursos o activos tangibles. 2. Obstaculizar la misión de la institución. 3. Causar lesiones graves o incluso muerte en los empleados.
Medio	La materialización de la amenaza puede: 1. Ocasionar la pérdida de bienes o recursos costosos para la institución. 2. Violar, dañar o impedir el seguimiento a la misión institucional. 3. Ocasionar daños personales.
Bajo	La materialización de la amenaza puede: 1. Resultar en la pérdida de algunos materiales, bienes o recursos. 2. Afectar notablemente en los intereses, reputación y misión de la institución.

Tabla 46: Definiciones de la Magnitud del Impacto de las amenazas.

e. Análisis del Impacto del Riesgo.

El objetivo de este proceso es evaluar el nivel del impacto del riesgo para las TIC. La determinación del riesgo de una amenaza o vulnerabilidad particular puede expresarse como una función de:

- El grado del ejercicio de la vulnerabilidad mediante la materialización de una determinada fuente de amenaza.
- La magnitud del impacto en caso de una amenaza procedente de ejercer con éxito la vulnerabilidad.
- La adecuación de controles existentes o previstos para reducir o eliminar el riesgo.

Para medir el nivel del impacto del riesgo se presenta una matriz de evaluación del riesgo y una descripción de los niveles de riesgo resultantes.

i. Matriz de evaluación del impacto del riesgo.

A continuación se presenta un ejemplo de la obtención del nivel del impacto del riesgo para un grado de ejercicio de vulnerabilidad Medio, con un valor de 0.5, y con impacto alto (100), se tiene:

Nivel del impacto del riesgo = Grado de ejercicio de vulnerabilidad * Impacto

Nivel del impacto del riesgo = 0.5 * 100

Nivel del impacto del riesgo = 50

Este valor se compara con la Tabla 47 en la cual se puede ver que el nivel del impacto del riesgo es "medio" para esta amenaza específica.

La matriz de la Tabla 47 es una matriz 3x3 del grado de ejercicio de la vulnerabilidad mediante una amenaza (Alto, Medio, Bajo) y el nivel de impacto (Alto, Medio, Bajo). Esta determinación o clasificación de niveles de riesgos es subjetiva ya que:

- El grado de ejercicio de la vulnerabilidad es 1.0 cuando es Alto, 0.5 cuando es Medio y 0.1 cuando es Bajo.
- El valor asignado para cada nivel de impacto es de 100 cuando es Alto, 50 cuando es Medio y 10 cuando es Bajo.

Grado del Ejercicio de la Vulnerabilidad	**Magnitud del Impacto**		
	Bajo (10)	**Medio (50)**	**Alto (100)**
Alto (1.0)	Bajo 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Medio (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Bajo (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10

Tabla 47. Matriz de evaluación de riesgos.

En la página siguiente se presenta el Formulario 7 [NIR] para determinar el nivel del impacto del riesgo para un servicio específico:

MINISTERIO DE EDUCACIÓN
DIRECCIÓN DE INFORMÁTICA
GERENCIA DE NORMAS Y CALIDAD

MARMINED
"DETERMINACIÓN DEL NIVEL DEL IMPACTO DEL RIESGO"
CÓDIGO: FOR-GNC-NIR-009
VERSIÓN: 1.0 **Página 1 de 1**

[NIR] Formulario para determinar el Nivel del Impacto del Riesgo.

Indicaciones:

- *Parte I:* Para las secciones Ia – If escriba los elementos que se solicitan.
- *Parte II:* En la tabla que se presenta cruce los valores del grado de ejercicio de la vulnerabilidad (filas) con la magnitud de impacto (columnas) y marque con una X la celda en la que se interceptan. La casilla marcada determina el Nivel del Impacto del Riesgo para un servicio específico.

Parte Ia. **Código de Servicio de TIC:**	*Parte Ib.* **Nombre de Servicio de TIC:**
Parte Ic. **Código de Tipo de Amenaza:**	*Parte Id.* **Código Fuente de Amenaza:**
Parte Ie. **Grado del Ejercicio de la Vulnerabilidad:**	*Parte If.* **Magnitud de Impacto:**

Parte II.

Grado del Ejercicio de la Vulnerabilidad	**Magnitud del Impacto**		
	Bajo (10)	**Medio (50)**	**Alto (100)**
Alto (1.0)	Bajo	Medio	Alto
Medio (0.5)	Bajo	Medio	Medio
Bajo (0.1)	Bajo	Bajo	Bajo

Formulario 7: Formulario para determinar el Nivel del Impacto del Riesgo.

ii. Descripción de nivel de riesgo.

En la siguiente página se puede visualizar la Tabla 48 en la cual se describen los niveles del impacto del riesgo y las acciones necesarias que los altos directivos de la institución deben tomar para cada nivel de riesgo asociado a la materialización de una amenaza y su impacto mostrados en la matriz anterior.

Nivel de Impacto del Riesgo	Descripción y acciones necesarias
Alto	Si una observación o hallazgo es evaluado como un riesgo alto, existe una gran necesidad de acciones correctivas. Un sistema existente puede seguir operando, pero el plan de acción correctivo debe ser implementado lo más pronto posible.
Medio	Si una observación o hallazgo es evaluado como un riesgo moderado, acciones correctivas son necesarias y un plan o solución debe desarrollarse para incorporar estas acciones dentro de un período razonable de tiempo.
Bajo	Si una observación o hallazgo es evaluado como un riesgo bajo, la dirección junto con sus gerencias deberá decidir si implementa acciones correctivas o acepta el riesgo.

Tabla 48. Descripción y acciones necesarias para cada nivel de riesgo.

f. Recomendación de controles.

Este proceso de la evaluación de riesgos es importante porque se convierte en una aportación para la fase de mitigación de riesgos. Esta sección da como resultado los controles que serán capaces de atenuar o eliminar los riesgos de las TIC en la institución.

Con el propósito de prevenir la materialización de amenazas mediante el aprovechamiento de posibles vulnerabilidades en la administración de riesgos de TIC, se recomienda atender los criterios de seguridad generales que se muestran a continuación:

Área de Seguridad	Criterios de Seguridad
Seguridad Administrativa	• Asignación de responsabilidades. • Capacidad de respuesta a incidentes. • La revisión periódica de controles de seguridad. • Personal de limpieza. • La seguridad y la formación técnica. • Separación de funciones. • Sistema de autorización. • Sistema o plan de seguridad de aplicaciones.
Seguridad Operativa	• Control de contaminantes del aire (humo, polvo y productos químicos). • Controles para garantizar la calidad del suministro eléctrico. • Eliminación de acceso a medios. • Etiquetado de datos externos. • Control de humedad. • Control de la temperatura. • Control del inventario de equipos portátiles y ordenadores personales.
Seguridad Técnica	• Comunicaciones (marcación telefónica, interconexión de sistemas, enrutadores). • Control de acceso discrecional. • Identificación y autenticación. • Detección de intrusos. • Reutilización de objetos. • Sistema de auditoría informática.

Tabla 49. Criterios de seguridad a revisar para evitar amenazas en posibles focos de vulnerabilidad.

Para la atender los criterios de seguridad descritos en el cuadro anterior se seguirán los siguientes pasos, según sus categorías:

i. Seguridad Administrativa:

❖ *Asignación de responsabilidades:*

1) La Gerencia de Normas y Calidad deberá asignar un empleado responsable a cada servicio de TIC. Para el caso del hardware, el responsable serán

dos: el empleado al que se le ha asignado el equipo en cuestión y la Gerencia de Atención a Usuarios, quien es la encargada de velar porque dicho equipo se mantenga en funcionamiento. Esta asignación se realizará en la fase de configuración de TIC.

- *Capacidad de respuesta a incidentes:*
  1) Verificar las fuentes de amenaza listadas al principio de esta sección.
  2) Verificar las acciones que materializan las amenazas.
  3) Identificar los controles que contrarresten el tipo de amenazas identificado.
  4) Implementar los controles específicos.
  5) Si no existen controles para un incidente o amenaza específica, éstos se deberán registrar en la base de datos, por medio del Formulario de Recomendación de Controles [FRC], que se muestra en la Tabla 57.

- *La revisión periódica de controles de seguridad.*
  1) Verificar el comportamiento del sistema de marcación biométrico al hacerle pasar una tarjeta adulterada.
  2) Verificar el comportamiento de los usuarios al proporcionarles una nueva contraseña de acceso a los sistemas. (Con el propósito de ver si la comparten con sus compañeros.)
  3) Verificar si los usuarios tienen acceso única y exclusivamente a la información de las bases de datos que les competen para la ejecución de sus obligaciones.

- *El personal de limpieza.*
  1) Instalar cámaras de seguridad a través de las cuales se monitoree el posible contacto que tenga el personal de limpieza con el hardware.
  2) No dejar en lugares visibles la contraseña de acceso a los diferentes sistemas de información, de manera que no pueda ser hurtada por el personal de limpieza.
  3) Turnarse los usuarios de los sistemas la permanencia en el lugar al momento de realizarse la limpieza, con el propósito de vigilar que el

personal de limpieza no tenga contacto físico con el hardware que compone las TIC.

- *La seguridad y la formación técnica.*
  1) Capacitar constantemente a los usuarios de las TIC sobre las características, potencialidades, ventajas, alcances y limitaciones de las TIC que utiliza en sus operaciones.

- *Separación de funciones.*
  1) En la caracterización de las TIC se definirán los responsables de las TIC. Esto es importante porque se establece la competencia de atención a cada una de las TIC para cada Gerencia de la Unidad de Informática, de manera que no se tengan dudas respecto de los servicios de TIC que están bajo su administración.

- *Sistema de autorización.*
  1) Verificar las funciones atribuidas a cada uno de los usuarios respecto de las TIC para determinar el hardware que necesita para realizar sus tareas.
  2) Verificar las funciones atribuidas a cada uno de los usuarios respecto de las TIC para determinar los permisos que debe tener en cada uno de los sistemas de información a los que tiene acceso.

- *Sistema o plan de seguridad de aplicaciones.*
  1) En base a la Evaluación Anual del Análisis de Impacto, determinar los sistemas de información con mayor cantidad de procesos dependientes.
  2) Adquirir un sistema de seguridad de aplicaciones que detecte invasiones maliciosas a los sistemas de información para cada uno de los sistemas de información seleccionados en el paso anterior.
  3) Implementar los sistemas de seguridad de aplicaciones a los sistemas de información seleccionados según la capacidad financiera de la institución lo permita.
  4) Capacitar al personal encargado de la administración de dichos sistemas de información, así como de los sistemas de seguridad instalados.

ii. Seguridad Operativa:

- *Control de contaminantes del aire (humo, polvo y productos químicos).*
    1) Es preventivo tener un ambiente agradable para la funcionalidad de los diferentes procesos de negocio del MINED.
    2) Contar con los mecanismos adecuados de dispersión de los contaminantes del aire con el hecho de no detener la productividad del MINED.
    3) Verificar las fuentes de los contaminantes del aire para poder hacer una decisión acertada que beneficie las operaciones y disminuya la contaminación.

- *Controles para garantizar la calidad del suministro eléctrico.*
    1) Suspender la alimentación de corriente eléctrica en horarios laborales con el propósito de verificar el rendimiento de los UPS al mantener a los servidores en funcionamiento. Se medirá el tiempo que el equipo se mantenga encendido. Para esta clase de pruebas se notificará previamente a todos los usuarios de los sistemas de información al menos tres veces antes de la hora de prueba programada.
    2) Corroborar periódicamente el funcionamiento de la planta generadora de corriente eléctrica mediante períodos de prueba que permitan verificar su funcionamiento.
    3) Verificar si los UPS a los que están conectados el hardware que utilizan los empleados cumple eficazmente su función de regular el voltaje, así como de proporcionar el tiempo suficiente para que el usuario pueda apagar correctamente el equipo informático.

- *Eliminación de acceso a medios.*
    1) Cada jefatura de un departamento o sub-departamento deberá establecer un lugar dentro de cada oficina[29] para depositar los medios magnéticos de almacenamiento tales como discos, almacenamiento en red, disquetes, CD-ROM, Dispositivos USB y DVD´s.

[29] El término *Oficina se usa* para denotar a un espacio físico separado por divisiones en las que uno o varios empleados realizan sus funciones de manera coordinada pero cada uno con un equipo informático independiente.

2) Almacenar todos los medios de almacenamiento magnéticos en el lugar previamente definido para cada una de las oficinas.

- *Etiquetado de datos externos.*
  1) Etiquetar cada uno de los medios de almacenamiento con un nombre que defina su contenido, autor y fecha de creación/modificación.

- *Control de humedad y temperatura:*
  1) Adquirir e instalar sensores de humedad integrados con sistemas de ventilación y aire acondicionado en cada uno de los cuartos de servidores.
  2) Adquirir e instalar sistemas de aire acondicionado que mantengan la temperatura de las oficinas a 24ºC.

- *Control del inventario de equipos portátiles y ordenadores personales.*
  1) Llevar un registro, verificación de existencia y funcionamiento del equipo informático de escritorio así como también de los equipos portátiles, según la competencia de la Gerencia de Atención a Usuarios.

iii. Seguridad Técnica:

- *Comunicaciones (marcación telefónica, interconexión de sistemas, enrutadores).*
  1) Llevar el registro de la utilización de las marcaciones telefónicas, el conocimiento y funcionamiento de la interconexión de sistemas y de los enrutadores que sirven en el proceso comunicativo.
  2) Protección de los canales de comunicación a través de medios como firewall, tipologías de comunicación, paquetes de encriptación y antivirus.

- *Control de acceso discrecional.*
  1) Se debe registrar quien es el que utiliza las tecnologías a fin que su acceso sea discrecional.
  2) A través de un dispositivo de seguridad tratar de comprobar el acceso para evitar malas praxis.
  3) Verificación a través de diferentes medios del acceso para que las vulnerabilidades no se conviertan en objetos de explotación.

- *Identificación y autenticación.*
    1) Dependiendo la función que se necesite realizar el poder identificarse y autenticarse depende de los privilegios que se le han otorgados.
    2) Se controlará la identificación y autentificación con el fin de proteger la información crítica y sensible para el MINED.

- *Reutilización de objetos.*
    1) Definir un lugar para el desecho de los soportes de información electrónicos y degradables como el papel.
    2) Controlar si algún objeto será reutilizado para no perder información que pueda contener el objeto o que sea empleado para realizar un ataque contra la información esencial y los procesos de negocios.

- *Sistema de auditoría informática.*
    1) Capacitar al personal de la Gerencia de Normas y Calidad en materia de auditoría informática.
    2) Delimitar las unidades organizativas a auditar.
    3) Delimitar los límites, alcances y objetivos de la auditoría.
    4) Realizar una auditoría informática interna considerando todos los elementos que intervienen en un sistema de información.
    5) Análisis del Informe Final.
    6) Determinar acciones a tomar en base a las debilidades o problemas detectados en la auditoría interna.

El objetivo que se busca es el de reducir el nivel de riesgo de las TIC a niveles aceptables a través de los controles. Los factores a ser considerados en la recomendación de controles para minimizar o eliminar los riesgos identificados son las siguientes:

i. La efectividad de las opciones recomendadas.
ii. Las legislaciones y reglamentación.
iii. Políticas institucionales.
iv. Impacto operacional.
v. Seguridad y confiabilidad.

Aunque se manejen estos factores para hacer la recomendación de controles, éstos serán evaluados en la fase siguiente para poder así determinar cuáles controles recomendados son los más adecuados y con menos costos para la institución.

En síntesis, lo que se obtiene de la recomendación de controles es un listado de controles que pueden disminuir o eliminar los riesgos identificados a lo largo de la fase de evaluación de riesgos generando soluciones alternativas para la mitigación de riesgos. A continuación se muestra el Formulario 8 [RCO] de recomendación de controles, el cual se utilizará en caso que la vulnerabilidad no se mitigue con alguno de los controles listados anteriormente.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"RECOMENDACIÓN DE CONTROLES"** **CÓDIGO: FOR-GNC-RCO-009** **VERSIÓN: 1.0** **Página 1 de 1**	
[RCO] Formulario de Recomendación de Controles.	
Código fuente de amenaza:	
Tipo de origen:	**Fuente de amenaza:**
Código de Vulnerabilidad:	
Vulnerabilidad:_____ _____	
Nivel de riesgo:	
Magnitud de Impacto:	
Controles Recomendados: _____ _____	

Formulario 8: Formulario de Recomendación de Controles.

g. Documentación.

Una vez finalizada la evaluación del riesgo, los resultados se deberán documentar en un registro oficial correspondiente al período de evaluación en curso.

El informe de la evaluación de riesgos[30] es un documento donde se exponen los resultados obtenidos, los cuales son de mucha ayuda a las máximas autoridades del Ministerio de Educación en la adopción de políticas, procedimientos y presupuesto que fortalezcan y respalden la administración de riesgos en materia de TIC. Los resultados de esta documentación se expondrán en un documento de forma sistemática y analítica. El propósito central de este documento es hacer del conocimiento de las autoridades del MINED los riesgos que amenazan constantemente el desarrollo normal de las operaciones basadas en los servicios de TIC, y de esta manera asignar los recursos para reducir y corregir las posibles pérdidas.

3. FASE 3: "Mitigación de Riesgos".

A partir de la información que se produzca en la fase anterior, la mitigación de riesgos comprende el proceso de priorizar, evaluar y aplicar los controles apropiados para mitigar los riesgos.

La mitigación asume que en muchas circunstancias no es posible, ni factible controlar totalmente el riesgo existente; es decir, que en muchos casos es muy difícil impedir o evitar totalmente los daños y sus consecuencias, y más bien se pretende reducirlos a niveles aceptables y viables para las instituciones. Los altos mandos deben de estar conscientes de que la mitigación debe ser con el menor costo y con la aplicación de los controles apropiados para disminuir los riesgos a niveles aceptables de manera que tengan un impacto negativo mínimo en los recursos del MINED.

Esta fase que toma como insumo lo que se procese en la evaluación de los riesgos, conlleva una participación imprescindible de parte de la Unidad Informática porque es en esta fase donde se toman decisiones acerca de los que se debe hacer para solucionar el riesgo de sufrir una amenaza, valiéndose de las vulnerabilidades existentes, pudiendo afectar negativamente a los servicios de las TIC.

[30] En el Anexo 6 se presenta un formato para el Informe de Evaluación de Riesgos.

Para realizar el proceso de mitigación de riesgos se deberán seguir los pasos que se ilustran en la siguiente figura, para lograr el objetivo de disminuir los riesgos.

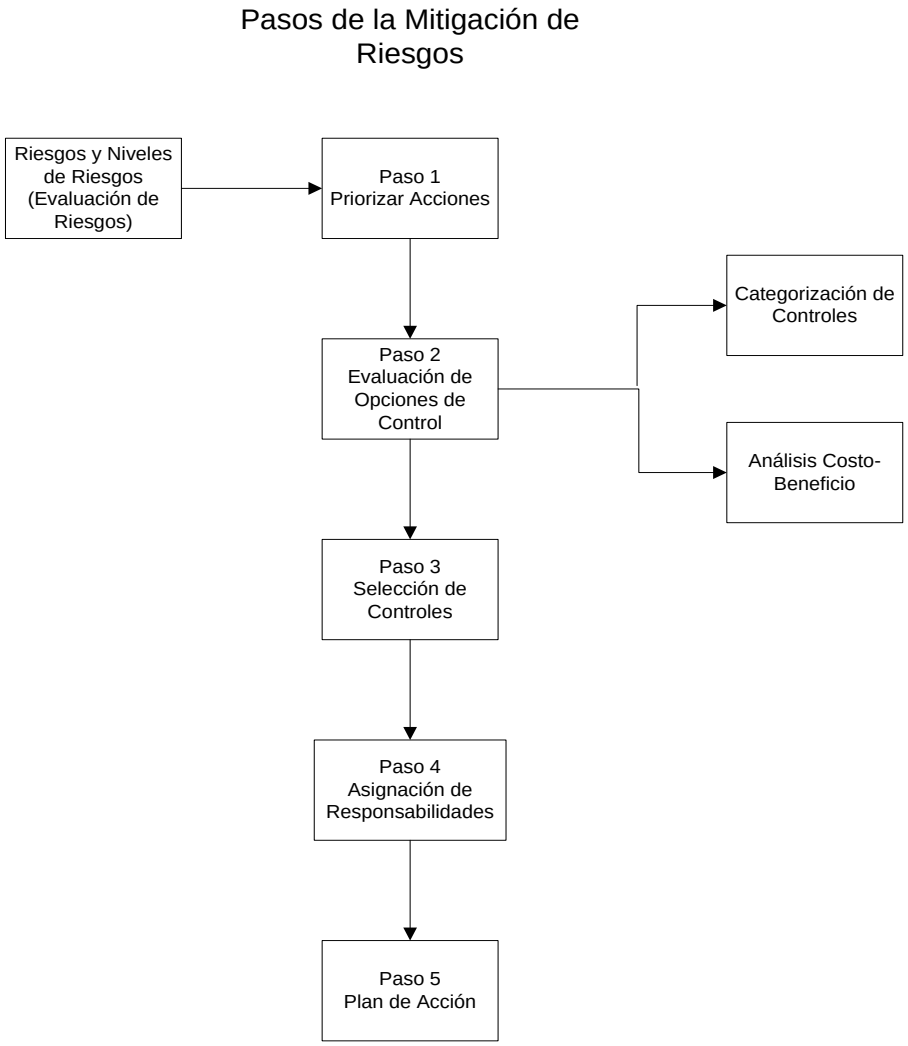


Figura 5. Pasos que componen la Fase de la Mitigación de Riesgos.

a. Priorizar Acciones

Los datos que se obtengan en la evaluación de riesgos servirán de insumo para escoger las acciones que se aplicarán prioritariamente, y todo esto dependerá en sobremanera de la clasificación de los riesgos que se haya generado en el reporte de la fase anterior donde los niveles de riesgo catalogados como *Altos* serán los que requerirán medidas de acción inmediatas para proteger los intereses del MINED de vulnerabilidades y amenazas.

Para priorizar las acciones de mitigación de riesgos de TIC se deberá efectuar el proceso siguiente:

Paso 1: Revisar el reporte de la evaluación de riesgos.

Paso 2: Del reporte de evaluación de riesgo tomar la información del servicio al que se le hará la mitigación de riesgos.

Paso 3: Verificar el nivel de riesgo del servicio y los controles recomendados en el reporte de la evaluación de riesgos.

Paso 4: Con la información recolectada llenar el Formulario 9 [PAC] Priorizar Acciones que se muestra a continuación.

Paso 5: Separar los formularios de los servicios de las TIC de acuerdo a el nivel de riesgo para poder listarlos.

Paso 6: Ordenar los servicios de las TIC de acuerdo al nivel de riesgo para poder realizar alguna acción de mitigación a estos servicios.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"PRIORIZACIÓN DE ACCIONES"** **CÓDIGO: FOR-GNC-PAC-009** **VERSIÓN: 1.0** **Página 1 de 1**	
[PAC] Formulario Priorizar Acciones	
Indicaciones: • En la Parte I complete los espacios en blanco con la información solicitada.	
Parte I	
Código de servicio de TIC: _____	**Nombre de servicio de TIC:** _____
Nivel de Impacto del Riesgo: _____	
Controles Recomendados: _____ _____ _____ _____ _____ _____	

Formulario 9: Formulario Priorizar Acciones.

b. Evaluar Opciones de Control.

Conociendo de antemano los controles que se han recomendado en la fase de evaluación de riesgos y que se retoman en esta fase, es necesario verificar si dichas recomendaciones son las más acertadas para el MINED en lo que respecta a tiempo de implementación, capacidad adquisitiva y otros criterios que el Gerente de Normas y Calidad considere pertinentes de evaluar; todo esto está enfocado en escoger el control idóneo que cumpla con la tarea de disminuir los riesgos de TIC en el MINED. La evaluación de los controles al final genera una lista de posibles controles aplicables al MINED para mitigar sus riesgos.

La evaluación de los controles a su vez tiene una serie de pasos que se exponen a continuación:

i. Categorización de los controles.

Con la información de la evaluación de riesgos que contiene los controles recomendados orientados a la seguridad de las TIC. Estos controles se subdividen en:

- *Controles de seguridad técnica.*

  Son usados para protegerse de determinados tipos de amenazas. Van desde los más sencillos hasta los más complejos y todo con el fin de proteger los datos críticos y sensibles, la información y las TIC. Sus categorías principales son:

  - De prevención.

    Se centran en la prevención de violaciones de seguridad.
  - De detección y recuperación.

    Se centran en la detección y recuperación de alguna violación de la seguridad.

- *Controles de seguridad administrativa.*

  Son aplicados para reducir el riesgo de pérdida y asegurar el cumplimiento de los objetivos de la institución; serán llevados a cabo a través de procedimientos operacionales que cumplan las metas y objetivos del MINED. Sus categorías principales son:

  - Detección.

Los controles de detección en la administración son aquellos como la aplicación de seguridad personal, la realización de verificaciones periódicas a la seguridad técnica, efectuar auditorias periódicas de los sistemas.

- Recuperación.

  Son controles que dan su apoyo para la continuidad de las operaciones durante emergencias y desastres, también se establece el nivel de respuesta a los incidentes.

❖ *Controles de seguridad Operativa.*

Se utilizan para corregir las deficiencias operacionales que podrían ser ejercidas por fuentes potenciales de amenaza y para garantizar la coherencia y uniformidad en la seguridad de operaciones. Sus categorías principales son:

- Prevención

  Son estos controles los que se refieren a lo que le puede pasar a los activos de un servicio, en todas sus fuentes presentables.

- Detección

  Se refiere a controles de seguridad física y del medio ambiente.

ii. Análisis Costo-Beneficio.

Este análisis se hace para corroborar de manera cuantitativa que los costos de la aplicación de los controles no sobrepase los valores de los servicios y se toman en cuenta tanto los costos de aplicar dichos controles como los costos de no aplicarlos, así se determinará la viabilidad económica de lo que se desea proteger en el MINED.

El Gerente de Normas de Calidad deberá realizar una estimación de los costos de implementación del control, incluyendo los costos de capacitación y seguimiento del control (o controles) a implementar. Si se estimara conveniente la aplicación de más de un control, entonces los costos deberán sumarse para representar un costo total.

A continuación se describen los pasos a seguir:

Paso 1: Determinar el costo de la aplicación de un nuevo control o mejorar el control existente.

Paso 2: Determinar el costo de la no aplicación de un nuevo control, es decir, asumir los gastos que se originen de la continuación de la falla en los servicios de TIC.

Paso 3: Estimar el valor de los servicios[31] de TIC que se pretende proteger de posibles amenazas.

Ejemplo de análisis Costo - Beneficio de un control.

- Costo del impacto de la aplicación de un nuevo control o mejora de dicho control……..……...$ 0.00
- Costos de la aplicación del control (personal, capacitaciones, presentación de informes)…….……...……$ 0.00
- Mantenimiento de la aplicación……..…….$ 0.00

Costo total……..…..$ 0.00

Beneficio es el valor cuantitativo del servicio (Costo de todo el servicio).

Beneficio……$ 0.00

iii. Evaluación de Controles.

El Formulario 10 [ECO] que se muestra en la siguiente página describe los pasos a realizar para la evaluación de los controles.

Paso 1: Revisar del Formulario 9 [PAC] donde se muestran los controles recomendados y se escoge uno de ellos (el costo de no hacer nada se podría evaluar como un posible control).

Paso 2: Realizar la caracterización de controles. Esta parte se efectuará mediante el llenado de las secciones Ia y Ib del Formulario 10 [ECO].

Paso 3: Calcular la razón beneficio/costo, para la aplicación del control que se está evaluando.

Paso 4: Colocar el resultado de la operación en la parte II en el espacio de resultado. Si el resultado es mayor que 1 se marcará que es factible este control, caso contrario se tomará como no factible.

[31] Los servicios incluyen al hardware y software relacionados a ese servicio.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"EVALUACIÓN DE CONTROLES"**	
CÓDIGO: FOR-GNC-ECO-009	
VERSIÓN: 1.0	**Página 1 de 1**
[ECO] Formulario de Evaluación de Controles	
Indicaciones: • En la Parte Ia y Ib coloque un cheque (√) en la opción que más se adecúe al control. • En la Parte II complete los espacios en blanco con la información solicitada.	
Control Recomendado:	
Parte Ia	
Seguridad Técnica ( )	**Seguridad Administrativa ( )**
Seguridad Operativa ( )	
Parte Ib	
Apoyo ( )	**Prevención ( )**
Detección ( )	**Recuperación ( )**
Parte II	
Costos: _____ _____	
Beneficios: _____ _____	
Análisis Costo-Beneficio. Total de Beneficio:_____	Total de Costos:_____
Resultado:	**Factible ( )** **No Factible ( )**

Formulario 10: Formulario de Evaluación de Controles.

c. Selección de Controles.

Para realizar este paso se hará uso de los resultados de los dos pasos anteriores. El objetivo es seleccionar los controles más adecuados que permitan mantener activos los servicios soportados por las TIC. La Unidad Informática del MINED es la encargada de hacer la selección de los controles.

Los controles seleccionados deben tener implícitamente técnicas, operaciones y elementos de administración de los mismos con la finalidad de que se logre disminuir los riesgos en el MINED.

Se concluye este paso con el listado de los controles seleccionados.

d. Asignar Responsabilidades.

Cuando se ha logrado determinar los controles adecuados y viables para evitar la materialización de amenazas que perjudiquen el correcto funcionamiento de los servicios de TIC en el MINED, se deberá escoger quién o quiénes serán las personas o grupos de personas que estarán a cargo de gestionar estos controles. Dicha selección del personal responsable se deberá realizar basándose en las habilidades, aptitudes y capacidad de los candidatos al momento de asignarles una responsabilidad. Es importante tener en cuenta que los responsables de los controles pueden ser personas de la misma institución o personas contratadas externamente para efectuar dicha tarea.

Queda a disposición de la Unidad Informática del MINED asignar los responsables para implementar estos controles.

e. Plan de Acción.

Toda institución busca protegerse continuamente de los riesgos que pueden afectar los recursos, en este caso los activos tecnológicos con los que se cuenta, y hacerlo a través de una mitigación de los riesgos a manera que se satisfagan las necesidades de seguridad y que los costos no sean muy elevados.

El Plan de Acción es el documento estructurado que formara parte de la estrategia de MARMINED para la mitigación de riesgos, ya que a través de este instrumento se busca materializar las medidas que han resultado de todo el proceso de la administración de riesgos de TIC.

Todo Plan de Acción para cada servicio debe contener la siguiente información:

- Los riesgos y los niveles de riesgos; los primeros obtenidos de las vulnerabilidades y amenazas y los niveles del reporte generado en la fase de evaluación de riesgos.
- Los controles recomendados por la fase de evaluación de riesgos.
- La selección de controles en base a los criterios de viabilidad, eficiencia y costos de la evaluación de controles.
- Los recursos necesarios para la implementación de los controles seleccionados previamente.
- Personal responsable.
- Fecha de inicio y de finalización de la ejecución.

El Formulario 11 [PLAN] que se muestra en la siguiente página presenta los elementos indispensables para un Plan de Acción efectivo.

El código del Plan de Acción se colocará de la siguiente manera: PA-0001, donde PA- significará Plan de Acción y 0001 su número correlativo.

MINISTERIO DE EDUCACIÓN **DIRECCIÓN DE INFORMÁTICA** **GERENCIA DE NORMAS Y CALIDAD** **MARMINED** **"PLAN DE ACCIÓN"** **CÓDIGO: FOR-GNC-PLAN-009** **VERSIÓN: 1.0** **Página 1 de 1**	
[PLAN] Plan de Acción	
Código de Plan de Acción:	**Nombre del Plan de Acción:**
Código de Servicio:	**Nombre de Servicio:**
Código de Fuente de Amenaza:	**Fuente de Amenaza:**
Grado del Ejercicio de la Vulnerabilidad:	**Magnitud de impacto:**
Nivel de Impacto de Riesgo:	
Controles recomendados:	
_____ _____ _____ _____	
Controles seleccionados después de la evaluación de controles	
_____ _____ _____ _____	
Recursos necesarios para aplicar los controles.	
_____ _____ _____ _____	
Personal responsable:	
Fecha de inicio:	**Fecha de finalización:**

Formulario 11: Formulario de un Plan de Acción.

CAPÍTULO IV: DISEÑO DEL PROTOTIPO DE SOFTWARE.

A. GENERALIDADES DEL PROTOTIPO.

Para desarrollar una aplicación de software se pueden usar muchas metodologías las cuales son un marco de trabajo usado para estructurar, planificar y controlar el proceso de desarrollo en sistemas de información.

Existen en el universo informático muchas metodologías que circulan desde la década de los 60 como por ejemplo la programación estructurada, pero para nuestra aplicación la metodología a utilizar es la de la programación orientada a objetos. La orientación a objetos promete mejoras de amplio alcance en la forma de diseño, desarrollo y mantenimiento del software ofreciendo una solución a largo plazo en el desarrollo de software.

Un modelo de ciclo de vida define el estado de las fases a través de las cuales se mueve un proyecto de desarrollo de software y como complemento a la metodología se agrega lo que es el modelo de ciclo de vida de la aplicación el cual para nuestra aplicación es Modelo de Prototipado.

El Modelo de Prototipado es la creación de una implementación parcial de un sistema, para el propósito explícito de aprender sobre los requerimientos del sistema. Un prototipo es construido de una manera rápida tal como sea posible. Esto es dado a los usuarios, clientes o representantes de ellos, posibilitando que ellos experimenten con el prototipo. Se presenta el modelado en forma de un diseño rápido que se centra en una representación de aquellos aspectos del software que serán visibles para el cliente o el usuario final.las técnica de casos de usos se consideran como las más formales para representar dichos aspectos, pero para comenzar la programación, los diagramas mínimos necesarios son los diagramas de clases y los diagramas de bases de datos[32].

[32] Basado en el libro de ingeniería de software, un enfoque practico (sexta edición).

B. DISEÑO DEL PROTOTIPO DE SOFTWARE MARMINED.

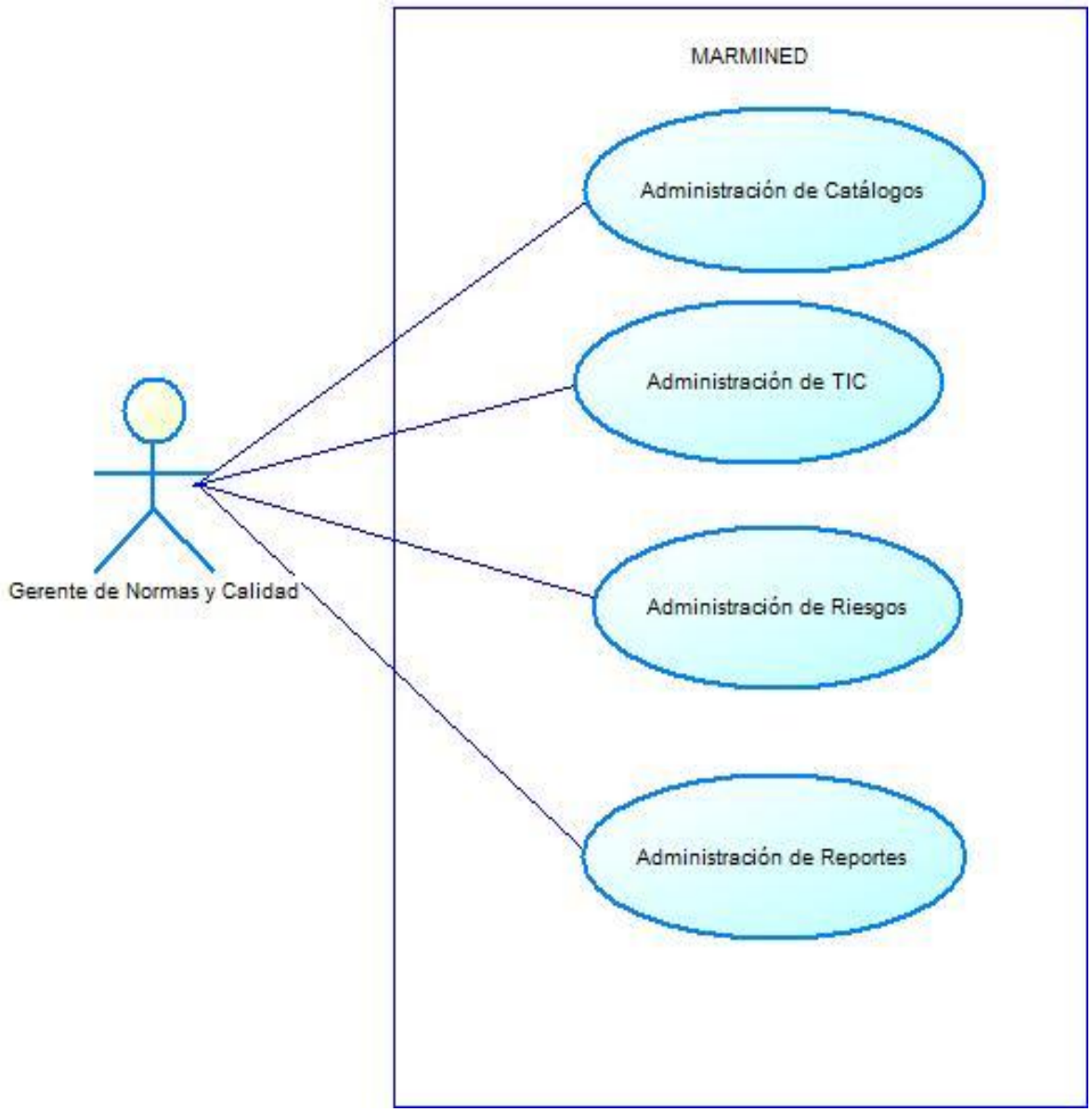


Figura 6. Diagrama de caso de uso de Sistema MARMINED.

1. Personal Involucrado.

Usuarios:

- Gerente de Normas y Calidad.

No usuarios:

- Personal de la Unidad Informática.
- Empleados.

2. Listas actor- objetivo.

Actor:

Gerente de Normas y Calidad.

Administración de Catálogos.

- Agregar información de Catálogos
- Modificar información de Catálogos
- Eliminar información de Catálogos
- Consultar información de Catálogos

Administración de TIC.

- Agregar nuevas TIC
- Modificar TIC
- Eliminar TIC
- Consultar las TIC

Administración de Riesgos.

- Gestión de fuente de amenaza.
- Gestión de motivación de amenaza.
- Gestión de acciones que materializan la fuente de amenaza
- Gestión de vulnerabilidades
- Gestión de controles

Administración de Reportes.

- Generar reportes

3. Descripción de los casos de usos.

a. Nombre: Administración de Catálogos.

Objetivo: Administrar los catálogos que son los insumos para los reportes que se soliciten en el MINED

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicitan que se gestionen los catálogos de los cuales ellos son responsables, por lo que se registran en el Sistema[33].

Precondiciones:

Los datos de los catálogos tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de los diferentes catálogos relacionados con las TIC en el MINED consiguiendo una mayor profundización.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria para los catálogos de las TIC.
2. El Gerente de Normas y Calidad selecciona cual es el tipo de catálogo.
3. El Sistema solicita los datos del catálogo a registrar (unidad organizativa, usuario o tipo de fuente de amenaza).
4. El Gerente de Normas y Calidad agrega la información del catálogo seleccionado.
5. El Sistema genera un nuevo registro del catálogo especificado por el Gerente de Normas y Calidad.
6. El Sistema solicita si desea realizar otra acción en los diferentes catálogos.

[33] En la descripción de los Casos de Uso se utiliza el término *Sistema* para referirse al Prototipo de Software.

Extensiones:

1. En cualquier momento el sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de catálogo anterior.
- El Sistema reconstruye el registro del catálogo anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b. Nombre: Administración de TIC.

Objetivo: Administrar las TIC que son utilizadas en el MINED.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Se requiere que la información de las TIC sea registrada en el sistema de manera acorde a sus características.

Precondiciones:

Las TIC deben poseer las características básicas para el funcionamiento del sistema.

Garantías de éxito (post-condiciones):

Se registrará la información de las TIC de manera que estén listas para generar informes y reportes que se soliciten.

Escenario principal de éxito:

1. El Empleado presenta la información de las características de la TIC
2. El Gerente de Normas y Calidad selecciona que TIC desea agregar.
3. El Sistema solicita los datos de la TIC seleccionada.
4. El Gerente de Normas y Calidad agrega las características de la TIC seleccionada.
5. El Sistema genera un nuevo registro de la TIC seleccionada.

Extensiones:

1. En cualquier momento el sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al estado anterior.
- El Sistema reconstruye el estado anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c. Nombre: Administración de Riesgos.

Objetivo: Administrar los riesgos de las TIC teniendo como insumos las fuentes de amenazas, motivaciones de amenazas, acciones que materializan la amenaza, vulnerabilidades de las TIC y recomendaciones de control de las TIC que son utilizadas en el MINED.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Se requiere que la información relacionada con los riesgos de las TIC sea registrada o generada en el sistema de manera acorde a los riesgos que éstas puedan estar expuestas por medio de las fuentes de amenazas y sus vulnerabilidades.

Precondiciones:

Las fuentes de amenazas, motivaciones de amenazas, acciones que materializan la amenaza, vulnerabilidades de las TIC, deben estar identificadas previamente para determinar el grado de ejercicio de una vulnerabilidad, la magnitud del impacto de amenaza y el nivel de impacto del riesgo para una TIC.

Garantías de éxito (post-condiciones):

Se registrará la información de las fuentes de amenazas, motivaciones de amenazas, acciones que materializan la amenaza, vulnerabilidades de las TIC y los controles a recomendar de manera que estén listos para generar informes y reportes que se soliciten.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información de la fuente de amenaza de la TIC
2. El Gerente de Normas y Calidad agrega la información de la fuente de amenaza de TIC al sistema.
3. El Gerente de Normas y Calidad selecciona el tipo de fuente de amenaza de la TIC.
4. El Gerente de Normas y Calidad agrega la motivación y las acciones que materializan esa amenaza de la TIC.
5. El Gerente de Normas y Calidad asocia la fuente de amenaza agregando una vulnerabilidad y el grado del ejercicio de dicha vulnerabilidad.
6. El Sistema genera el registro de la fuente de amenaza de la TIC.
7. El Sistema genera la información sobre la vulnerabilidad de la fuente de amenaza de la TIC con su respectivo grado de materialización de la fuente de amenaza.
8. El Gerente de Normas y Calidad agrega los controles de la vulnerabilidad de la fuente de amenaza de la TIC.
9. El sistema genera el registro de controles de vulnerabilidad de las fuentes de amenazas de TIC.

Extensiones:

1. En cualquier momento el sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al estado anterior.
- El Sistema reconstruye el estado anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

d. Nombre: **Administración de Reportes**.

Objetivo: Administrar los diferentes reportes relacionados con la administración de riesgos de TIC del MINED.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Se requiere que la información de la administración de riesgos de TIC sea presentada en reportes.

Precondiciones:

Los datos de los diferentes catálogos deben de existir.

La información de la administración de riesgos de TIC debe existir.

Garantías de éxito (post-condiciones):

Se presentará la información a través de los diferentes reportes de la administración de riesgos de TIC del MINED para tener una mejor decisión sobre dichos riesgos.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita un reporte de administración de riesgos de TIC.
2. El Gerente de Normas y Calidad escoge el reporte.
3. El Sistema genera el reporte seleccionado.
4. El Gerente de Normas y Calidad visualiza el reporte en pantalla.

Extensiones:

1. En cualquier momento el sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y escoge un nuevo reporte.
- El Sistema recupera el reporte anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

4. Gráficas de casos de usos.

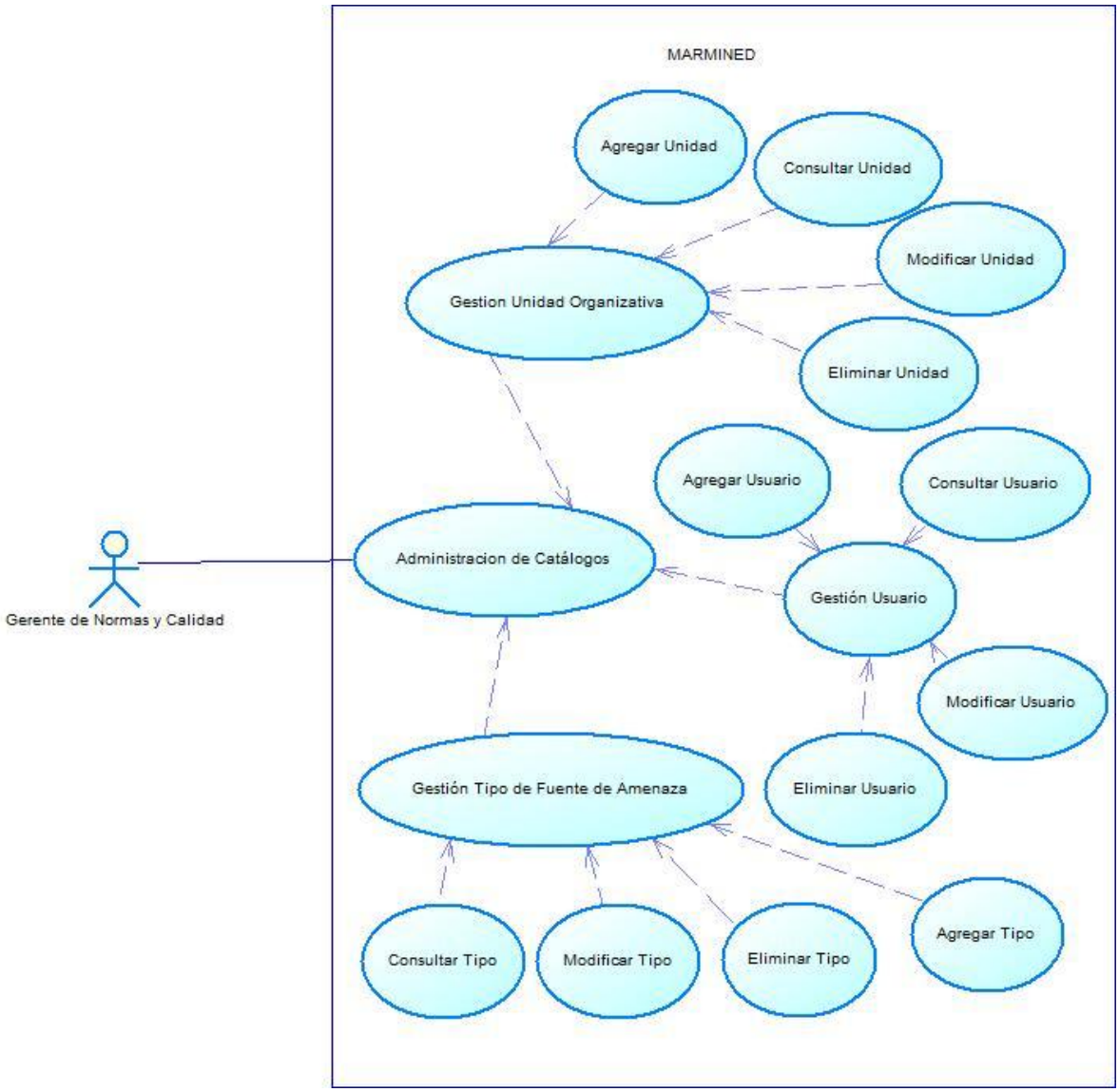


Figura 7. Caso de uso Administración de Catálogos.

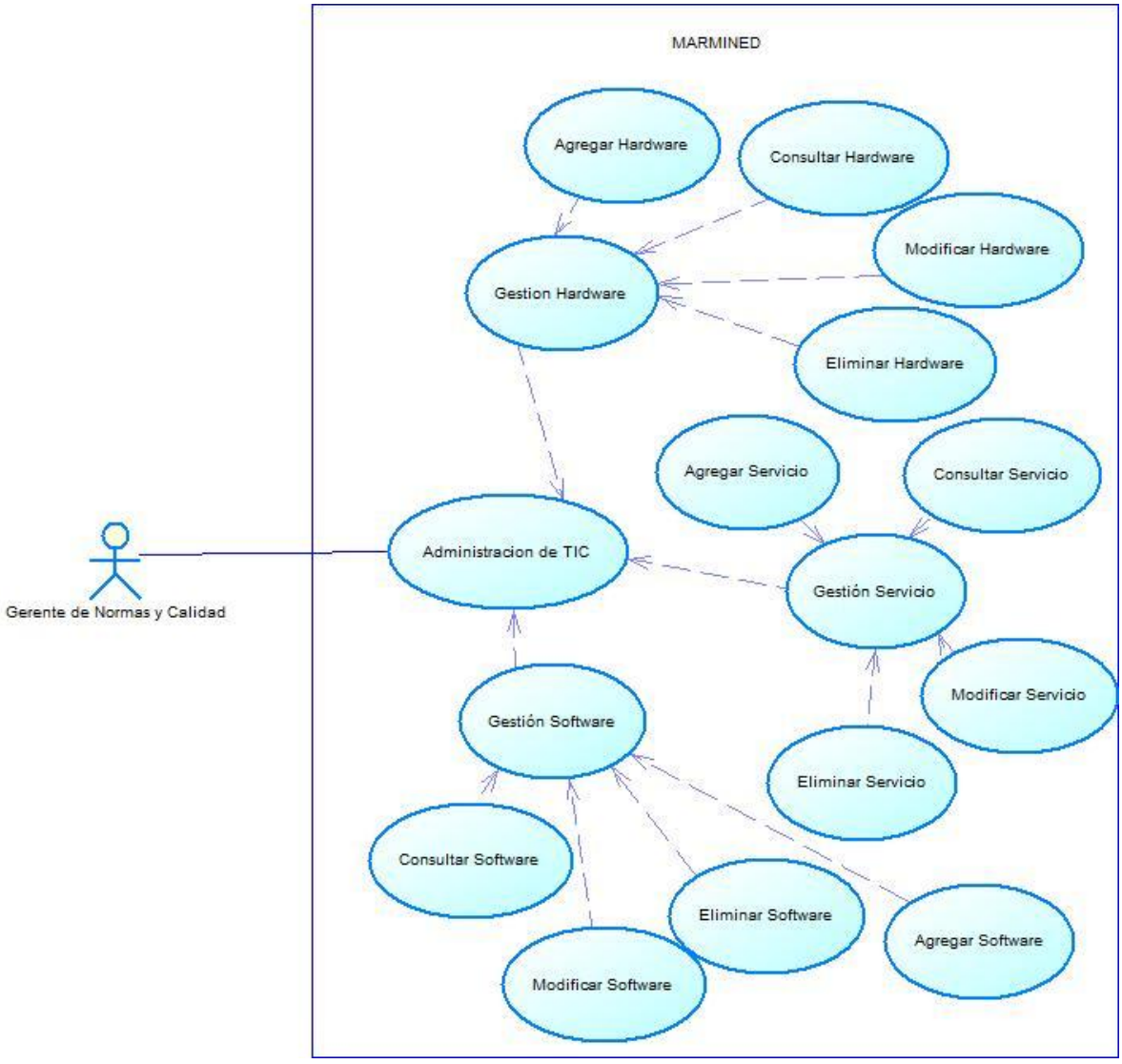


Figura 8. Caso de uso Administración de TIC

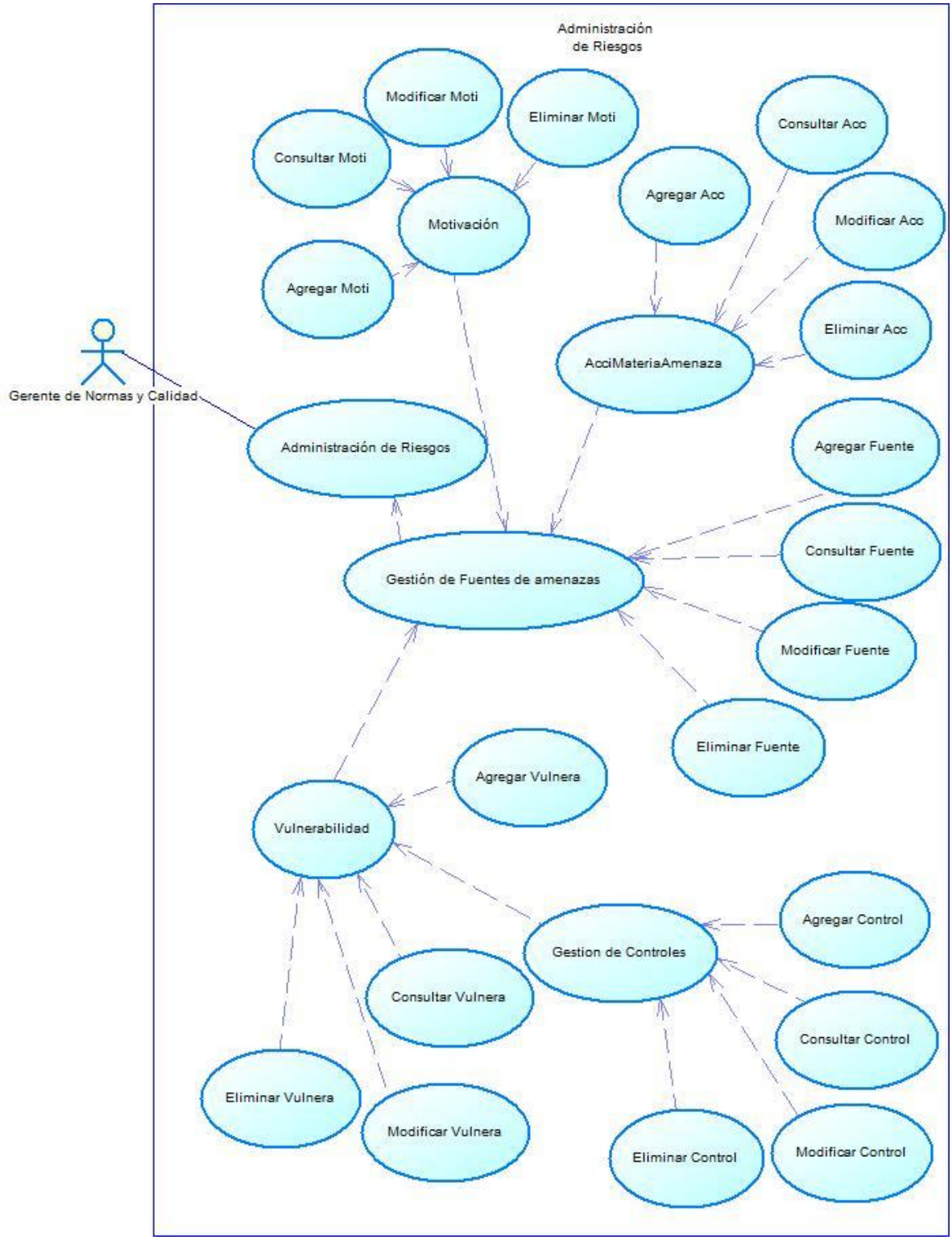


Figura 9. Caso de uso Administración de Riesgos.

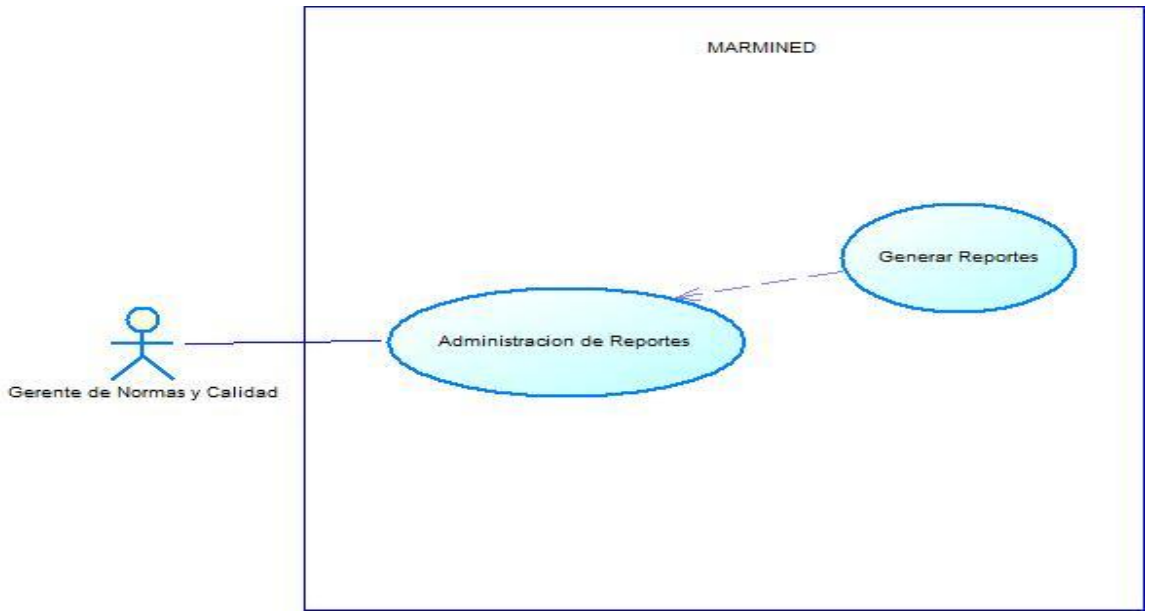


Figura 10. Caso de uso Administración de Reportes.

5. Diagramas de secuencias.

Flujo principal.

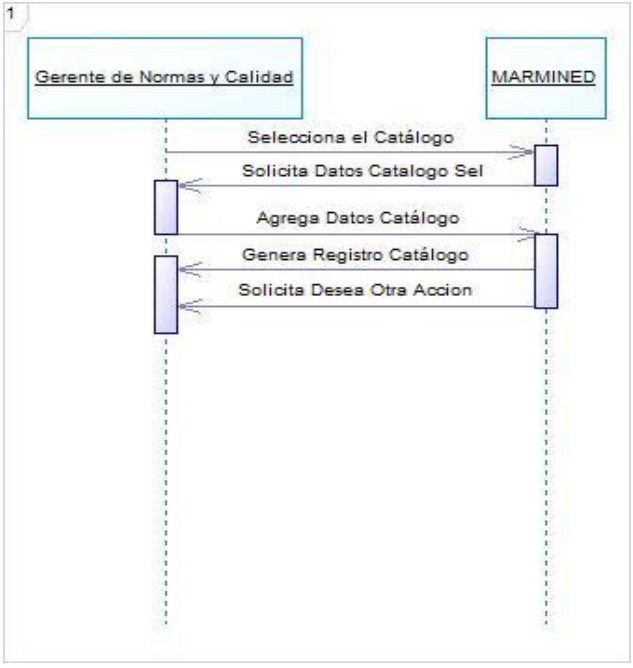


Figura 11. Diagrama de secuencia Administración de Catálogos.

Extensiones.

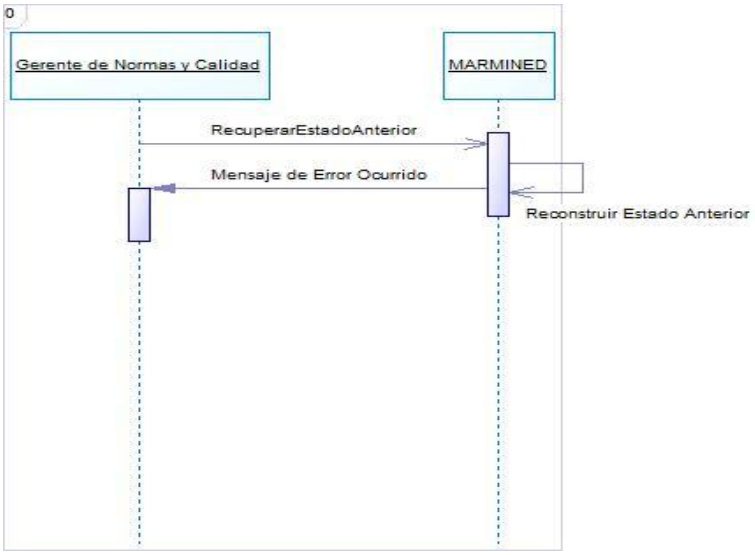


Figura 12. Diagrama de secuencia Error de Administración de Catálogos.

Flujo principal.

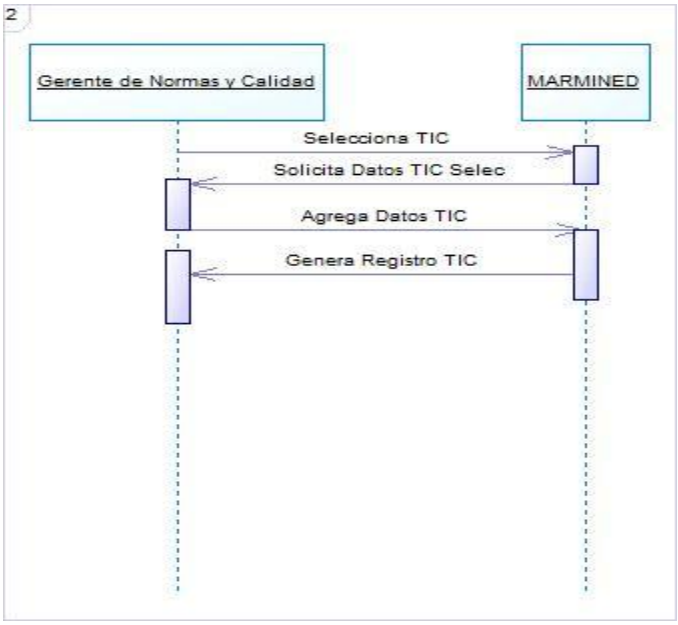


Figura 13. Diagrama de secuencia Administración de TIC.

Extensiones.

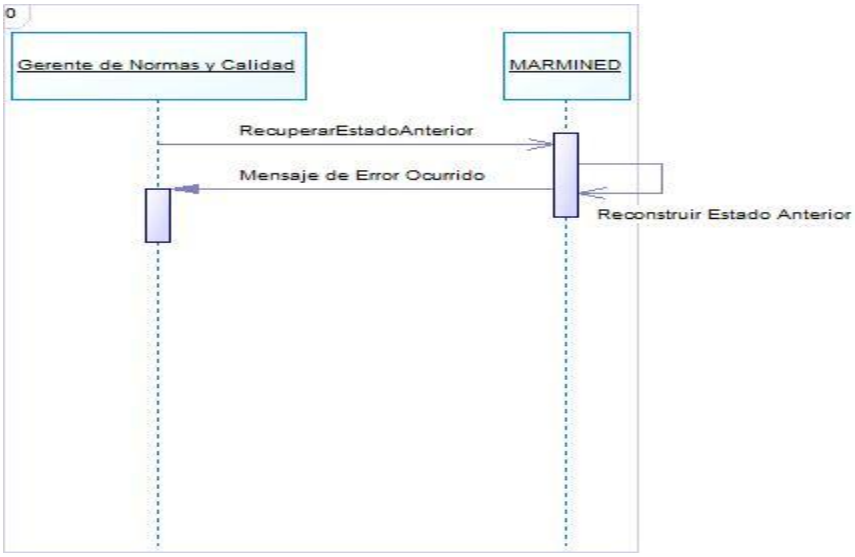


Figura 14. Diagrama de secuencia Error en Administración de TIC.

Flujo principal.

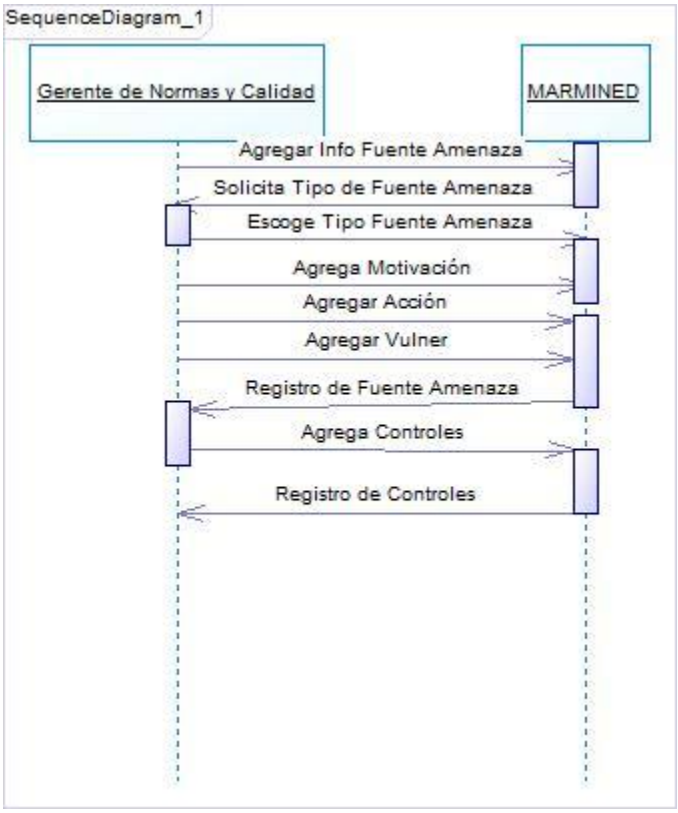


Figura 15. Diagrama de secuencia Administración de Riesgos.

Extensiones.

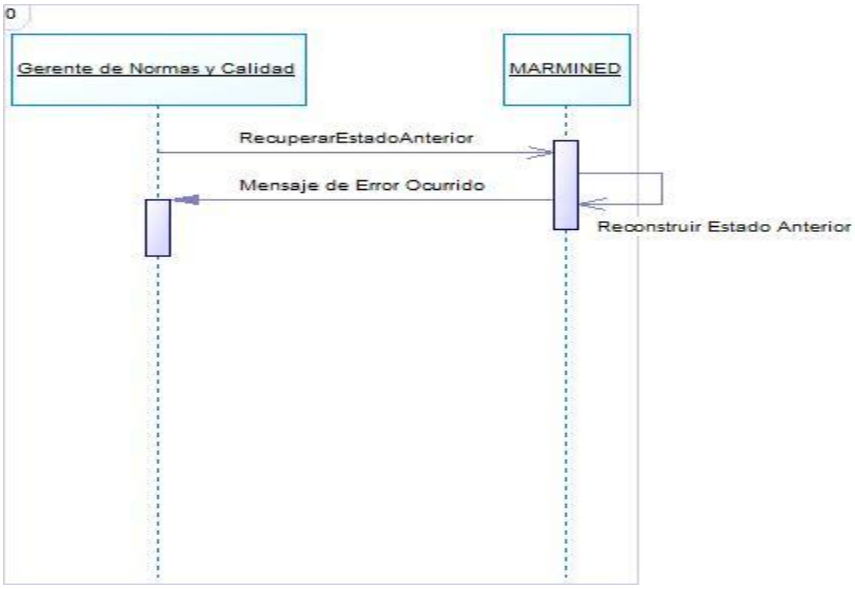


Figura 16. Diagrama de secuencia Error en Administración de Riesgos.

Flujo principal.

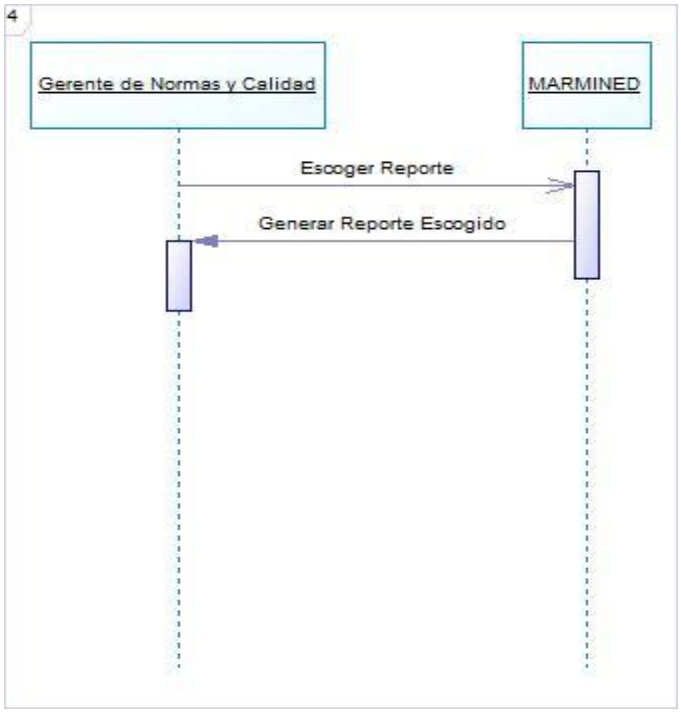


Figura 17. Diagrama de secuencia Administración de Reportes.

Extensiones.

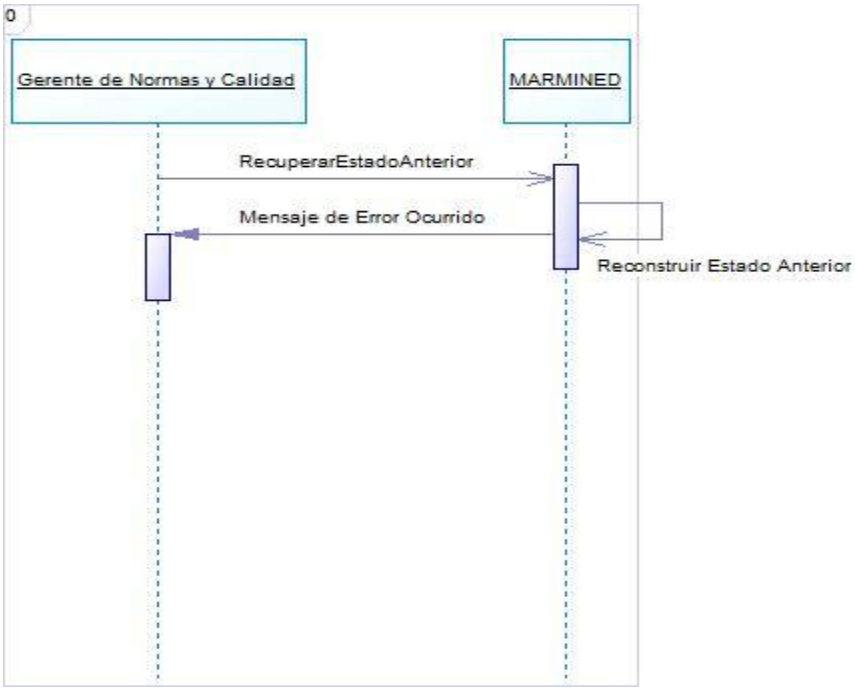


Figura 18. Diagrama de secuencia Error Administración de Reportes.

6. Casos de uso extendidos.

a.1. Nombre: Agregar Unidad Organizativa.

Objetivo: Ingresar la información de la unidad organizativa que pertenece al MINED

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Cada persona debe pertenecer a una unidad por lo que debe esta unidad organizativa estar registrada en el Sistema.

Precondiciones:

Los datos de la unidad organizativa tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de las diferentes unidades organizativas que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de la unidad organizativa del MINED.
2. El Gerente de Normas y Calidad selecciona el catálogo unidad organizativa.
3. El Sistema solicita los datos de la unidad organizativa a registrar.
4. El Gerente de Normas y Calidad agrega la información de la unidad organizativa.
5. El Sistema genera el registro de la unidad organizativa especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de unidad organizativa anterior.
- El Sistema reconstruye el registro de unidad organizativa anterior.

- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.2. Nombre: Consulta de Unidad Organizativa.

Objetivo: Consultar la información de la unidad organizativa que pertenece al MINED.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de la unidad organizativa y que se encuentre registrada en el Sistema.

Precondiciones:

Los datos de la unidad organizativa tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de las diferentes unidades organizativas que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de una Unidad Organizativa del MINED.
2. El Gerente de Normas y Calidad selecciona el catálogo unidad organizativa.
3. El Sistema muestra los datos registrados de las unidades organizativas.
4. El Gerente de Normas y Calidad verifica la información de la unidad organizativa.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de unidad organizativa anterior.
- El Sistema reconstruye el registro de unidad organizativa anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.3. Nombre: Modificar Unidad Organizativa.

Objetivo: Modificar la información de la unidad organizativa que pertenece al MINED.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de la unidad organizativa y que se encuentra registrada en el Sistema debido a un cambio en el MINED.

Precondiciones:

Los datos de la unidad organizativa tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información de las diferentes unidades organizativas que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de una unidad organizativa del MINED.
2. El Gerente de Normas y Calidad selecciona el catálogo unidad organizativa.
3. El Sistema muestra los datos registrados de las unidades organizativas.
4. El Gerente de Normas y Calidad cambia la información de la unidad organizativa seleccionada.
5. El Sistema guarda los datos modificados de las unidades organizativas.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de unidad organizativa anterior.
- El Sistema reconstruye el registro de unidad organizativa anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.4. Nombre: Eliminar Unidad Organizativa.

Objetivo: Borrar la información de la unidad organizativa que pertenece al MINED.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de la unidad organizativa que se encuentra registrada en el Sistema debido a un cambio en el MINED.

Precondiciones:

Los datos de la unidad organizativa tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información de las diferentes unidades organizativas que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información de una unidad organizativa del MINED.
2. El Gerente de Normas y Calidad selecciona el catálogo unidad organizativa.
3. El Sistema muestra los datos registrados de las unidades organizativas.
4. El Gerente de Normas y Calidad selecciona la información de la unidad organizativa a borrar.
5. El Sistema elimina los datos de las unidades organizativas.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de unidad organizativa anterior.
- El Sistema reconstruye el registro de unidad organizativa anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.5. Nombre: Agregar Usuario.

Objetivo: Ingresar la información de un usuario que manejara el Sistema.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Requiere utilizar el Sistema por lo que debe tener un registro en el Sistema.

Precondiciones:

Los datos del usuario tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información del usuario que utilizara el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de un usuario del Sistema.
2. El Gerente de Normas y Calidad selecciona el catálogo Usuario.
3. El Sistema solicita los datos del usuario a registrar.
4. El Gerente de Normas y Calidad agrega la información del usuario.
5. El Sistema genera el registro del usuario especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de usuario anterior.
- El Sistema reconstruye el registro de usuario anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.6. Nombre: Consulta de Usuario.

Objetivo: Consultar la información de un usuario del Sistema

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de un usuario registrado en el Sistema.

Precondiciones:

Los datos del usuario tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de los diferentes usuarios del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de un usuario.
2. El Gerente de Normas y Calidad selecciona el catálogo usuario.
3. El Sistema muestra los datos registrados de los usuarios.
4. El Gerente de Normas y Calidad verifica la información del usuario.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de usuario anterior.
- El Sistema reconstruye el registro de usuario anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.7. Nombre: Modificar Usuario.

Objetivo: Modificar la información de un usuario del Sistema

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información del usuario que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del usuario tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información del usuario del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de un usuario.
2. El Gerente de Normas y Calidad selecciona el catálogo usuario.
3. El Sistema muestra los datos registrados de los usuarios.
4. El Gerente de Normas y Calidad cambia la información del usuario seleccionado.
5. El Sistema guarda los datos modificados del usuario.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de usuario anterior.
- El Sistema reconstruye el registro de usuario anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.8. Nombre: Eliminar Usuario.

Objetivo: Borrar la información del usuario del Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de su usuario que se encuentra registrada en el Sistema debido a un cambio en el MINED.

Precondiciones:

Los datos del usuario tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información del usuario del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información del usuario.
2. El Gerente de Normas y Calidad selecciona el catálogo usuario.
3. El Sistema muestra los datos registrados de los usuarios.
4. El Gerente de Normas y Calidad selecciona la información del usuario a borrar.
5. El Sistema elimina los datos del usuario.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de usuario anterior.
- El Sistema reconstruye el registro de usuario anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.9. Nombre: Agregar Tipo de Fuente de Amenaza.

Objetivo: Ingresar la información de un tipo de fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: requiere agregar en el Sistema un tipo de fuente de amenaza.

Precondiciones:

Los datos de tipo de fuente de amenazas tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de los tipos de fuentes de amenazas que utilizará el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de un tipo de fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el catálogo Tipo de fuente de amenaza.
3. El Sistema solicita los datos del tipo de fuente de amenaza a registrar.
4. El Gerente de Normas y Calidad agrega la información del tipo de fuente de amenazas.
5. El Sistema genera el registro del tipo de fuente de amenaza especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de tipo de fuente de amenaza anterior.
- El Sistema reconstruye el registro de tipo de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.10. Nombre: Consulta de Tipo de Fuente de Amenazas.

Objetivo: Consultar la información de un tipo de fuente de amenazas en el Sistema

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de un tipo de fuente de amenaza registrado en el Sistema.

Precondiciones:

Los datos del tipo de fuente de amenaza tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de los diferentes tipos de fuentes de amenazas del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de un tipo de fuente de amenazas.
2. El Gerente de Normas y Calidad selecciona el catálogo tipo de fuente de amenaza.
3. El Sistema muestra los datos registrados de los tipos de fuentes de amenazas.
4. El Gerente de Normas y Calidad verifica la información del tipo de fuente de amenaza.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de tipo de fuente de amenaza anterior.
- El Sistema reconstruye el registro de tipo de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.11. Nombre: Modificar Tipo de Fuente de Amenaza.

Objetivo: Modificar la información de un tipo de fuente de amenaza del Sistema

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de un tipo de fuente de amenaza que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del tipo de fuente de amenaza tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información del tipo de fuente de amenaza en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de un tipo de fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el catálogo tipo de fuente de amenaza.
3. El Sistema muestra los datos registrados de los tipos de fuentes de amenazas.
4. El Gerente de Normas y Calidad cambia la información del tipo de fuente de amenaza seleccionado.
5. El Sistema guarda los datos modificados del tipo de fuente de amenaza.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de tipo de fuente de amenaza anterior.
- El Sistema reconstruye el registro de tipo de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

a.12. Nombre: Eliminar Tipo de Fuente de Amenaza.

Objetivo: Borrar la información del tipo de fuente de amenaza del Sistema

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de un tipo de fuente de amenaza que se encuentra registrada en el Sistema debido a un cambio en los tipos de fuentes en el MINED.

Precondiciones:

Los datos del tipo de fuente de amenaza tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información del tipo de fuente de amenaza del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información del tipo de fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el catálogo tipo de fuente de amenaza.
3. El Sistema muestra los datos registrados de los tipos de fuentes de amenazas.
4. El Gerente de Normas y Calidad selecciona la información del tipo de fuente de amenaza a borrar.
5. El Sistema elimina los datos del tipo de fuente de amenaza.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de tipo de fuente de amenaza anterior.
- El Sistema reconstruye el registro de tipo de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.1. Nombre: Agregar Servicios de TIC.

Objetivo: Ingresar la información de los servicios de TIC del MINED.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita ingresar un servicio para que sea registrado en el Sistema.

Precondiciones:

Los datos del servicio tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de los servicios de TIC que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria del servicio de TIC del MINED.
2. El Gerente de Normas y Calidad selecciona en el menú servicio de TIC.
3. El Sistema solicita los datos del servicio de TIC a registrar.
4. El Gerente de Normas y Calidad agrega la información del servicio de TIC.
5. El Sistema genera el registro del servicio de TIC especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro del servicio de TIC anterior.
- El Sistema reconstruye el registro del servicio de TIC anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.2. Nombre: Consulta de Servicio de TIC

Objetivo: Consultar la información del servicio de TIC del MINED.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia del servicio de TIC y que se encuentre registrada en el Sistema.

Precondiciones:

Los datos del servicio de TIC tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de los diferentes servicios de TIC que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información de un servicio de TIC del MINED.
2. El Gerente de Normas y Calidad selecciona en el menú servicio de TIC.
3. El Sistema muestra los datos registrados de los servicios de TIC.
4. El Gerente de Normas y Calidad verifica la información del servicio de TIC.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro del servicio de TIC anterior.
- El Sistema reconstruye el registro del servicio de TIC anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.3. Nombre: Modificar Servicio de TIC.

Objetivo: Modificar la información del servicio de TIC del MINED.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información del servicio de TIC y que se encuentra registrado en el Sistema debido a un cambio en el MINED.

Precondiciones:

Los datos del servicio de TIC tienen que estar registrados en el sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información de los servicios de TIC que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información del servicio de TIC del MINED.
2. El Gerente de Normas y Calidad selecciona el menú servicio de TIC.
3. El Sistema muestra los datos registrados del servicio de TIC.
4. El Gerente de Normas y Calidad cambia la información del servicio de TIC seleccionado.
5. El Sistema guarda los datos modificados del servicio de TIC.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro del servicio de TIC anterior.
- El Sistema reconstruye el registro del servicio de TIC anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.4. Nombre: Eliminar Servicio de TIC.

Objetivo: Borrar la información del servicio de TIC del MINED

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información del servicio de TIC que se encuentra registrada en el Sistema debido a un cambio en el MINED.

Precondiciones:

Los datos del servicio de TIC tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información de los servicios de TIC que pertenecen al MINED.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información del servicio de TIC del MINED.
2. El Gerente de Normas y Calidad selecciona el menú servicio de TIC.
3. El Sistema muestra los datos registrados del servicio de TIC.
4. El Gerente de Normas y Calidad selecciona la información del servicio de TIC a borrar.
5. El Sistema elimina los datos del servicio de TIC.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro del servicio de TIC anterior.
- El Sistema reconstruye el registro del servicio de TIC anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.5. Nombre: Agregar Hardware.

Objetivo: Ingresar la información de un hardware en el Sistema.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Requiere agregar hardware en el Sistema por lo que debe ser registrado.

Precondiciones:

Los datos del hardware tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información del hardware en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria del hardware.
2. El Gerente de Normas y Calidad selecciona en el menú hardware.
3. El Sistema solicita los datos del hardware a registrar.
4. El Gerente de Normas y Calidad agrega la información del hardware.
5. El Sistema genera el registro del hardware especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de hardware anterior.
- El Sistema reconstruye el registro de hardware anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.6. Nombre: Consulta de Hardware.

Objetivo: Consultar la información de un hardware en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de un hardware registrado en el Sistema.

Precondiciones:

Los datos del hardware tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de los diferentes hardwares registrados en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de un hardware.
2. El Gerente de Normas y Calidad selecciona el menú hardware.
3. El Sistema muestra los datos registrados de los hardwares.
4. El Gerente de Normas y Calidad verifica la información del hardware.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de hardware anterior.
- El Sistema reconstruye el registro de hardware anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.7. Nombre: Modificar Hardware.

Objetivo: Modificar la información de un hardware registrado en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información del hardware que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del hardware tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información del hardware en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de un hardware.

2. El Gerente de Normas y Calidad selecciona el menú hardware.
3. El Sistema muestra los datos registrados de los hardwares.
4. El Gerente de Normas y Calidad cambia la información del hardware seleccionado.
5. El Sistema guarda los datos modificados del hardware.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de hardware anterior.
- El Sistema reconstruye el registro de hardware anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.8. Nombre: Eliminar Hardware.

Objetivo: Borrar la información del hardware registrado en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información del hardware que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del hardware tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información del hardware en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información del hardware.
2. El Gerente de Normas y Calidad selecciona el menú hardware.

3. El Sistema muestra los datos registrados de los hardwares.
4. El Gerente de Normas y Calidad selecciona la información del hardware a borrar.
5. El Sistema elimina los datos del hardware.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de hardware anterior.
- El Sistema reconstruye el registro de hardware anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.9. Nombre: Agregar Software.

Objetivo: Ingresar la información de un software en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: requiere agregar en el Sistema un software.

Precondiciones:

Los datos del software tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información del software que se registrarán en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de un software.
2. El Gerente de Normas y Calidad selecciona el menú software.
3. El Sistema solicita los datos del software a registrar.
4. El Gerente de Normas y Calidad agrega la información del software.

5. El Sistema genera el registro del software especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de software anterior.
- El Sistema reconstruye el registro de software anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

b.10. Nombre: Consulta de Software.

Objetivo: Consultar la información de un software en el Sistema.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de un software registrado en el Sistema.

Precondiciones:

Los datos del software tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información del software en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de un software.
2. El Gerente de Normas y Calidad selecciona el menú Software.
3. El Sistema muestra los datos registrados del software.
4. El Gerente de Normas y Calidad verifica la información del software.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de software anterior.
- El Sistema reconstruye el registro de software anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

b.11. Nombre: Modificar Software.

Objetivo: Modificar la información de un software registrado en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de un software que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del software tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información del software en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de un software.
2. El Gerente de Normas y Calidad selecciona el menú software.
3. El Sistema muestra los datos registrados del software.
4. El Gerente de Normas y Calidad cambia la información del software seleccionado.
5. El Sistema guarda los datos modificados del software.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de software anterior.
- El Sistema reconstruye el registro de software anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

b.12. Nombre: Eliminar Software.

Objetivo: Borrar la información del software registrado en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de un software que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del software tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información del software en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información del software.
2. El Gerente de Normas y Calidad selecciona el menú software.
3. El Sistema muestra los datos registrados del software.
4. El Gerente de Normas y Calidad selecciona la información del software a borrar.
5. El Sistema elimina los datos del software.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de software anterior.
- El Sistema reconstruye el registro de software anterior
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.1. Nombre: Agregar Fuente de Amenaza.

Objetivo: Ingresar la información de una fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: requiere agregar en el Sistema una fuente de amenaza.

Precondiciones:

Los datos de la fuente de amenaza tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de las fuentes de amenazas que utilizará el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de una fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema solicita los datos de la fuente de amenaza a registrar.
4. El Gerente de Normas y Calidad agrega la información de la fuente de amenaza.
5. El Sistema genera el registro de la fuente de amenaza especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED y solicita la recuperación al registro de fuente de amenaza anterior.
- El Sistema reconstruye el registro de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.2. Nombre: Consulta de Fuente de Amenaza.

Objetivo: Consultar la información de una fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de una fuente de amenaza registrada en el Sistema.

Precondiciones:

Los datos de la fuente de amenaza tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de las fuentes de amenazas del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de una fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las fuentes de amenazas.
4. El Gerente de Normas y Calidad verifica la información de la fuente de amenaza.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de fuente de amenaza anterior.
- El Sistema reconstruye el registro de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.3. Nombre: Modificar Fuente de Amenaza.

Objetivo: Modificar la información de una fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de una fuente de amenaza que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la fuente de amenaza tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información de la fuente de amenaza en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de una fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las fuentes de amenazas.
4. El Gerente de Normas y Calidad cambia la información de la fuente de amenaza seleccionada.
5. El Sistema guarda los datos modificados de la fuente de amenaza.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro fuente de amenaza anterior.
- El Sistema reconstruye el registro fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.4. Nombre: Eliminar Fuente de Amenaza.

Objetivo: Borrar la información de la fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de una fuente de amenaza que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la fuente de amenaza tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información de la fuente de amenaza del Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información de la fuente de amenaza.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las fuentes de amenazas.
4. El Gerente de Normas y Calidad selecciona la información de la fuente de amenaza a borrar.
5. El Sistema elimina los datos de la fuente de amenaza.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de fuente de amenaza anterior.
- El Sistema reconstruye el registro de fuente de amenaza anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.5.i. Nombre: Agregar Motivación.

Objetivo: Ingresar la información de una motivación para ejecutar una fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Requiere agregar la motivación en el Sistema por lo que debe ser registrado.

Precondiciones:

Los datos de la motivación tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de la motivación en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de la motivación.
2. El Gerente de Normas y Calidad selecciona el menú riesgo.
3. El Sistema solicita los datos de la motivación a registrar.
4. El Gerente de Normas y Calidad agrega la información de la motivación.
5. El Sistema genera el registro de la motivación especificada por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la motivación anterior.
- El Sistema reconstruye el registro de la motivación anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.5.ii. Nombre: Consulta de Motivación.

Objetivo: Consultar la información de una motivación en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de una motivación registrada en el Sistema.

Precondiciones:

Los datos de la motivación tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de las diferentes motivaciones registradas en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de una motivación.
2. El Gerente de Normas y Calidad selecciona el menú riesgo.
3. El Sistema muestra los datos registrados de las motivaciones.
4. El Gerente de Normas y Calidad verifica la información de la motivación.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la motivación anterior.
- El Sistema reconstruye el registro de la motivación anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.5.iii. Nombre: Modificar Motivación.

Objetivo: Modificar la información de una motivación registrada en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de la motivación que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la motivación tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información de la motivación en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de una motivación.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las motivaciones.
4. El Gerente de Normas y Calidad cambia la información de la motivación seleccionada.
5. El Sistema guarda los datos modificados de la motivación.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la motivación anterior.

- El Sistema reconstruye el registro de la motivación anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.5.iv. Nombre: Eliminar Motivación.

Objetivo: Borrar la información de la motivación registrada en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de la motivación que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la motivación tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información de la motivación en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información de la motivación.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las motivaciones.
4. El Gerente de Normas y Calidad selecciona la información de la motivación a borrar.
5. El Sistema elimina los datos de la motivación.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la motivación anterior.
- El Sistema reconstruye el registro de la motivación anterior.

- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.6.i. Nombre: Agregar Acción.

Objetivo: Ingresar la información de una acción para ejecutar una fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Requiere agregar la acción en el Sistema por lo que debe ser registrado.

Precondiciones:

Los datos de la acción tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de la acción en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de la acción.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema solicita los datos de la acción a registrar.
4. El Gerente de Normas y Calidad agrega la información de la acción.
5. El Sistema genera el registro de la acción especificada por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la acción anterior.
- El Sistema reconstruye el registro de la acción anterior.

- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.6.ii. Nombre: Consulta de Acción.

Objetivo: Consultar la información de una acción en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de una acción registrada en el Sistema.

Precondiciones:

Los datos de la acción tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de las diferentes acciones registradas en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de una acción.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las acciones.
4. El Gerente de Normas y Calidad verifica la información de la acción.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la acción anterior.
- El Sistema reconstruye el registro de la acción anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.6.iii. Nombre: Modificar Acción.

Objetivo: Modificar la información de una acción registrada en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de la acción que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la acción tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información de la acción en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de una acción.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las acciones.
4. El Gerente de Normas y Calidad cambia la información de la acción seleccionada.
5. El Sistema guarda los datos modificados de la acción.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la acción anterior.
- El Sistema reconstruye el registro de la acción anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.6.iv. Nombre: Eliminar Acción.

Objetivo: Borrar la información de la acción registrada en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de la acción que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la acción tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información de la acción en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información de la acción.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las acciones.
4. El Gerente de Normas y Calidad selecciona la información de la acción a borrar.
5. El Sistema elimina los datos de la acción.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la acción anterior.
- El Sistema reconstruye el registro de la acción anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.7.i. Nombre: Caso de uso Agregar Vulnerabilidad.

Objetivo: Ingresar la información de una vulnerabilidad para ejecutar una fuente de amenaza en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Requiere agregar la vulnerabilidad en el Sistema por lo que debe ser registrado.

Precondiciones:

Los datos de la vulnerabilidad tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de la vulnerabilidad en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de la vulnerabilidad.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema solicita los datos de la vulnerabilidad a registrar.
4. El Gerente de Normas y Calidad agrega la información de la vulnerabilidad.
5. El Sistema genera el registro de la vulnerabilidad especificada por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la vulnerabilidad anterior.
- El Sistema reconstruye el registro de la vulnerabilidad anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.7.ii. Nombre: Caso de uso Consulta de Vulnerabilidad.

Objetivo: Consultar la información de una vulnerabilidad en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de una vulnerabilidad registrada en el Sistema.

Precondiciones:

Los datos de la vulnerabilidad tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de las diferentes vulnerabilidades registradas en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de una vulnerabilidad.
2. El Gerente de Normas y Calidad selecciona el menú riesgo.
3. El Sistema muestra los datos registrados de las vulnerabilidades.
4. El Gerente de Normas y Calidad verifica la información de la vulnerabilidad.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la vulnerabilidad anterior.
- El Sistema reconstruye el registro de la vulnerabilidad anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.7.iii. Nombre: Caso de uso Modificar Vulnerabilidad.

Objetivo: Modificar la información de una vulnerabilidad registrada en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de la vulnerabilidad que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la vulnerabilidad tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información de la vulnerabilidad en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de una vulnerabilidad.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las vulnerabilidades.
4. El Gerente de Normas y Calidad cambia la información de la vulnerabilidad seleccionada.
5. El Sistema guarda los datos modificados de la vulnerabilidad.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la vulnerabilidad anterior.
- El Sistema reconstruye el registro de la vulnerabilidad anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.7.iv. Nombre: Caso de uso Eliminar Vulnerabilidad.

Objetivo: Borrar la información de la vulnerabilidad registrada en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de la vulnerabilidad que se encuentra registrada en el Sistema.

Precondiciones:

Los datos de la vulnerabilidad tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información de la vulnerabilidad en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información de la vulnerabilidad.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de las vulnerabilidades.
4. El Gerente de Normas y Calidad selecciona la información de la vulnerabilidad a borrar.
5. El Sistema elimina los datos de la vulnerabilidad.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de la vulnerabilidad anterior.
- El Sistema reconstruye el registro de la vulnerabilidad anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.7.v.1. Nombre: Caso de uso Agregar Control.

Objetivo: Ingresar la información de un control en el Sistema.

Actor principal: Gerente de Normas y Calidad

Personal involucrado e interés:

Personal de la Unidad Informática: requiere agregar en el Sistema un control.

Precondiciones:

Los datos del control tienen que estar revisados por el Gerente de Normas y Calidad.

Garantías de éxito (post-condiciones):

Se almacenará la información de los controles que se registrarán en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática presenta la información necesaria de un control.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema solicita los datos del control a registrar.
4. El Gerente de Normas y Calidad agrega la información del control.
5. El Sistema genera el registro del control especificado por el Gerente de Normas y Calidad.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de control anterior.
- El Sistema reconstruye el registro de control anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.7.v.2. Nombre: Caso de uso Consulta de Control.

Objetivo: Consultar la información de un control en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Verificar la existencia de un control registrado en el Sistema.

Precondiciones:

Los datos del control tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se verificará la información de los diferentes controles en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática requiere la información necesaria de un control.
2. El Gerente de Normas y Calidad selecciona el menú riesgo.
3. El Sistema muestra los datos registrados de los controles.
4. El Gerente de Normas y Calidad verifica la información del control.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de control anterior.
- El Sistema reconstruye el registro de control anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

c.7.v.3. Nombre: Modificar Control.

Objetivo: Modificar la información de un control registrado en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Cambiar la información de un control que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del control tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se confirmará el cambio de la información del control en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita el cambio a la información de un control.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de los controles.
4. El Gerente de Normas y Calidad cambia la información del control seleccionado.
5. El Sistema guarda los datos modificados del control.

Extensiones:

1. En cualquier momento el Sistema falla.

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de control anterior.
- El Sistema reconstruye el registro de control anterior.
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error, y pasa a un estado limpio.

c.7.v.4. Nombre: Caso de uso Eliminar Control.

Objetivo: Borrar la información del control registrado en el Sistema.

Actor principal: Gerente de Normas y Calidad.

Personal involucrado e interés:

Personal de la Unidad Informática: Solicita borrar la información de un control que se encuentra registrado en el Sistema.

Precondiciones:

Los datos del control tienen que estar registrados en el Sistema.

Garantías de éxito (post-condiciones):

Se borrará la información del control en el Sistema.

Escenario principal de éxito:

1. El personal de la Unidad Informática solicita borrar la información del control.
2. El Gerente de Normas y Calidad selecciona el menú Riesgo.
3. El Sistema muestra los datos registrados de los controles.
4. El Gerente de Normas y Calidad selecciona la información del control a borrar.
5. El Sistema elimina los datos del control.

Extensiones:

1. En cualquier momento el Sistema falla

Para dar soporte a la recuperación y el registro correcto, se asegura que todos los estados y eventos significativos de una transacción puedan recuperarse desde cualquier paso del escenario.

- El Gerente de Normas y Calidad reinicia el Sistema MARMINED, y solicita la recuperación al registro de control anterior.
- El Sistema reconstruye el registro de control anterior
- El Sistema informa el error al Gerente de Normas y Calidad, registra el error y pasa a un estado limpio.

CAPITULO V: PLAN DE IMPLEMENTACIÓN.

A. INTRODUCCIÓN.

El Plan de Implementación es un documento en el cual se especifican todos los requerimientos necesarios para poner en funcionamiento un producto desarrollado. Además de definir todas las actividades a ejecutar para la puesta en marcha del nuevo producto.

El presente Plan de Implementación define un objetivo de ejecución así como el establecimiento de los subsistemas que reflejan los objetivos específicos dentro de los cuales se identifican paquetes de trabajo que son un conjunto de actividades a realizar para lograr la puesta en marcha de la "Metodología de Administración de Riesgos de TIC para el MINED" (MARMINED)[34] de manera exitosa en las instalaciones de dicho ministerio.

Los subsistemas que se deberán llevar a cabo para la implementación de la metodología, se han dividido en: subsistema de instalación y configuración, subsistema de ejecución y subsistema de capacitación.

Para la implementación del proyecto se consideró un período de un mes (22 días hábiles), iniciando en enero del año 2010.

[34] El nombre MARMINED hace referencia tanto a la metodología como al prototipo de software.

B. OBJETIVOS DEL PLAN DE IMPLEMENTACIÓN.

Objetivo de Ejecución.

Implementar la Metodología de Administración de Riesgos de TIC para el MINED (MARMINED) en un período de un mes (22 días hábiles) a un costo de $ 4,037.00.

Objetivos Específicos.

- Determinar los recursos tecnológicos, físicos, económicos y humanos necesarios para la ejecución del proyecto.

- Realizar las pruebas de la metodología para verificar que cumpla con los requerimientos del MINED.

- Garantizar la funcionalidad de MARMINED, la integridad y consistencia de la información.

- Realizar las capacitaciones necesarias al personal que utilizará MARMINED para una mejor funcionalidad y aprovechamiento de ésta.

C. SUBSISTEMA DE INSTALACIÓN Y CONFIGURACIÓN.

Tiene como objetivo instalar y configurar el hardware, software, acondicionamiento del local en donde se ubicará el mobiliario requerido para la implementación de MARMINED.

1. Metas del subsistema de Instalación y Configuración.

i. Controlar avances de instalación y configuración
ii. Garantizar el adecuado funcionamiento de MARMINED
iii. Garantizar la protección del equipo instalado

2. Paquetes de trabajo.

i. Hardware.
   - Acondicionar Red Eléctrica.
   - Ubicar e instalar físicamente el equipo informático.
   - Instalar equipo de protección.
   - Realizar el cableado de red.
   - Realizar pruebas de comunicación.

ii. Software.
   - Configurar red.
   - Instalar software requerido.
   - Configurar conexión a internet.
   - Instalar y configurar Servidor Web.
   - Instalar y configurar la Base de Datos.
   - Instalar y configurar MARMINED.
   - Realizar pruebas de conexión de MARMINED y la base de datos.

D. SUBSISTEMA DE EJECUCIÓN.

Tiene como objetivo la puesta en marcha de MARMINED, para lograrlo se realizarán las actividades relacionadas con las pruebas pilotos, migración de datos e integración de MARMINED, para verificar que MARMINED cumple con los requerimientos demandados por los usuarios potenciales de la misma.

1. Metas del subsistema de Ejecución.

i. Verificar cada uno de los procesos que manejará MARMINED para visualizar posibles errores en su ejecución.
ii. Controlar las actividades de la Prueba Piloto.
iii. Corregir errores en el desarrollo de un determinado proceso para evitar errores posteriores.
iv. Agilizar la ejecución de MARMINED.

2. Paquetes de trabajo.

i. Realizar prueba piloto de identificación de fuentes de amenazas.
ii. Realizar prueba piloto de identificación de vulnerabilidades.
iii. Realizar prueba piloto del cálculo de la probabilidad del ejercicio de la vulnerabilidad.
iv. Realizar prueba piloto del cálculo de la magnitud de impacto.
v. Realizar prueba piloto del cálculo del nivel de impacto del riesgo.

E. SUBSISTEMA DE CAPACITACIÓN.

Tiene como objetivo instruir a los usuarios de MARMINED, específicamente al administrador de MARMINED y personal de la Gerencia de Normas y Calidad.

1. Metas del subsistema de Capacitación.

i. Garantizar el aprendizaje de los usuarios en el manejo MARMINED.
ii. Coordinar las actividades de capacitación.

iii. Dar a conocer al personal de Gerencia de Normas y Calidad sus responsabilidades y el plan de capacitación.

2. Paquetes de trabajo.

i. Elaborar y reproducir el material de capacitación.
ii. Capacitar al Administrador de MARMINED.
iii. Capacitar al Personal de la Gerencia de Normas y Calidad.

3. Capacitación de usuarios.

La capacitación de usuarios tiene por objetivo explicar el funcionamiento de todos los procedimientos intrínsecos de MARMINED permitiendo una mayor eficiencia en la implementación.

La capacitación estará basada en actividades tales como:

i. **Mantenimiento de Servicios de TIC, Hardware, Software, Fuentes de Amenazas y Vulnerabilidades:** Estas actividades incluyen registros, modificaciones, consultas e impresión de información de estos elementos.

ii. **Envío y recepción de registros:** Estas actividades incluyen el envío y recepción de registros a la base de datos de MARMINED.

iii. **Emisión de reportes y catálogos** En dicha actividad se describirán los reportes y catálogos generados por la metodología los cuales podrán ser de Servicios de TIC, de Hardware, de Software, de Fuentes de Amenazas, de Vulnerabilidades y de riesgos.

iv. **Personal Encargado de la capacitación:** Director del proyecto y encargado de capacitación.

v. **Personal a quien estará dirigida la capacitación:** Personal de la Dirección de Informática y sus dependencias que utilizarán MARMINED. La Cantidad de técnicos de normas y

calidad que laboran en el MINED son cuatro personas las cuales son los que utilizarán la metodología de administración de riesgos de TIC del MINED.

vi. **Metodología de capacitación:** La capacitación técnica se realizará por medio de un instructor que con la ayuda de manuales impresos, un proyector multimedia y un computador expondrá todo el contenido de dicha capacitación. Los usuarios deberán realizar prácticas sobre lo desarrollado en la capacitación después de concluido cada tema, contando con el apoyo del instructor quien aclarará las dudas existentes en el momento.

vii. **Lugar de capacitación:** La capacitación se llevará a cabo en las instalaciones del MINED.

viii. **Preparación de la capacitación** Las condiciones ideales para la preparación de la capacitación deberán ser:

- Local mediano, de preferencia con aire acondicionado o buena ventilación.
- Instalación de computadora con cañón proyector.
- Una copia del manual de usuario y de especificaciones técnicas para cada uno de los asistentes.
- Una copia del CD de la metodología para cada asistente.
- Una computadora con ambiente de prueba para los asistentes (Máximo 2 personas por computador).

ix. **Contenido de la capacitación.**

TEMA	ACTIVIDADES
Conociendo MARMINED	➢ Conceptualización de MARMINED. ➢ Conociendo cada fase y sus formularios. ➢ Documentos de salida de la metodología.
Llenado de Formularios	➢ Llenado de formularios de Fase 1. ➢ Llenado de formularios de Fase 2. ➢ Llenado de formularios de Fase 3.
Ingresando a MARMINED	➢ Acceso a MARMINED. ➢ Navegación por MARMINED. ➢ Salir de MARMINED.
Administración de Catálogos	➢ Administración de Usuarios. ➢ Administración de Unidad Organizativa. ➢ Administración de Tipo de Fuente de Amenaza.
Administración de TIC	➢ Administración de Servicios de TIC. ➢ Administración de Software. ➢ Administración de Hardware.
Administración de Riesgo	➢ Administración de Fuente de Amenaza. ➢ Administración de Vulnerabilidades. ➢ Administración de Motivaciones. ➢ Administración de Acciones de Materialización de Amenaza. ➢ Administración de Controles.
Administración de Reportes	➢ Reporte de Riesgo. ➢ Reporte de Servicios de TIC. ➢ Reporte de Software. ➢ Reporte de Hardware. ➢ Reporte de Fuentes de Amenaza. ➢ Reporte de Vulnerabilidades.

Tabla 50. Contenido de la capacitación de MARMINED.

F. ESTRATEGIAS DE EJECUCIÓN.

Para el logro de cada uno de los objetivos específicos de implementación, se formulan las siguientes estrategias:

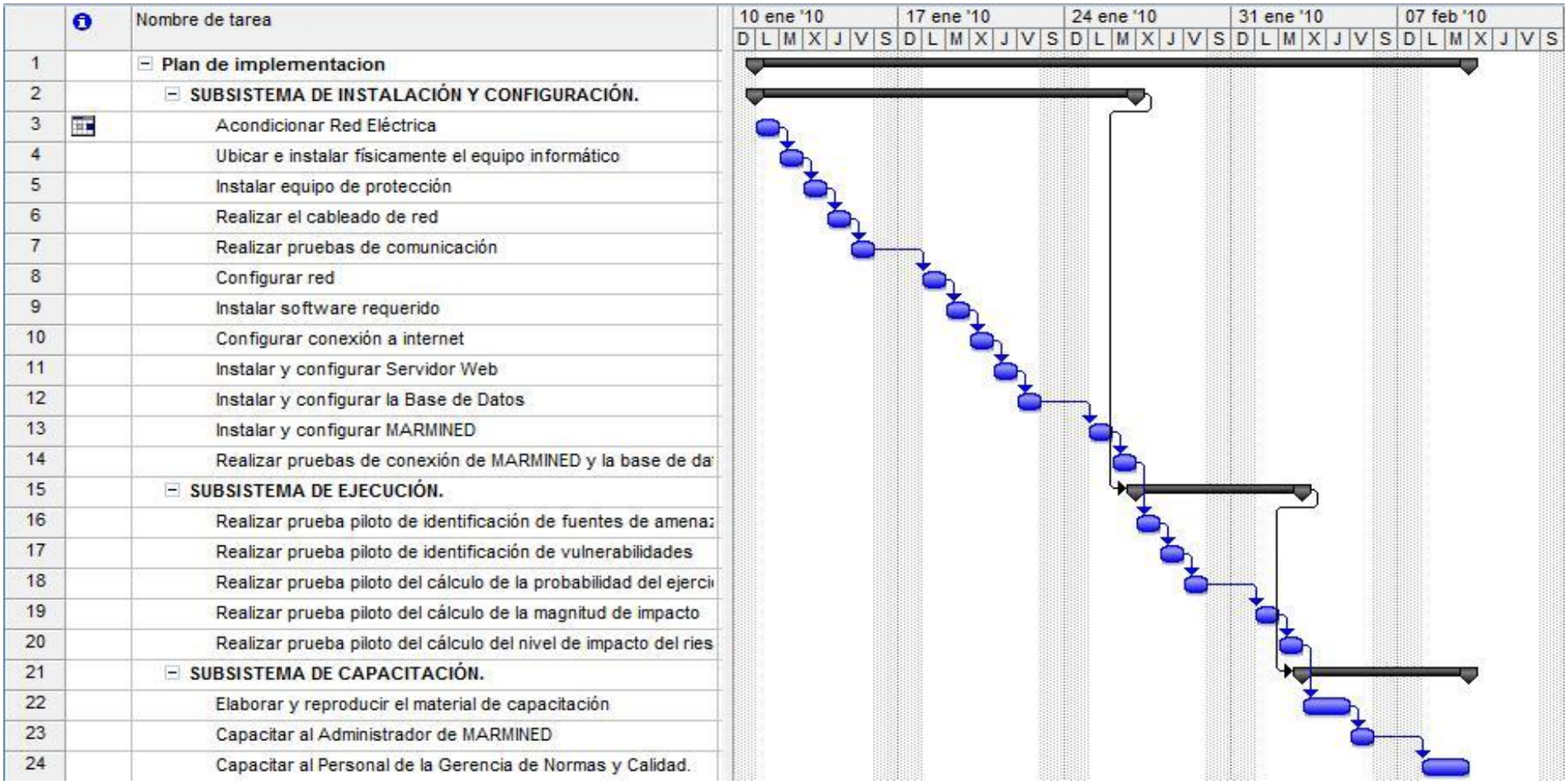
a. Capacitar al personal de la Gerencia de Normas y Calidad, así como también al administrador de MARMINED en las herramientas de desarrollo y base de datos.
b. Realizar monitoreo interno de MARMINED (una vez al año).
c. Disponer de la asesoría oportuna para la instalación y configuración de la tecnología a utilizar en la implementación de MARMINED.
d. La capacitación para el recurso humano que operará MARMINED se deberá efectuar inmediatamente después que ésta sea implementada.
e. Elaborar políticas y procedimientos que fomenten el buen uso de MARMINED y la cultura informática con relación a la seguridad de la misma.
f. Presentar el proyecto a las entidades que tengan la autoridad suficiente para la toma de decisiones sobre la ejecución del proyecto.

G. PROGRAMACIÓN PARA LA IMPLEMENTACIÓN DE MARMINED.

Comprende el listado de actividades, tiempos y secuencias para la implementación de MARMINED; incluye además la distribución de los recursos financieros en el mismo período de tiempo. Las Figuras 19 y 20 muestran el cronograma de actividades que comprende un período de 22 días hábiles.

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Costos
1	**Plan de implementacion**	**22 días**	**lun 11/01/10**	**mar 09/02/10**		**$3,838.00**
2	**SUBSISTEMA DE INSTALACIÓN Y CONFIGURACIÓN.**	**12 días**	**lun 11/01/10**	**mar 26/01/10**		**$1,019.00**
3	Acondicionar Red Eléctrica	1 día	lun 11/01/10	lun 11/01/10		$55.00
4	Ubicar e instalar físicamente el equipo informático	1 día	mar 12/01/10	mar 12/01/10	3	$35.00
5	Instalar equipo de protección	1 día	mié 13/01/10	mié 13/01/10	4	$45.00
6	Realizar el cableado de red	1 día	jue 14/01/10	jue 14/01/10	5	$145.00
7	Realizar pruebas de comunicación	1 día	vie 15/01/10	vie 15/01/10	6	$85.00
8	Configurar red	1 día	lun 18/01/10	lun 18/01/10	7	$55.00
9	Instalar software requerido	1 día	mar 19/01/10	mar 19/01/10	8	$67.00
10	Configurar conexión a internet	1 día	mié 20/01/10	mié 20/01/10	9	$30.00
11	Instalar y configurar Servidor Web	1 día	jue 21/01/10	jue 21/01/10	10	$85.00
12	Instalar y configurar la Base de Datos	1 día	vie 22/01/10	vie 22/01/10	11	$215.00
13	Instalar y configurar MARMINED	1 día	lun 25/01/10	lun 25/01/10	12	$77.00
14	Realizar pruebas de conexión de MARMINED y la base de d	1 día	mar 26/01/10	mar 26/01/10	13	$125.00
15	**SUBSISTEMA DE EJECUCIÓN.**	**5 días**	**mié 27/01/10**	**mar 02/02/10**	**2**	**$1,019.00**
16	Realizar prueba piloto de identificación de fuentes de amena	1 día	mié 27/01/10	mié 27/01/10	14	$150.00
17	Realizar prueba piloto de identificación de vulnerabilidades	1 día	jue 28/01/10	jue 28/01/10	16	$150.00
18	Realizar prueba piloto del cálculo de la probabilidad del ejerc	1 día	vie 29/01/10	vie 29/01/10	17	$219.00
19	Realizar prueba piloto del cálculo de la magnitud de impacto	1 día	lun 01/02/10	lun 01/02/10	18	$300.00
20	Realizar prueba piloto del cálculo del nivel de impacto del rie	1 día	mar 02/02/10	mar 02/02/10	19	$200.00
21	**SUBSISTEMA DE CAPACITACIÓN.**	**5 días**	**mié 03/02/10**	**mar 09/02/10**	**15**	**$1,800.00**
22	Elaborar y reproducir el material de capacitación	2 días	mié 03/02/10	jue 04/02/10	20	$400.00
23	Capacitar al Administrador de MARMINED	1 día	vie 05/02/10	vie 05/02/10	22	$500.00
24	Capacitar al Personal de la Gerencia de Normas y Calidad.	2 días	lun 08/02/10	mar 09/02/10	23	$900.00

Figura 19: Cronograma de actividades con sus respectivos costos por actividad.



	Nombre de tarea
1	**Plan de implementacion**
2	**SUBSISTEMA DE INSTALACIÓN Y CONFIGURACIÓN.**
3	Acondicionar Red Eléctrica
4	Ubicar e instalar físicamente el equipo informático
5	Instalar equipo de protección
6	Realizar el cableado de red
7	Realizar pruebas de comunicación
8	Configurar red
9	Instalar software requerido
10	Configurar conexión a internet
11	Instalar y configurar Servidor Web
12	Instalar y configurar la Base de Datos
13	Instalar y configurar MARMINED
14	Realizar pruebas de conexión de MARMINED y la base de da
15	**SUBSISTEMA DE EJECUCIÓN.**
16	Realizar prueba piloto de identificación de fuentes de amena
17	Realizar prueba piloto de identificación de vulnerabilidades
18	Realizar prueba piloto del cálculo de la probabilidad del ejerci
19	Realizar prueba piloto del cálculo de la magnitud de impacto
20	Realizar prueba piloto del cálculo del nivel de impacto del ries
21	**SUBSISTEMA DE CAPACITACIÓN.**
22	Elaborar y reproducir el material de capacitación
23	Capacitar al Administrador de MARMINED
24	Capacitar al Personal de la Gerencia de Normas y Calidad.

Figura 20: Cronograma de actividades con su respectiva ruta crítica (en azul).

H. ASIGNACIÓN DE RECURSOS.

Para la implementación de MARMINED, se asignarán tres personas que serán las encargadas de realizar todas las actividades de cada subsistema definido para el proyecto. Las personas asignadas serán el director del proyecto, un técnico de calidad y un encargado de capacitaciones.

1. Subsistema de Instalación y Configuración.

i. Recurso Humano.

Técnico de Calidad.

ii. Material a Utilizar.

Plan de Implementación: 1 Copia.

Manual Técnico: 1 Copia.

Manual de Usuario: 1 Copia.

iii. Recurso Tecnológico.

Equipo Informático.

Cable.

Conectores.

Tarjetas de red.

UPS.

2. Subsistema de Ejecución.

i. Recurso Humano.

Director del proyecto.

Técnico de Calidad.

3. Subsistema de Capacitación.

i. Recurso Humano.

Director del proyecto.

Encargado de capacitaciones.

I. PROGRAMACIÓN FINANCIERA.

La programación financiera se efectúo haciendo una distribución de los egresos a realizarse durante del tiempo programado para la implementación de MARMINED (1 mes).

El monto total de la implementación se muestra en la Tabla 51 y es de $4,037.00, el cual cubre el pago de salarios a los encargados de la implementación, capacitaciones y costos incurridos en materiales correspondiente a los cd´s, manuales, tintas de impresor y el gasto de papel necesario para la ejecución de las pruebas necesarias para verificar su correcto funcionamiento.

Descripción	Monto
Recurso Humano (Salarios y Capacitaciones)	$3,700.00
Recursos Material	$337.00
Total:	$4,037.00

Tabla 51. Monto Total de la Implementación de MARMINED.

1. Recurso Humano.

Recurso	Sueldo	Tiempo	Costo
Director de Proyecto	$1,600.00	1 mes	$1,600.00
Encargado de Capacitaciones	$1,000.00	1 mes	$1,000.00
Técnico de Calidad	$1,100.00	1 mes	$1,100.00
		Total:	$3,700.00

Tabla 52. Monto Total del Recurso Humano encargado de la implementación.

2. Recurso Material.

Cantidad	Descripción	Costo Unitario ($)	Costo Total($)
7	CD con Metodología	$1.00	$7.00
7	Manual de Usuario	$5.00	$35.00
7	Manual de Técnico	$5.00	$35.00
7	Resmas de papel bond	$5.00	$35.00
5	Cartucho de Tinta Impresor	$45.00	$225.00
		TOTAL	$337.00

Tabla 53. Monto Total de los Recursos Materiales.

J. ESTRUCTURA ORGANIZATIVA DE LA UNIDAD EJECUTORA DEL PROYECTO.

Para la implementación del proyecto es necesario definir la organización que tendrá la unidad ejecutora de dicha actividad a fin de facilitar el cumplimiento de cada una de las actividades necesarias para la implementación. Tomando en cuenta los subsistemas se determinó la estructura que se muestra en la Figura 21.

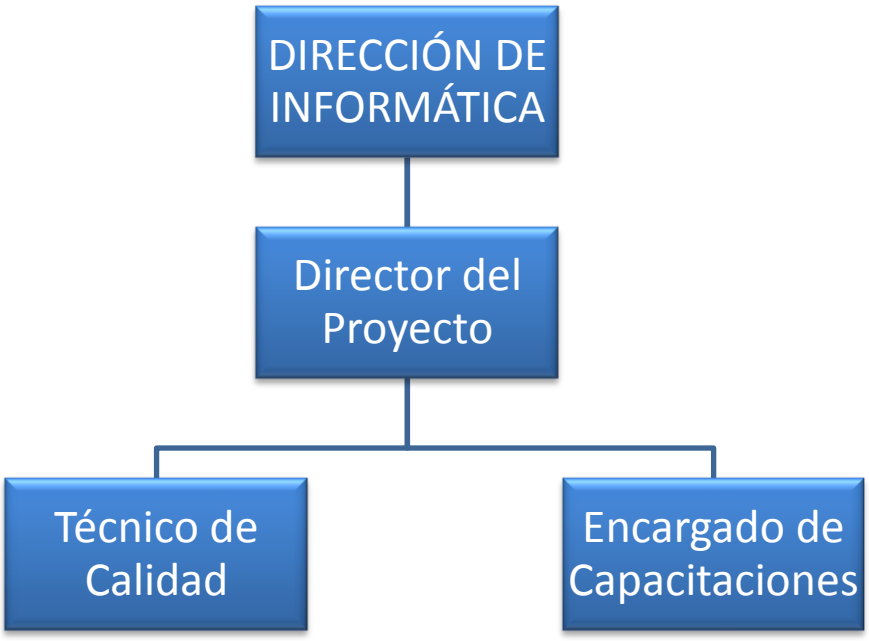


Figura 21: Estructura Organizativa de la Unidad Ejecutora.

La ubicación de la Unidad Ejecutora dentro de la estructura organizacional del MINED se puede observar en la Figura 22.

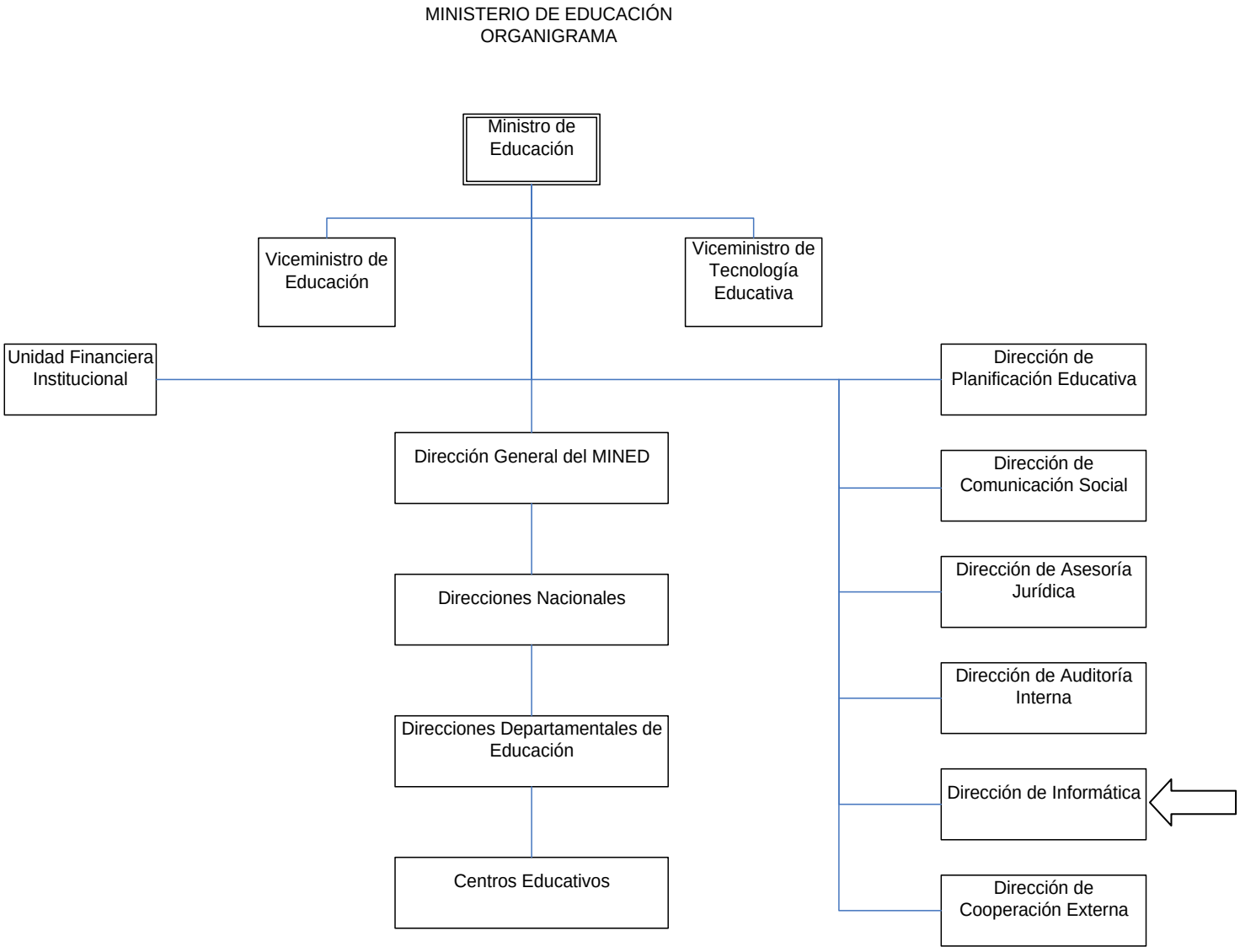


Figura 22. Organigrama del MINED. La flecha indica la ubicación de la Unidad Ejecutora.

K. MANUAL DE PUESTOS DE LA UNIDAD EJECUTORA.

METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TIC PARA EL MINED (MARMINED)	
Puesto	Director del Proyecto
Depende de	Dirección de Informática
Función General	Planificar, coordinar y dirigir todas las actividades del proyecto para alcanzar los objetivos de implementación
Funciones Específicas	1. Planificar, organizar dirigir y coordinar todas las actividades del plan de implementación de MARMINED. 2. Dirigir y coordinar los recursos relacionados con el proyecto. 3. Realizar la programación financiera del Proyecto. 4. Supervisar la reproducción y distribución del material didáctico a utilizar durante las capacitaciones. 5. Elaborar los estados financieros del Proyecto cuando le sean solicitados. 6. Controlar y archivar todos los documentos que requieran ser contabilizados. 7. Controlar los avances de la implementación de acuerdo a lo planificado. 8. Coordinar las actividades relacionadas con las pruebas piloto. 9. Diseñar el material didáctico para capacitaciones. 10. Toma de decisiones relacionadas a cambios relevantes y en todo lo que la institución considere necesario para la eficiente implementación de MARMINED. 11. Programar y controlar las actividades a realizar por el Técnico de Calidad. 12. Aplicar las medidas correctivas correspondientes, en caso de desviaciones según la programación. 13. Proporcionar informes a la Dirección de Informática.
Requisitos mínimos del puesto:	Educación: Ing. de Sistemas Informáticos. Experiencia: 3 años o más en administración de proyectos. Aptitudes: Alto grado de flexibilidad, visión, imaginación, creatividad, relaciones personales, liderazgo y capacidad para el trabajo en equipo. Edad: Mayor de 25 años; Sexo: Masculino o Femenino.

METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TIC PARA EL MINED (MARMINED)	
Puesto	Técnico de Calidad
Depende de	Director del proyecto
Función General	Realizar las actividades de instalación y configuración del equipo, así como también las relacionadas con el acondicionamiento del mobiliario adquirido e impartir las capacitaciones de MARMINED.
Funciones Específicas	1. Verificar las condiciones del lugar en que se instalará el equipo adquirido. 2. Instalar todo el recurso tecnológico para la implementación de MARMINED. 3. Controlar la instalación del cableado, polarizado y otras instalaciones. 4. Instalar y configurar la Intranet. 5. Coordinar actividades de instalación del recurso tecnológico y mobiliario. 6. Realizar pruebas de comunicación en la Intranet. 7. Presentar informes al Director del Proyecto. 8. Configurar la conexión a Internet. 9. Revisar y depurar la data contenida en la base de datos de MARMINED. 10. Realizar la configuración de MARMINED, así como también de la Base de Datos. 11. Realizar pruebas de conexión de MARMINED con la Base de Datos.
Requisitos mínimos del puesto:	Educación: Estudios de Ing. de Sistemas Informáticos. Experiencia: 2 años o más en administración de proyectos. Aptitudes: Alto grado de flexibilidad, visión, imaginación, creatividad, relaciones personales, liderazgo y capacidad para el trabajo en equipo. Edad: Mayor de 25 años; Sexo: Masculino o Femenino.

METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TIC PARA EL MINED (MARMINED)	
Puesto	Encargado de Capacitaciones
Depende de	Director del proyecto
Función General	Planificar, organizar y controlar las actividades relacionadas con las capacitaciones a impartir a los usuarios de MARMINED.
Funciones Específicas	1. Planificar y coordinar las actividades de las capacitaciones que se impartirán. 2. Supervisar la reproducción y distribución del material didáctico a utilizar durante las capacitaciones. 3. Capacitar a los usuarios de MARMINED en todo lo relacionado con el buen uso de esta, específicamente al Administrador de MARMINED y al personal de la Gerencia de Normas y Calidad.
Requisitos mínimos del puesto:	Educación: Estudios de Ing. de Sistemas Informáticos. Experiencia: 2 años o más en administración de proyectos. Aptitudes: Alto grado de flexibilidad, visión, imaginación, creatividad, relaciones personales, liderazgo y capacidad para el trabajo en equipo. Edad: Mayor de 25 años; Sexo: Masculino o Femenino.

CONCLUSIONES.

- La administración efectiva de los riesgos de TIC en el Ministerio de Educación no debe considerarse como una responsabilidad más de la Gerencia de Normas y Calidad, sino como una garantía de la continuación de las diferentes actividades diarias que en la institución se realizan valiéndose de las diversas tecnologías de información y comunicaciones que las agilizan, a la vez que potencializan su productividad. La administración de riesgos de TIC, por tanto, constituye una tarea a desarrollar con fines puramente preventivos, es decir, se anticiparán los escenarios posibles de vulnerabilidades y amenazas, se evaluarán y se establecerán acciones concretas orientadas a disminuir el impacto que pudieran tener las amenazas en los servicios de TIC.

- Se estima que los beneficios de la implementación de MARMINED serán perceptibles a partir de un año después de la ejecución completa y ordenada de cada una de las actividades establecidas en las fases, incluyendo la implementación de los controles seleccionados en el Plan de Acción. La metodología deberá implementarse en todos los servicios de TIC que se deseen administrar.

- Con la implementación de MARMINED se pronostica un reducción del 75% de los gastos anuales presupuestados en concepto reparación de fallos de TIC, los cuales se podrían reorientar al fortalecimiento de la infraestructura tecnológica del Ministerio de Educación.

- Una vez implementada la Metodología de Administración de Riesgos de Tecnologías de Información y Comunicaciones en el MINED se verán beneficiados alrededor de 2,600 usuarios administrativos, 32,000 docentes y 250,000 estudiantes de educación media en centros públicos; 90,000 estudiantes en centros privados, que se consideran usuarios indirectos ya que forman parte del sistema educativo nacional y que utilizan diferentes servicios de sistemas de información que presta el MINED como son:

Sistema de Notas de Educación Básica y Media, Sistema de Matrícula, Sistema de Censo, entre otros.

- MARMINED presenta una manera metódica, precisa y exacta de resolver el problema de la gestión de riesgos de TIC, proporcionando una guía fácil de seguir para el implementador. Cuenta con un catálogo de controles predefinido orientados a resolver las amenazas más comunes en materia de seguridad de la información.

- MARMINED cuenta con una descripción minuciosa y detallada de los pasos a seguir para lograr los resultados esperados; explica de manera clara y sencilla los conceptos que sirven de indicadores para la toma de decisiones; determina los responsables de la gestión de la administración de riesgos de TIC, así como de las tareas a realizar; cuenta con un prototipo de software evolutivo el cual agiliza la realización de las tareas correspondientes a las fases de Configuración de los Elementos de TIC y Evaluación de los Riesgos.

- MARMINED ofrece facilidad para su constante actualización mediante la correspondiente documentación, posibilitando la adaptabilidad a los nuevos requerimientos que vayan surgiendo; permitiéndole el mantenimiento y la incorporación de otras tareas que los usuarios estimen convenientes, procurando de esta manera su continuidad a través del tiempo.

RECOMEDACIONES.

- Se recomienda a los capacitadores el estudio detallado del documento que contiene la Metodología, así como de cada uno de sus Manuales, con el propósito de impartir a los usuarios clara y satisfactoriamente los conceptos y procedimientos de todos los pasos que comprenden las actividades de las tres fases de MARMINED.

- La participación activa del usuario final en el diseño de una solución constituye una ventaja significativa a la hora de presentar la propuesta, pues de esta manera se garantiza un apoyo importante a la misma, a la vez que se disminuye la resistencia al cambio.

- La documentación técnica del prototipo de software evolutivo de una aplicación informática es sumamente importante pues es la guía que el usuario deberá seguir para enriquecer la funcionalidad del mismo, actualizándolo y modificándolo de manera que sea posible su adaptación a los nuevos requerimientos que van surgiendo gradualmente.

- Al elaborar una Metodología para la Administración de Riesgos de Tecnologías de Información y Comunicaciones es importante conocer los requerimientos legales que ésta debe cumplir, tal es el caso de las que establece la Corte de Cuentas de la República a través de las Normas Técnicas de Control Interno, en lo que se refiere a las Normas Relativas a la Valoración de Riesgos.

GLOSARIO DE TÉRMINOS.

A

- **Aptitud:** Idoneidad para un cargo.
- **ADSL:** *Assimetric Digital Suscriber Line,* Línea de Suscripción Digital Asimétrica, es un servicio que se paga periódicamente a un proveedor de Internet.

B

- **Bitácora:** Registro manual o electrónico de un evento o suceso repetitivo, del que son importantes sus características particulares.

C

- **Caracterización:** Determinar con precisión. Término utilizado como sinónimo de "configuración" en la 1ra. Fase de MARMINED en el que se establecen las características de los elementos de TIC.
- **Coherencia:** Conexión, relación de varias cosas entre sí.
- **Configuración:** Disposición de las partes o elementos que componen un cuerpo u objeto y le dan su peculiar forma o figura.
- **Cintas de respaldo:** Recursos adicionales o copias duplicadas de datos como prevención contra emergencias. También conocidos como *backup*.

D

- **Desastre:** Desgracia grande, calamidad. Pérdida significativa de una empresa que afecta en sus operaciones.

E

- **Eficacia:** Virtud, actividad y poder para obrar.
- **Eficiencia:** Relación existente entre el trabajo desarrollado, el tiempo invertido, la inversión realizada en hacer algo y el resultado logrado.
- **Equipo Informático:** Conjunto de monitores, CPU, teclados, mouse y UPS de una computadora. Esta definición obedece a la Gerencia de Atención a Usuarios del MINED.

- **Estándar:** Que sirve como tipo, modelo, norma, patrón o referencia por ser corriente, de serie.
- **Extintor:** Aparato para extinguir incendios, que por lo común arroja sobre el fuego un chorro de agua o de una mezcla que dificulta la combustión.

H

- **Hardware:** Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un ordenador, incluidos sus periféricos.
- **Híbrido:** Formado por elementos de distinta naturaleza u origen.

I

- **Implícito:** Que se incluye en una proposición sin que haya necesidad de explicarlo.
- **Impacto:** Repercusión, influencia importante.
- **Inundación:** Cubrimiento del agua u otro líquido en un lugar al desbordarse del cauce que lo limita.
- **Interinstitucional:** Grupo de trabajo entre instituciones afines.

M

- **MINED:** Ministerio de Educación de El Salvador. Entidad encargada de la gestión de todos los niveles educativos públicos y privados. Institución para la que se elaborará un prototipo funcional de la propuesta de Metodología para la Administración de Riesgos de Tecnologías de Información y Comunicaciones.
- **Mecanismo:** Manera de producirse o de realizar una actividad.

N

- **Norma:** Regla de obligado cumplimiento.

P

- **Plan de Acción:** Salida del Sistema MARMINED en la que se establecen los controles a implementar para conseguir la mitigación de los riesgos de TIC luego que hayan pasado por la correspondiente evaluación.
- **Prioridad:** Anterioridad de una cosa respecto de otra.
- **Proactivo:** Hacer una acción antes de que suceda algún evento, desde el plano personal se refiere a estar preparado contra los sucesos de la vida misma.

- **Prototipo:** Primer ejemplar de alguna cosa que se toma como modelo para crear otros de la misma clase.

S

- **Servicios de TIC:** Son aplicaciones informáticas y funciones gerenciales que se valen de TIC para ejecutarse (o llevarse a cabo), en las que se produce un importante flujo de datos en doble dirección. Son, por ejemplo, las transferencias electrónicas de dinero o de documentos, la mensajería electrónica, los diversos servicios de acceso a bases de datos nacionales o internacionales, entre otros.
- **Sistema de Información:** Es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Entre esos elementos se incluyen: equipo computacional, recurso humano, datos o información fuente y los programas.
- **Software:** Software es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.
- **Spoofing:** En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

T

- **TIC:** Conjunto de Tecnologías de Información y Comunicaciones.

V

- **Vulnerabilidad:** Carácter de lo que es fácilmente atacable, desestabilizándolo.

BIBLIOGRAFÍA.

I. LIBROS

1. García, Carlos E.; *"Gerencia Informática"*; Informatik, SA de CV, Cuarta Edición, San Salvador, febrero de 2007. ISBN: 970-17-1948-3.

2. Krick, Edward V.; *"Introducción a la ingeniería y al diseño en la ingeniería";* Editorial Limusa, México, 1997. ISBN: 968-18-0176-8.

3. Ortez, Eladio Zacarías. *Así se Investiga, "Pasos para hacer una Investigación".* Clásicos Roxsil. El Salvador, 2000. ISBN 84-89899-30-4.

4. Douglas A. Lind, William G. Marchal, Samuel A. Wathen. *"Estadística aplicada a los negocios y a la economía"*, Editorial McGraw-Hill 2005, México. ISBN 970-10-4834-2.

5. Taylor, George A., *"Ingeniería Económica";* Editorial Limusa, Segunda Edición, México, 1991. ISBN: 968-18-0096-6.

6. Deitel & Deitel *"Java Cómo Programar",* Grupo Editorial Pearson, Quinta Edición 2004, España. ISBN: 97-026-0518-0.

7. Cervigon Ruckaüer, Carlos; Pressman, Roger S.; Hernández Yañez, Luis; *"Ingeniería del Software, Un enfoque practico",* Grupo Editorial McGraw-Hill, Edición 1995, España. ISBN: 84-761-5222-1.

8. Larousse.; *"Diccionario Enciclopédico";* Editorial Larousse, Colombia, 2004. ISBN: 958-8058-78-3.

9. *"Océano Uno Color",* Grupo Editorial Océano, Edición 1998, España. ISBN: 84-494-0188-7.

10. Oxford University Press; *"Diccionario de Informática";* Editorial Díaz de Santos, España, 1993. ISBN: 84-7978-068-1.

II. SITIOS WEB

1. Mi espacio "El Diagnóstico Organizacional; *elementos, métodos y técnicas*", (Página Web), <http://www.miespacio.org/cont/gi/menu.html >; 01/Julio/2009.

2. Delloite "inteligencia en riesgo", (Página Web), <http://www.deloitte.com/dtt/article/0,1002,cid%253D163583,00.html>; 01/Julio/2009.

3. Security Art Work, "Seguridad y riesgos en las TIC (IV): Proceso de Administración del Riesgo", (Página Web), <http://www.securityartwork.es/2009/01/30/seguridad-y-riesgos-en-las-tic-iv-proceso-de-administracion-del-riesgo/ >; 04/Julio/2009.

4. The free dictionary by Farlex "Conceptos y definiciones", (Página Web), <http://es.thefreedictionary.com/>; 15/agosto/2009.

5. INACAP, "Metodología de Investigación", <http://www.angelfire.com/emo/tomaustin/Met/metinacap.htm>, 28-03-2009

6. Asemex, "Que es administración de riesgos", (documento web), 2008 <http://201.158.1.169/agroasemex/index.php/seguro-reaseguro/administracion-riesgos-agropecuarios/que-es-administracion-riesgos.html>; 27-03-2009

III. DOCUMENTOS ELECTRÓNICOS

1. Banco Hipotecario; "Ley de impuestos sobre la renta" (documento pdf), <http://www.bancohipotecario.com.sv/Red_Hipotecario/Asesor_Legal/Ley_de_impuesto_sobre_la_renta_de_El_Salvador.pdf>, 31/Marzo/2009.

2. NIST, "Guía de planes de contingencia para sistemas de información tecnologías" (documento pdf), <http://www.nist.org/nist_plugins/content/content.php?content.40>, 3/Abril/2009.

3. Fernando Izquierdo Duarte, "Administración de Riesgos de TI" (presentación), <http://www.felaban.com/pdf/fernando_izquierdo_%20Administracion_de_riesgos.ppt >, 02/Abril/2009.

4. Jennifer Dennise Maxinata Cevallos, "Administración de riesgos de tecnología de información de una empresa del sector informático "(documento pdf), <http://www.dspace.espol.edu.ec/bitstream/123456789/261/1/437.pdf>, 2/Abril/2009.

5. Segovia Héctor Daniel, "Prototipo de Sistemas" (documento word), <http://tinpan.fortunecity.com/eltonjohn/914/prototipos.doc>, 18/Abril/2009.

IV. OTROS DOCUMENTOS.

1. Corte de Cuentas de la República; "Normas Técnicas de Control Interno"; Publicadas en Diario Oficial No. 180, Tomo No. 364, 29 de septiembre de 2004.

2. DOC-DIR-003 - Catalogo de servicios del MINED basado en TI al 19-06-09 (Documento Excel MINED).

3. ITIL V3 Foundation Study Guide (Documento pdf).

4. ITIL Esential Study Guide (Documento pdf).

5. Risk IT Framework (Documento pdf).

6. COBIT4.1 OVERVIEW (Documento pdf).

7. Mapping ITILV3 With COBIT (Documento pdf).

ANEXOS

ANEXO 1A. CRITERIOS DE MEDICIÓN DE RIESGO (Tomado de NIST 800-30)

Matriz de evaluación del riesgo para definir el nivel de riesgo en función de la probabilidad de ocurrencia de una amenaza y su impacto.

Probabilidad de la amenaza	Impacto		
	Bajo (10)	Moderado (50)	Alto (100)
Alta (1.0)	Bajo 10 x 1.0 = 10	Moderado 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Media (0.5)	Bajo 10 x 0.5 = 5	Moderado 50 x 0.5 = 25	Moderado 100 x 0.5 = 50
Baja (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10

Cuadro: Matriz del evaluación del riesgo. *Fuente:* Dirección de Informática del Ministerio de Educación.

Nivel de Riesgo	Descripción y acciones necesarias
Alto	Si una observación o hallazgo es evaluado como un riesgo alto, existe una gran de necesidad de acciones correctivas. Un sistema existente puede seguir operando, pero el plan de acción correctivo debe ser implementado lo más pronto posible.
Moderado	Si una observación o hallazgo es evaluado como un riesgo moderado, acciones correctivas son necesarias y un plan o solución debe desarrollarse para incorporar estas acciones dentro de un período razonable de tiempo.
Bajo	Si una observación o hallazgo es evaluado como un riesgo bajo, la dirección junto con sus gerencias deberá decidir si implementa acciones correctivas o acepta el riesgo.

Cuadro: Descripción del Impacto del Riesgo. *Fuente:* Dirección de Informática del Ministerio de Educación.

ANEXO 1B. RESULTADO PARCIAL DE LA EVALUACIÓN DE ANÁLISIS DE IMPACTO 2008[35].

No.	Nombre del Servicio TI	Gerencia a la que pertenece	Cantidad de Procesos Críticos Dependientes	Tiempo Máximo de Suspensión Promedio (En Horas)	Porcentaje de Criticidad	Nivel de Impacto
1	*Administración de Redes*	*Infraestructura Tecnológica*	222	4.9	95%	*Alto*
2	*Atención a usuarios in situ de hardware y software*	*Atención a Usuarios*	170	4.6	73%	*Alto*
3	*Servicios de impresión*	*Atención a Usuarios*	167	5.4	72%	*Alto*
4	*Administración de la infraestructura central de correo electrónico*	*Infraestructura Tecnológica*	89	5.9	38%	*Medio*
5	*Reparación y mantenimiento de equipos de cómputo (correctivo, preventivo y gestión de garantías)*	*Atención a Usuarios*	74	11.3	32%	*Medio*
6	*Rediseño de la capa de presentación del módulo UACI. (Sistemas Administrativos y Financieros - SIAP - 2008)*	*Sistemas*	44	7.7	19%	*Bajo*
7	*Soporte técnico a sistemas*	*Sistemas*	42	7	18%	*Bajo*
8	*Administración de Servidores*	*Infraestructura Tecnológica*	41	4	18%	*Bajo*
9	*Instalación y Actualización de programas en uso*	*Atención a Usuarios*	41	7.1	18%	*Bajo*
10	*Sistema SAFI*	*Sistemas*	20	3.9	9%	*Bajo*
11	*Sistema SIRH*	*Sistemas*	16	3.6	7%	*Bajo*
12	*Administración de Seguridad*	*Infraestructura Tecnológica*	13	2.3	6%	*Bajo*
13	*Pago a Cuenta Programa EDUCO*	*Sistemas*	12	4	5%	*Bajo*
14	*Sistema de Liquidación SMAEL*	*Sistemas*	10	11.8	4%	*Bajo*
15	*SMAEL 2004*	*Sistemas*	9	6.9	4%	*Bajo*
16	*Transferencia EDUCO*	*Sistemas*	9	6.1	4%	*Bajo*
17	*CENSO 2008*	*Sistemas*	8	5.5	3%	*Bajo*
18	*Sistema de Registro Académico Institucional, módulo Matricula.*	*Sistemas*	7	6.1	3%	*Bajo*
19	*Sistema de Becas*	*Sistemas*	6	11	3%	*Bajo*
20	*Escalafón EDUCO*	*Sistemas*	5	4	2%	*Bajo*

[35] **Cuadro:** Evaluación Análisis de Impacto 2008. *Fuente:* Dirección de Informática, Ministerio de Educación.

ANEXO 1C. FORMATO DE MATRIZ DE EVALUACIÓN DE RIESGOS A LOS SERVICIOS BASADOS EN TECNOLOGÍA DE LA INFORMACIÓN.

MATRIZ DE EVALUACIÓN DE RIESGOS

DOCUMENTO EVALUADO: Portafolio de servicios.

UNIDAD ORGANIZATIVA: Gerencia de Infraestructura Tecnológica.

Actividades /Servicios	**Amenazas**	**Vulnerabilidad**	**Probabilidad**	**Controles**	**Impacto**	**Riesgo**
Correo Electrónico	SPAM	BAJA	*Menor de 1%*	*Herramienta de Filtrado McAfee*	ALTO	BAJO
	Fallo de Servidores	BAJA	Menor de 1%	Herramienta de Monitoreo de Infraestructura de Servidores	ALTO	BAJO
	Fallo de Unidad de Almacenamiento.	BAJA	Menor de 1%	Diseño redundante	ALTO	BAJO
	Fallo de red de datos.	ALTA	Mayor de 50%	Mantenimiento preventivo y correctivo.	ALTO	ALTO
Red de datos	Obsolescencia	ALTA	Mayor de 50%	Mantenimiento preventivo y correctivo.	ALTO	ALTO
Reparación de equipos	Falta de repuestos	ALTA	Mayor del 50%	Contrato de mantenimiento preventivo y correctivo.	MEDIO	MODERADO

ANEXO 2.

UNIVERSIDAD DE EL SALVADOR, FACULTAD DE INGENIERÍA Y ARQUITECTURA, ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS.

ENCUESTA DIRIGIDA A PERSONAL DE INFORMÁTICA

Objetivo: Conocer la situación actual de la utilización de metodologías de administración de riesgos de tecnologías de información y comunicaciones en instituciones de gobierno que pertenecen a la zona metropolitana y alrededores de San Salvador y que cuentan con una metodología de administración de riesgos de TIC.

Código: _____

Indicaciones:

Parte I, II y III. Marque con una X la respuesta que considere pertinente; en algunos casos complemente, explique u ordene las opciones según el grado de importancia de la pregunta en cuestión.

Parte I.

1. ¿Conoce usted alguna metodología de administración de riesgos de TIC?

   Sí_____ Mencione su(s) nombre(s):_____
   No____

2. ¿Existe una unidad o entidad organizativa que administre los riesgos de las TIC?

   Sí_____ ¿Cuál es su nombre?_____
   No_____

3. ¿Cómo administran los riesgos de las TIC en esta institución?

   Metodología _____ Políticas Internas _____
   Normas _____ Manuales de Procedimientos _____
   Otros: _____

4. ¿Qué beneficios le ha aportado a su institución el aplicar este mecanismo?

   Mayor Eficiencia_____ Mayor Productividad_____ Buena Imagen _____

   Mayor Calidad _____ Mayor Seguridad _____ Mayor Integridad _____

   Otros: _____

5. ¿Qué grado de eficiencia considera usted que poseen las TIC si se emplea una adecuada administración de riesgos de TIC?

   100%_____ 75%_____ 50%____ 25%_____

6. ¿Poseen planes de contingencias en caso de fallos de las TIC?

   Sí_____ No_____

Parte II.

7. ¿Tienen un registro o bitácora de la frecuencia de los fallos en las TIC?

   Sí_____ No_____

8. ¿Cuántos sistemas se administran en la unidad informática de la institución?

   0-10_____ 11-30_____ 31-50_____ 51-70_____ 71 ó más_____

9. ¿Cuántos equipos tienen bajo su administración?

   0-100_____101-300_____ 301-800_____ 801-1500_____ 1500 ó más _____

10. ¿Cuántos usuarios utilizan dichos equipos?

0-200_____201-500_____ 501-1000_____ 1001-2000_____ 2001 ó más_____

11. ¿Cómo evaluaría la calidad de servicios prestados por las TIC?

    Malo _____ Regular _____ Bueno_____
    Muy bueno_____ Excelente_____

12. ¿Cada cuánto tiempo fallan los servicios prestados por las TIC?

    Menos de 10 horas_____ Más de 10 horas _____ Más de 20 horas_____
    Más de 50 horas _____ No se ha calculado _____

13. ¿Cuáles de estos son los servicios de TIC que presentan fallos más frecuentes en su institución? (Puede seleccionar más de una opción).

    Administración de Redes _____ Atención de usuarios in situ de HW y SW_____
    Servicios de Impresión _____ Infraestructura de correo electrónico _____
    Reparación de equipo _____ Soporte técnico a sistemas _____
    Admón. de servidores _____ Instalación y actualización de software _____

14. ¿Cuáles son las causas más comunes de fallos de las TIC en la institución?

    De origen natural _____ Provocados por ataques intencionados _____

    De origen industrial _____ Provocados por errores y fallos no intencionados _____

15. De los siguientes rubros de TIC, establezca un orden de los que presentan fallos más repetitivos en la institución (1: menos fallos; 5: más fallos).

    Hardware _____ Instalaciones y configuraciones _____
    Redes de comunicaciones _____ Soportes de información _____
    Software _____

16. De los siguientes rubros de TIC, establezca un orden de importancia de los rubros de TIC para la institución (1: menos importante; 5: más importante).

    Hardware _____ Instalaciones y configuraciones _____
    Redes de comunicaciones _____ Soportes de información _____
    Software _____

Parte III.

17. ¿Tienen un registro de costos o gastos que se han incurrido por los fallos en TIC?

    Sí_____ No_____
    ¿Podría brindarnos un aproximado anual de estos gastos?_____

18. ¿Cuáles son los rubros de TIC que han tenido mayor inversión en los últimos años?

    Hardware _____ Instalaciones y configuraciones _____
    Redes de comunicaciones _____ Soportes de información _____
    Software _____ No sabe _____

19. ¿Cuáles son los rubros de TIC que han tenido más gastos por fallos en los últimos años?

    Hardware _____ Instalaciones y configuraciones _____
    Redes de comunicaciones _____ Soportes de información _____
    Software _____ No sabe _____

* *Muchas gracias por su colaboración* *

ANEXO 3.

UNIVERSIDAD DE EL SALVADOR, FACULTAD DE INGENIERÍA Y ARQUITECTURA, ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS.

GUÍA DE ENTREVISTA PARA EL PERSONAL ENCARGADO DE LA ADMINISTRACIÓN DE RIESGOS DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (TIC) DEL MINISTERIO DE EDUCACIÓN.

Objetivo: Conocer la situación actual del Ministerio de Educación referente a la administración de riesgos de Tecnologías de Información y Comunicaciones (TIC) relacionados a los aspectos económicos, calidad de servicio de las TIC y procedimentales.

Indicación: Por favor, responda en forma objetiva, pues de ella depende la validez de los resultados de esta investigación.

Lugar: _____ Fecha: _____

Entrevistado: _____

PARTE I

1. ¿Cuál es el nombre de la Unidad Organizativa que administra los riesgos de administración de riesgos de TIC?
2. ¿De qué manera se administran los riesgos de TIC?
3. ¿Qué beneficios le ha aportado a su institución el aplicar este mecanismo de administración de riesgos de TIC?
4. ¿Qué grado de eficiencia considera usted que poseen las TIC si se emplea una adecuada administración de riesgos de TIC?
5. ¿Poseen planes de contingencias en caso de fallos de las TIC?
6. ¿Cuáles son las áreas que involucran los planes de contingencia?

PARTE II

1. ¿Tienen un registro o bitácora de la frecuencia de los fallos en las TIC?
2. ¿Cuántos sistemas se administran en la unidad informática de la institución?
3. ¿Cuántos equipos tienen bajo su administración?
4. ¿Cuántos usuarios utilizan dichos equipos?
5. ¿Cómo evaluaría la calidad de servicios prestados por las TIC?
6. ¿Cada cuánto tiempo fallan los servicios prestados por las TIC?
7. ¿Cuáles son los servicios de TIC que presentan fallos más frecuentes?
8. ¿Cuáles son las causas más comunes de fallos de las TIC en la institución?
9. ¿Cuáles son los rubros de TIC más importantes para la institución?

PARTE III

1. ¿Tienen un registro de costos o gastos que se han incurrido por los fallos en TIC?
2. ¿Cuáles son los rubros de TIC que han tenido mayor inversión en los últimos años?
3. ¿Cuáles son los rubros de TIC que han tenido más gastos por fallos en los últimos años?

ANEXO 4.

UNIVERSIDAD DE EL SALVADOR, FACULTAD DE INGENIERÍA Y ARQUITECTURA, ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS.

GUÍA DE OBSERVACIÓN PARA EL DIAGNÓSTICO INTERNO Y RECOPILACIÓN DE REQUERIMIENTOS PARA EL DISEÑO DE LA METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (TIC) PARA EL MINISTERIO DE EDUCACIÓN.

Objetivo: Observar las características particulares de las tecnologías de información y comunicaciones en el MINED para poder verificar el estado, la calidad de servicios y la cantidad de infraestructura en la institución para descubrir los riesgos que les afectan.

Observador(a):_____
Lugar: _____Fecha: _____
Hora de observación: _____

Variables a observar:

- Manuales de procedimientos.
- Normas utilizadas.
- Personal encargado.
- Beneficios prestados por el uso de la metodología
- Fallos de servicios de TIC
- Grado de aplicabilidad de las TIC
- Beneficios de TIC.
- Productividad.
- Eficiencia y efectividad de servicios de TIC.
- Soporte a los servicios de TIC.
- Costos por fallos de TIC.
- Inversión en TIC.

Para realizar el diagnóstico interno en el MINED se utilizará la técnica "Observación".

El objeto de estudio son las tecnologías de información y comunicaciones, las cuales incluyen el hardware, software, soportes de información, la seguridad física, instalaciones físicas, los usuarios de los sistemas, redes de comunicación, servicios prestados, equipamiento auxiliar y requerimientos para el funcionamiento normal de los sistemas.

La observación se registrará con anotaciones personales, fichas y record anecdóticos. Además de la clásica observación simple y crítica respecto del objeto de estudio.

Las TIC a observar en el Ministerio de Educación son:

Servicios

- Anónimo (sin requerir identificación del usuario)
- Al público en general (sin relación contractual)
- A usuarios externos (bajo una relación contractual)
- Interno (usuarios y medios de la propia organización)
- Contratado a terceros (se presta con medios ajenos)
- World Wide Web
- Acceso remoto a cuenta local
- Correo electrónico
- Almacenamiento de ficheros
- Transferencia de ficheros
- Intercambio electrónico de datos
- Gestión de identidades
- Gestión de privilegios
- Infraestructura de clave pública.

Aplicaciones (software)

- Desarrollo propio (in house)
- Desarrollo a medida (subcontratado)
- Estándar (off the shelf)
- Navegador web
- Servidor de aplicaciones
- Cliente de correo electrónico
- Servidor de ficheros
- Sistema de gestión de bases de datos
- Ofimática
- Anti virus
- Sistema operativo
- Servidor de terminales
- Sistema de backup

Equipo informático

- Grandes equipos
- Equipos medios
- Informática móvil
- Agendas electrónicas
- Periféricos
- Medios de impresión
- Escáneres

- Dispositivos criptográficos
- Módems
- Concentradores
- Conmutadores
- Encaminadores
- Pasarelas
- Cortafuegos
- Punto de acceso wireless
- Centralita telefónica

Redes de comunicaciones

- Red telefónica
- ADSL
- Punto a punto
- Red inalámbrica
- Red local
- Internet
- Red privada virtual

Soportes de información

- Electrónicos
- Discos
- Almacenamiento en red
- Disquetes
- CD-ROM
- Dispositivos USB
- DVD
- Cinta magnética
- Tarjetas de memoria
- Tarjetas inteligentes
- Material impreso
- Cinta de papel

Equipamiento auxiliar

- Fuentes de alimentación
- Sistemas de alimentación ininterrumpida
- Equipos de climatización
- Cableado
- Robots de cintas
- Suministros esenciales
- Mobiliario: armarios, etc.
- Cajas fuertes

Instalaciones

- Edificio
- Local
- Plataformas móviles
- Canalización

Personal

- Usuarios externos
- Usuarios internos
- Operadores
- Administradores de sistemas
- Administradores de comunicaciones
- Administradores de BBDD
- Desarrolladores
- Outsourcing
- Proveedores

ANEXO 5

Factores:

- Riesgos críticos
- Riesgos no críticos
- Riesgos genéricos.

Factores	Ponderaciones	Subfactores	Ponderaciones
Riesgos Críticos	81.66%	Riesgos críticos de alto impacto	75%
		Riesgos críticos de mediano impacto	80%
		Riesgos críticos de bajo impacto	90%
Riesgos no Críticos	83.33%	Riesgos no críticos de alto impacto	75%
		Riesgos no críticos de mediano impacto	85%
		Riesgos no críticos de bajo impacto	90%
Riesgos Genéricos	62.5%	Terremotos	50%
		Inundaciones	75%
		Incendios	60%
		Riesgos Sociales	65%
Total de confiabilidad	76%		

Tabla de factores y ponderaciones de confiabilidad de la metodología propuesta.

ANEXO 6. ESQUEMA DEL REPORTE DE EVALUACIÓN DE RIESGOS.

Resumen Ejecutivo

I. Introducción.

- Propósito.
- Ámbito de aplicación de la evaluación de riesgos.

II. Responsables de la evaluación de riesgos.

III. Amenazas.

Presentar la lista de amenazas potenciales, así como también las fuentes de las mismas aplicables al Sistema de evaluación.

IV. Resultados de la evaluación de riesgos.

Listado de las observaciones. Cada observación deberá incluir:

- Fuente de la amenaza relacionada con la observación.
- Identificación de los controles para reducción de vulnerabilidades.
- Determinación de riesgo.
- Análisis de impacto.
- Recomendación de controles alternativos para reducir el riesgo.

V. Resumen.

Se especificará el número total de observaciones, un resumen de las mismas, los niveles de riesgos asociados y la recomendación de nuevos controles.

APÉNDICES

A. Manual de Usuario

"METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TIC PARA EL MINED"

A. INTRODUCCIÓN

Este Manual del Usuario ha sido diseñado con el propósito de facilitar al personal de la Gerencia de Normas y Calidad de la Unidad Informática del Ministerio de Educación el manejo del Prototipo MARMINED[36] en lo que respecta a la realización de los cálculos de evaluación de riesgos que necesite realizar.

El Prototipo de software "MARMINED" se ha desarrollado como una herramienta complementaria de la Metodología de Administración de Riesgos de TIC, que lleva el mismo nombre, con el fin de facilitar su aplicación mediante la automatización de varias de sus funciones.

Este documento contiene información acerca de todas las operaciones básicas de las pantallas del Prototipo MARMINED. Se presenta una visión completa sobre su utilización, explicando con detalle su funcionamiento e incluyendo imágenes útiles para el seguimiento de las explicaciones.

El Manual de Usuario del Prototipo MARMINED proporciona el debido soporte al usuario para que éste pueda obtener el máximo provecho de las facilidades que ofrece, agilizando la Administración de los Riesgos de TIC.

B. OBJETIVOS DEL MANUAL DE USUARIO.

Objetivo General:

- Proporcionar al usuario de MARMINED una guía práctica sobre las principales características de la utilización del software.

Objetivos Específicos:

- Proporcionar los pasos necesarios para utilizar correctamente cada una de las pantallas con que cuenta el software para garantizar la obtención de los resultados esperados.

- Proporcionar una descripción acerca del uso correcto de las consultas del software, para facilitar su operación.

- Describir la forma de acceder a los reportes que genera el software.

C. INICIO DEL SISTEMA

Una vez instalados los archivos .war y el script .sql entregados al MINED se observará la siguiente pantalla en el navegador web.

[36] El Prototipo de software lleva por nombre "MARMINED", y con el propósito de evitar confusiones es importante aclarar que cada vez que en el Manual de Usuario se cite ese nombre, se hará referencia únicamente al Prototipo en cuestión.

Menú Principal.

Menú:

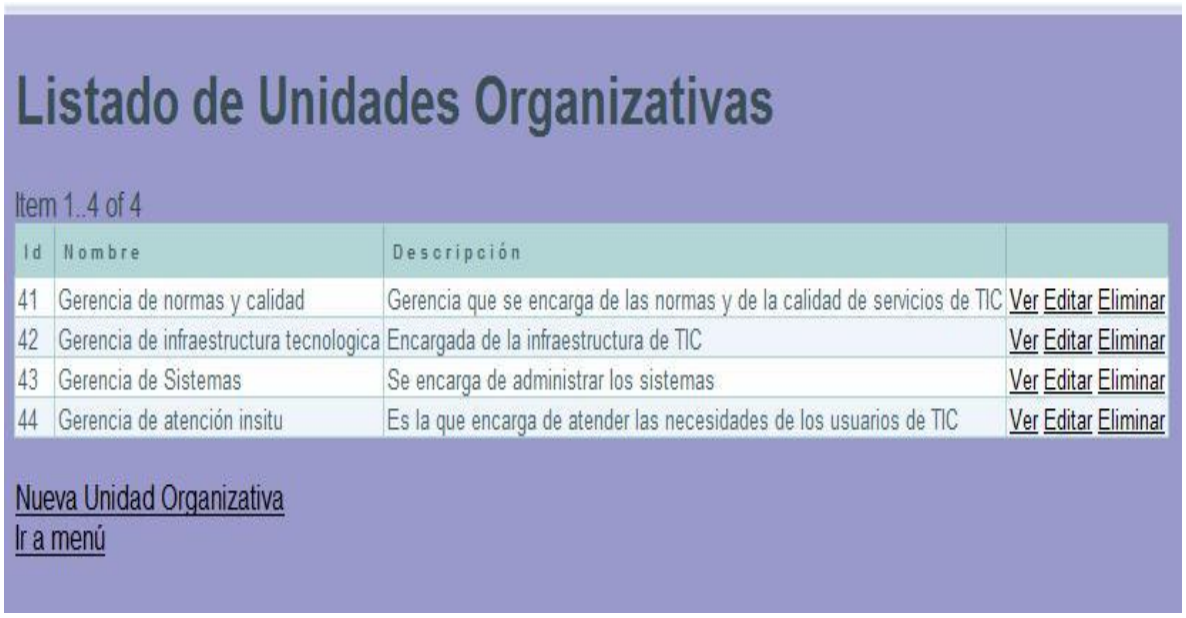
Como se puede observar, en la pantalla se muestra el Menú Principal, en el cual a su vez cada opción muestra un menú desplegable.

Ejemplo: para la opción *Administración de Catálogos* se tiene el menú desplegable:

- Unidad Organizativa.
- Tipo de Fuente de Amenaza.
- Usuario.

Al dar clic en cualquier botón nos envía a la pantalla de ingreso de la opción seleccionada.

Unidad Organizativa.



Al dar clic en la opción *Unidad Organizativa* se desplegará la siguiente pantalla:

Se presentará un Listado de las Unidades Organizativas, el cual tendrá lo siguiente:

- Un vínculo *Ver:* A través del cual se puede consultar el registro.
- Un vínculo E*ditar*: A través del cual se puede modificar el registro.
- Un vínculo *Eliminar:* A través del cual se puede eliminar el registro.
- Un vínculo *Nueva Unidad Organizativa:* Al dar clic en este vínculo abre una pantalla para ingresar una nueva Unidad Organizativa.
- Un vínculo *Ir a menú:* Al dar clic en este vínculo el usuario regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

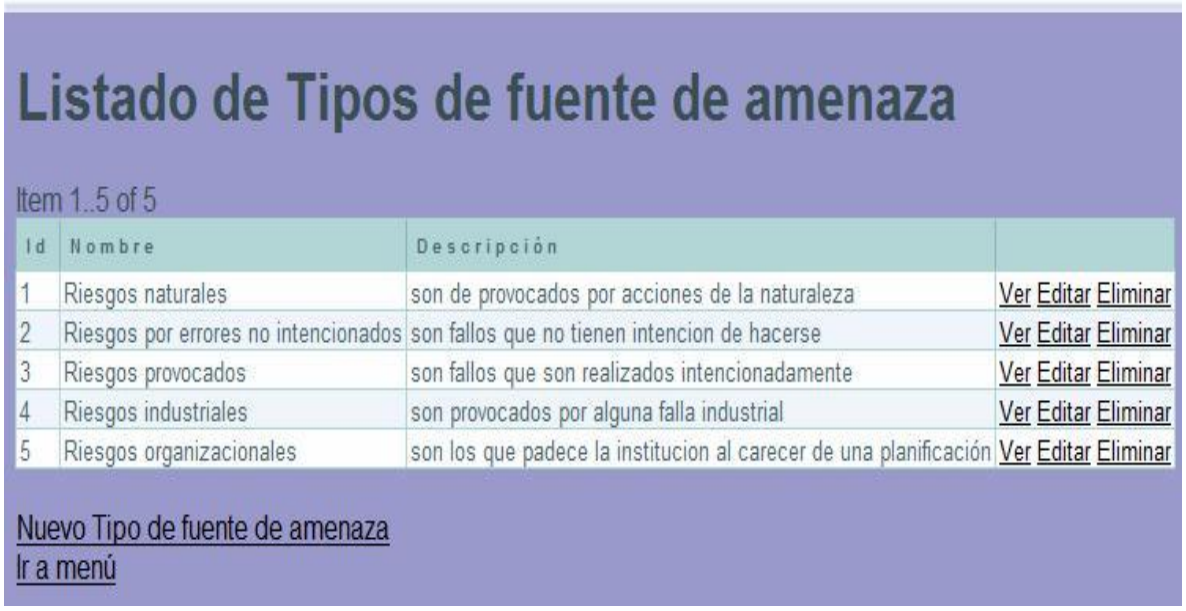
Esta es la pantalla donde se muestra cómo hacer la gestión de Unidad Organizativa.

Donde:

- ID: Código de la nueva Unidad Organizativa.
- Nombre: El nombre a ingresar de la Unidad Organizativa.
- Descripción: El detalle de la Unidad Organizativa.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar Listado de Unidades Organizativas:* Al dar clic en el vínculo regresa a la pantalla de Unidad Organizativa.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Tipo Fuente de Amenaza.

Si el usuario da clic en la opción *Tipo de Fuente de Amenaza* se desplegará la siguiente pantalla:



Se presentará un listado de los Tipos de fuente de amenazas el cual contendrá lo siguiente:

- Un vínculo *Ver:* Por medio del cual se puede consultar el registro.
- Un vínculo *Editar:* Por medio del cual se puede modificar el registro.
- Un vínculo *Eliminar:* Por medio del cual se puede eliminar el registro.
- Un vínculo *Nuevo Tipo de Fuente de Amenaza:* Al dar clic en el vínculo abre una pantalla para ingresar un nuevo tipo de fuente de amenaza, el cual se muestra en el siguiente apartado.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

Esta es la pantalla donde se muestra cómo hacer la gestión de Tipo de Fuente de Amenaza.

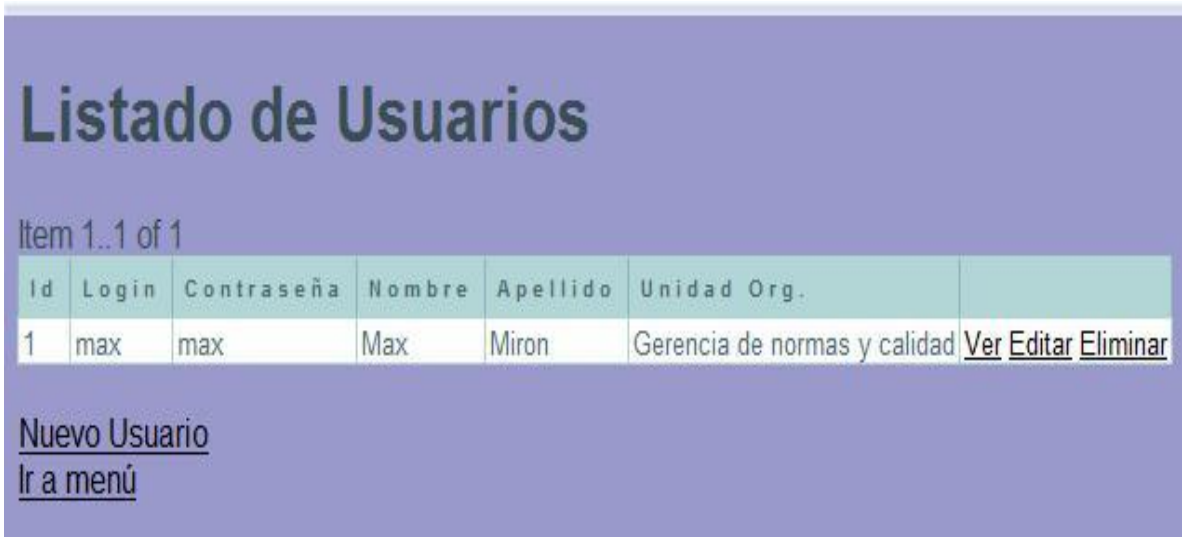
.

Donde:

- ID: Código del nuevo Tipo de Fuente de Amenaza.
- Nombre: El nombre a ingresar del tipo de fuente de amenaza.
- Descripción: El detalle de lo que es el tipo de fuente de amenaza.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar Listado de Tipos de Fuente de amenazas:* Al dar clic en el vínculo regresa a la pantalla de Tipo de Fuente de Amenaza.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Usuario.

Al dar clic en la opción *Usuario* se desplegará la siguiente pantalla:



Se presentará un Listado de los Usuarios el cual contendrá lo siguiente:

- Un vínculo *Ver:* A través del cual se puede consultar el registro.
- Un vínculo *Editar:* A través del cual se puede modificar el registro.
- Un vínculo *Eliminar:* A través del cual se puede eliminar el registro.
- Un vínculo *Nuevo Usuario:* Al dar clic en el vínculo abre una pantalla para ingresar un nuevo usuario.
- Un vínculo *Ir a menú*: Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

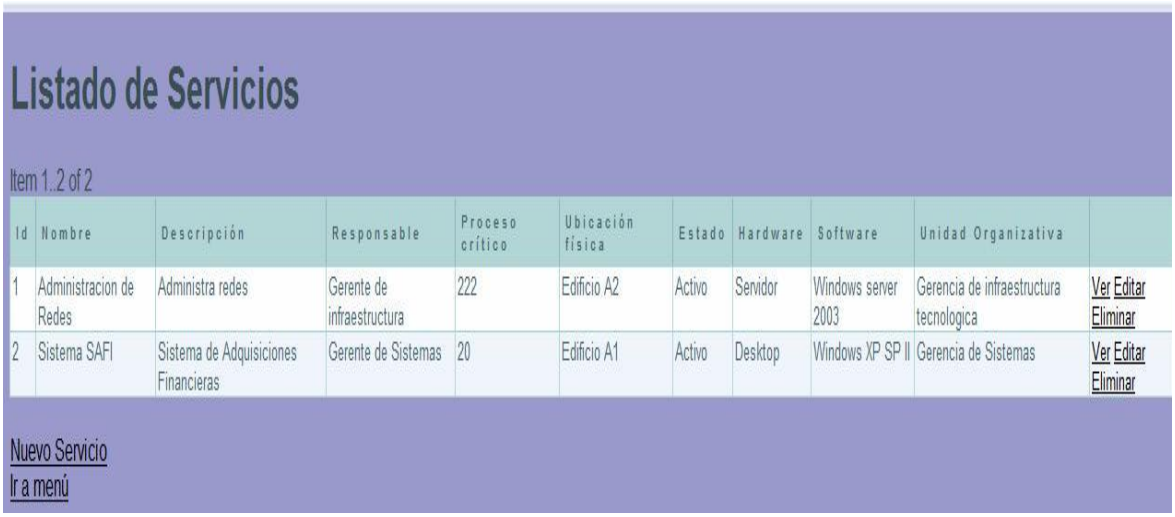
Esta es la pantalla donde se muestra cómo hacer la gestión de usuario.

Donde:

- ID: Código del nuevo usuario.
- Login: Es el nombre de usuario que tendrá en el sistema el usuario.
- Contraseña: Es la clave de acceso del usuario para acceder al sistema.
- Nombre: El nombre a ingresar del usuario.
- Apellido: El apellido de la persona que es usuario del sistema.
- Unidad Organizativa: es una lista con las unidades organizativas existentes que debe ser seleccionada.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar lista de usuarios:* Al dar clic en el vínculo regresa a la pantalla de usuario.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Servicio.

Al dar clic en la opción *Servicio,* se desplegará la siguiente pantalla:



Listado de Servicios

Item 1..2 of 2

Id	Nombre	Descripción	Responsable	Proceso crítico	Ubicación física	Estado	Hardware	Software	Unidad Organizativa	
1	Administracion de Redes	Administra redes	Gerente de infraestructura	222	Edificio A2	Activo	Servidor	Windows server 2003	Gerencia de infraestructura tecnologica	Ver Editar Eliminar
2	Sistema SAFI	Sistema de Adquisiciones Financieras	Gerente de Sistemas	20	Edificio A1	Activo	Desktop	Windows XP SP II	Gerencia de Sistemas	Ver Editar Eliminar

Nuevo Servicio
Ir a menú

Se presentará un Listado de los Servicios el cual contendrá lo siguiente:

- Un vínculo *Ver:* Mediante el cual se puede consultar el registro.
- Un vínculo *Editar:* Mediante el cual se puede modificar el registro.
- Un vínculo *Eliminar:* Mediante el cual se puede eliminar el registro.
- Un vínculo *Nuevo Servicio:* Al dar clic en el vínculo abre una pantalla para ingresar un nuevo usuario.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

Esta es la pantalla donde se muestra cómo hacer la gestión de servicios.

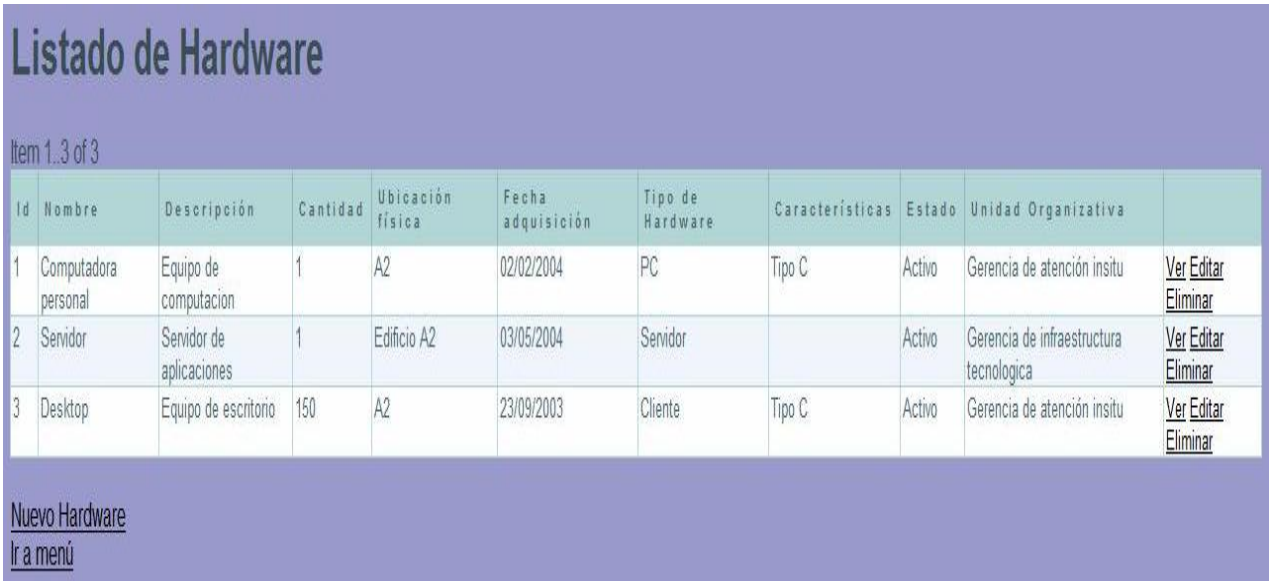
Donde:

- ID: Código del nuevo servicio.
- Nombre: El nombre a ingresar del servicio.
- Descripción: Es una descripción de lo que es el servicio.
- Responsabilidad: Es el nombre que tendrá la responsabilidad del servicio.
- Proceso crítico: Representa la cantidad de procesos críticos dependientes del servicio.
- Ubicación física: Es el lugar donde está el servicio.
- Estado: Es la que indica si se encuentra activo o inactivo.
- Hardware: Es el nombre de hardware asociado al servicio.
- Software: Es el nombre del software asociado al servicio.
- Unidad Organizativa: Es una lista con las unidades organizativas existentes que debe ser seleccionada.

- Un vínculo *Crear*: Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar lista de servicios:* Al dar clic en el vínculo regresa a la pantalla de servicio.
- Un vínculo *Ir a menú*: Al dar clic en el vínculo regresa a la pantalla del menú principal.

Hardware.

Si da clic en la opción hardware, se desplegará la siguiente pantalla:



Listado de Hardware

Item 1..3 of 3

Id	Nombre	Descripción	Cantidad	Ubicación física	Fecha adquisición	Tipo de Hardware	Características	Estado	Unidad Organizativa	
1	Computadora personal	Equipo de computacion	1	A2	02/02/2004	PC	Tipo C	Activo	Gerencia de atención insitu	Ver Editar Eliminar
2	Servidor	Servidor de aplicaciones	1	Edificio A2	03/05/2004	Servidor		Activo	Gerencia de infraestructura tecnologica	Ver Editar Eliminar
3	Desktop	Equipo de escritorio	150	A2	23/09/2003	Cliente	Tipo C	Activo	Gerencia de atención insitu	Ver Editar Eliminar

Nuevo Hardware
Ir a menú

Se presentará un Listado del Hardware el cual contendrá lo siguiente:

- Un vínculo *Ver*: Por medio del cual se puede consultar el registro.
- Un vínculo *Editar*: Por medio del cual se puede modificar el registro.
- Un vínculo *Eliminar*: Por medio del cual se puede eliminar el registro.
- Un vínculo *Nuevo Hardware*: Al dar clic en el vínculo abre una pantalla para ingresar un nuevo hardware.
- Un vínculo *Ir a menú*: Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

Esta es la pantalla donde se muestra cómo hacer la gestión de hardware.

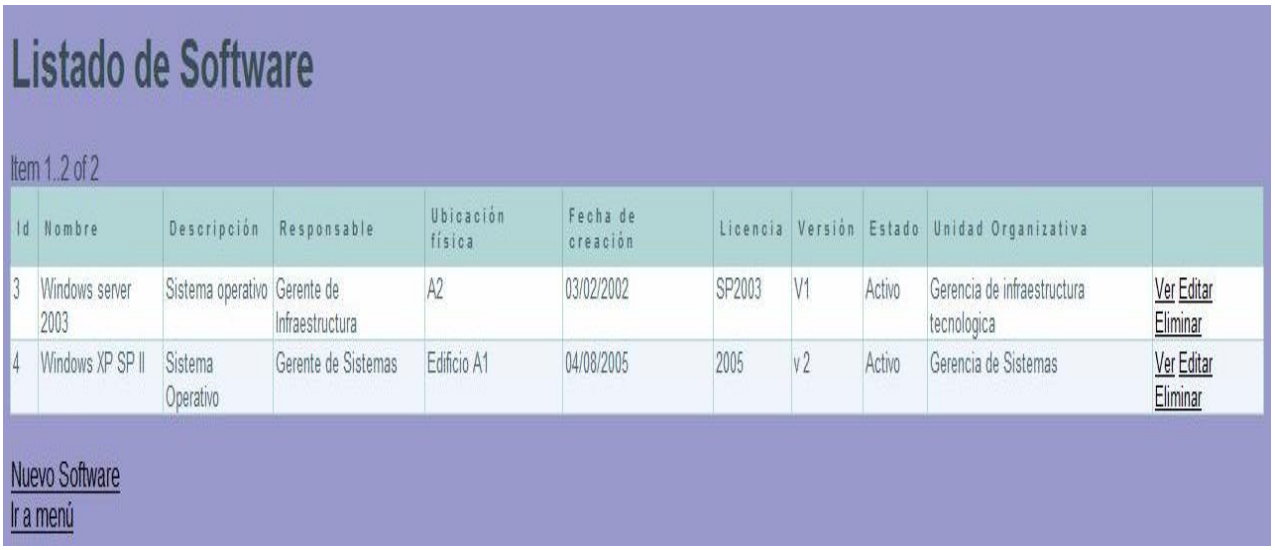
Donde:

- ID: Código del nuevo hardware.
- Nombre hardware: El nombre a ingresar del hardware.
- Descripción hardware: Es una descripción del hardware.
- Cantidad: Es el número de hardware existente del tipo y características que se está registrando.
- Ubicación física: Es el lugar donde está el hardware.
- Fecha adquisición: Es el la fecha de cuando se adquirió el hardware.
- Tipo hardware: Se refiere a que si es del tipo servidor o cliente.
- Características: Son las particularidades del hardware dependiendo de su tipo.

- Estado: Indica si se encuentra activo o inactivo.
- Unidad organizativa: Es una lista con las unidades organizativas existentes que debe ser seleccionada para especificar la Unidad Organizativa responsable de su correcto funcionamiento.
- Un vínculo *Crear*: Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar lista de hardware:* Al dar clic en el vínculo regresa a la pantalla de hardware.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Software.

Si da clic en la opción Software se desplegará la siguiente pantalla:



Se presentará un Listado del Software el cual contendrá lo siguiente:

- Un vínculo *Ver:* Mediante el cual se puede consultar el registro.
- Un vínculo *Editar:* Mediante el cual se puede modificar el registro.
- Un vínculo *Eliminar:* Mediante el cual se puede eliminar el registro.
- Un vínculo *Nuevo Software*: Al dar clic en el vínculo abre una pantalla para ingresar un nuevo software.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

Esta es la pantalla donde se muestra cómo hacer la gestión de software.

Donde:

- ID: Código del nuevo software.
- Nombre: El nombre del software a ingresar.
- Descripción: Es una descripción del software.
- Responsable: Es la Unidad Organizativa responsable del mantenimiento del software.
- Ubicación física: Es el lugar donde está instalado el software.
- Fecha adquisición: Es la fecha de la adquisición del software.
- Licencia: Es el derecho legal que autoriza el uso del software.
- Versión: Es el número de actualización del sistema.
- Estado: Indica si se encuentra activo o inactivo el software.

- Unidad Organizativa: es una lista con las unidades organizativas existentes que debe ser seleccionada.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar Listado de Software:* Al dar clic en el vínculo regresa a la pantalla de software.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Fuente de amenaza.

Si da clic en la opción fuente de amenaza desplegará la siguiente pantalla:

Se presentará un Listado de Fuentes de Amenaza el cual contendrá lo siguiente:

- Un vínculo *Ver:* El cual permite consultar el registro.
- Un vínculo *Editar:* El cual permite modificar el registro.
- Un vínculo *Eliminar:* Poder eliminar el registro.
- Un vínculo *Nueva Fuente de amenaza:* Al dar clic en el vínculo abre una pantalla para ingresar una nueva fuente de amenaza.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

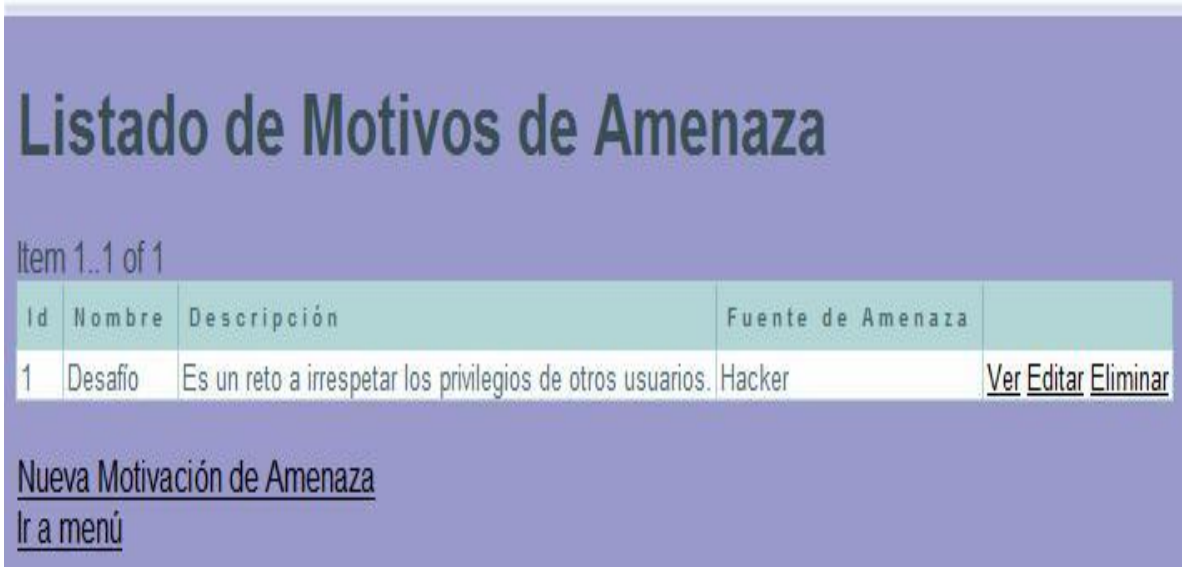
Esta es la pantalla donde se muestra cómo hacer la gestión de fuente de amenaza.

Donde:

- Nombre de fuente de amenaza: El nombre de la fuente de amenaza a ingresar.
- Descripción de fuente de amenaza: Es una breve descripción de la fuente de amenaza.
- Servicio: Es el código del servicio relacionado a la fuente de amenaza que se está registrando.
- Tipo de fuente de amenaza: Es el código del tipo de fuente de amenaza relacionado a esa fuente de amenaza.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar Listado Fuente de amenaza:* Al dar clic en el vínculo regresa a la pantalla de fuente de amenaza.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Motivación.

Al dar clic en la opción *Motivación* se desplegará la siguiente pantalla:



Se presentará un Listado de Motivos de Amenaza que contendrá lo siguiente:

- Un vínculo *Ver:* Permite consultar el registro.
- Un vínculo *Editar:* Permite modificar el registro.
- Un vínculo *Eliminar:* Permite eliminar el registro.
- Un vínculo *Nueva Motivación de Amenaza:* Al dar clic en el vínculo abre una pantalla para ingresar una nueva motivación de amenaza.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

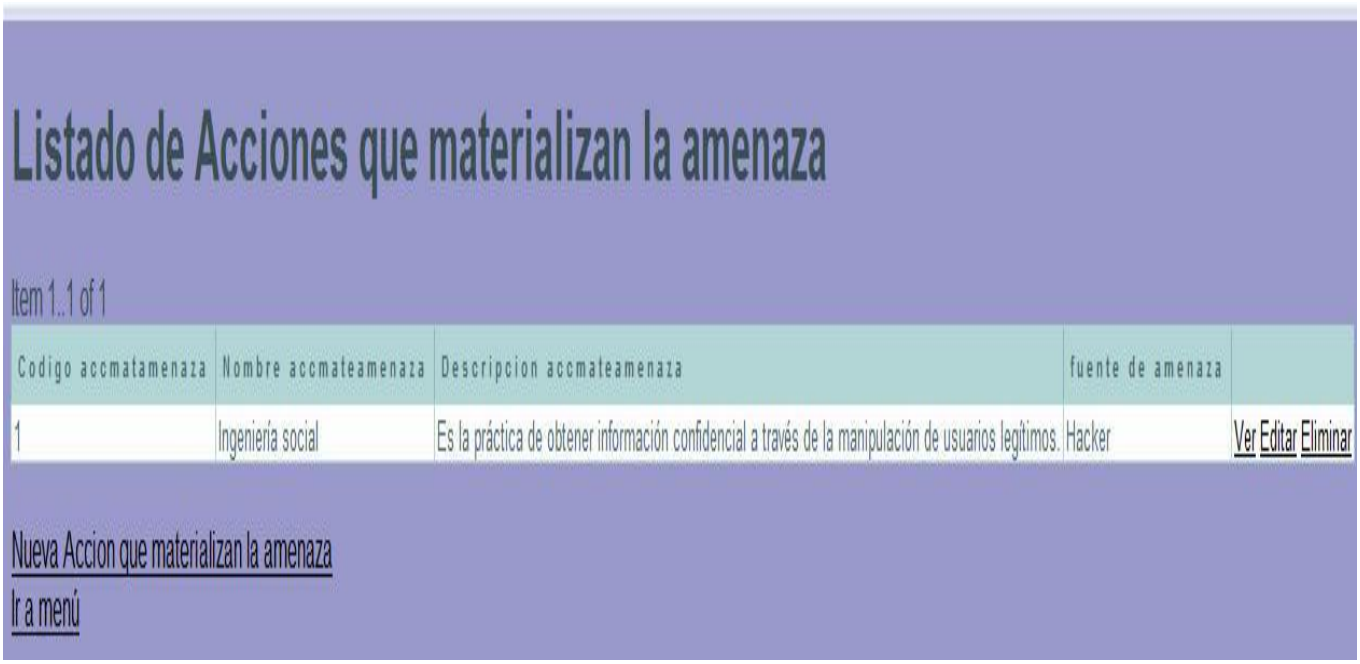
Esta es la pantalla donde se muestra cómo hacer la gestión de motivación de amenaza.

Donde:

- Nombre: El nombre a ingresar de la motivación de amenaza.
- Descripción: Es una descripción de la motivación de amenaza.
- Fuente de Amenaza: Es el nombre de la fuente de amenaza relacionada a la motivación
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar Listado de Motivaciones de Amenaza:* Al dar clic en el vínculo regresa a la pantalla de motivación de amenaza.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Acciones que materializan la amenaza.

Al dar clic en la opción *Acciones que Materializan la Amenaza* se desplegará la siguiente pantalla:



Se presentará un Listado de Acciones que materializan la amenaza, el cual tendrá lo siguiente:

- Un vínculo *Ver:* Permite consultar el registro.
- Un vínculo *Editar:* Permite modificar el registro.
- Un vínculo *Eliminar:* Permite eliminar el registro.
- Un vínculo *Nueva Acción que materializan la amenaza:* Al dar clic en el vínculo abre una pantalla para ingresar una nueva acción que materializan la amenaza.
- Un vínculo *Ir a menú*: Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

Esta es la pantalla donde se muestra cómo hacer la gestión de acciones que materializan la amenaza.

Donde:

- Nombre: El nombre a ingresar de la acción que materializan la amenaza.
- Descripción: Es una descripción de la acción que materializan la amenaza.
- Fuente de amenaza: Es el nombre de la fuente de amenaza relacionada a las acciones que materializan la amenaza
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar listado de acciones que materializan la amenaza:* Al dar clic en el vínculo regresa a la pantalla de acciones que materializan la amenaza.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Vulnerabilidades.

Si da clic en la opción *Vulnerabilidades*, se desplegará la siguiente pantalla:

Se presentará un Listado de Vulnerabilidades el cual tendrá lo siguiente:

- Un vínculo *Ver*: Permite consultar el registro.
- Un vínculo *Editar:* Permite modificar el registro.
- Un vínculo *Eliminar:* Permite eliminar el registro.
- Un vínculo *Efectuar cálculo riesgo:* calcula la evaluación del riesgo y lo guarda en el registro.
- Un vínculo *Nueva Vulnerabilidad:* Al dar clic en el vínculo abre una pantalla para ingresar una nueva vulnerabilidad.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

Esta es la pantalla donde se muestra cómo hacer la gestión de vulnerabilidad.

Donde:

- Nombre: El nombre a ingresar de la vulnerabilidad.
- Descripción: Es una descripción de la vulnerabilidad.
- Fuente de Amenaza: Es el nombre de la fuente de amenaza relacionada a la vulnerabilidad.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar Lista de Vulnerabilidades:* Al dar clic en el vínculo regresa a la pantalla de vulnerabilidad.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Control.

Al dar clic en la opción *Control* se desplegará la siguiente pantalla:

Se presentará un Listado de Controles el cual contendrá lo siguiente:

- Un vínculo *Ver:* Mediante el cual se puede consultar el registro.
- Un vínculo *Editar:* Mediante el cual se puede modificar el registro.
- Un vínculo *Eliminar:* Mediante el cual se puede eliminar el registro.
- Un vínculo *Nuevo Control:* Al dar clic en el vínculo abre una pantalla para ingresar un nuevo control.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

Pantalla de agregar, modificar y consultar.

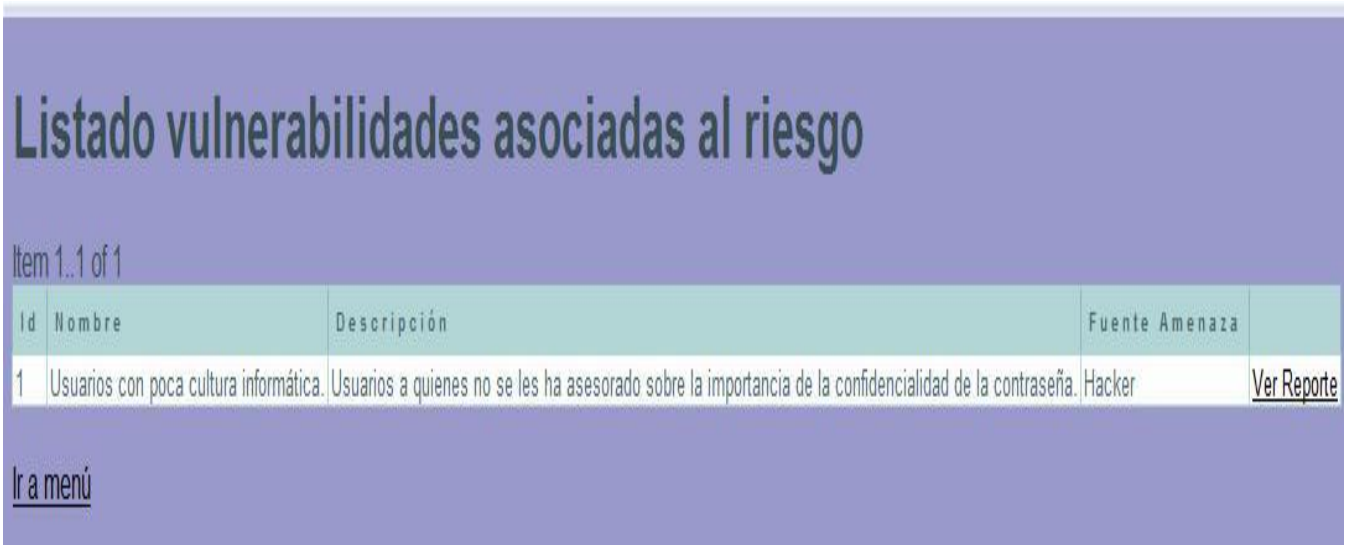
Esta es la pantalla donde se muestra cómo hacer la gestión de control.

Donde:

- Nombre control: El nombre a ingresar del control.
- Descripción: Es una descripción del control.
- Vulnerabilidad: Es el código de la vulnerabilidad relacionada a el control.
- Un vínculo *Crear:* Al hacer clic se agrega la información al registro de la base de datos.
- Un vínculo *Mostrar listado de controles:* Al dar clic en el vínculo regresa a la pantalla de control.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.

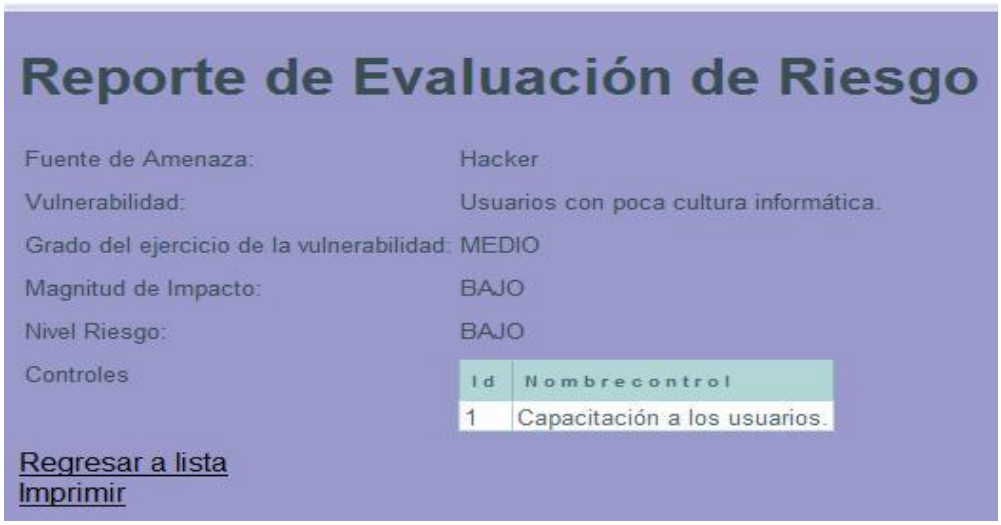
Riesgo.

Al dar clic en la opción *Reportes* se desplegará la siguiente pantalla:



Se presentará un Listado de vulnerabilidades asociadas al riesgo, el cual tendrá lo siguiente:

- Un vínculo *Ver Reporte:* Muestra el reporte de evaluación de riesgo.
- Un vínculo *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del menú principal.
- La pantalla que se muestra en la página siguiente corresponde al Reporte de Evaluación Riesgo.



Reporte de Evaluación de Riesgo

Fuente de Amenaza: Hacker

Vulnerabilidad: Usuarios con poca cultura informática.

Grado del ejercicio de la vulnerabilidad: MEDIO

Magnitud de Impacto: BAJO

Nivel Riesgo: BAJO

Controles

Id	Nombrecontrol
1	Capacitación a los usuarios.

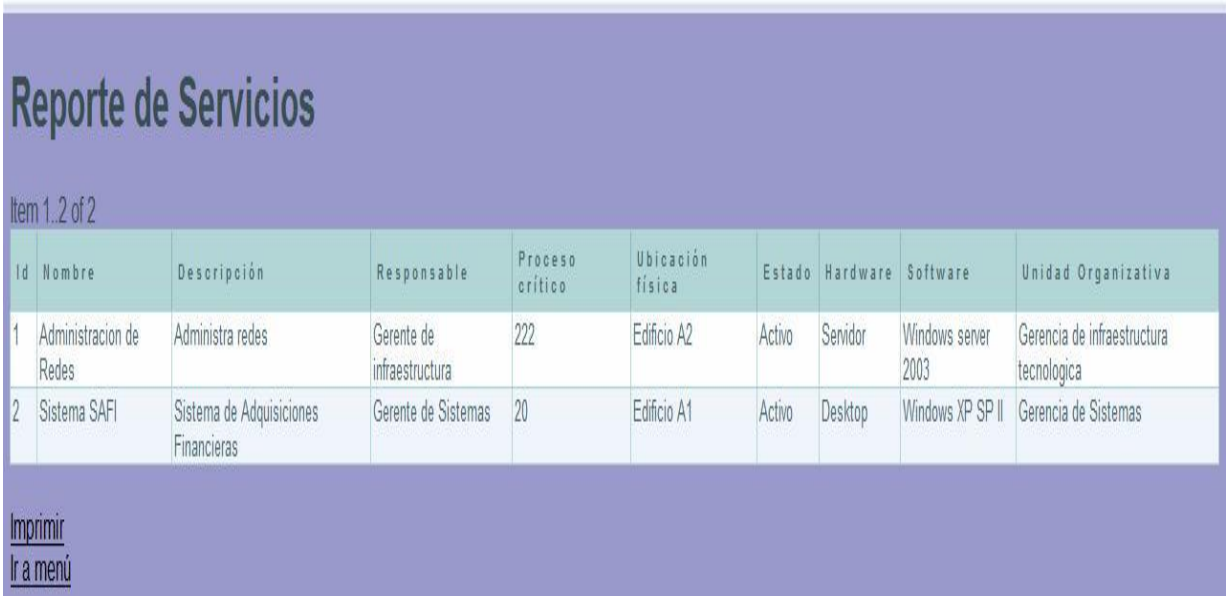
Regresar a lista
Imprimir

El cual contiene lo siguiente:

- Un vínculo *Regresar a lista* de vulnerabilidades asociadas al riesgo: Al dar clic regresa a la pantalla riesgo.
- Un vínculo *Imprimir:* Al dar clic en el vínculo imprime el reporte.

Reporte de Servicios.

Si da clic en la opción Reporte de Servicios se desplegará la siguiente pantalla:



Reporte de Servicios

Item 1..2 of 2

Id	Nombre	Descripción	Responsable	Proceso crítico	Ubicación física	Estado	Hardware	Software	Unidad Organizativa
1	Administracion de Redes	Administra redes	Gerente de infraestructura	222	Edificio A2	Activo	Servidor	Windows server 2003	Gerencia de infraestructura tecnologica
2	Sistema SAFI	Sistema de Adquisiciones Financieras	Gerente de Sistemas	20	Edificio A1	Activo	Desktop	Windows XP SP II	Gerencia de Sistemas

Imprimir
Ir a menú

Se presentará un Reporte de Servicios, el cual contendrá los siguientes vínculos:

- *Imprimir:* Imprime el Reporte de Servicios.
- *Ir a menú:* Al dar clic en el vínculo regresa a la pantalla del Menú Principal.

B. Manual Técnico

"METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS DE TIC PARA EL MINED"

A. INTRODUCCION.

El presente manual técnico contiene información clasificada sobre la estructura del Prototipo de Software de la "Metodología de Administración de Riesgos de TIC para el MINED" (MARMINED)[37] y que se será de mucha importancia ya que provee una descripción de las principales características técnicas que posee, la infraestructura mínima para su instalación y las especificaciones de su arquitectura y de la base de datos.

En las especificaciones de la base de datos se detallan las tablas y campos que la conforman, el diseño lógico y físico, el diccionario de datos y los procedimientos almacenados con su respectivo nombre, descripción y su respectivo código.

Este manual está orientado al personal encargado de proporcionar mantenimiento a MARMINED, entre los cuales podrían ser los programadores y el administrador de MARMINED.

[37]El nombre del Prototipo de Software es la abreviatura de la metodología o sea MARMINED, por lo cual en el presente manual cuando se mencione MARMINED nos estaremos refiriendo al Prototipo de Software.

B. OBJETIVOS DEL MANUAL.

Objetivo General:

- Proporcionar al administrador de MARMINED y programadores una guía práctica sobre las principales características técnicas que posee MARMINED.

Objetivos Específicos:

- Proporcionar la estructura de los componentes utilizados en la implementación de MARMINED

- Proporcionar información de los componentes o módulos para que sirva de apoyo para el administrador y los programadores.

- Analizar la arquitectura de MARMINED.

- Elaborar una descripción de los elementos y la base de datos que aseguren la compresión de la misma.

- Brindar una descripción de los principales procedimientos almacenados utilizados en MARMINED, para facilitar su comprensión.

C. DESCRIPCIÓN DE MARMINED.

Nombre:

Metodología de Administración de Riesgos de TIC para el MINED **(MARMINED)**.

1. Lenguaje de Programación.

MARMINED es un prototipo de software en ambiente web distribuido diseñado e implementado en su totalidad en el lenguaje Java usando la plataforma J2EE/J2SE.

Diseñado bajo plataforma Web lo cual le permite ser multiplataforma funcionando en sistema operativos ya sean Unix, Linux o Windows, está desarrollado totalmente bajo la plataforma J2EE Java 2 Enterprice Edition de JAVA usando JavaBeans, JSP y JSF.

2. Gestor de la Base de Datos.

MARMINED está desarrollado utilizando el manejador de base de datos Oracle 10g Express Edition, esta versión está diseñada para ayudar a los desarrolladores a construir aplicaciones robustas y fiables ofreciendo una sencilla pero potente base de datos que es además gratuita. Serán accedidos de la forma más eficiente mediante Java Database Connectivity (JDBC) utilizando un pool de conexiones.

D. INFRAESTRUCTURA MÍNIMA NECESARIA PARA LA INSTALACIÓN DE MARMINED.

Dadas las características de MARMINED es necesario que se cuente con los siguientes requerimientos mínimos de operación, a fin de asegurar un óptimo funcionamiento de MARMINED:

1. Requerimientos de Software.

Para la máquina servidor:

- Sistema operativo Windows XP con SP2 o Linux
- Gestor de Base de Datos Oracle 10g
- Servidor de Aplicaciones Jakarta- Tomcat 6.0
- Maquina virtual de JAVA JRE Versión 1.6

Para la máquina cliente:

- Sistema Operativo Windows XP o Linux
- Navegador de Internet (Mozilla Firefox, Internet Explorer).

2. Requerimientos de Hardware.

Para la Máquina servidor:

Elemento del equipo	Especificación técnica
Tipo y Velocidad del Procesador	Intel Pentium IV o AMD a 2 Ghz
Memoria RAM	Tecnología - DDR II de 1 GB a 667 Mhz
Disco Duro	80 GB a 7500 rpm
Monitor	SVGA de 14"
Periféricos	Tarjeta de red PCI integrada Fast Ethernet Ratón y teclado en español Unidad de CD/DVD ROM UPS con regulador de voltaje.

Tabla 1. Requisitos de hardware para máquina Servidor.

Para la Máquina Cliente:

Elemento del equipo	Especificación técnica
Tipo y Velocidad del Procesador	Intel Pentium III o AMD a 450 Mhz
Memoria RAM	Tecnología - DDR I de 256 MB a 133 Mhz
Disco Duro	10 GB
Monitor	SVGA de 14"
Periféricos	Tarjeta de red PCI integrada Fast Ethernet Ratón y teclado en español Unidad de CD / DVD ROM UPS con regulador de voltaje.

Tabla 2. Requisitos de hardware para máquina Cliente.

E. ARQUITECTURA DE MARMINED.

MARMINED se ha dividido en los siguientes módulos (ver Figura 1):

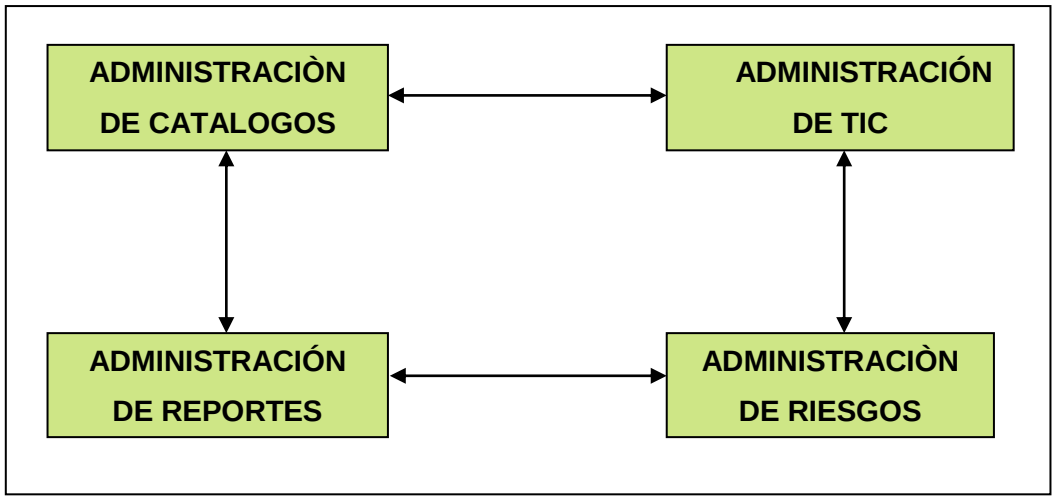


Figura 1. Módulos de MARMINED.

A continuación se describe brevemente cada uno de los módulos de MARMINED (Ver Tabla 3):

Módulo	Descripción
ADMINISTRACIÓN DE CATÁLOGOS	Permite la administración de usuarios, tipos de fuentes de amenaza y las unidades organizativas
ADMINISTRACIÓN DE TIC	Permite la administración de los servicios de TIC, software y hardware que posee el MINED.
ADMINISTRACIÓN DE RIESGOS	Permite la administración de fuentes de amenazas, motivaciones, acciones que materializan amenazas, vulnerabilidades y controles asociados a las vulnerabilidades.
ADMINISTRACIÓN DE REPORTES	Permite la Administración de reportes de servicios de TIC y de los riesgos calculados para una vulnerabilidad asociada a fuentes de amenaza.

Tabla 3: Descripción de Módulos de MARMINED.

F. TIPOS DE USUARIOS.

Los usuarios que interactúan con MARMINED son:

Administrador de MARMINED: Este usuario puede realizar las siguientes acciones: Agregar, modificar, eliminar y buscar usuarios, tipos de fuentes de amenaza, unidades organizativas, servicios de TIC, software, hardware, fuentes de amenazas, motivaciones, acciones que materializan amenazas, vulnerabilidades y controles, verificar modificaciones y visualizar e imprimir reportes de riesgos y servicios de TIC.

G. ESPECIFICACIÓN DE LA BASE DE DATOS.

1. Diseño Lógico.

EL Modelo Conceptual de MARMINED nos permitirá llevar el control de los tipos de fuentes de amenaza, unidades organizativas, servicios de TIC, software, hardware, fuentes de amenazas, motivaciones, acciones que materializan amenazas, vulnerabilidades y cuando sea oportuno la generación de reportes. La Figura 2 muestra el modelo conceptual de la base de datos de MARMINED.

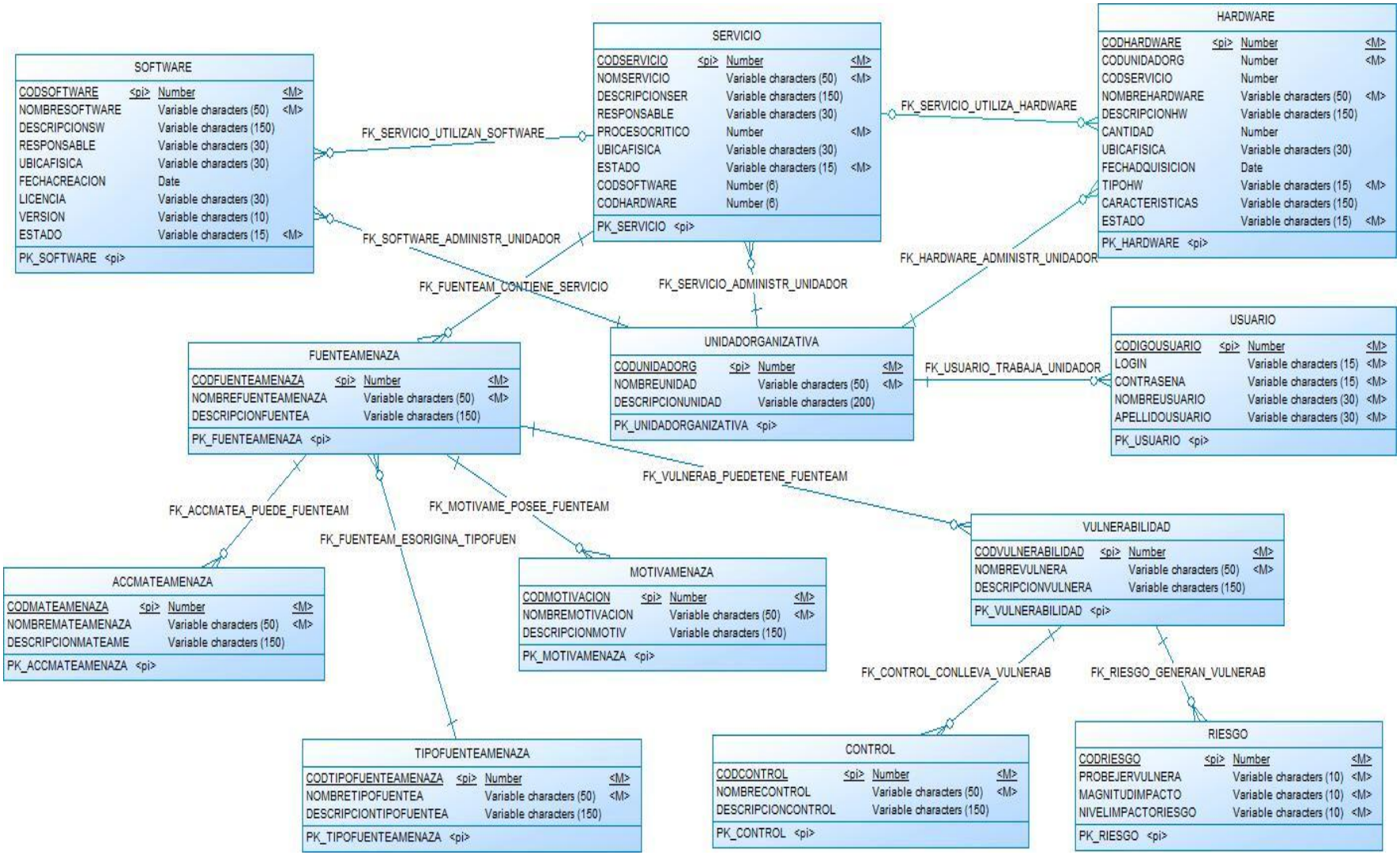


Figura 2. Modelo Conceptual.

2. Diseño Físico.

El Modelo Físico de la Figura 3 se ha generado a partir del diagrama lógico o modelo conceptual de la base de datos de MARMINED.

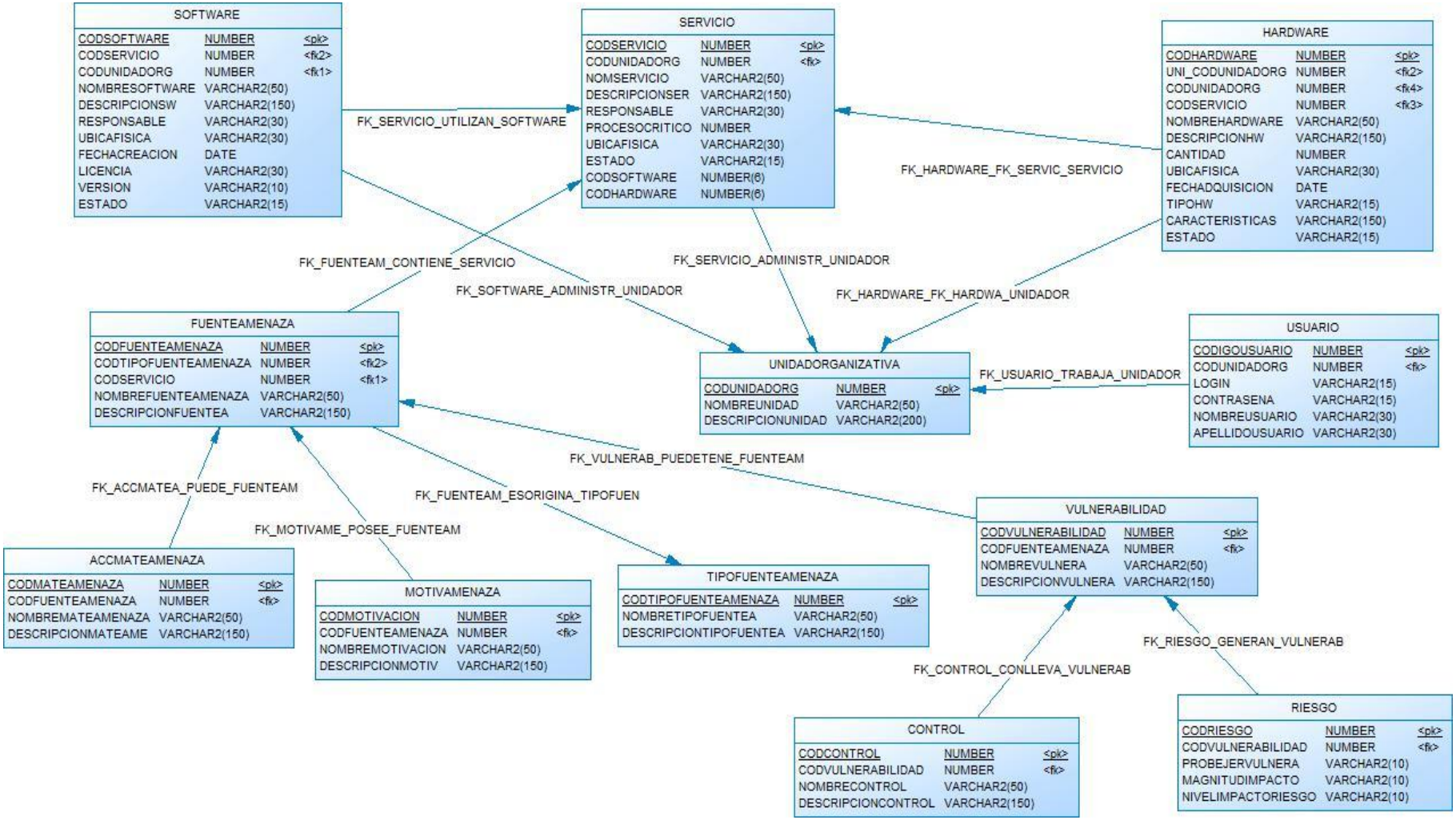


Figura 3. Modelo Físico.

3. Tablas Utilizadas.

A continuación se describen las tablas de la base de datos utilizadas en el sistema.

1) USUARIO

Tabla que almacena los usuarios de MARMINED.

2) UNIDADORGANIZATIVA

Tabla que almacena las unidades organizativas.

3) TIPOFUENTEAMENAZA

Tabla que almacena los tipos de fuente de amenaza.

4) SERVICIO

Tabla que almacena los servicios de TIC.

5) SOFTWARE

Tabla que almacena las aplicaciones informáticas.

6) HARDWARE

Tabla que almacena los equipos informáticos.

7) FUENTEAMENAZA

Tabla que almacena las fuentes de amenazas relacionadas a un tipo de fuente de amenaza.

8) VULNERABILIDAD

Tabla que almacena las vulnerabilidades de las TIC.

9) MOTIVAMENAZA

Tabla que almacena las motivaciones que pueden tener las amenazas.

10) ACCMATEAMENAZA

Tabla que almacena las acciones que podrían materializar una amenaza.

11) CONTROL

Tabla que almacena los controles relacionados a las vulnerabilidades de las TIC.

12) RIESGO

Tabla que almacena los cálculos de la probabilidad del riesgo, magnitud de impacto y el nivel del impacto del riesgo relacionado a las vulnerabilidades asociadas con las fuentes de amenazas.

4. Diccionario de Datos.

En este apartado se detalla una descripción de los campos de las tablas que conforman la Base de Datos de MARMINED detallando los siguientes elementos para cada tabla en orden alfabético: el nombre del campo, código, tipo, longitud y descripción.

Tabla: ACCMATEAMENAZA

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código de la acción que materializaría una amenaza.	CODMATEAMENAZA	Number	--	Almacena el código de la acción que materializaría una amenaza.
Nombre de la acción que materializaría una amenaza.	NOMBREMATEAMENAZA	Variable characters	50	Almacena el nombre de la acción que materializaría una amenaza.
Descripción de la acción que materializaría una amenaza.	DESCRIPCIONMATEAME	Variable characters	150	Almacena la descripción de la acción que materializaría una amenaza.

Tabla: CONTROL

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del control relacionado con una vulnerabilidad.	CODCONTROL	Number	--	Almacena el código del control relacionado con una vulnerabilidad.
Nombre del control relacionado con una vulnerabilidad.	NOMBRECONTROL	Variable characters	50	Almacena el nombre del control relacionado con una vulnerabilidad.
Descripción del control relacionado con una vulnerabilidad.	DESCRIPCIONCONTROL	Variable characters	150	Almacena la descripción del control relacionado con una vulnerabilidad.

Tabla: FUENTEAMENAZA

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código de la fuente de amenaza	CODFUENTEAMENAZA	Number	--	Almacena el código de la fuente de amenaza
Nombre de la fuente de amenaza	NOMBREFUENTEAMENAZA	Variable characters	50	Almacena el nombre de la fuente de amenaza
Descripción de la fuente de amenaza	DESCRIPCIONFUENTEA	Variable characters	150	Almacena la descripción de la fuente de amenaza

Tabla: HARDWARE

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del hardware	CODHARDWARE	Number	--	Almacena el código del hardware
Código de la unidad organizativa	CODUNIDADORG	Number	--	Almacena el código de la unidad organizativa responsable
Código del servicio	CODSERVICIO	Number	--	Almacena el código del servicio que soporta
Nombre del hardware	NOMBREHARDWARE	Variable characters	50	Almacena el nombre del hardware
Descripción del hardware	DESCRIPCIONHW	Variable characters	150	Almacena la descripción del hardware
Cantidad de hardware	CANTIDAD	Number	--	Almacena la cantidad del hardware
Ubicación física	UBICAFISICA	Variable characters	30	Almacena la ubicación física del hardware
Fecha de adquisición	FECHADQUISICION	Date	--	Almacena la fecha de adquisición
Tipo de hardware	TIPOHW	Variable characters	15	Almacena el tipo de hardware
Características	CARACTERISTICAS	Variable characters	150	Almacena las características
Estado	ESTADO	Variable characters	15	Almacena el estado en que se encuentra el hardware

Tabla: MOTIVAMENAZA

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código de la motivación que puede tener una amenaza	CODMOTIVACION	Number	--	Almacena el código de la motivación que puede tener una amenaza
Nombre de la motivación que puede tener una amenaza	NOMBREMOTIVACION	Variable characters	50	Almacena el nombre de la motivación que puede tener una amenaza
Descripción de la motivación que puede tener una amenaza	DESCRIPCIONMOTIV	Variable characters	150	Almacena la descripción de la motivación que puede tener una amenaza

Tabla: RIESGO

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del riesgo	CODRIESGO	Number	--	Almacena el código del riesgo
Probabilidad del ejercicio de la vulnerabilidad	PROBEJERVULNERA	Variable characters	10	Almacena el valor de la probabilidad del ejercicio de la vulnerabilidad
Magnitud del impacto	MAGNITUDIMPACTO	Variable characters	10	Almacena el valor de la magnitud del impacto
Nivel del impacto del riesgo	NIVELIMPACTORIESGO	Variable characters	10	Almacena el valor del nivel del impacto del riesgo

Tabla: SERVICIO

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del servicio	CODSERVICIO	Number	--	Almacena el código del servicio
Nombre del servicio	NOMSERVICIO	Variable characters	50	Almacena el nombre del servicio
Descripción del servicio	DESCRIPCIONSER	Variable characters	150	Almacena la descripción del servicio
Responsable del servicio	RESPONSABLE	Variable characters	30	Almacena el responsable del servicio
Cantidad de procesos críticos dependientes	PROCESOCRITICO	Number	--	Almacena la cantidad de procesos críticos dependientes
Ubicación física	UBICAFISICA	Variable characters	30	Almacena la ubicación física del servicio
Estado	ESTADO	Variable characters	15	Almacena el estado en que se encuentra el servicio
Código del software asociado al servicio	CODSOFTWARE	Number	--	Almacena el código del software asociado al servicio
Código del hardware asociado al servicio	CODHARDWARE	Number	--	Almacena el código del hardware asociado al servicio

Tabla: SOFTWARE

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del software	CODSOFTWARE	Number	--	Almacena el código del software
Nombre del software	NOMBRESOFTWARE	Variable characters	50	Almacena el nombre del software
Descripción del software	DESCRIPCIONSW	Variable characters	150	Almacena la descripción del software
Responsable del software	RESPONSABLE	Variable characters	30	Almacena el responsable del software
Ubicación física	UBICAFISICA	Variable characters	30	Almacena la ubicación física del software
Fecha de creación	FECHACREACION	Date	--	Almacena la fecha de su creación
Licencia	LICENCIA	Variable characters	30	Almacena la licencia del software
Versión	VERSION	Variable characters	10	Almacena la versión del software
Estado	ESTADO	Variable characters	15	Almacena el estado en que se encentra el software

Tabla: TIPOFUENTEAMENAZA

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del tipo de fuente de amenaza	CODTIPOFUENTEAMENAZA	Number	--	Almacena el código del tipo de fuente de amenaza
Nombre del tipo de fuente de amenaza	NOMBRETIPOFUENTEA	Variable characters	50	Almacena el nombre del tipo de fuente de amenaza
Descripción del tipo de fuente de amenaza	DESCRIPCIONTIPOFUENTEA	Variable characters	150	Almacena la descripción del tipo de fuente de amenaza

Tabla: UNIDADORGANIZATIVA

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código de la unidad organizativa	CODUNIDADORG	Number	--	Almacena el código de la unidad organizativa
Nombre de la unidad organizativa	NOMBREUNIDAD	Variable characters	50	Almacena el nombre de la unidad organizativa
Descripción de la unidad organizativa	DESCRIPCIONUNIDAD	Variable characters	200	Almacena la descripción de la unidad organizativa

Tabla: USUARIO

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código del usuario	CODIGOUSUARIO	Number	--	Almacena el código del usuario
Login del usuario	LOGIN	Variable characters	15	Almacena el login del usuario
Contraseña del usuario	CONTRASENA	Variable characters	15	Almacena la contraseña del usuario
Nombre del usuario	NOMBREUSUARIO	Variable characters	30	Almacena el nombre del usuario
Apellido del usuario	APELLIDOUSUARIO	Variable characters	30	Almacena el apellido del usuario

Tabla: VULNERABILIDAD

Nombre de Campo	Código	Tipo	Longitud	Descripción
Código de la vulnerabilidad	CODVULNERABILIDAD	Number	--	Almacena el código de la vulnerabilidad
Nombre de la vulnerabilidad	NOMBREVULNERA	Variable characters	50	Almacena el nombre de la vulnerabilidad
Descripción de la vulnerabilidad	DESCRIPCIONVULNERA	Variable characters	150	Almacena la descripción de la vulnerabilidad

5. Procedimientos Almacenados.

Se ha utilizado un procedimiento para calcular la probabilidad del riesgo, magnitud de impacto y el nivel del impacto del riesgo, este procedimiento se ha creado directamente en el gestor de la base de datos.

A continuación se presentan el nombre, descripción y código del procedimiento:

Nombre: SPC_CALC_RIESGO

Descripción: Este procedimiento calcula la probabilidad del riesgo tomando como parámetros el número de fuentes de amenaza, motivaciones, vulnerabilidades y controles que se hayan introducido en la base de datos, suma dichos valores y los almacena en una variable, dependiendo del valor de esta variable la probabilidad del riesgo puede ser ALTA, MEDIA o BAJA.

Para calcular la magnitud de impacto toma como parámetro el número de procesos críticos que posee un servicio, con ese dato realiza una regla de tres simple con la mayor cantidad de procesos críticos que un servicio puede tener, este resultado lo almacena en una variable y dependiendo del valor de esta variable la magnitud de impacto puede ser ALTA, MEDIA o BAJA

Por último para calcular el nivel del impacto del riesgo multiplica los valores numéricos obtenidos anteriormente de la probabilidad y de la magnitud de impacto, nuevamente almacena este resultado en una variable y dependiendo del valor de esta variable el nivel del impacto del riesgo puede ser ALTO, MEDIO o BAJO.

Código:

```
create or replace PROCEDURE "SPC_CALC_RIESGO"
( idVulnerabilidad IN NUMBER
) AS
 faNum integer;
```

```
maNum integer;
controlNum integer;
probV NUMBER;
probVStr VARCHAR2(10);
impacto NUMBER;
impactoStr VARCHAR2(10);
riesgoStr VARCHAR2(10);
riesgo NUMBER;
BEGIN
 SELECT COUNT(*) INTO faNum FROM fuenteamenaza fa JOIN vulnerabilidad V
ON (fa.codfuenteamenaza= v.codfuenteamenaza)
 WHERE v.codvulnerabilidad=idVulnerabilidad;

 SELECT COUNT(*) INTO maNum FROM motivamenaza ma JOIN vulnerabilidad V
ON (ma.codfuenteamenaza= v.codfuenteamenaza)
 WHERE v.codvulnerabilidad=idVulnerabilidad;

 SELECT COUNT(*) INTO controlNum FROM control ctrl JOIN vulnerabilidad V
ON (ctrl.codvulnerabilidad= v.codvulnerabilidad)
 WHERE v.codvulnerabilidad=idVulnerabilidad;

 probV:= controlnum+ fanum+ manum;

 case probV
  when 0 then
    probV:=0.1;
    probVStr:='BAJO';
  when 1 then
    probV:=0.1;
    probVStr:='BAJO';
  when 2 then
```

```
    probV:=0.5;
    probVStr:='MEDIO';
  when 3 then
    probV:=1;
    probVStr:='ALTO';
end case;

SELECT PROCESOCRITICO INTO maNum FROM servicio srv JOIN fuenteamenaza fa ON (srv.codservicio = fa.codservicio) JOIN vulnerabilidad V ON (fa.codfuenteamenaza= v.codfuenteamenaza)
WHERE v.codvulnerabilidad=idVulnerabilidad;

impacto:=maNum*100/233;

IF impacto>70 THEN
  impacto:=100;
  impactoStr:='ALTO';
ELSE
 IF impacto>30 THEN
   impacto:=50;
  impactoStr:='MEDIO';
 ELSE
   impacto:=10;
   impactoStr:='BAJO';
 END IF;
END IF;

riesgo:=impacto* probv;

if riesgo>50 then
  riesgostr:='ALTO';
```

```
else
  if riesgo<=10 then
   riesgostr:='BAJO';
  else
   riesgostr:='MEDIO';
  end if;
end if;

faNum:=0;
SELECT COUNT(*) INTO faNum FROM riesgo WHERE CODVULNERABILIDAD= idvulnerabilidad;

IF faNum > 0 THEN
 UPDATE RIESGO SET CODVULNERABILIDAD= idvulnerabilidad, probejervulnera= probvstr, magnitudimpacto= impactostr, nivelimpactoriesgo= riesgostr
 WHERE CODVULNERABILIDAD= idvulnerabilidad;
ELSE
 INSERT INTO RIESGO VALUES(SEQ_RIESGO_ID.nextval, idvulnerabilidad, probvstr, impactostr, riesgostr);
END IF;
END SPC_CALC_RIESGO;
```