ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS

ESTUDIO PARA EL DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES MILITARES

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGISTER EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

DIANA PIEDAD ESTÉVEZ AGUILAR
dianaest4@hotmail.com

DIRECTOR: Msc. Ing. Cesar Gustavo Samaniego Burbano
gustavo.samaniego@epn.edu.ec

Quito, junio 2014

DECLARACIÓN

Yo, Diana Piedad Estévez Aguilar, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Diana Piedad Estévez Aguilar

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diana Piedad Estévez Aguilar, bajo mi supervisión.

Ing. Gustavo Samaniego

DIRECTOR

RESUMEN

La presente tesis detalla la investigación de una fusión de dos metodologías como son Magerit y Octave, las mismas que se encargan de analizar y gestionar los riesgos, en el mercado de las tecnologías de la información, y sirven de base para el desarrollo de este proyecto.

Contiene cuatro capítulos que describen las funciones y desarrollo de etapas con sus actividades para llegar al análisis, evaluación y tratamiento de los riesgos, monitoreo y comunicación conjuntamente con la seguridad de la información, aplicados a institución militar como es la Fuerza Naval. Este estudio de desarrollo de una metodología de Gestión de Riesgos y seguridad de la información, destinado a instituciones militares, es de fácil implementación ya que estas organizaciones conforman la sociedad ecuatoriana acorde a la realidad nacional.

El primer capítulo comprende, el análisis y estudio de los riesgos de la información a que están sometidos las fuerzas armadas en el Ecuador y como implementar técnicas que ayuden a mitigar los riesgos con una nueva metodología de gestión de riesgos y seguridad de la información.

El segundo capítulo comprende, la propuesta del modelo de gestión de riesgos y seguridad de la información, compuesto por seis fases y cada una de ellas contiene etapas y actividades para llevar a cabo el modelo propuesto.

El tercer capítulo comprende, la aplicabilidad del modelo en un caso de estudio, discutiendo los resultados obtenidos y especificando su fácil implementación.

Por último, en el cuarto capítulo, se especifica las conclusiones y recomendación sobre este proyecto.

CONTENIDO

INDICE DE FIGURAS

INDICE DE PLANTILLAS

INDICE DE TABLAS

CAPITULO 1.

ESTUDIO DE LOS RIESGOS EN INSTITUCIONES MILITARES

1.1. RECONOCIMIENTO DE LAS INSTITUCIONES MILITARES

En el Ecuador las Fuerzas Armadas son un punto indispensable para la seguridad y salvaguardar el territorio ecuatoriano; es por eso que existe el Comando Conjunto de las Fuerzas Armadas (como se distingue en el *Gráfico 1*), como órgano de máxima planificación, preparación y conducción estratégica de las operaciones militares y de asesoramiento sobre las políticas militares, de guerra y defensa nacional, es el encargado de organizar y mantener el poder militar en los procesos que garanticen la seguridad de la nación y propendan a su desarrollo, con la finalidad de contribuir a la consecución de la agenda política de la Defensa Nacional, de acuerdo a la planificación prevista para tiempo de paz, de conflicto y/o guerra [1]. La misma que está integrada por las tres ramas que son: el Ejército (Constituirse en la institución líder del respeto a los Derechos Humanos y al Derecho Internacional Humanitario en el ámbito nacional e internacional, obtenido así la confianza y respaldo del pueblo ecuatoriano por sus actos transparentes y leales de acuerdo a la Constitución de la República [2].), la Fuerza Naval (Desarrollar las capacidades marítimas y proveer la seguridad integral en los espacios acuáticos que fortalezcan el Poder Naval y que contribuyan a la defensa de la soberanía y la integridad territorial; y, con su contingente apoyar al desarrollo marítimo nacional y a la seguridad pública y del Estado [3].) y la Fuerza *Aérea (Ser una Fuerza Aérea disuasiva, respetada y aceptada por la sociedad; pionera en el desarrollo aeroespacial nacional [4]).*

En la actualidad la sociedad ecuatoriana demanda de un modelo de Fuerzas Armadas acorde a la realidad nacional, el desarrollo social, la situación internacional, el avance de la ciencia y tecnología, las nuevas amenazas, los factores de riesgo y los escenarios prospectivos, en este sentido las Fuerzas Armadas se proyectan como una fuerza profesional, operativa, flexible, disciplinada, jerarquizada, con capacidad conjunta para la defensa de los intereses nacionales [1].

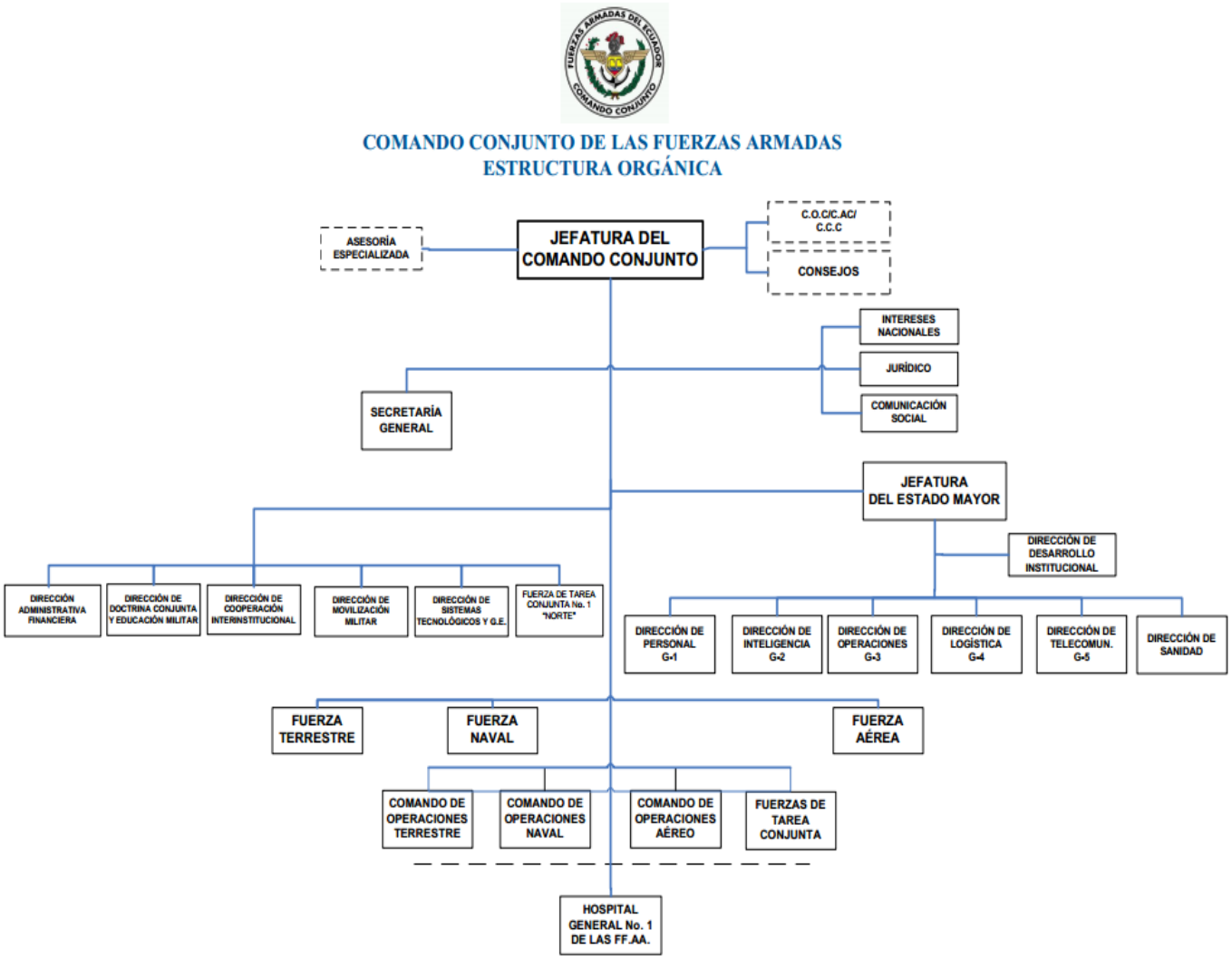

Figura 1.1: Estructura Orgánica (CCFFAA) [1]

[1] Fuente: C.C.F.F.A, Organigrama, http://www.ccffaa.mil.ec.

Como se aprecia en la *Figura 1.1,* de la estructura Orgánica del Comando conjunto de las Fuerzas Armadas, ahí se distingue las tres ramas de las fuerzas donde La Fuerza Naval es la segunda rama más antigua.

1.1.1. COMANDANCIA GENERAL DE LA MARINA (FUERZA NAVAL)

Todas las disposiciones y directrices que efectúa el COGMAR (Comandancia General de Marina), serán aceptadas por los repartos navales, que harán uso de estas políticas. Dentro del organigrama de la Fuerza Naval que se aprecia en el *Figura 1.2,* se encuentra detallado las direcciones que lo conforman tanto el nivel asesor, nivel de apoyo y nivel operativo. Dentro del nivel de apoyo se encuentra la Dirección General del Material (DIGMAT), el mismo que se preocupa de toda la parte logística de la Marina, y es una de las direcciones de órganos técnicos y administrativos. La DIGMAT, administra las funciones logísticas de abastecimientos, mantenimiento y reparación, transporte, desarrollo y servicios de bases, para satisfacer las necesidades de las unidades y repartos navales en los lugares y tiempos requeridos en forma eficiente, privilegiando la investigación y el desarrollo [7].

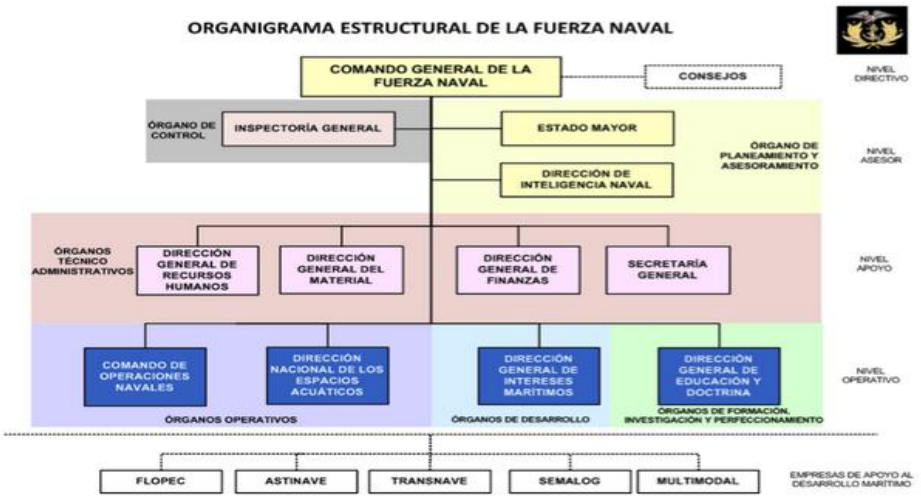

Figura 1.2: Estructura Orgánica (COGMAR) [2]

[2] Fuente: COGMAR, Organigrama, http://www.armada.mil.ec/organigrama

Dentro de la Dirección General del Material (DIGMAT) se encuentra la Dirección de Tecnologías de la Información (DIRTIC) como se distingue en el *Figura 1.3.* Esta dirección planifica, gestiona, estandariza, controla, integra e implementa proyectos, sistemas y servicios telemáticos, manteniendo la disponibilidad y flujo de información segura, confiable y oportuna, para optimizar la toma de decisiones y facilitar el cumplimiento de tareas operativas y administrativas de la Fuerza Naval [7].

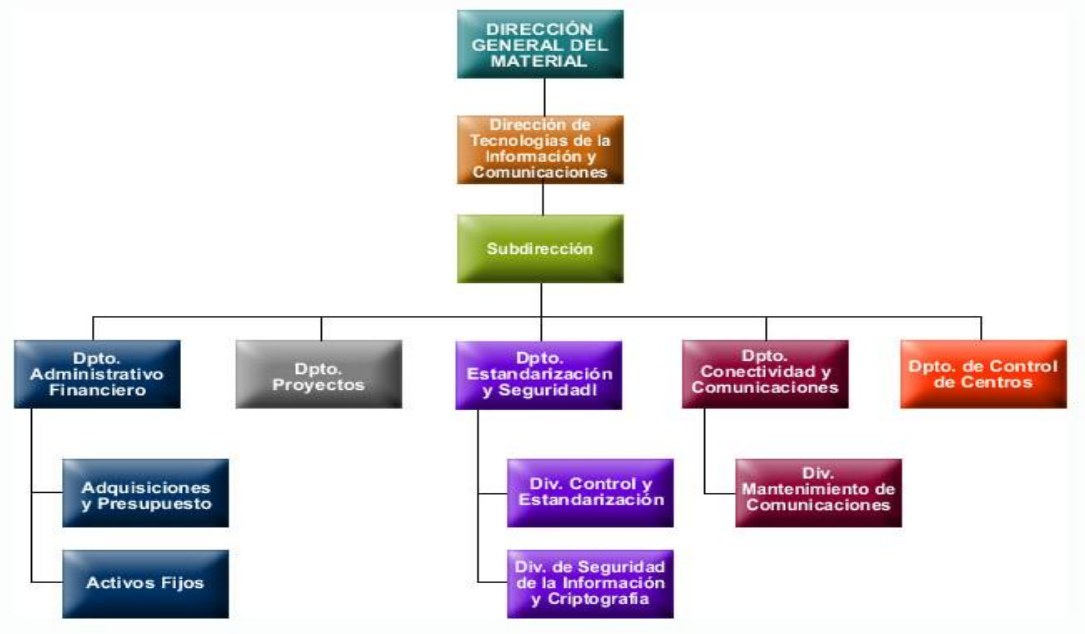

Figura 1.3: Estructura Orgánica (DIRTIC) [3]

Como se aprecia en el *Figura 1.3,* la DIRTIC es un ente principal en lo que respecta a las Tecnologías de las comunicaciones e información de todo la Fuerza Naval, dentro de esta se desglosa dos Centros de Tecnologías importantes que son CETEIQ, y CETEIG. Estos son los organismos responsables de administrar, desarrollar, integrar, operar y dar soporte a la plataforma de sistemas de información al software y hardware de los Sistemas Informáticos asignados, aplicando estándares institucionales y prácticas de control de calidad para las Tecnologías de

[3] Fuente: DIRTIC, Organigrama, http://www.dirtic.armada.mil.ec

la Información, empleando los recursos asignados en forma adecuada para dotar de tecnología de punta que sea operada por un equipo humano calificado, manteniendo la Red Naval de Datos y la seguridad de la información, a fin de contribuir al cumplimiento de la función básica de la DIRTIC [7].

Tanto el CETEIG (Centro de Tecnologías de la Información Guayaquil), da soporte y desarrollo de sistemas a repartos de la costa; como el CETEIQ (Centro de Tecnologías de la Información Quito), da soporte y desarrollo a repartos de la sierra. Estos dos entes tienen sus políticas y manejos de la seguridad de la información; hay que aclarar que esta seguridad de la información se rige principalmente de una Directiva puesta por la COGMAR (Comandancia General de Marina): COGMAR-INF-002-2010-O [5].

1.1.2. DIRECTIVA COGMAR SEGURIDAD DE LA INFORMACION COGMAR-INF-002-2010-O [5]

Esta directiva dispuesta por COGMAR (Comandancia General de Marina), es una política que debe seguirse en todos los repartos y unidades navales de la Fuerza Naval. Dentro de la Modernización Institucional emprendida por la Fuerza Naval en la actualidad, dentro del campo de los sistemas de información, se ve reflejada por la incorporación de nuevas tecnologías que apoyan a la gestión administrativa y operativa de la Fuerza a través del uso de: el Sistema de Comunicaciones Navales (SCN) está conformado por el sistema de comunicaciones navales fijas (red de área extendida a nivel nacional-WAN, redes de área local de los repartos navales-LAN, estaciones de radio) y el sistema de comunicaciones navales móviles(redes inalámbricas-WIRELESS, etc. Producto de la utilización de los servicios proporcionados a través del Sistema de Comunicaciones Navales (SCN) y de la integración a la red de datos de Fuerzas Armadas y a la Internet, se comenzó a evidenciar el acceso indebido a la información en determinadas redes locales de la Fuerza Naval, por lo que es necesario implementar seguridades para el uso de los servicios por parte de los Sectores y Repartos Navales [5].

Estas políticas de seguridad de la información tienen el objetivo de informar e incentivar al usuario final a colaborar con la seguridad de la infraestructura del Sistema de Comunicaciones Navales (SCN) y la información contenida en ella, como un valor que hay que proteger, informando a los usuarios técnicos y administrativos en términos generales por seguridad de la información, qué está y qué no está permitido realizar en la operación de la red y sus servicios tecnológicos. Al tratarse de términos generales, las políticas son aplicables a situaciones o recursos muy diversos y que de ser necesario se emitirán los requisitos de la política para convertirlos en indicaciones precisas de lo que se permite en la operación de la red y sus servicios, lo que se utilizará como una política de aplicación específica contemplando todas las actividades que se pueden realizar en los sistemas, las no contempladas, serán consideradas ilegales por lo tanto motivo de sanción. Por otro lado estas normas y políticas desarrolladas en el documento, se han elaborado de la mejor manera y estructuradas de acuerdo al estándar ISO/IEC 27002:2005 [6].

En esta directiva cada reparto tiene implementada su seguridad en la información y dentro de la Dirección de Tecnologías de la Información y Comunicaciones (DIRTIC) están entre algunas: Asegurar el cumplimiento y la observación de las políticas y estándares de informática y de comunicaciones por parte de los CETEINs y repartos navales [5]. Con esto se especifica que se cumplirá las políticas manifestadas en este documento y poder observar, detallar y mejorar las mismas.

1.1.3. CETEIQ (CENTRO DE TECNOLOGIAS DE LA INFORMACION QUITO), COMO ENTE DE APOYO EN LA FUERZA NAVAL

La función del CETEIQ es dirigir las acciones de análisis, diseño, desarrollo e implantación de sistemas informáticos, bases de datos; así como mantener operativa la Red Naval de Datos y la comunicación con los diferentes repartos, además de coordinar los servicios de mantenimiento y asistencia al usuario del Nodo Norte [8], (Dentro del nodo norte se encuentran integradas alrededor de 12 repartos navales las mismas que dependen de la red naval de datos del CETEIQ).

Como se visualizar en el *Figura 1.4,* el CETEIQ (Centro de Tecnologías de la Información Quito), está conformado por divisiones departamentales las mismas que se distinguen como: administración, recursos humanos informáticos y sistemas de información.

Figura 1.4: Estructura Orgánica (CETEIQ) [4]

Dentro del Centro de Tecnologías de la Información Quito (CETEIQ), existe una estructura de procesos que permiten el logro de los objetivos estratégicos; tanto productos como servicios del Centro de Tecnología de Información Quito, se ordenan y se clasifican en función de su grado de contribución o valor agregado al cumplimiento de la misión institucional.

El Centro de Tecnología de Información Quito, para el cumplimiento de su función y objetivos institucionales, desarrolla su gestión a través de sus procesos internos que están conformada por:

- ✓ Procesos gobernantes.- Monitorean la demanda de los clientes externos y apoyan la gestión del CETEIQ a través del cumplimiento de políticas y la

[4] Fuente: CETEIQ, Organigrama, http://www.dirtic.armada.mil.ec

expedición de normas e instrumentos para poner en funcionamiento la capacidad informática de la organización.

- ✓ Procesos agregadores de valor.- Generan, administran y controlan los productos y servicios destinados a usuarios internos y/o externos para cumplir con la función del CETEIQ, denotan la especialización de la función consagrada por la Armada, su operatividad se sustenta en las guías funcionales internas.
- ✓ Procesos habilitantes.- Los procesos habilitantes de asesoría y apoyo, están encaminados a generar productos y servicios para los procesos gobernantes, agregadores de valor y para sí mismos, viabilizando la gestión.

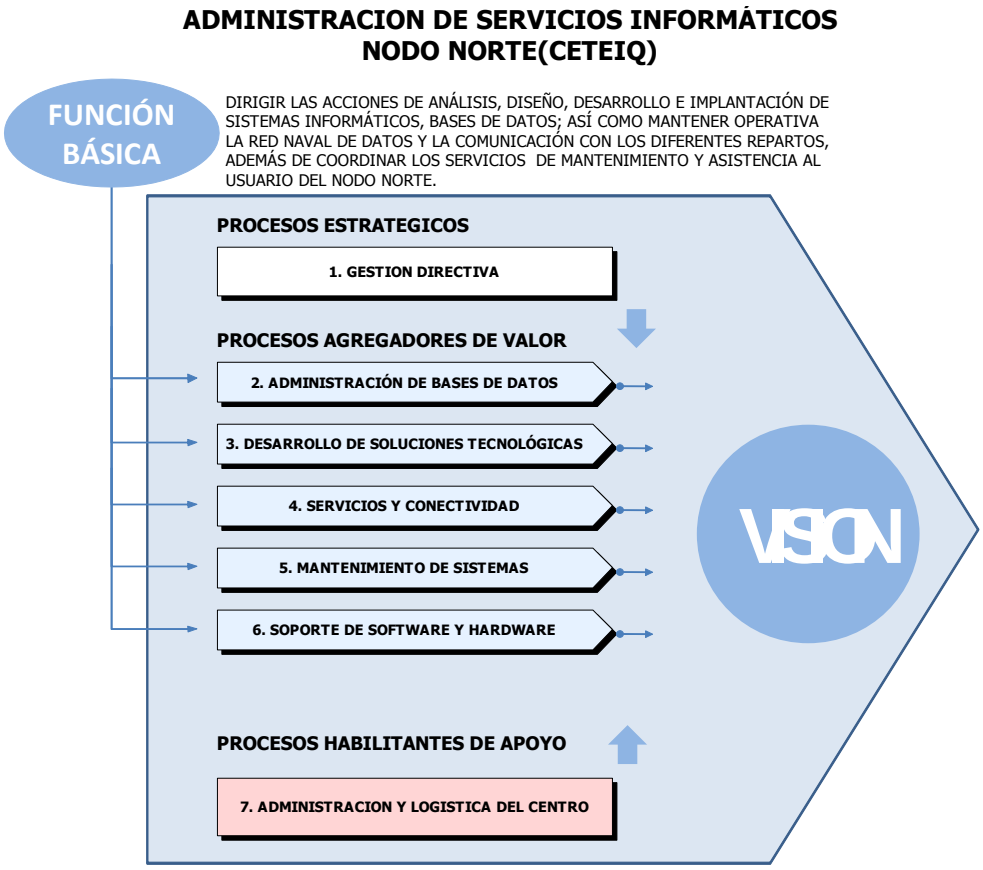

Figura 1.5: Cadena de Valor (CETEIQ) [5]

[5] Fuente: CETEIQ, Manual de Organización del Centro de Tecnologías de la Información, nodo norte, documento tipo reservado.

Según la representación *Figura 1.5, se visualiza* la interacción de los procesos que intervienen en la gestión institucional del Centro de Tecnología de Información Quito, responsables de la generación de productos y servicios que demandan los clientes/usuarios internos y externos de la Fuerza Naval.

1.2. DETERMINACION DE LOS RIESGOS

Tanto la Fuerza Naval, Fuerza Terrestre como Fuerza Aérea, tienen sus propias políticas y planes estratégicos que conllevan al uso y mejoramiento de la seguridad de la información. Como se detalló en páginas anteriores la Fuerza Naval tiene implantado su políticas de seguridad de la información y deben regirse a estas políticas todos los repartos navales que conforman la Fuerza Naval.

La incorporación de Tics en estas instituciones militares, conllevan a obtener una ventaja competitiva, es uno de los temas principales que concierne hoy en día a altos ejecutivos y dirigentes de estas instituciones. Esto ha producido una creciente demanda en el desarrollo de los sistemas de información (SI) y los componentes tecnológicos, para soportar las actividades de una organización. Sin embargo, es una realidad que el riesgo de las instituciones militares también se ha incrementado ya que en el complejo mundo actual de la tecnología, la administración de los recursos de TICs, la consolidación e integración de los mismos es cada vez más compleja.

En la Fuerza Naval se ha facilitado la adopción generalizada de medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en los diferentes sistemas de información empleados, garantizando el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos y operativos que utilicen medios electrónicos, informáticos y telemáticos [9]. Una de estas adopciones es en lo que respecta a las Telecomunicaciones deben estar normados por una Directiva expuesta por la COGMAR**, COGMAR-TIC-002-2012-R [12],** esta se encuentra alineada al plan de capacidades estratégicas de las Fuerzas Armadas, donde rige

entre otras cosas a elaborar proyectos tecnológicos requeridos por los repartos y unidades de la Fuerza Naval conforme al PEDETIC [9] y normas establecidas.

Algunas de las estrategias de las TICs en la Fuerza Naval, no ha considerado la visión global de los recursos con que cuenta la Institución a fin de optimizarlos en base a criterios de trazabilidad y convergencia de los sistemas, lo que ha dificultado el desarrollo armónico de las TICs en la Armada y han sido los requerimientos del mando en los diferentes sectores, presionando a ejecutar trabajos no planificados, generando que el desarrollo tecnológico responda en forma espontánea a la solución de las necesidades urgentes de cada sector de la Institución, esto produce islas de TICs que no crecen coherentemente hacia una arquitectura integrada de sistemas, tecnología e información.

Para fortalecer los servicios de TICs, en la Fuerza Naval y automatizar los diferentes procesos institucionales y sectoriales, directivos, agregadores de valor y de soporte; es necesario mejorar y reducir los tiempos de respuesta, los costos de operación, minimizar los riesgos y transparentar la gestión institucional; contribuyendo al logro de una Institución Altamente Efectiva.

El análisis de riesgos introduce un enfoque riguroso y consecuente para la investigación de los factores que contribuyen a los riesgos. En general, implica la evaluación del impacto que una violación de la seguridad que tendría en la empresa; señala los riesgos existentes, identificando las amenazas que afectan al sistema informático, y la determinación de la vulnerabilidad del sistema a dichas amenazas. [10]. La gestión de riesgos tiene como objetivo articular los tipos de intervención sobre el riesgo, de tal manera que se puedan establecer las políticas preventivas que en largo plazo conduzcan a disminuir de manera significativa las necesidades de intervenir sobre los riesgos ocurridos, por lo que desempeña un papel decisivo en acciones preventivas.

Dentro de este contexto en la Fuerza Naval a nivel profesional del personal antiguo de TICS, las competencias del personal de los departamentos de tecnología de la Armada están reducidas debido al incorrecto proceso de selección de nuevo

personal, a la escasa inversión en capacitación realizada y la falta de un proceso de evaluación constante. Esto ha producido que la institución esté muy lejos de estar en el nivel tecnológico con respecto a las grandes corporaciones privadas.

En cuanto a la dificultad de reestructuración de CETEINs (Centros Tecnológicos de la Información) (Financiero): El presupuesto para comprar las renuncias al personal que ocupa plazas en los CETEINs (Centros Tecnológicos de la Información) y cuyo perfil no es el requerido por la institución debe ser contemplado anualmente a fin de proceder a la conformación de equipos de trabajo más dinámicos y sin los vicios de lentitud, displicencia y carencia de compromisos que aquejan a los departamentos de tecnología de la Armada.

También existe la falta de compromiso de los usuarios finales (Logístico): Los departamentos usuarios deben ser los encargados de liderar los procesos de levantamiento de requerimientos, diagramación de procesos y fiscalización de cumplimiento y satisfacción. Si existe desinterés por automatizar procesos o mejorar servicios con el objeto de evitar responsabilidades será muy difícil para los departamentos de tecnología asumir el rol tecnológico y de usuario final a la vez.

Dentro de todas estas premisas se puede evidenciar que los riesgos potenciales que se puede percibir dentro de la Fuerza Naval son:

- ✓ Falta de seguridad en la administración de claves y accesos a los recursos de las redes (Existen políticas pero no implementadas)
- ✓ Falta de entrenamiento al personal encargado de administrar las redes
- ✓ Falta de controles de seguridad de la información (Existen políticas pero no implementadas)
- ✓ Falta de cultura en seguridad informática por parte de los usuarios de la red
- ✓ No existen sistemas implementados para el cifrado de archivos
- ✓ Falta de protección de documentos o mensajes mediante permisos
- ✓ No existe un análisis de contenido en mensajería y correo (interno y/o externo)

- ✓ Falta de control de la información interna (Secreta, Confidencial, Uso Interno, Público, etc.).
- ✓ No existe medios para el cifrado del tráfico de red entre servidores y/o clientes críticos.
- ✓ No se han implementado firmas digitales en documentos y/o mensajes de correo electrónico
- ✓ No se han implementado medidas de encriptación de discos duros en equipos portables que contengan información confidencial.
- ✓ No existe auditoría y control de los registros de Seguridad y de control de cambios

Se realizo una encuesta al personal de jefatura de sistemas de las tres fuerzas del Comando Conjunto en el cual se obtuvo información importante para verificar que no existe una metodología de gestión de riesgos y seguridad de la información.

El modelo de la encuesta es el siguiente:

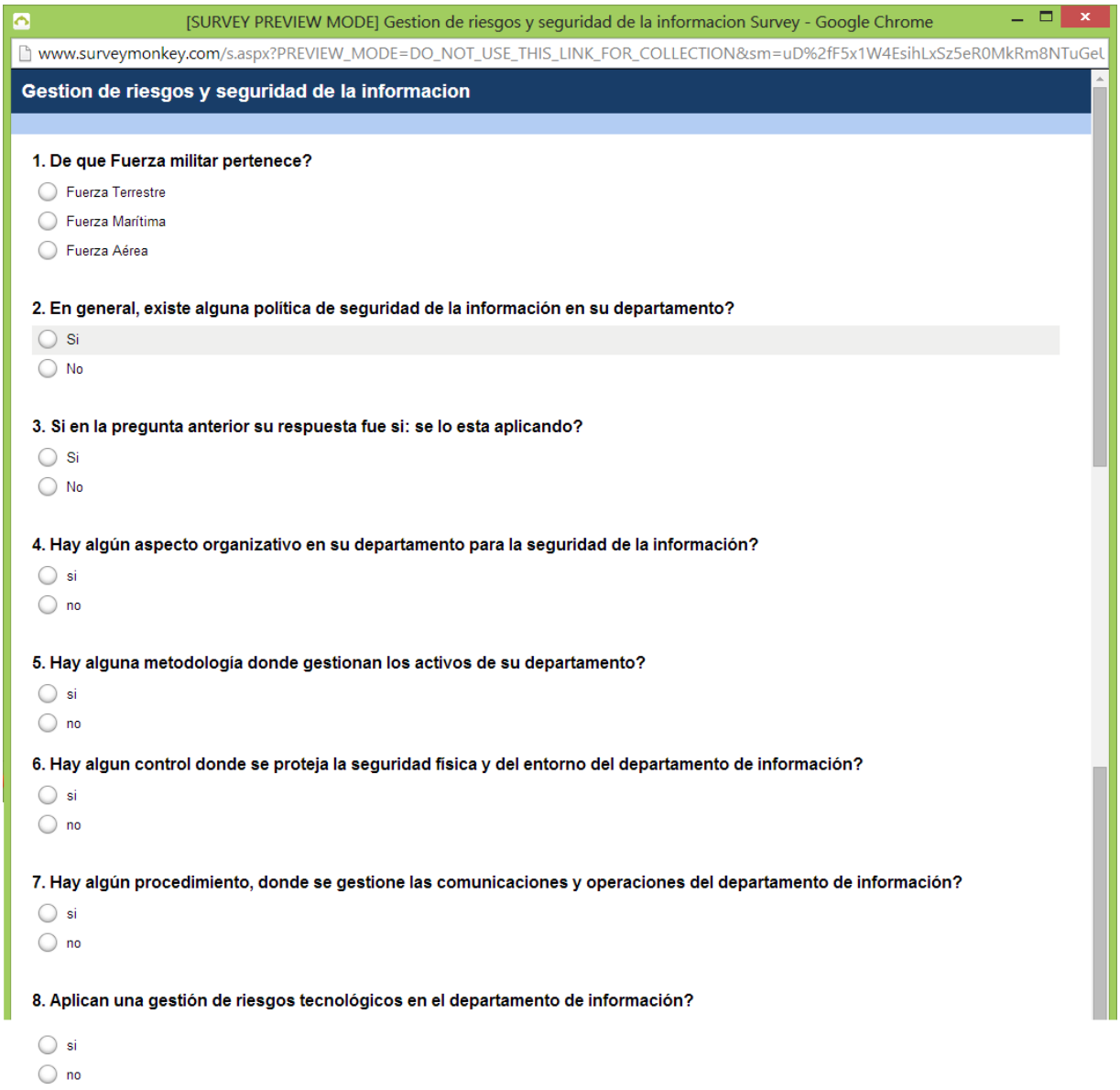

Figura 1.6: Encuesta [6]

Los resultados de las encuestan fueron que en resumen no existe ninguna metodología de gestión de riesgos y seguridad informática se adjunta los resultados:

[6] Fuente: La autora

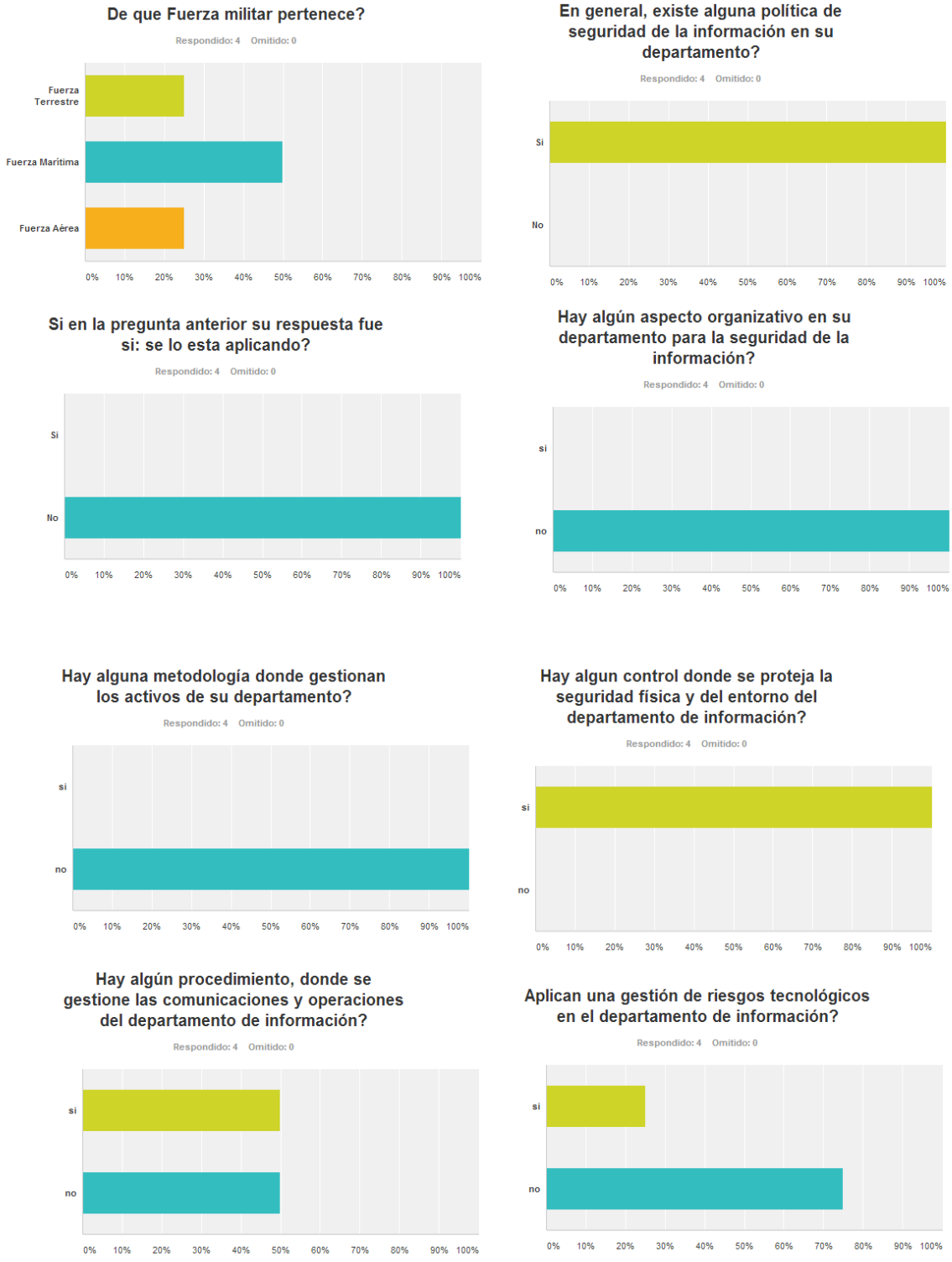

Figura 1.7: Resultado de Encuesta [7]

[7] Fuente: La autora

1.3. TÈCNICAS QUE AYUDAN A SOLUCIONAR LA GESTIÒN DE RIESGOS

Desde los inicios de los sistemas informáticos se han visto involucrados en diferentes riesgos por no poseer seguridades ya sea en los recursos humanos, técnicos, de infraestructura, organizativos entre otros. Para evitar los efectos de la inseguridad informática y riesgos que se encuentren dentro de la Fuerza Naval, se realizó un estudio del análisis funcional de las metodologías de Gestión de Riesgos que son: MAGERIT v.3 y OCTAVE v.1 para evitar los peligros de riesgo en el Centro de Tecnologías de la Información Quito (CETEIQ). El análisis de riesgo ayudará a buscar cada una de las vulnerabilidades que posee la institución y una vez obtenidos los resultados se podrá minimizar cada uno de los riesgos con las dos metodologías que se propone.

En el mundo de las tecnologías de la información se encuentran varias metodologías para tratar la gestión de riesgos por lo que a continuación se detalla alguna de ellas y realizando una comparación técnica contra OCTAVE y MAGERIT. Se tomaron algunas consideraciones técnicas de cada metodología principalmente metodologías que son direccionadas al riesgo de la seguridad de la información:

CARACTERISTICAS A COMPARAR	ISO 27005	ITIL	ISO 31000	CORAS (Construct a plataform for Risk Analysis of Security critical system)	MEHARI	MAGERIT	OCTAVE
Costos de implementación	Sobre los 10000. Para implementar esta norma se necesita de una persona certificada.	Sobre los 10000. Para implementar esta metodología se necesita de una persona certificada.	Sobre los 10000. Para implementar esta metodología se necesita de una persona certificada.	Es de implementación libre se puede descargar el core y tools	Sobre los 10000. Para implementar esta metodología se necesita de una persona certificada.	Requiere licencia para uso de herramienta EAR, es de uso publico, no necesita autorizacion previa para el uso.	No requiere licencia de uso
Estándares para el tratamiento de riesgos específicos	Para los sistemas de seguridad de la información	Para riesgos tecnológicos	Para riesgos tecnológicos con modelamientos UML	Metodología de análisis de riesgos basados en la elaboración de modelos	Conjunto de herramientas diseñadas para la seguridad y gestión de los riesgos	Investiga los riesgos que soportan los sistemas de información	Metodología de riesgos de TI
Estándares para el tratamiento de riesgos de			que recoge y unifica todos los				

todo tipo de riesgos			estándares mencionados. Está diseñado para que cualquier tipo de organización pueda identificar y evaluar todos sus riegos de una forma estructurada				
Facilidades de obtención en el país y las mas usadas en el país	X	X	No es la más usada pero es de fácil obtención	No es la más usada pero es de fácil obtención	No es la más usada pero es de fácil obtención	X Es de uso publico	X Es flexible y adaptable en cualquier entorno
Facilidad en obtención de versiones actuales		X		X	X	X	X

1.3.1. JUSTIFICACION DE LA UTILIZACION DE LAS METODOLOGIAS MAGERIT Y OCTAVE

Existen varias metodologías para el análisis y gestión de riesgos, por el análisis anterior las dos metodologías propuestas son las más nombradas y aceptadas, ya que si bien es cierto MAGERIT está basado en las normas ISO, ya algunas instituciones extranjeras lo han aplicado [16], en cuanto la metodología OCTAVE también es un método de evaluación y de gestión de riesgos para garantizar la seguridad del sistema informático y desarrollado por el estándar internacional ISO 27001. Estas dos son las más utilizadas a nivel mundial, MAGERIT porque es en español ya que fue desarrollada por el Consejo Superior de Administración Electrónica que hace parte del Ministerio de Administraciones Publicas de España y OCTAVE porque es muy resumida en cuanto a la identificación de los activos de la organización y no los clasifica demasiado.

Con estas premisas se realiza el análisis funcional de estas dos metodologías y se implementa los pasos necesarios para analizar un sistema, identificar las amenazas, las vulnerabilidades asociadas, calcular la probabilidad de ocurrencia de esas amenazas, determinar del impacto en caso de su materialización y por último la obtención del riesgo al que se está expuesto.

Con este análisis se propone una nueva metodología de Gestión de Riesgos y Seguridad Informática de rápida aplicación. Así, esta metodología sería una herramienta de fácil implementación en instituciones militares que permitirá identificar y gestionar los riesgos de tecnología de la información en cuestión.

Esta metodología propuesta tendrá un enfoque de análisis de riesgos cualitativo, este enfoque emplea valoraciones de escala de niveles. Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo. [11].

En un análisis de riesgos cuantitativo se busca saber qué y cuánto hay, cuantificando todos los aspectos posibles. [13]. El enfoque cuantitativo de análisis de riesgos consiste en la obtención de un valor a partir del producto de estos elementos. La forma de calcularlo, para un evento dado, es realizando la multiplicación del valor de la pérdida potencial por el valor de la probabilidad de ocurrencia. De esta manera es prácticamente concreto y posible valorar los eventos y calcular el riesgo a fin de tomar las decisiones correspondientes. Son numerosas las organizaciones que han adoptado y aplicado con éxito el análisis de riesgo cualitativo. De hecho se recomienda fuertemente comenzar con un análisis de riesgo cualitativo y luego, si el negocio lo amerita, hacer un análisis cuantitativo.

1.3.2. ANALISIS FUNCIONAL METODOLOGIA MAGERIT v3.0

La metodología MAGERIT, implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. [11]. La versión más reciente de esta metodología es la v3: donde hay un mejor alineamiento con la normativa ISO, buscando una integración de las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno. [14].

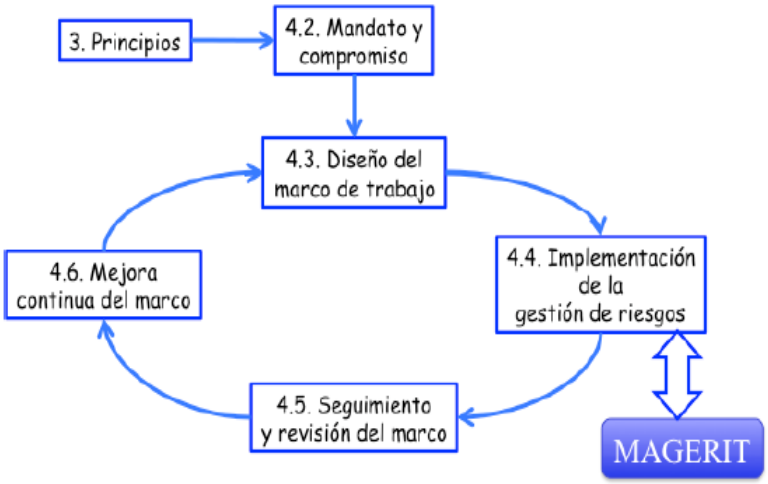

Figura 1.8: ISO 31000 – Marco de Trabajo para la gestión de riesgos[8]

Como se distingue en el *Figura 1.6,* dentro del Marco de trabajo de una gestión de riesgos según la ISO 31000, MAGERIT implementa la gestión de riesgos dentro de un marco de trabajo.

MAGERIT persigue los siguientes objetivos:

Directos:

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Como parte importante de esta metodología se tomará como puntos de partidas: el análisis de riesgos y la gestión de riesgos; en cuanto al análisis de riesgos en MAGERIT, determina en forma metódica el riesgo que están sometidos los activos y amenazas que puedan ocurrir; esto servirá de mucho para realizar de una mejor manera el análisis respectivo.

[8] Fuente: ISO 31000, ISO 31000:2009, “Risk management – principles and guidelines”. UNE-ISO 31000:2010, “Gestión del riesgo. Principios y directrices”

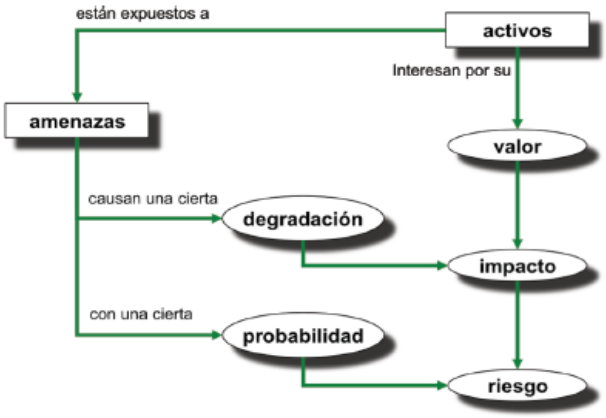

Figura 1.9: Elementos de análisis de riesgos potenciales[9]

Lo primordial de MAGERIT es analizar los riesgos potenciales de una organización, cuáles son las probabilidades y degradación a los que están amenazados como se visualiza en el *Figura 1.7.*

En cuanto al proceso de gestión de riesgos, ayudará a tomar decisiones con respecto a la gravedad del impacto y/o riesgo, las obligaciones a las que por ley esté sometida la Organización, los reglamentos sectoriales y obligaciones de contratos a los que está sometida la misma.

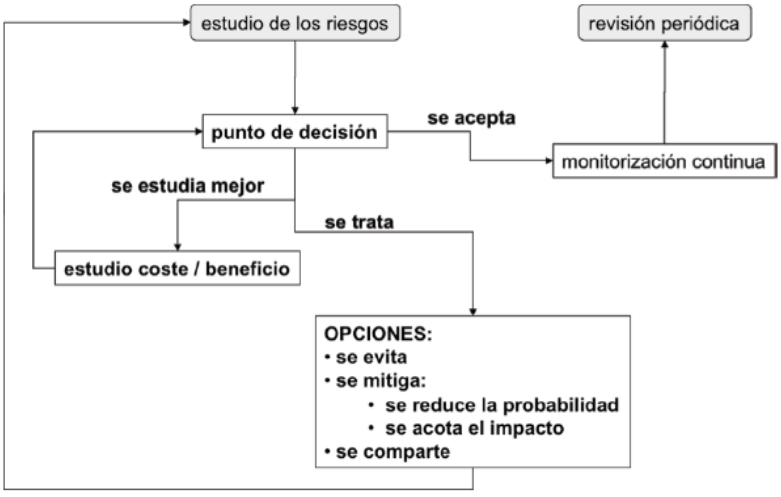

Figura 1.10: Decisiones de tratamiento de los riesgos[10]

[9] Fuente: Ministerio de Hacienda y Administraciones Públicas, MAGERIT Vs3, Metodología de análisis y gestión de riesgos de los sistemas de información, Libro 1, Ilustración 7.

Después de analizar los riesgos expuestos se procede a su proceso de gestión como se muestra en la *Figura 1.8,* donde hay su evaluación y su tratamiento.

En lo que respecta a los principales elementos de MAGERIT, que ayudarán a integrar la nueva metodología que se propone para la institución militar, dentro de los puntos de análisis y gestión de riesgos antes mencionados será:

- ✓ Escala de valores cualitativos, cuantitativos y de indisponibilidad del servicio

  Este elemento ayudara a tener una mejor escala práctica para valorar los activos, comparar los riesgos con homogeneidad y realizar un mejor análisis. En estas escalas de riesgos cuantitativos ayudará a saber qué y cuanto hay, cuantificando todos los aspectos posibles [15].
- ✓ Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia

  Ayudará a determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a los activos y causar un daño [14]. Con esto ayudara a verificar que amenazas se encuentran con frecuencia en la institución y analizarlas.
- ✓ Escala alternativa de estimación del riesgo

  Este elemento ayudara a procesar todos los datos para realizar informes del estado de riesgo con estimaciones de impacto, deficiencias o debilidades en el sistema de salvaguardas; teniendo así registradas salvaguardas analizadas frente a las amenazas que se pretendan mitigar [14]. Esto ayudará a determinar los riesgos potenciales que está sometida la institución y con respaldos de informes a analizar.
- ✓ Catálogos de amenazas

  Este catálogo de amenazas ayudará a tener las posibles amenazas sobre los activos de un sistema de información [15]. Esto contribuirá a los administradores

[10] Fuente: Ministerio de Hacienda y Administraciones Públicas, MAGERIT Vs3, Metodología de análisis y gestión de riesgos de los sistemas de información, Libro 1, Ilustración 11.

de activos, con base a su experiencia e información a detectar las amenazas que pueden afectar a más de un tipo de activo.

- ✓ Catálogos de medidas de control

  Este catálogo de medidas contribuirá al análisis de riesgos, basándose en estudios y resultados para la seguridad de la información. Esto facilitara a las personas a la labor del proyecto que se les ofrecerá un estándar rápido y centrándose en el objetivo del análisis de la seguridad de la información.

Con estos dos puntos principales de MAGERIT, ayudará a tener una mejor manera de gestión y análisis de los riesgos en que está expuesta la institución militar ya que si bien es cierto tienen políticas de seguridad implantadas; con este análisis y gestión será un punto clave en el ámbito de la administración electrónica con la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos para una protección adecuada de la información que se requiere en la Fuerza Naval.

1.3.3. ANALISIS FUNCIONAL METODOLOGIA OCTAVE v2.0

La metodología OCTAVE, es un conjunto de herramientas, técnicas y métodos para la evaluación del riesgo basada en seguridad de la información estratégica y la planificación [17].

OCTAVE se enfoca en el riesgo organizacional y su objetivo principal son los temas relativos a la estrategia y a la práctica. OCTAVE equilibra los siguientes aspectos: Riesgos operativos, Prácticas de seguridad, Tecnología.

Lo cual permite a las compañías tomar decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

Características:

- ✓ Es diferente de los análisis tradicionales enfocados a la tecnología

- ✓ Es Auto-dirigido
- ✓ Flexible

OCTAVE percibe los siguientes objetivos

- ✓ Permitir la comprensión del manejo de los recursos
- ✓ Identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización.
- ✓ Exige llevar la evaluación de la organización y del personal de la tecnología de información.

El método OCTAVE se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos:

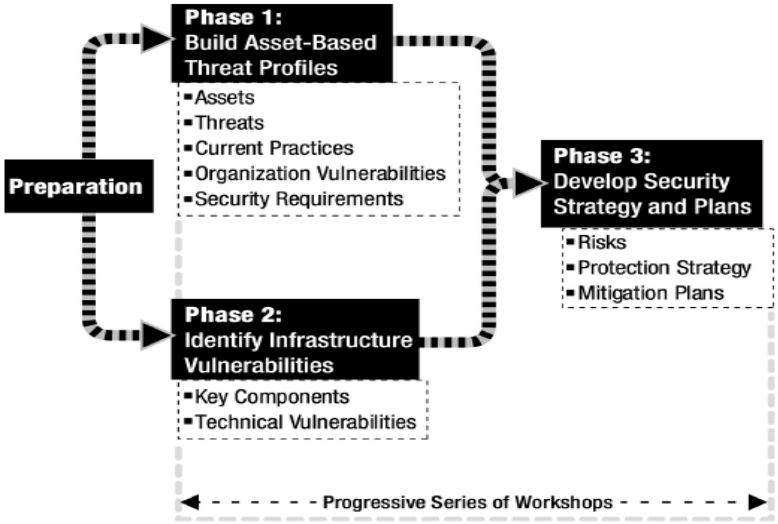

Figura 1.11: Fases de la metodología OCTAVE[11]

[11] Fuente: Carnegie Mellon University, OCTAVE Catalogo of Practices Versión 2.0.pdf, Octubre 2001, Figura 2. http://www.cert.org/octave/

Como se distingue en el *Figura 1.9,* las 3 fases de OCTAVE son:

- ✓ Construcción de los Perfiles de amenazas Basados en Activos

  Durante esta fase se identifica la información de la organización, que se refiere a dos tareas importantes que es la obtención de información de los distintos niveles de la organización, y la consolidación y el análisis de esa información.

- ✓ Identificación de la infraestructura de vulnerabilidades

  En esta fase se examina y analiza las vulnerabilidades tecnológicas que se aplican a los activos críticos y los componentes clave de infraestructura que apoyan esos activos.

- ✓ Desarrollo de planes y estrategias de seguridad

  Durante esta fase se realiza la identificación de los riesgos, así como también se realizan estrategias de mitigación y planes de protección se definen los riesgos asociados a los activos críticos, crea planes de mitigación de esos riesgos, y construye una estrategia de protección de la organización. Los planes y la estrategia son revisados y aprobados por los altos directivos.

Como elementos importantes que se tomará de estas fases y que integraran la nueva metodología propuesta serán:

- ✓ Medidas de probabilidad considerando un rango de frecuencias

  Estas medidas de probabilidad ayudaran en la institución a utilizarlas como se desee considerando matrices de riesgo para clasificar los riesgos identificados del departamento en cuestión.

- ✓ Análisis de límites entre niveles de probabilidad

  Este análisis ayudara a la institución a realmente ver hasta que limites se llegaran los niveles de probabilidades que ocurran en un riesgo y/o amenaza y mejorar la mitigación de estrategias.

Con estos elementos importantes de OCTAVE, permitirá identificar los riesgos, que permitirán crear planes de mitigación para hacer frente a esos riesgos que se

encuentran en la Fuerza Naval. La amenaza de vista operativo crítico, activo y vulnerabilidad, ayudará a un enfoque para las evaluaciones de riesgos de seguridad de información ya se integral, sistemática, basada en contexto que se materializarán en un conjunto de criterios que definen los elementos esenciales de una evaluación de riesgo de los activos basada en la información de seguridad.

1.3.4. CUADRO COMPARATIVO DE LAS METODOLOGIAS MAGERIT Y OCTAVE

Realizando un cuadro comparativo de las características más importantes de estas dos metodologías se obtiene lo siguiente:

MAGERIT	OCTAVE
Se enfatiza en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contra medidas para evitar así cualquier inconveniente	Es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo
Ofrece un método sistemático para analizar tales riesgos	Maneja tres métodos: auto-dirigido, flexibles y evolucionado
Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.	Desmitifica la falsa creencia: La Seguridad Informática es un asunto meramente técnico
Prepara a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso	Presenta los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos
Concientiza a los responsables de los sistemas de información de la existencia	Divide los activos en dos tipos: sistemas, (Hardware. Software y

de riesgos y de la necesidad de atajarlos a tiempo	Datos) y personas
Genera el uso de las tecnologías de la información	Se especializa en el riesgo organizacional y el foco son los temas relativos a la estrategia y la practica
Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema	Consolidación de la información y creación de perfiles de amenazas
Relación de las amenazas a que están expuestos los activos	Identifica los elementos críticos y las amenazas para los activos
Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos	Identifican las vulnerabilidades tanto organizativas como tecnológicas que exponen a las amenazas creando un riesgo a la organización
Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos	Desarrollar una estrategia de protección basada en la práctica así como planes de migración de riesgos para mantener la misión y prioridades de la organización

Con este cuadro se puede observar que las dos metodologías buscan un mismo objetivo el analizar y gestionar el riesgo y la seguridad de la información. Por ende se puede combinarlas y aplicar una nueva metodología propuesta para la institución militar. Se incorporarán los elementos principales descritos anteriormente de cada una y valores que proporcionarán una metodología nueva y consistente y que a su vez permitirá aplicarla a la realidad de las instituciones militares, en cuanto a riesgos informáticos se trate.

1.4. PLANTEAMIENTO DEL PROBLEMA

Existen vulnerabilidades dentro del CETEIQ, como Centro Tecnológico Informático de la Fuerza Naval, en cuestión de seguridad de la información, ya que se tiene las Directivas de políticas de seguridad plasmado por COGMAR [5]; pero no se aplica en si la mayor parte de esas políticas; no existe documentación para respaldar una mejor gestión informática. Estos sistemas de información son vulnerables a una diversidad de amenazas y atentados por parte de personas que pueden o no pertenecer a la institución, ya sean por: desastres naturales, a causa de intromisiones, o por errores humanos errores (de utilización y negligencia personal), o amenazas provocadas (robo, fraude, sabotaje o interrupción de actividades de cómputos). No se encuentra desarrollado en si estrategias y planes de protección y gestión como lo es también un análisis e identificación de riesgos y amenazas que puedan mejorar el acceso a la información como son: software, aplicaciones o servicios. Se ha visto en la necesidad de tener estrategias de gestión y análisis, en el que permita un mejor funcionamiento sobre los activos de información ya que en el (CETEIQ) no se encuentra definido los niveles de riesgo y determinación de controles para mejorarlos.

Existiendo estos problemas en el centro de tecnologías de información Quito (CETEIQ), se ha visto en la necesidad de generar una administración y análisis de riesgos que ayude a la identificación de las distintas amenazas, vulnerabilidades y riesgos de la información que poseen sus sistemas, debiéndose implementar los controles necesarios para la seguridad de su información para salvaguardar su disponibilidad, confidencialidad e integridad.

Se realizó una matriz FODA, donde se ha identificado en forma general sus principales debilidades y amenazas en la que está expuesta la Fuerza Naval en cuestión de Tecnología Informática.

FORTALEZAS	OPORTUNIDADES
✓ Dependencias del Estado Mayor de la Armada ✓ Existencia de talento humano capaz en el área técnica ✓ Existencia de una Planificación Estratégica Institucional ✓ Existencia de una planificación presupuestaria ✓ Existencia de servicios en la RND (Red Naval de Datos) como herramienta para difundir información y políticas ✓ Existencia de aplicaciones informáticas y proyectos en desarrollo que aportan directamente a la automatización de los procesos de cada sector y de la institución ✓ Plataforma de comunicaciones Institucional basado en redes de comunicaciones, multi-acceso. ✓ Estructura Organizacional para la Gestión de las Tecnologías de la Información y comunicaciones a nivel institucional (DIRTIC) ✓ CETEINs, funcionando de acuerdo a la necesidad de su sector o reparto	✓ Surgimiento de telecomunicaciones dedicadas al desarrollo ✓ Existencia de infraestructura de RED WAN a cargo del COMACO (Comando conjunto de las Fuerzas Armadas) para servicio de las FFAA ✓ Existencia de metodologías de Gestión de Riesgos Informáticos listas para ser implementadas
DEBILIDADES	**AMENAZAS**

✓ No está definida en su totalidad ni se aplica un análisis y gestión de riesgos para la seguridad informática ✓ Falta de controles de seguridad de la información (Existen políticas pero no implementadas en su totalidad) ✓ Falta de cultura en seguridad informática por parte de los usuarios de la red ✓ Falta de control de la información interna (Secreta, Confidencial, Uso Interno, Público, etc.). ✓ No existe auditoría y control de los registros de Seguridad ✓ Falta de metodologías estándar para una mejor Gestión de Riesgos informáticos ✓ Poco uso de herramientas en línea que permita el control y evaluación de amenazas y riesgos informáticos ✓ No existen sistemas implementados para el cifrado de archivos ✓ Falta de protección de documentos o mensajes mediante permisos de acceso ✓ Los cambios en los sistemas de procesamiento de información e instalaciones no son controlados ✓ No hay un proceso de gestión para	✓ Crecimiento del hacking y ataques informáticos que vulneran la seguridad ✓ Alto costos de equipos y mantenimiento de tecnologías de uso militar ✓ Acelerado desarrollo tecnológico ✓ Des actualización del personal informático ✓ Perdida de información crítica institucional ✓ Existencia de herramientas modernas y agiles para una mejor gestión informática

las configuraciones y los cambios ✓ No existe un modelo para asignar niveles de importancia a los componentes del entorno informático ✓ No mantiene planes de recuperación ante desastres y de reanudación de negocio	

Bajo esta premisa no existe un Modelo de Gestión de Riesgos y seguridad informática que se acople a la Fuerza Naval, y que se encuentre definido con su viabilidad y las exigencias expuestas para una mejor administración de seguridad informática, con todos estos antecedentes la probabilidad de ocurrencia de riesgos hay en mayor parte, por ende tampoco existen para que se disminuyan tales riesgos. Es por esto que dentro del campo de la informática hay un sin número de Modelos de Gestión de Riesgos que permitirán analizar y administrar los riesgos a los que están sometidos los elementos del trabajo [11], facilitando así la implementación en una organización mediana o pequeña empresa para tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos y controlarlos es decir una mejor gestión de riesgos.

1.5. OBJETIVOS DE LA INVESTIGACION

Es una realidad que el riesgo de las instituciones militares se ha incrementado ya que en el complejo mundo actual de la tecnología, la administración de los recursos de TICs, la consolidación e integración de los mismos es cada vez más compleja. Dentro de este contexto como se aprecia en la Fuerza Naval no se tiene establecido un Modelo de Gestión de Riesgos que administre y mitigue tales riesgos para un mejor control. Con esto es necesario proponer un Modelo de Gestión de Riesgos y Seguridad Informática, para la protección y mejoramiento administrativa de la seguridad en general de las instituciones militares, que analizados para un mejor

análisis y gestión servirán para aplicarlas y tener un mejor respaldo que poseen las mismas.

Se desarrollará un Modelo de Gestión de riesgos y Seguridad de la información para instituciones militares donde se estudiará los riesgos existentes dentro de la Fuerza Naval y se evaluará la propuesta del modelo para determinar la aplicabilidad del mismo.

Al final de este desarrollo se discutirá los resultados que se aplicarán en un caso de estudio real y se verificará que el Modelo de Gestión de Riesgos y Seguridad de la información propuesta, va a permitir tomar decisiones como: reducir, eliminar y mitigar los riesgos en un 50%; logrando obtener un mejor control y gestión de los mismos, para la satisfacción y cumplimiento de requisitos institucionales de protección adecuada de la información logrando así un mejoramiento del 80% en su infraestructura, desarrollo de planes y estrategias de seguridad.

CAPITULO 2.

PROPUESTA DEL MODELO DE GESTIÓN DE RIESGOS EN INSTITUCIONES MILITARES

2.1. FILOSOFÍA DEL MODELO

El proceso para desarrollar la nueva metodología comenzó con la investigación y el estudio pormenorizado de las principales metodologías existentes en el mercado para al análisis de los riesgos informáticos que son: MAGERIT v.3 y OCTAVE v.1. Estas metodologías se han analizado en el *Capítulo 1*, generando un análisis funcional de sus mejores elementos y un cuadro comparativo de las mismas, donde se observó que las dos metodologías buscan un mismo objetivo: el analizar, gestionar el riesgo y la seguridad de la información. Por ende se puede combinarlas y proponer una nueva metodología para luego aplicarla. Esta nueva metodología será consistente y de rápida aplicación que implementará los pasos necesarios para analizar un sistema, identificar las amenazas, las vulnerabilidades asociadas, calcular las ocurrencias de esas amenazas, determinar el impacto en caso de su materialización y por último la obtención del riesgo al que se está expuesto y que a su vez permitirá aplicarla a la realidad de las instituciones militares, en cuanto a riesgos informáticos se trate y a la vez identificar y gestionar los riesgos de tecnologías de la información.

Las dos metodologías estudiadas tienen por objetivo los siguientes puntos:

- ✓ Planificación de la reducción de riesgos
- ✓ Planificación de la prevención de accidentes
- ✓ Visualización y detección de las debilidades existentes en los sistemas
- ✓ Ayuda en la toma de las mejores decisiones en materia de seguridad de la información.

El modelo propuesto se enfocará en un análisis cualitativo de riesgos, este enfoque emplea valoraciones de escala de niveles. Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo. [11].

Este modelo brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001, y esta diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo. El enfoque de este modelo es el adecuado para el entorno de la organización y en particular cumple con los lineamientos de toda la gestión de riesgos de una empresa. Este modelo de Gestión de riesgos y seguridad de la información, es una parte integral de todas las actividades de gestión de seguridad de la información y que se lo aplica tanto a la implementación como al funcionamiento continuo de un SGSI.

En un SGSI, el establecimiento del contexto, la valoración de los riesgos, el desarrollo del plan del riesgo y la aceptación del riesgo son parte de la fase “Planificar”. En la fase de “Hacer” del SGSI, se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo. En la fase de “Verificar” del SGSI, los directores determinaran la necesidad de revisiones de las valoraciones y el tratamiento del riesgo ante los incidentes. En la fase de “Actuar” del SGSI, se lleva a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

Con esta breve explicación de cómo funciona un SGSI; se quiere decir que este modelo propuesto se encuentra alineado a las fases del SGSI, a continuación se describe la alineación del SGSI, con el modelo en contexto:

PROCESO DEL SGSI	FASES DE MODELO DE GESTION DE RIESGOS Y SEGURIDAD DE LA INFORMACION
Planificar	Contexto organizacional Identificación de los riesgos Evaluación de los riesgos Estimar el riesgo
Hacer	Tratamiento de los riesgos
Verificar	Monitoreo y revisión de los factores de riesgo
Actuar	Monitoreo revisión y mejora de la gestión del riesgo Comunicar el riesgo

2.1.1. DESCRIPCION DE LA METODOLOGIA

Para el diseño y desarrollo de la nueva metodología de gestión de riesgos y seguridad de la información, se partió del proceso de Gestión de Riesgos que tiene la ISO 31000 (*Ver Figura 2.1);* hay que puntualizar que la metodología MAGERIT v.3, sigue la terminología de la normativa ISO 31000 que responde al proceso de Gestión de Riesgos dentro de un marco de trabajo. En cuanto a la metodología OCTAVE v.1, es un método de evaluación y de gestión de los riesgos para garantizar la seguridad del sistema informático desarrollado bajo el estándar internacional ISO 27001. Como se puede ver estas dos metodologías están normadas y guiadas por las normas ISO.

A continuación se describe el proceso de Gestión de Riesgos de la norma ISO 31000, la cual se tomó como referencia para la nueva metodología:

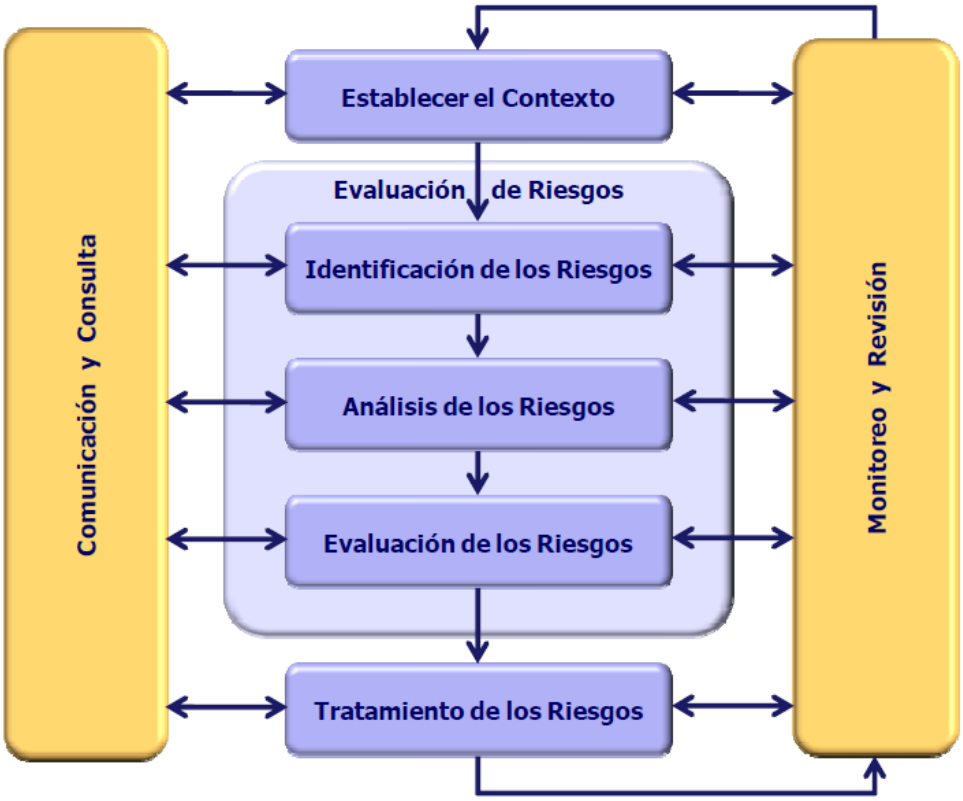

Figura 2.1: Proceso de Gestión de Riesgos[12]

En la *Figura 2.1,* se detalla los procesos que tiene la Gestión de riesgos normada por la ISO 31000, partiendo de esto la nueva metodología propuesta, tendrá elementos y valores que proporcionarán una metodología consistente y que a su vez permita aplicarla a la realidad de la institucional militar. La nueva metodología, se obtiene mediante la unificación de las metodologías MAGERIT y OCTAVE, considerando las similitudes y características propias de cada una de ellas, logrando obtener como resultado cuatro fases juntas con sus etapas y actividades.

[12] Fuente: ISO 31000:2009

A continuación se da una breve descripción de cómo se abordo el diseño de estas cuatro fases mencionadas:

PROCESO DE GESTION DE RIESGOS ISO 31000:2009

PROCESO: ESTABLECER EL CONTEXTO

De este proceso se obtiene la Fase 1 siguiente:

FASE 1: Contexto Organizacional

Esta fase contemplará 2 etapas:

1. Alcance
2. Contexto de Gestión de Riesgos

PROCESO: IDENTIFICACIÓN DE LOS RIESGOS

PROCESO: ANÁLISIS DE RIESGOS

De la vinculación de estos dos procesos se obtiene la Fase 2 siguiente:

FASE 2: Identificación de los riesgos

Esta fase contemplará 4 etapas:

1. Determinación de los activos
2. Determinación de las amenazas
3. Determinación de controles de seguridad
4. Determinación de las vulnerabilidades

PROCESO: EVALUACIÓN DE LOS RIESGOS

De este proceso se obtiene la Fase 3 siguiente:

FASE 3: Evaluación de los Riesgos

Esta fase contemplará 3 etapas:

1. Determinación del impacto
2. Determinación de la probabilidad de incidentes
3. Estimación del riesgo

PROCESO: TRATAMIENTO DE LOS RIESGOS

De este proceso se obtuvo la Fase 4 siguiente:

FASE 4: Tratamiento de los Riesgos

Esta fase contemplará 2 etapas:

1. Estrategias de protección
2. Plan de mitigación

PROCESO: COMUNICACIÓN Y CONSULTA

De este proceso se obtiene la Fase 5 siguiente:

FASE 5: Comunicación

Esta fase contemplará 1 etapa:

1. Comunicar el riesgo

PROCESO: MONITOREO Y REVISION

De este proceso se obtiene la Fase 6 siguiente:

FASE 6: Monitoreo y Revisión

Esta fase contemplará 2 etapas:

1. Monitoreo y revisión de los factores del riesgo
2. Monitoreo, revisión y mejora de la gestión del riesgo

Las 6 fases detalladas anteriormente componen el marco de trabajo de la metodología propuesta, misma que permitirá analizar y administrar los riesgos en los siguientes ámbitos:

- ✓ Evaluación de los activos informáticos sujetos a riesgos
- ✓ Evaluación de los servicios de seguridad o controles existentes
- ✓ Evaluar las vulnerabilidades ante amenazas identificadas
- ✓ Evaluación de amenazas o causas de riesgos
- ✓ Determinación y valoración del daño causado
- ✓ Estimación del nivel de riesgo y determinación de controles

2.2. DESARROLLO DEL MODELO

El modelo propuesto de Gestión de riesgos y seguridad de la información, tiene como objetivo el mejorar la seguridad, y una mejor gestión de análisis y riesgos para instituciones militares, esta metodología será específica para estas instituciones, facilitando la adopción generalizada de medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en los diferentes sistemas, garantizando así el cumplimiento de requisitos para la validez y eficacia de los procedimientos administrativos y operativos que exigen las Instituciones militares.

Los procedimientos y las actividades del modelo de Gestión de riesgos y seguridad de la información propuesto, se han integrado los mejores elementos de las metodologías MAGERIT y OCTAVE, estas son la base referencial sobre el cual se ha establecido el nuevo marco del proceso de Gestión de Riesgos y seguridad de la información.

A continuación se realiza un check list de cómo se formó el modelo propuesto con la unión de los mejores elementos de las metodologías:

ETAPAS DEL MODELO PROPUESTO	MAGERIT	OCTAVE	ISO 27001
Alcance	X		
Contexto de Gestión de riesgos	X	X	
Determinación de los activos	X		
Determinación de las amenazas	X	x	
Determinación de las vulnerabilidades	X	X	
Determinación de controles de seguridad existentes			X
Determinación del impacto		X	
Determinación de la probabilidad de incidentes	X		
Estimación del estado del riesgo		X	
Estrategias de protección		X	X
Plan de mitigación	X		X
Comunicar el riesgo	X		
Monitoreo y revisión de los factores de riesgo	X		
Monitoreo, revisión y mejora de la gestión del riesgo	X		

A continuación se detalla el modelo el mismo que está dirigido al personal técnico y administrativo involucrado en la Gestión de Seguridad y Tecnologías de la Información.

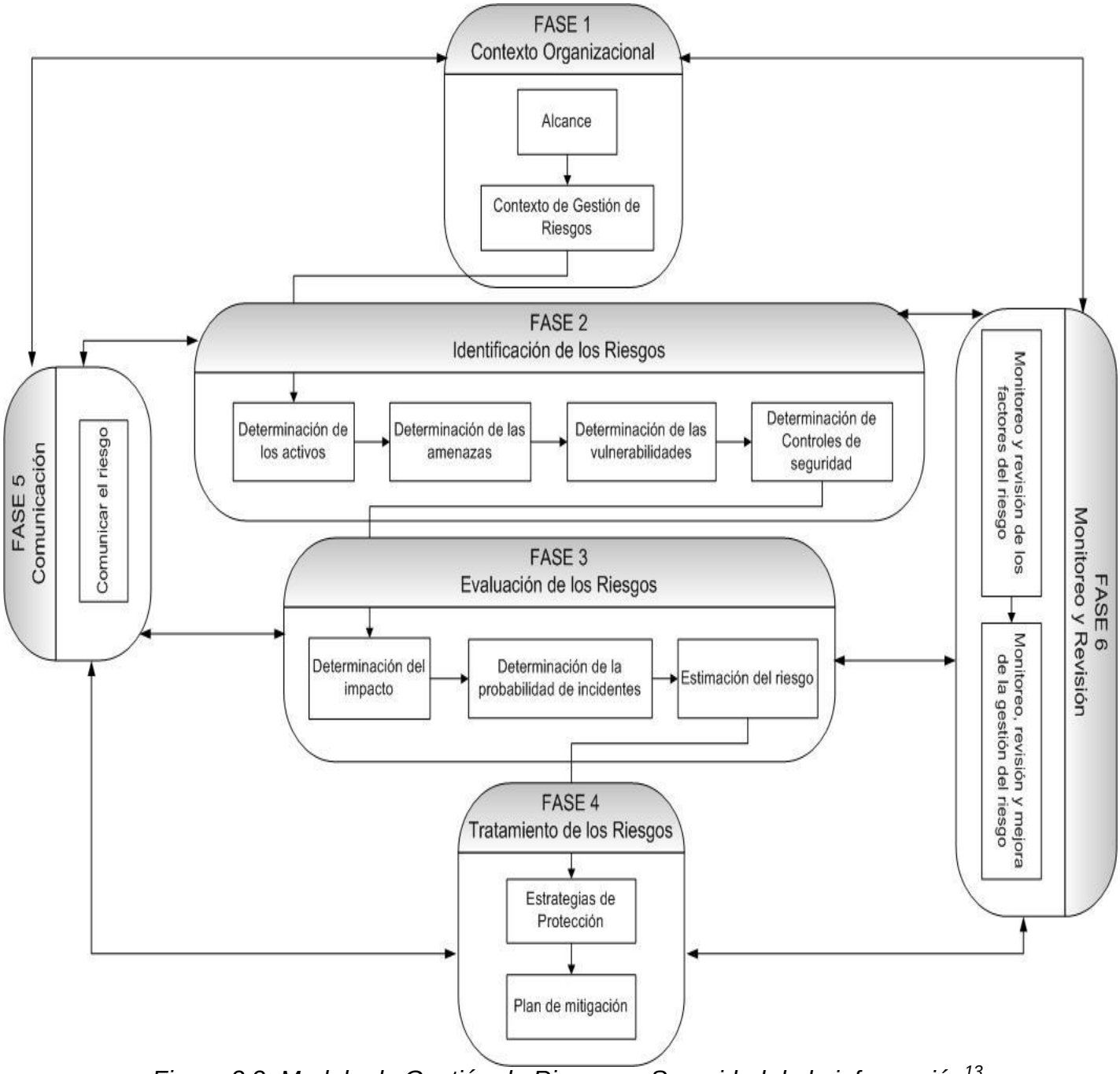

Figura 2.2: Modelo de Gestión de Riesgos y Seguridad de la información[13]

[13] Fuente: La autora

Como se puede observar en la *Figura 2.2,* la metodología de Gestión de Riesgos y Seguridad contiene las siguientes fases:

Fase1: Contexto Organizacional.- Lleva a una determinación de los parámetros y condicionantes externos e internos, que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados.

Fase 2: Identificación de los riesgos.- Buscará una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente fase, lo que no se identifique quedará como riesgo oculto o ignorado.

Fase 3: Evaluación de los riesgos.- Buscará calificar los riesgos identificados, ordenando su importancia relativa (análisis cualitativo). Como resultado del análisis, se tendrá una visión estructurada que permita centrar en lo más importante para su análisis y proceder a evaluar, donde se integran factores de percepción, de estrategia y de política, permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como, en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

Fase 4: Tratamiento de los riesgos.- Recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones como veremos más adelante.

Fase 5: Comunicación.- Es importante recordar que los sistemas de información deben ser soporte de la productividad de la Organización. Siempre hay que buscar

un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores.

Fase 6: Monitoreo y revisión.- Es imprescindible ver qué ocurre en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

2.2.1. FASE 1: CONTEXTO ORGANIZACIONAL

Dentro de esta fase se realizará una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados. En cuanto al otro elemento a destacar es la identificación de contexto organizacional, en el que se desarrollará el proceso de gestión de riesgos y que debe ser objeto de una revisión continua para adaptarse a las circunstancias de cada momento.

2.2.1.1 Etapa 1: Alcance

2.2.1.1.1. Actividad 1: Definición del Alcance

FASE 1. CONTEXTO ORGANIZACIONAL
E1: Alcance **A1: Definición del Alcance**
Objetivo • Obtener de los procesos estratégicos existentes de la institución, procesos agregados de valor y procesos habilitantes de apoyo que conforman la cadena

de valor que se encuentran implementados en las instituciones militares. • Identificar los miembros de cada área operativa dentro de área a definir. • Considerar si tienen políticas de seguridad de la información en la organización
Criterios de Entrada ❑ Procesos estratégicos, agregados de valor y habilitantes de apoyo ❑ Misión, Visión de la institución ❑ Áreas operativas con miembros pertenecientes ❑ Políticas de seguridad de la información de la organización si lo hubiere
Criterio de Salida ❑ Organigrama Estructural ❑ Misión, Visión de la institución ❑ Procesos estratégicos, agregados de valor y de apoyo ❑ Miembros de áreas operativas de procesos ❑ Plantilla de definición del alcance.
Recomendaciones Se recomienda especificar cada división o departamento del organigrama estructural resultante especificando lo más puntual de sus funciones y las personas integrantes de los mismos para definir el alcance; una vez realizado esto obtener el patrocinio de la directiva o alta gerencia de la organización y a su vez especificar el alcance de la gestión del riesgo que puede ser una aplicación tecnológica de la información, infraestructura de tecnología de la información, un proceso del negocio o una parte definida de la organización.

A continuación se detalla la plantilla de ayuda:

Definición del Alcance	
DEPARTAMENTO / REPARTO:	
SECCION / DIVISION:	
Área:	**Descripción del Área:**
Miembros integrados:	
Observaciones:	
Fecha:	**Realizado por:**
Aprobado por:	

Plantilla 2.1: Definición del alcance[14]

2.2.1.2. Etapa 2: Contexto del Proceso de Gestión de Riesgos

En esta etapa, se establece el contexto del proceso de Gestión de Riesgos y se define los parámetros básicos para la gestión de riesgos estableciendo el ámbito y los criterios para el resto del proceso.

2.2.1.2.1. Actividad 1: Selección de miembros responsables

FASE 1. CONTEXTO ORGANIZACIONAL
E2: Contexto de Gestión de Riesgos **A1: Selección de miembros responsables**
Objetivo • Determinar los miembros responsables de acuerdo al criterio de la directiva de la institución a comprometerse al desarrollo y mejoramiento de los procesos al que el alcance se refiere.
Criterio de Entrada ❑Plantilla Definición Alcance, con miembros integrados de cada área: *Fase1, E1,*

[14] Fuente: La autora

A1, Plantilla 2.1: Definición del alcance. ❑Estructura Orgánica Funcional de la institución
Criterio de Salida ❑Determinación de personas responsables de cada proceso ❑Plantilla de Equipo para el análisis de cada proceso o área de la organización
Recomendaciones Asegurarse que cada persona responsable de la actividad asignada se comprometa a llevar a conformar el equipo de análisis tomando en cuenta que se debe también nombrar personas de respaldo para asignaciones en caso que faltare algún miembro del equipo, estas definiciones de responsables lo realizará la directiva o alta gerencia de la institución.

A continuación se detalla la plantilla de ayuda:

Equipo para el Análisis de Riesgos			
REPARTO:		**DEPARTAMENTO/ DIVISIÓN/ SECCIÓN:**	
Área o proceso:		**Descripción del Proceso o Área:**	
Responsables		**Participa como**	**Cargo**
Observaciones:			
Fecha:		**Realizado Por:**	
		Aprobado Por:	

Plantilla 2.2: Equipo para el Análisis de Riesgos[15]

[15] Fuente: La autora

2.2.1.2.2. Actividad 2: Definir la metodología de Evaluación de Riesgos

FASE 1. CONTEXTO ORGANIZACIONAL
E2: Contexto de Gestión de Riesgos **A2: Definir la Metodología de Evaluación de Riesgos**
Objetivo • Determinar escalas de valoración de probabilidad e impacto basándose en un enfoque cualitativo • Determinar marcos de probabilidad e impacto basándose en un enfoque cualitativo • Determinar el nivel de riesgo
Criterios de Entrada ❑ Información de Seguridad de procesos ❑ Procedimientos de gestión ❑ Procesos de probabilidades de riesgos si lo tuviere
Criterios de Salida ❑ Escalas de riesgo, probabilidad e impacto ❑ Matriz de cálculo del riesgo ❑ Plantilla de resultados de la metodología de evaluación del riesgo
Recomendaciones Se recomienda para valorar el riesgo, aplicar un enfoque cualitativo, ya que es de mayor rapidez y eficaz. Si la institución no tiene evaluaciones previas de riesgos de seguridad de la información, es recomendable definir escalas cualitativas descritas más adelante, para la estimación del riesgo. Considerar que la metodología de evaluación del riesgo puede tener varios enfoques y en esta metodología propuesta se ha considerado un enfoque asequible y personalizado para instituciones militares. Esta metodología de evaluación del riesgo deberá ser aprobada por la alta dirección o gerencia.

A continuación se detallan las escalas para la evaluación del riesgo donde se presenta impacto, probabilidad y el riesgo por medio de escalas cualitativas:

IMPACTO
A: alto
M: medio
B: bajo

Tabla 2.1: Escala para definir el impacto[16]

RIESGO
A: alto
M: medio
B: bajo

Tabla 2.2: Escala para definir el riesgo[17]

PROBABILIDAD OCURRENCIA	
MA: muy frecuente	- A diario
A: frecuente	- Mensualmente
M: posible	- Una vez al año
B: poco frecuente	- Cada varios años
MB: muy poco o raro	- Siglos

Tabla 2.3: Escala para definir la probabilidad[18]

La siguiente matriz indica la combinación del impacto y la probabilidad para calcular el riesgo donde el riesgo puede ser ALTO, MEDIO Y BAJO:

		PROBABILIDAD				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	**A**	M	M	A	A	A
	M	B	M	M	A	A

[16] Fuente: OCTAVE
[17] Fuente: MAGERIT, La autora
[18] Fuente: MAGERIT, La autora

	B	B	B	B	M	M

Tabla 2.4: Matriz para calcular el riesgo[19]

A continuación se detalla la plantilla de resultados aplicados en las matrices anteriores:

Resultado de Definir la Metodología de Evaluación del riesgo			
Escala de probabilidad de ocurrencia:			
Escala de impacto:			
Escala del riesgo:			
Matriz de cálculo del riesgo:			
Observaciones:			
Fecha:		**Realizado Por:**	
		Aprobado Por:	

Plantilla 2.3: Plantilla de Resultados de la metodología de evaluación del riesgo[20]

2.2.1.2.3. Actividad 3: Definir criterios de evaluación del riesgo

FASE 1. CONTEXTO ORGANIZACIONAL
E2: Contexto de Gestión de Riesgos **A3: Definir los Criterios de evaluación del riesgo**
Objetivo • Definir criterios de evaluación del riesgo con el fin de determinar el riesgo

[19] Fuente: La autora
[20] Fuente: La autora

en la seguridad de la información en la organización. • Permitir priorizar el riesgo teniendo en cuenta aspectos como: el valor estratégico del proceso de negocio, la criticidad de los activos, los requisitos legales y reglamentarios, importancia de la disponibilidad, confidencialidad e integridad de operaciones y del negocio, y reputación de consecuencias negativas y percepciones de partes interesadas.
Criterio de Entrada ❑ Lista de riesgos o vulnerabilidades de seguridad de la información de la organización.
Criterio de Salida ❑ Plantilla de Definir los criterios de evaluación del riesgo
Recomendaciones Se recomienda aplicar la plantilla de resultados de criterios de evaluación del riesgo y aplicar criterios propios, que definan dentro del equipo de análisis conjuntamente con la aprobación de alta directiva o gerencia junto con la lista de riesgos y/o vulnerabilidades de la organización que se encuentran prioritarios y latentes. Los criterios que se especificarán en la matriz definida dependerán de la institución y negocio del mismo.

Se recomienda desarrollar criterios para la evaluación del riesgo, con el fin de determinar el riesgo en la seguridad de la información de la organización, se tendrá en cuenta los siguientes aspectos:

- ✓ El valor estratégico del proceso de información del negocio
- ✓ La criticidad de los activos de información involucrados
- ✓ Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- ✓ La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio
- ✓ Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación

A continuación se detalla la plantilla de resultados de los criterios de evaluación del riesgo:

Resultado de Definir los criterios de evaluación del riesgo			
Criterios	**Bajo**	**Medio**	**Alto**
Observaciones:			
Fecha:		**Realizado Por:**	
		Aprobado Por:	

Plantilla 2.4: Plantilla de Resultados de definir los criterios de evaluación del riesgo[21]

2.2.1.2.4. Actividad 4: Definir criterios de Impacto

FASE 1. CONTEXTO ORGANIZACIONAL
E2: Contexto de Gestión de Riesgos **A4: Definir los Criterios de Impacto**
Objetivo • Definir criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de la seguridad de la información.
Criterio de Entrada ❑ Plantilla de Definir los criterios de evaluación del riesgo: *Fase1, E2, A3, Plantilla 2.4.*
Criterio de Salida ❑ Plantilla de Definir los criterios de impacto

[21] Fuente: La autora

Recomendaciones

Se recomienda aplicar la plantilla de criterios de impacto, se debe considerar las áreas de impacto que deben ser elegidas, de acuerdo a la importancia que tengan en relación al negocio. Se debe tomar en cuenta que la *Plantilla 2.5, Fase1, E2, A4, de Definir los criterios de evaluación del riesgo,* sobre este se definirá los criterios de impacto y sobre las áreas de riesgos implementadas. Se debe determinar estos criterios con el equipo de análisis conjuntamente con la aprobación de alta directiva o gerencia.

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- ✓ Nivel de clasificación de los activos de información impactados
- ✓ Brechas en la seguridad de la información
- ✓ Daños a la reputación
- ✓ Incumplimiento de requisitos legales, reglamentarios o contractuales
- ✓ Perdida del negocio y del valor financiero
- ✓ Alteraciones de planes y fechas limites

Hay que puntualizar que no todos los aspectos a considerar serán obligatorios en la institución, si se toman estos aspectos o se aumentaran, esto se definirá en el equipo de análisis.

A continuación se detalla la plantilla de resultados de los criterios de impacto:

Resultado de Definir los criterios de impacto			
Área de impacto	**Bajo**	**Medio**	**Alto**
Observaciones:			
Fecha:		**Realizado Por:**	

		Aprobado Por:	

Plantilla 2.5: Plantilla de Resultados de definir los criterios de impacto[22]

2.2.1.2.5. Actividad 5: Definir criterios de aceptación de riesgo

FASE 1. CONTEXTO ORGANIZACIONAL
E2: Contexto de Gestión de Riesgos **A5: Definir criterios de aceptación de riesgo**
Objetivo • Desarrollar y especificar criterios de aceptación de riesgo que dependan con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.
Criterios de Entrada ❑ Relacionar factores de criterios de negocio, aspectos legales, reglamentarios, operaciones, tecnológica y finanzas
Criterio de Salida ❑ Plantilla de Definir criterios de aceptación del riesgo
Recomendaciones Se recomienda que la organización defina sus propias escalas para los niveles de aceptación del riesgo y esto será aprobado por alta gerencia o dirección.

La Dirección de la Organización sometida al análisis de riesgos, debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. 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. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, etc.). Los criterios de

[22] Fuente: La autora

aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo, deberían considerarse los siguientes elementos:

- ✓ Criterios del negocio
- ✓ Aspectos legales y reglamentaros
- ✓ Operaciones
- ✓ Tecnológica
- ✓ Finanzas
- ✓ Factores sociales y humanas

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Gerencia o alta dirección; siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- ✓ cuando el impacto es asumible
- ✓ cuando el riesgo es asumible
- ✓ cuando el coste de las seguridades oportunas es desproporcionado en comparación al impacto y riesgo

A continuación se detalla la plantilla de aceptación del riesgo, y que dependerá de la institución el determinar el nivel y escala de aceptación del mismo:

Resultado de Definir los criterios de aceptación del riesgo		
Nivel de riesgo estimado	**Criterio de aceptación**	**Descripción del criterio**
Alto		
Medio		
Bajo		
Observaciones:		

Fecha:		**Realizado Por:**
		Aprobado Por:

Plantilla 2.6: Resultado de Definición de aceptación del riesgo[23]

2.2.2. FASE 2: IDENTIFICACIÓN DE LOS RIESGOS

Dentro de esta fase se encontrará, se reconocerá y se registrará los riesgos. El propósito es identificar lo que podría suceder o que situaciones podrían existir que puedan afectar a la consecución de los objetivos del sistema u organización. Una vez que se identifique el riesgo, la institución debe identificar los controles existentes, tales como el diseño, características, personas, procesos y sistemas. El proceso de identificación de riesgos incluye la identificación de las causas y el origen del riesgo, hechos, situaciones o circunstancias que podrían tener un impacto material sobre los objetivos y la naturaleza de ese impacto.

2.2.2.1. Etapa 1: Determinación de los Activos

En esta etapa, se identificará los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en que dimensiones de seguridad son importantes y valorando esa importancia.

2.2.2.1.1. Actividad 1: Identificación de los Activos

FASE 2. IDENTIFICACIÓN DE LOS RIESGOS
E1: Determinación de los Activos **A1: Identificación de los Activos**
Objetivo • Identificar los activos que componen el sistema dentro de una organización, determinando sus características, atributos y clasificación en los tipos determinados

[23] Fuente: La autora

Criterios de Entrada
❑ Lista de activos identificados con su propietario, su responsabilidad y rendición de cuentas sobre este; hay que tomar en cuenta que este listado será identificado dentro del alcance que se determinó en la *Fase 1*
Criterios de Salida
❑ Relación de activos a considerar ❑ Plantilla de identificación de activos
Recomendaciones Se recomienda una buena identificación de los activos, ya que se materializará con precisión el alcance del proyecto, determinará la interlocución con los grupos de usuarios, permitirá determinar las dependencias precisas entre activos, permitirá valorar los activos con precisión, permitirá identificar y valorar las amenazas con precisión y permitirá determinar qué seguridad serán necesarias para proteger el sistema. Hay que tomar en cuenta que el propietario del activo puede no tener derechos de propiedad sobre este, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad. Este propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización.

Para identificar los activos lo esencial es primero verificar cuales activos son importantes y los que llenan los objetivos de la institución; segundo cuales activos adicionales se tendrá que proteger por obligación legal; y tercero, si hay activos relacionados con los anteriores. Si por ejemplo en su unidad tiene 300 puestos de trabajo (PC), todos idénticos a efectos de configuración y datos que manejan, no es conveniente analizar 300 activos idénticos. Basta con analizar un PC genérico cuya problemática representa la de todos. Agrupar simplifica el modelo. Una buena idea es tener los activos agrupados por perfiles de configuración de equipos.

Guiarse en el *Anexo 6: Catálogo de elementos.pdf, Tipo de Activos*, el contenido de este catálogo contiene los tipos de activos para especificar la plantilla; esta será modificable dependiendo de la organización.

A continuación se detalla la plantilla de ayuda para identificación de activos:

Resultado de la Identificación de los Activos								
Reparto:				**Departamento:**		**Unidad Responsable:**		
No.	**Nombre del Activo**	**Descripción del Activo**	**Tipo de Activo**	**Detalle del tipo de activo**	**Persona Responsable del activo**	**Funciones principales del activo**	**Relación con otro activo**	**Cantidad**
Observaciones:								
Fecha:			**Realizado Por:**		**Aprobado Por:**			

Plantilla 2.7: Resultado de la Identificación de Activos[24]

[24] Fuente: La autora

2.2.2.1.2. Actividad 2: Valoración de Activos

FASE 2. IDENTIFICACIÓN DE LOS RIESGOS
E1: Determinación de los Activos **A2: Valoración de Activos**
Objetivo • Identificar las dimensiones que se van a utilizar y los criterios para valorar los activos • Valorar el coste cualitativo para cada uno de los activos valorados
Criterio de Entrada ❑ Resultados de la identificación de activos: *Fase2, E1, A1, Plantilla 2.7.*
Criterios de Salida ❑ Modelo de valoración de activos ❑ Plantilla de valoración de los activos
Recomendaciones Se recomienda realizar entrevistas a personas responsables de servicios que conocen las consecuencias de sus fallos de seguridad, que conocen las consecuencias de la no prestación de servicios o de su prestación degradada, que conocen las consecuencias de un incidente o también responsables de sistemas de información, y responsables de operación. Se debe escoger el modelo de valoración y escalas; aptos para la institución.

Para las características de valoración que se utilizará para cada uno de los activos véase: *Anexo 6(Catálogo de elementos.pdf, Características de Valoración),* en donde los activos incurrirán en la disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad y trazabilidad. Para cada una de estas dimensiones se aplicará la siguiente tabla de criterio de valoración en donde el valor 0 es despreciable (a efectos del riesgo), y 10 para un daño extremadamente grave:

valor		***criterio***
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Tabla 2.5: Matriz Valoración del activo sobre las características[25]

A continuación se detalla una plantilla de ayuda para especificar por cada dimensión de activo y escala de valoración:

[25] Fuente: MAGERIT

Resultado de la Valoración del activo									
No.	**Tipo de Activo**	**Nombre del Activo**	**Funciones principales del Activo**	**Escala de dimensión**					
				Disponibilidad	**Integridad**	**Confidencialidad**	**Autenticidad**	**Trazabilidad**	**Resultado Valoración**
				Valoración	Valoración	Valoración	Valoración	Valoración	
	Observaciones:					**Realizado Por:**			
	Fecha					**Aprobado Por:**			

Plantilla 2.8: Plantilla de Valoración de Activos[26]

[26] Fuente: La autora

A continuación se detalla otra valoración de los activos que dependerán de las siguientes dimensiones a describirse:

INCUMPLIMIENTO DE LA LEGISLACIÓN Y/O REGLAMENTACIÓN	
VALORACIÓN	**CRITERIO**
9	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	probablemente cause un incumplimiento grave de una ley o regulación
5	probablemente sea causa de incumplimiento de una ley o regulación
3	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	pudiera causar el incumplimiento leve o técnico de una ley o regulación

Tabla 2.6: Matriz Valoración del activo sobre el incumplimiento de la legislación[27]

ADMINISTRACIÓN Y GESTIÓN	
VALORACIÓN	**CRITERIO**
9	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	probablemente impediría la operación efectiva de la Organización
5	probablemente impediría la operación efectiva de más de una parte de la Organización
3	probablemente impediría la operación efectiva de una parte de la Organización
1	pudiera impedir la operación efectiva de una parte de la Organización

Tabla 2.7: Matriz Valoración del activo sobre el deterioro en la Administración y Gestión[28]

[27] Fuente: MAGERIT
[28] Fuente: MAGERIT

PERDIDA DEL BUEN NOMBRE EN LA REPUTACIÓN	
VALORACIÓN	**CRITERIO**
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con el público en general
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	Probablemente afecte negativamente a las relaciones internas de la Organización
2	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones

Tabla 2.8: Matriz Valoración del activo sobre la pérdida del buen nombre en la reputación[29]

[29] Fuente: MAGERIT

BRECHAS ASOCIADAS CON LA INFORMACIÓN PERSONAL	
VALORACIÓN	**CRITERIO**
6	probablemente afecte gravemente a un grupo de individuos
	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	probablemente afecte gravemente a un individuo
	probablemente quebrante seriamente leyes o regulaciones
4	probablemente afecte a un grupo de individuos
	probablemente quebrante leyes o regulaciones
3	probablemente afecte a un individuo
	probablemente suponga el incumplimiento de una ley o regulación
2	pudiera causar molestias a un individuo
	pudiera quebrantar de forma leve leyes o regulaciones
1	pudiera causar molestias a un individuo

Tabla 2.9: Matriz Valoración del activo sobre brechas asociadas con la información personal[30]

BRECHAS EN ORDEN PÚBLICO	
VALORACIÓN	**CRITERIO**
9	alteración sería del orden público
6	probablemente cause manifestaciones, o presiones significativas
3	causa de protestas puntuales
1	pudiera causar protestas puntuales

Tabla 2.10: Matriz Valoración del activo sobre brechas en orden público[31]

[30] Fuente: MAGERIT
[31] Fuente: MAGERIT

HACER PELIGRAR LA SEGURIDAD	
VALORACIÓN	**CRITERIO**
10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
1	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Tabla 2.11: Matriz Valoración del activo sobre hacer peligrar la seguridad[32]

A continuación se detalla la plantilla de ayuda para valorar por cada dimensión anteriormente especificada:

[32] Fuente: MAGERIT

Resultado de la Valoración del activo								
No.	**Activo**	**Funciones principales del Activo**	**Escala de dimensión**					
			Incumplimiento de la legislación y/o reglamentación	**Administración y gestión**	**Perdida del buen nombre**	**Brechas asociadas con la información personal**	**Brechas en Orden público**	**Hacer peligrar la seguridad**
			Valoración	*Valoración*	*Valoración*	*Valoración*		*Valoración*
	Observaciones:				**Realizado Por:**			
	Fecha:				**Aprobado Por:**			

Plantilla 2.9: Plantilla de Valoración de Activos[33]

[33] Fuente: La autora

2.2.2.2. Etapa 2: Determinación de las Amenazas

En esta etapa se identificará las amenazas relevantes sobre el sistema a analizar, caracterizándolas por estimaciones de ocurrencia (probabilidad) y daño causado (degradación). Esta etapa determina que puede pasar, que consecuencias se derivan y cuan probable es que pase.

2.2.2.2.1. Actividad 1: Identificación de las Amenazas

FASE 2. IDENTIFICACIÓN DE LOS RIESGOS
E2: Determinación de las Amenazas **A1: Identificación de las Amenazas**
Objetivo • Identificar las amenazas relevantes sobre cada activo
Criterios de Entrada ❑ Resultados de la identificación de activos *Fase2, E1, A1, Plantilla 2.7* ❑ Informes de vulnerabilidades en el producto, si lo hubiere.
Criterios de Salida ❑ Árboles de categorías de amenazas. *Ver Figura 2.3, Figura 2.4, Figura 2.5.* ❑ Tabla de relación entre tipo de activos y perfil de amenazas. *Ver Tabla 2.12.* ❑ Plantilla de identificación de amenazas
Recomendaciones Se recomienda aplicar los árboles de amenazas que se encuentran en el *Anexo 6: Catálogo de Elementos.pdf,* sobre los activos más críticos encontrados en la Actividad 1. También se recomienda aplicar los perfiles de amenazas dependiendo del tipo de activo para relacionar y llenar la plantilla de ayuda.

A continuación se describe las categorías de perfil de amenazas que se deben aplicar para la identificación de las mismas; estas categorías que se clasifican son extraídas del método OCTAVE y esta son las siguientes:

- ✓ Actores humanos con acceso a la red: Estas son las amenazas basadas en la red a sus activos críticos, estas pueden ser deliberadas o accidentales.
- ✓ Actores humanos con acceso físico: Estas son las amenazas físicas a sus activos críticos. Estas amenazas pueden ser deliberadas o accidentales.
- ✓ Problemas del sistema: Se trata de problemas con los sistemas de Tecnologías de la información. Pueden ser defectos del hardware, defectos del software, falta de disponibilidad de los sistemas relacionados, virus, código malicioso y otros problemas relacionados con los sistemas.
- ✓ Otros problemas: Estos son problemas que están fuera del control. Estos pueden ser desastres naturales que pueden afectar a los sistemas de TI de su organización, falta de disponibilidad de los sistemas mantenidos por otras organizaciones, y las cuestiones de interdependencia que incluyen problemas con los servicios de infraestructura, como cortes de energía eléctrica, tuberías de aguas rotas y cortes de telecomunicaciones.

Véase *Anexo 6 (Catálogo de elementos.pdf, Identificación de Amenazas),* donde se encontrará por cada categoría de amenazas; todos los tipos que pueden haber en cada una de ellas.

Cada amenaza tiene la siguiente descripción que le identifica:

- ✓ Activo: Cosa de valor para la organización
- ✓ Actor: Qué o quién puede violar los requisitos de seguridad (confidencialidad, integridad, disponibilidad) de un activo; estos pueden ser internos o externos.
- ✓ Motivo: Define si las intenciones del actor son deliberadas (actos intencionados) o accidentales.
- ✓ Acceso: Forma en que se accede al mismo por el actor (acceso a la red, el acceso físico).
- ✓ Resultado: El resultado de la amenaza detectada puede ser por (revelación: que el actor puede ver, modificación: que el actor modifique, destrucción- perdida: que el actor pierda alguna acción, interrupción: que el actor no pueda acceder).

A continuación se detalla por cada perfil de amenaza el árbol correspondiente que se deberá aplicar para identificar las mismas:

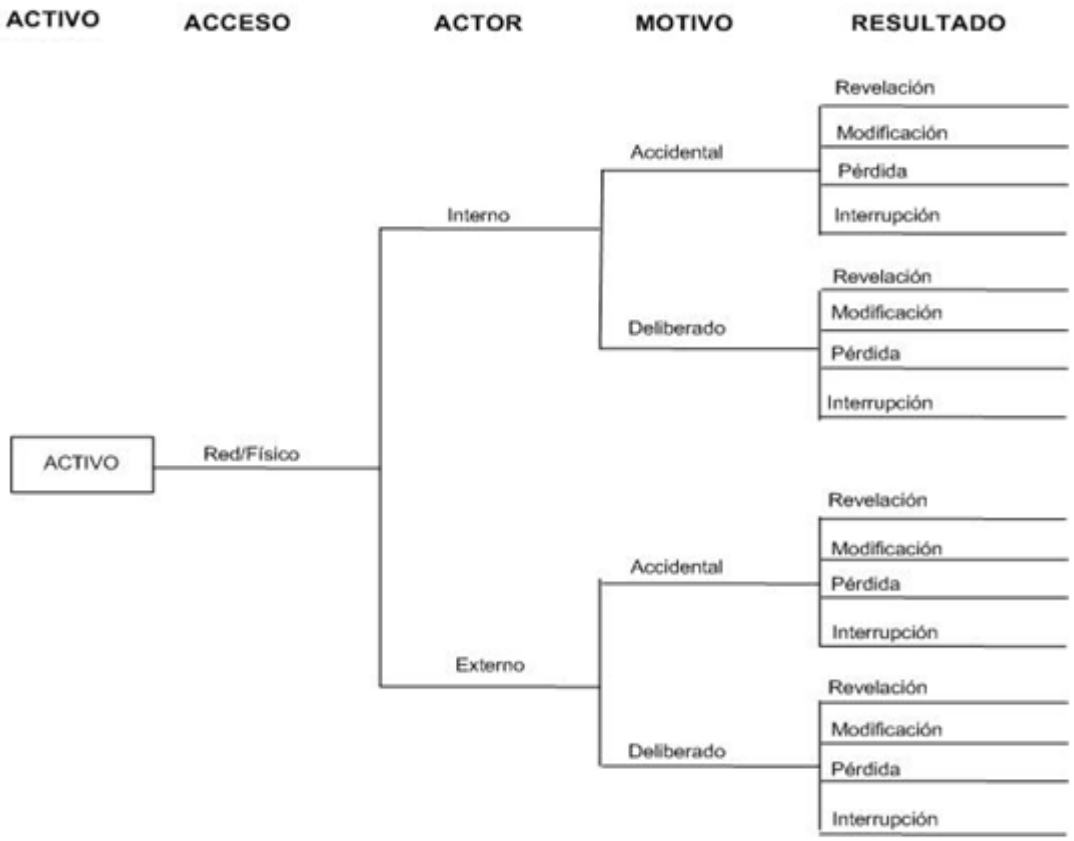

Figura 2.3: Árbol de amenazas basado en activos para actores humanos de acceso de red o acceso físico[34]

[34] Fuente: OCTAVE

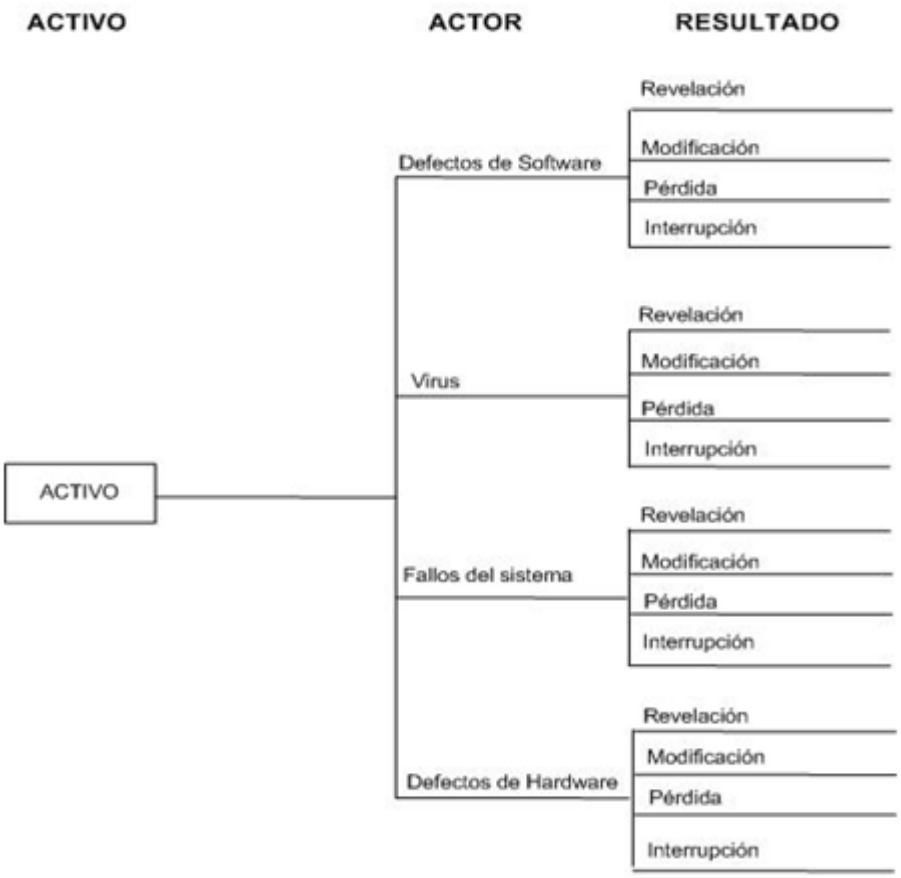

Figura 2.4: Árbol de amenazas basado en activos para problemas de sistema u otros problemas[35]

Dependerá de la organización el análisis para identificar las amenazas potenciales con colores rojos y las que no hay efecto de riesgo en verde o colores que representen críticos o no críticos; o llevar estas ramas que pueden ser de línea continua; que significa que son amenazas potenciales, y las ramas de línea punteada que no representan ningún riesgo.

A continuación se detalla un ejemplo de estas ramas:

[35] Fuente: OCTAVE

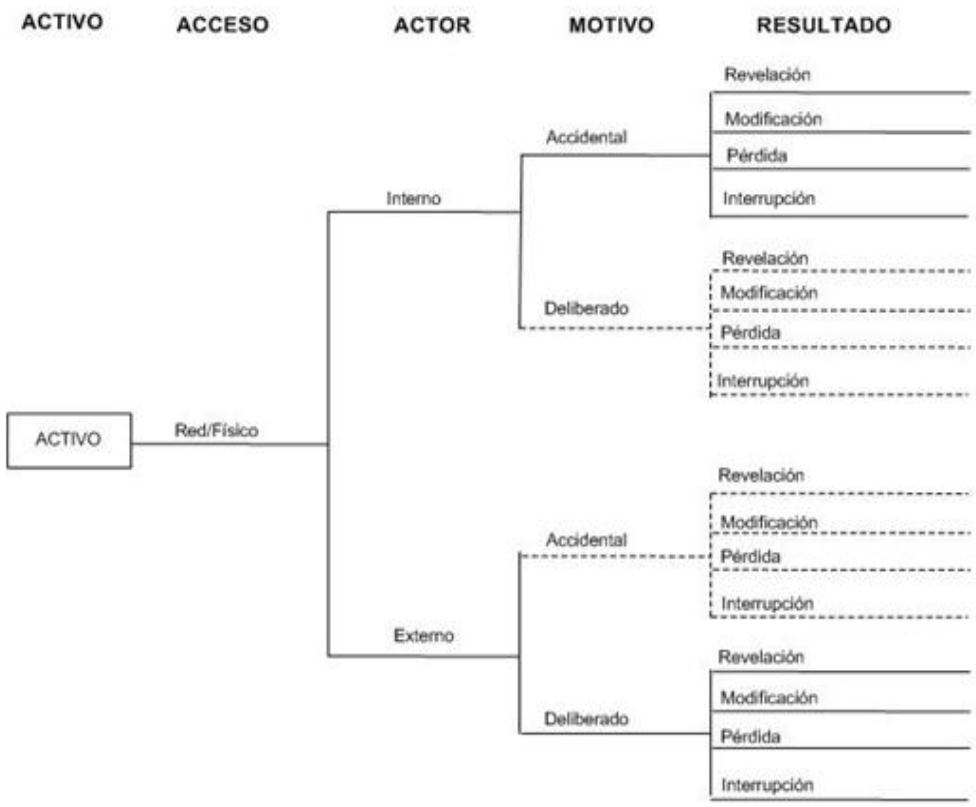

Figura 2.5: Árbol de amenazas basado en activos para actores humanos de acceso de red[36]

A continuación se detalla una plantilla de ayuda para mapear por cada activo crítico el resultado de su amenaza, esta plantilla será aplicada por cada activo su árbol respectivo de amenaza y los resultados se aplicarán ahí:

[36] Fuente: OCTAVE

Resultado de Identificación de las Amenazas								
No.	**Tipo de Activo**	**Funciones del Activo**	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Descripción de la amenaza**
	Observaciones:					**Realizado por:**		
	Fecha:					**Aprobado por:**		

Plantilla 2.10: Plantilla de Resultado de identificación de las amenazas sobre activos críticos[37]

A continuación se detalla las relaciones de los activos con los perfiles de amenazas detallados en el *Catálogo de Elementos.pdf (Amenazas) Ver Anexo 6:*

TIPO DE ACTIVO	CATEGORIA DE PERFIL DE AMENAZAS
Actividades y procesos del negocio	✓ Actores humanos con acceso a la red ✓ Actores humanos con acceso físico ✓ Otros Problemas
Información	✓ Actores humanos con acceso a la red ✓ Actores humanos con acceso físico ✓ Problemas del sistema ✓ Otros Problemas
Hardware	✓ Actores humanos con acceso a la red ✓ Actores humanos con acceso físico ✓ Problemas del sistema ✓ Otros Problemas

[37] Fuente: La autora

Software	✓ Actores humanos con acceso a la red ✓ Actores humanos con acceso físico ✓ Problemas del sistema
Redes	✓ Actores humanos con acceso a la red ✓ Actores humanos con acceso físico ✓ Problemas del sistema ✓ Otros Problemas
Personal	✓ Otros Problemas
Sitio	✓ Actores humanos con acceso a la red ✓ Actores humanos con acceso físico ✓ Otros Problemas
Estructura de la organización	✓ Otros Problemas

Tabla 2.12: Tabla de relación de tipo de activos por perfil de amenazas[38]

2.2.2.3. Etapa 3: Determinación de las vulnerabilidades

En esta etapa se busca identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la organización.

2.2.2.3.1. Actividad 1: Identificación de las vulnerabilidades

FASE 2. IDENTIFICACIÓN DE LOS RIESGOS
E3: Determinación de las vulnerabilidades **A1: Identificación de las vulnerabilidades**
Objetivo • Identificar las vulnerabilidades que pueden ser explotadas por una amenaza.
Criterios de Entrada ❑ Lista de amenazas conocidas: *Fase2, E2, A1, Plantilla 2.10: Resultado de identificación de las amenazas sobre activos críticos.* ❑ Lista de activos críticos: *Fase2, E1, A1, Plantilla 2.7: Resultado de la*

[38] Fuente: La autora

Identificación de Activos.
Criterios de Salida ❑Plantilla de resultado de identificación de vulnerabilidades
Recomendaciones Se recomienda aplicar el *Anexo 6: Catálogo de elementos, Vulnerabilidades,* para identificar por cada amenaza que vulnerabilidad puede tener. También se debe aplicar la plantilla de resultado de identificación de amenazas. Este catálogo designado está abierto para futuras vulnerabilidades encontradas y que desee incluir en el mismo.

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Las vulnerabilidades son todas las ausencias o ineficacias de las seguridades pertinentes para proteger el valor propio o acumulado sobre un activo. A veces se emplea el término "insuficiencia" para resaltar el hecho de que la eficacia medida de la seguridad es insuficiente para preservar el valor del activo expuesto a una amenaza. Con esto la identificación de las vulnerabilidades se detallará en las siguientes áreas:

- ✓ Organización
- ✓ Procesos y procedimientos
- ✓ Personal
- ✓ Ambiente físico
- ✓ Hardware, software , red y equipos de comunicaciones

Véase Anexo 6 (Catálogo de elementos.pdf, Vulnerabilidades), ahí se tendrá a detalle todo el catálogo de las vulnerabilidades frente a las amenazas detectadas.

A continuación se muestra una tabla con las relaciones del tipo de amenazas con las vulnerabilidades:

TIPO DE AMENAZAS	TIPO DE VULNERABILIDADES
Actores humanos con acceso a la red	Personal Procesos y Procedimientos Ambiente Físico Red y comunicaciones Hardware
Actores humanos con acceso físico	Organización Procesos y Procedimientos Personal Ambiente Físico Red y comunicaciones Hardware Software
Problemas del sistema	Procesos y Procedimientos Personal Ambiente Físico Red y comunicaciones Software
Otros problemas	Organización Procesos y Procedimientos Personal Ambiente Físico Red y comunicaciones Hardware Software

Tabla 2.13: Tabla de relaciones entre una amenaza y las vulnerabilidades que se pueden aplicar[39]

A continuación se detalla la plantilla de ayuda en la que se especificarán los resultados de las posibles vulnerabilidades que se encuentran en cada uno de los activos críticos:

[39] Fuente: La autora

Resultado de Identificación de las vulnerabilidades								
No.	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Descripción de la amenaza**	**Vulnerabilidad**	**Descripción de la vulnerabilidad**
	Observaciones:						**Realizado Por:**	
	Fecha:						**Aprobado Por:**	

Plantilla 2.111: Plantilla de Resultado de identificación de las vulnerabilidades[40]

2.2.2.3.2. Actividad 2: Valoración de las vulnerabilidades

FASE 2. IDENTIFICACIÓN DE LOS RIESGOS
E3: Determinación de las vulnerabilidades **A2: Valoración de las vulnerabilidades**
Objetivo • Valorar las vulnerabilidades que pueden ser aprovechadas por una amenaza.
Criterios de Entrada ❑ Lista de amenazas conocidas. *Fase 2, E2, A1, Plantilla 2.10: Resultado de identificación de las amenazas sobre activos críticos.* ❑ Lista de activos críticos. *Fase2, E1, A1, Plantilla 2.7: Resultado de la Identificación de Activos.* ❑ Lista de vulnerabilidades identificadas: *Fase2, E4, A1, Plantilla 2.12: Plantilla de*

[40] Fuente: La autora

la identificación de vulnerabilidades.
Criterios de Salida ❑ Tabla valoración de las vulnerabilidades, *Ver Tabla 2.14.* ❑ Plantilla de resultado de identificación de vulnerabilidades con su valoración
Recomendaciones Se recomienda aplicar el *Anexo 6, Catálogo de elementos.pdf, Vulnerabilidades,* para identificar y valorar por cada amenaza detectada. También se debe aplicar la plantilla de resultado de identificación de amenazas.

Para la valoración de las vulnerabilidades se tomo como referencia la tabla propuesta en OCTAVE a continuación se describe como se valorará, en la siguiente tabla se resume las definiciones de los niveles de gravedad que el equipo de análisis determinarán para los activos críticos y la organización:

NIVEL DE GRAVEDAD DE LA VULNERABILIDAD	SIGNIFICADO
Vulnerabilidades de alta gravedad	Debe fijarse inmediatamente (dentro de la próxima semana)
Vulnerabilidades a media de gravedad	Debe fijarse antes (a menos de 1 mes)
Vulnerabilidades de baja severidad	Puede ser fijado más adelante

Tabla 2.14: Tabla de valoración de las vulnerabilidades[41]

A continuación se detalla la plantilla de ayuda para valorar las vulnerabilidades identificadas:

[41] Fuente: OCTAVE

Resultado de Valoración de las vulnerabilidades									
No.	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Descripción de la amenaza**	**Vulnerabilidad**	**Descripción de la vulnerabilidad**	**Valoración de la vulnerabilidad**
									A,M,B
	Observaciones:							**Realizado Por:**	
	Fecha:							**Aprobado Por:**	

Plantilla 2.122: Plantilla de Resultado de valoración de las vulnerabilidades[42]

2.2.2.4. Etapa 4: Determinación de controles de seguridad

En esta etapa se busca identificar controles, planes para la implementación del tratamiento del riesgo calificándolas por su eficacia frente a las amenazas que se pretende mitigar. Su objetivo es determinar que se necesita para proteger el sistema y saber si se tiene un sistema de protección a la altura de las necesidades de la organización.

2.2.2.4.1. Actividad 1: Identificación de controles existentes

FASE 2. IDENTIFICACIÓN DE LOS RIESGOS
E4: Determinación de controles de seguridad existentes **A1: Identificación de los controles existentes**

[42] Fuente: La autora

Objetivo
• Identificar los controles existentes sobre las amenazas que se pretenden mitigar. Basándose en la norma ISO/IEC 27002:2005.
Criterios de Entrada
❑ Lista de procesos de gestión de seguridad de la información si lo tuviere y el listado de estado de su implementación. ❑ Verificación con personas responsables de la seguridad de la información
Criterios de Salida
❑ Controles ISO/IEC 27002:2005, *Véase ANEXO 5 CONTROLES ISO 27002: 2005.pdf* ❑ Plantilla de identificación de controles de seguridad existentes
Recomendaciones
Se recomienda verificar los controles de seguridad existentes en la compañía y comparar con los controles ISO 27002; después llenar plantilla de identificación de Control de seguridad existente; si no tuviere dichos controles se pondrá en la plantilla como no aplicable.

A continuación se presenta una plantilla de ayuda que servirá para esta identificación:

Resultado de Identificación de las controles de seguridad existentes			
Dominio	**Objetivos de control**	**Control**	**Cumple SI/NO**
Observaciones:		**Realizado Por:**	
Fecha:		**Aprobado Por:**	

Plantilla 2.133: Plantilla de Resultado de identificación de controles de seguridades existentes[43]

[43] Fuente: La autora

2.2.3. FASE 3: EVALUACIÓN DE LOS RIESGOS

Dentro de esta fase se procesa todos los datos recopilados en las fases anteriores con lo cual se procederá a estimar el impacto y el riesgo a que está expuesta la organización, con sus valoraciones. Se fundamenta en estimar lo que podría ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

2.2.3.1. Etapa 1: Determinación del impacto

En esta etapa, se identificará los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en que dimensiones de seguridad son importantes y valorando esta importancia.

2.2.3.1.1. Actividad 1: Identificación del impacto

FASE 3. EVALUACIÓN DE LOS RIESGOS
E1: Determinación del impacto **A1: Identificación y valoración del impacto**
Objetivo • Identificar y valorar el impacto al que está sometido el activo por la materialización de una amenaza
Criterios de Entrada ❑ Resultado de la determinación de los activos: *Fase 2, E1, A1, Plantilla 2.7: Resultado de la Identificación de Activos.* ❑ Resultado de la determinación de las amenazas: *Fase2, E2, A1, Plantilla 2.10: Resultado de identificación de las amenazas sobre activos críticos.* ❑ Resultado de la determinación de las seguridades existentes: *Fase2, E4, A1, Plantilla 2.14: Plantilla de la identificación de controles de seguridad existentes.* ❑ Resultado de la determinación de las vulnerabilidades: *Fase2, E3, A1, Plantilla 2.13: Plantilla de la identificación de vulnerabilidades.*

❑ Tabla de criterios para evaluar los impactos: *Fase1, E2, A4, Plantilla 2.5, de resultados de definición de criterios de impacto)*
Criterios de Salida ❑ Plantilla para identificar y evaluar el impacto aplicando las características de las amenazas, tales como: revelación, modificación, destrucción- perdida, interrupción.
Recomendaciones Se recomienda aplicar los criterios de impacto que se han definido en la *Fase 1, E2, A4; l*uego llenar la plantilla de resultados de identificación de amenazas existentes.

Para identificar el impacto por resultados de las amenazas se debe considerar las siguientes áreas a determinar:

- ✓ Reputación / confianza del cliente
- ✓ La vida / salud de los clientes
- ✓ Productividad
- ✓ Multas / sanciones legales
- ✓ Finanzas
- ✓ otros

A continuación se detalla la plantilla de identificación del impacto aplicando la característica de la amenaza para ayuda de detalle de los impactos detectados:

Plantilla de Resultado de identificación y evaluación del impacto								
No.	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Área de impacto**	**Descripción del impacto**	**Valor del impacto**
								A,M,B
	Observaciones						**Realizado Por:**	
	Fecha:						**Aprobado Por:**	

Plantilla 2.144: Plantilla de Resultado de identificación y evaluación del impacto sobre activos críticos[44]

A continuación se detalla el árbol de perfil de amenazas con valoración de impacto para llenar por cada activo crítico, cada árbol de perfil de amenaza, se deberá realizar el análisis de las descripciones de impacto por activo, en relación al criterio básico de impacto y a las escalas definidas en la metodología de estimación de riesgo, se obtiene un perfil de amenaza con el impacto valorado a continuación se detalla el resultado:

[44] Fuente: La autora

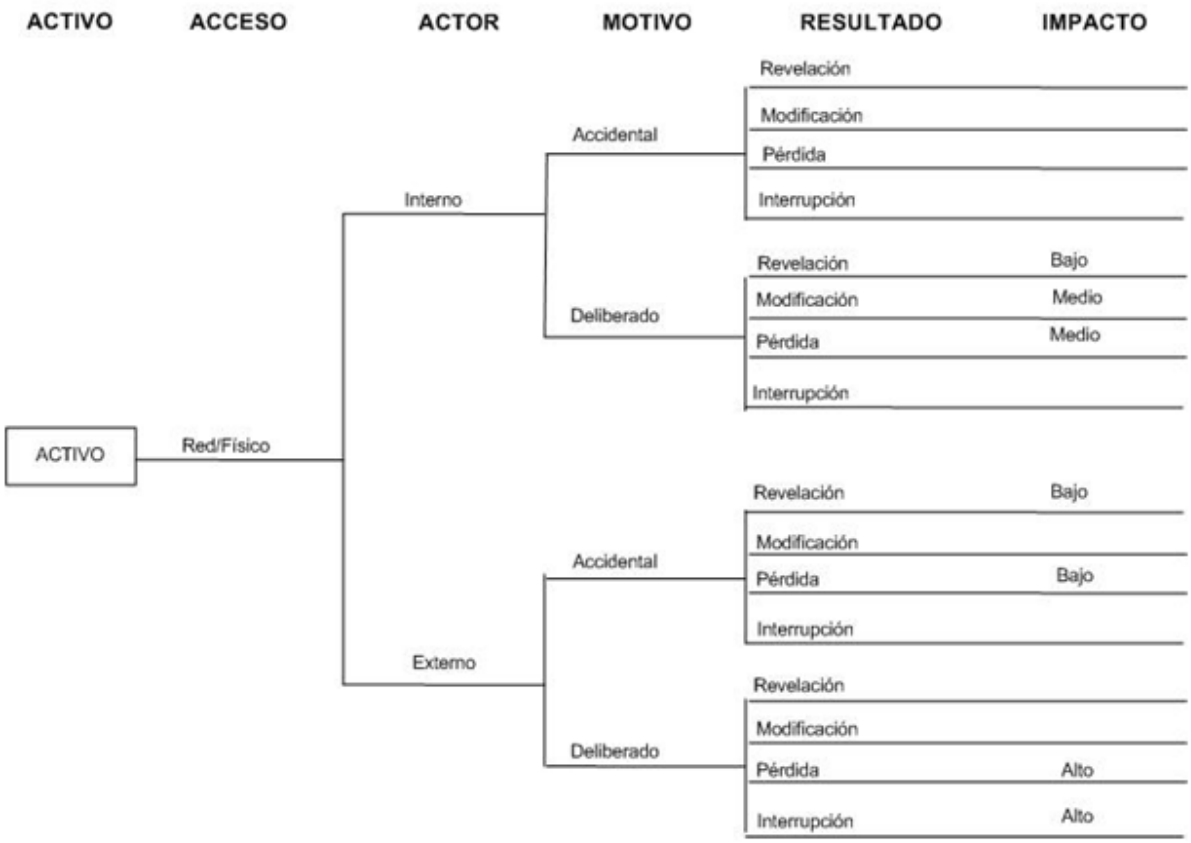

Figura 2.6: Árbol perfil de amenazas con valoración de impacto[45]

2.2.3.2. Etapa 2: Determinación de la probabilidad de incidentes

En esta etapa se busca identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la organización.

2.2.3.2.1. Actividad 1: Valorar la probabilidad de incidentes

FASE 3. IDENTIFICACIÓN DE LOS RIESGOS
E2: Determinación de la probabilidad de incidentes **A1: Valoración la probabilidad de incidentes**

[45] Fuente: OCTAVE

Objetivo

- Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo, y la facilidad con que las vulnerabilidades pueden ser explotadas
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Criterios de Entrada

❑ Resultados de la identificación de amenazas: *Fase2, E2, A1, Plantilla 2.10: Resultado de identificación de las amenazas sobre activos críticos.*

❑ Antecedentes: incidentes en la organización.

❑ Resultados de la identificación y valoración de vulnerabilidades: *Fase2, E4, A2, Plantilla 2.13: Plantilla de la valoración de vulnerabilidades.*

Criterios de Salida

❑ Tabla de valoración de Degradación que causan las amenazas, *Ver Tabla 2.15.*

❑ Plantilla de identificación de amenazas agregando la valoración de las mismas por cada activo

Recomendaciones

Se recomienda aplicar las tablas de valoración de amenazas que se encuentran en el *Anexo6 (Catálogo de elementos.pdf, Características de valoración de amenazas).* Una vez determinado el rango de valoraciones que tomará la institución, se procederá a llenar la Plantilla de Resultados de valoración de identificación de amenazas agregando dos columnas más para la valoración de las mismas. Hay que tomar en cuenta que si se tienen incidentes en la organización, se tratará de valorar estas amenazas con los incidentes que se obtengan.

A continuación se detalla las tablas para valorar las amenazas de un activo, *Véase Anexo 6 (Catálogo de elementos.pdf, características de valoración de amenazas),* para descripción más detallada de su funcionamiento; dependerá de los rangos que quiera tomar la institución para evaluar las amenazas existentes.

MA	Muy alta	100%
A	Alto	75%
M	Medio	50%
B	Bajo	20%
MB	Muy Bajo	5%

Tabla 2.15: Tabla de valores de Degradación que causan las amenazas[46]

A continuación se detalla la Plantilla de ayudará para la valoración de las amenazas, se usará la plantilla de identificación de amenazas agregando una columna para la valoración de las mismas:

[46] Fuente: La autora

Resultado de valoración de incidentes															
No.	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Descripción de la amenaza**	**Descripción de la vulnerabilidad**	**Valoración de la vulnerabilidad**	**Probabilidad de ocurrencia de la amenaza**	**Valor probabilidad de ocurrencia de amenaza**	**Degradación de dimensiones de seguridad**				
									A,M,B,MB		**C**	**A**	**I**	**D**	**T**
				Observaciones:						**Realizado Por:**					
	Fecha:									**Aprobado por:**					

Plantilla 2.155: Plantilla de Resultado de valoración de incidentes[47]

Notación: C: confidencialidad, A: autenticidad, I: integridad, D: disponibilidad, T: trazabilidad.

[47] Fuente: La autora

2.2.3.3. Etapa 3: Estimación del estado del riesgo

En esta etapa, se estima el riesgo al que están sometidos los activos críticos teniendo en cuenta el valor de los activos y la valoración de las amenazas. Estimar el nivel de riesgo en base a aplicar la metodología de estimación del riesgo con el método cualitativo.

2.2.3.3.1. Actividad 1: Estimación del riesgo

FASE 3. EVALUACIÓN DE LOS RIESGOS
E3: Estimación del estado del riesgo **A1: Estimación del riesgo**
Objetivo • Estimar el riesgo al que están sometidos los activos. Para cada perfil de amenaza valorar el riesgo estimado en base a analizarlo con el criterio de evaluación del riesgo.
Criterios de Entrada ❑ Matriz para calcular el riesgo (*Véase FASE1, E2, A2, Tabla 2.4: Matriz para calcular el riesgo)* ❑ Resultado de la determinación de valoración de incidentes (*Véase FASE3, E2, A1, Plantilla 2.15: Resultado de la valoración de identificación y valoración de las amenazas sobre activos críticos.*
Criterios de Salida ❑ Plantilla de resultados de riesgos estimados. *Ver plantilla 2.16. de esta actividad.*
Recomendaciones Se recomienda aplicar la Matriz para calcular el riesgo y valorar sobre el impacto y la probabilidad determinada en el E2. Llenar árbol de perfil de amenazas con el riesgo estimado.

A continuación se detalla el árbol de amenazas con riesgo estimado por cada activo crítico, esto se puede obtener del E2 de los incidentes encontrados. El proceso de

gestión de riesgos partirá de éstas valoraciones para reducir el riesgo a niveles aceptables:

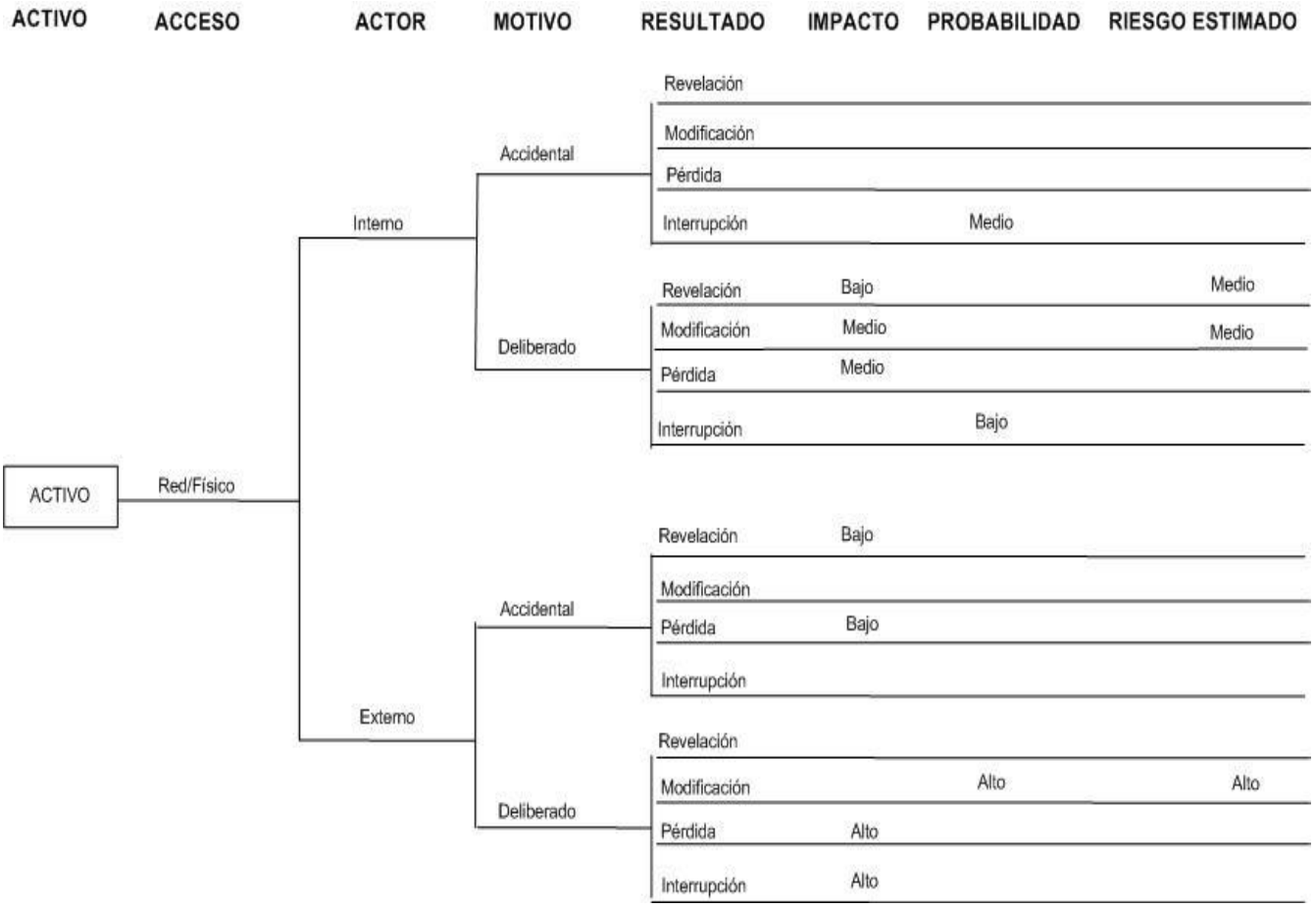

Figura2.7: Árbol de perfil de amenazas con probabilidad e impacto y riesgo estimado[48]

A continuación se detalla la plantilla de resultados del riesgo estimado más crítico; en esta plantilla se listará los riesgos de prioridad alta, y media como resultado del árbol de perfil de amenazas con probabilidad e impacto:

[48] Fuente: La autora, OCTAVE

Plantilla de Resultado del riesgo estimado										
No.	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Área de impacto**	**Descripción del impacto**	**Valor del impacto**	**Probabilidad de ocurrencia de la amenaza**	**Nivel de riesgo estimado**
										A,M,B
	Observaciones								**Realizado Por:**	
	Fecha:								**Aprobado Por:**	

Plantilla 2.16: Plantilla de Resultado de la determinación de niveles de riesgos estimados[49]

[49] Fuente: La autora

2.2.4. FASE 4: TRATAMIENTO DE LOS RIESGOS

Dentro de esta fase se empezará el tratamiento de los riesgos con una lista de resultados de la fase 3 de los riesgos críticos obtenidos sobre los activos, se los llamará críticos a los riesgos que tengan como resultado el criterio de evaluación alto, que serán los riesgos prioritarios a tratarse; luego vendrán los riesgos con criterio de evaluación medio que serán los siguientes en tratarse. Se realizará estrategias de protección a la organización verificando las vulnerabilidades que tiene la misma por lo cual se recomienda seleccionar los controles; dichos controles se tomarán de la norma ISO 27002:2005 [19]. También se realizará plan de mitigación por lo que servirán para reducir el riesgo, retener el riesgo, evitar el riesgo o transferir el riesgo de los activos; así también se realizaran lista de acciones que apoyaran el plan de mitigación de los riesgos críticos.

2.2.4.1. Etapa 1: Estrategias de Protección.

En este proceso se realizarán y se discutirán estrategias de protección y vulnerabilidades de cada área de la organización; se definirán prácticas de seguridad enfocándose en conocer la situación actual de la organización y que se debería cambiar. Estas estrategias se basarán en los dominios de la norma ISO 27002:2005 [19]. Se definirán preguntas clave estableciendo enfoques para seguir utilizando los dominios de la norma.

2.2.4.1.1. Actividad 1: Crear estrategias de protección.

FASE 4. TRATAMIENTO DE LOS RIESGOS
E1: Estrategias de protección **A1: Crear estrategias de protección**
Objetivo • Identificar y crear estrategias de protección considerando los dominios de la norma ISO 27002:2005 • Realizar preguntas claves por cada dominio y estableciendo estrategias

actuales; revisando las vulnerabilidades de la organización.
Criterios de Entrada ❑ Plantilla de resultados de valoración de las vulnerabilidades (*Ver Fase 2, E4, A2, Plantilla 2.13: Plantilla de la valoración de vulnerabilidades.*) ❑ Controles ISO 27002-2005 (*Ver anexo 5*)
Criterios de Salida ❑ Plantilla de resultado de las estrategias de protección
Recomendaciones Se recomienda verificar la plantilla de resultados de valoración de las vulnerabilidades tanto de calificación alta, media y baja para especificar las estrategias de protección sobre cada dominio de la norma ISO 27002-2005.

A continuación se detalla la plantilla de identificación de estrategias listado por cada dominio de la norma ISO 27002-2005:

Resultado de identificar las estrategias de protección			
Dominio	**Preguntas clave**	**Existe actualmente**	**Se debe cambiar**
Políticas de seguridad	Se puede mejorar?, que se debe utilizar?, quiere hacer cambios?, existen mecanismos?, etc.	✓	
Aspectos organizativos de la seguridad de la información			
Gestión de activos			
Seguridad ligada a los recursos humanos			
Seguridad física y del entorno			
Gestión de comunicaciones y operaciones			

Control de acceso			
Adquisición, desarrollo y mantenimiento de los sistemas de información			
Gestión de incidentes en la seguridad de la información			
Gestión de la continuidad del negocio			
Cumplimiento			
Observaciones		**Realizado Por**	
Fecha		**Aprobado por**	

Plantilla 2.17: Plantilla de Resultado de las estrategias de protección[50]

2.2.4.2. Etapa 2: Plan de mitigación

En este proceso hay dos alternativas de tratamiento del riesgo que son: el aceptar el riesgo que dependerá de los criterios de evaluación del riesgo que se generó en la *Fase 1, A5* y el mitigar el riesgo que comprende el reducir el riesgo, evitar el riesgo, o transferir el riesgo. Para la selección de mitigar el riesgo se basará en la selección de los controles de la norma ISO 27002:2005; los mismos que se definió como estrategias de protección en el *Etapa 1.*

2.2.4.2.1. Actividad 1: Crear planes de mitigación del riesgo

FASE 4. TRATAMIENTO DE LOS RIESGOS
E2: Plan de mitigación **A1: Crear planes de mitigación del riesgo**

[50] Fuente: La autora

Objetivo
• Mitigar o aceptar el riesgo asociado del activo más crítico y establecer controles.
Criterios de Entrada
❑ Resultado de definir los criterios de aceptación del riesgo *(Ver Fase 1, E2, A5, Plantilla 2.6: Resultado de definición de aceptación del riesgo.)* ❑ Resultado de la determinación de niveles de riegos estimados. (*Ver Fase 3*, *E3, A1, Plantilla 2.16: Plantilla de Resultado de la determinación de niveles de riesgos estimados.*). ❑ Resultado de identificar las estrategias de protección. (*Ver Fase 4, E1, A1, Plantilla 2.17: Plantilla de Resultados de las estrategias de protección.*)
Criterios de Salida
❑ Plantilla de resultado de tratamiento de los riesgos.
Recomendaciones Se recomienda aplicar los controles definidos por la norma ISO 27002:2005, que se definió como estrategias de protección. Dependerá si se acepta o se mitiga el riesgo dependiendo de los criterios de aceptación del riesgo establecido.

Los criterios de aceptación del riesgo dependerán de la calificación que resulte de los riesgos estimados: estos serán tratados de la siguiente manera:

- Aceptar el riesgo: nivel del riesgo que satisface los criterios para su aceptación, no es necesario implementar controles adicionales así que el riesgo se puede retener pero siempre estará en comunicación a la directiva de que estos riesgos serán aceptados.
- Evitar el riesgo: cuando los riesgos se consideran como muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o conjunto de actividades planificadas o

existentes o mediante el cambio en las condiciones bajos las cuales se efectúa tal actividad.

- Transferir el riesgo: involucra una decisión para compartir algunos riesgos con las partes externas. Puede crear riesgos nuevos o modificar los riesgos identificados existentes. El transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo. Conviene anotar que puede ser posible transferir la responsabilidad para la gestión del riesgo, pero normalmente no es posible transferir la responsabilidad de un impacto.
- Reducir el riesgo: este nivel se debería reducir mediante la selección de controles, de manera tal que el riesgo se pueda evaluar como aceptable. Se recomienda seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo. En general los controles pueden brindar uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y toma de conciencia.

A continuación se detalla la plantilla de resultados de mitigar los riesgos:

Plantilla de Resultado del tratamiento del riesgo														
No.	**Activo**	**Acceso**	**Actor**	**Motivo**	**Resultado**	**Descripción de la amenaza**	**Descripción de la vulnerabilidad**	**Área de impacto**	**Descripción del impacto**	**Valor del impacto**	**Probabilidad de ocurrencia de la amenaza**	**Nivel de riesgo estimado**	**Tratamiento del riesgo**	**Plan de mitigación**
												A,M,B		
	Observaciones						**Realizado Por:**							
	Fecha:						**Aprobado Por:**							

Plantilla 2.18: Plantilla de Resultado del tratamiento del riesgo[51]

[51] Fuente: La autora

2.2.4.2.2. Actividad 2: Crear lista de acciones

FASE 4. TRATAMIENTO DE LOS RIESGOS
E2: Plan de mitigación **A2: Crear lista de acciones**
Objetivo • Crear lista de acciones que la organización lo realizará a corto o largo plazo para mitigar las amenazas de los activos críticos con responsables de cada acción.
Criterios de Entrada ❑Plantilla de Resultado de la determinación de niveles de riegos estimados *(Ver Fase 3, E3, A1, Plantilla 2.16.)*
Criterios de Salida ❑Plantilla de lista de acciones. . (*Ver Plantilla 2.19 de esta actividad).*
Recomendaciones Se recomienda revisar la plantilla de resultado del plan de mitigación y poner plazos y responsables de cada acción a asignarse.

Las acciones a crearse son consistentes con las estrategias de protección y planes de mitigación, pueden ser implementadas rápidamente no requiere de detalles de implementación que una estrategia de protección o un plan de mitigación requiere. A continuación se detalla la plantilla a aplicar:

<table>
<tr><th colspan="4">Resultado de lista de acciones</th></tr>
<tr><td>No.</td><td>Acción</td><td>Responsable</td><td></td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td>Fecha de finalización</td><td></td></tr>
<tr><td>Medidas de gestiones necesarias</td><td></td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td>Responsable</td><td></td></tr>
<tr><td>Fecha de finalización</td><td></td></tr>
<tr><td>Medidas de gestiones necesarias</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Observaciones</td><td>Realizado Por</td><td></td></tr>
<tr><td>Fecha</td><td></td><td>Aprobado por</td><td></td></tr>
</table>

Plantilla 2.19: Plantilla lista de acciones[52]

2.2.5. FASE 5: COMUNICACIÓN

Dentro de esta fase se comunicará el riesgo para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información, acerca de los riesgos entre quienes toman decisiones y las otras partes involucradas. La comunicación eficaz entre las partes involucradas es importante, dado que puede tener un impacto significativo en las decisiones que se deben tomar.

2.2.5.1. Etapa 1: Comunicar el riesgo

Esta etapa se encarga de que el equipo de Comité de Seguridad o el equipo de análisis comparta la información obtenida en las fases de la gestión del riesgo; a través de planes y coordinación entre quien toma decisiones y los interesados. La comunicación del riesgo se debería realizar con el fin de lograr lo siguiente:

[52] Fuente: La autora

- ✓ Brindar seguridad del resultado de la gestión del riesgo de la organización
- ✓ Recolectar información sobre el riesgo
- ✓ Compartir los resultados de la evaluación del riesgo y presentar el plan para el tratamiento del riesgo
- ✓ Brindar soporte para la toma de decisiones
- ✓ Obtener conocimientos nuevos sobre la seguridad de la información
- ✓ Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente
- ✓ Dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos
- ✓ Mejorar la concienciación

Para comunicar el riesgo a las partes interesadas, se pueden guiar con elaboraciones de informes finales a los altos medios sobre la evaluación y planes de mitigación que se llegó junto con el equipo de análisis.

A continuación se detalla el formato de informe final:

FUERZA NAVAL
CENTRO DE TECNOLOGIAS DE LA INFORMACION QUITO
- o -

Quito, ...

Asunto: **Informe Final de resultados de la gestión de riesgos y seguridad informática**
Para: **Capitán de Corbeta Ricardo Uquillas Soto**

Dignase Señor Capitán de Corbeta Ricardo Uquillas Soto, Jefe del Centro de tecnologías de la información Quito; encontrar en este informe los resultados de la evaluación de riesgos y seguridad. Donde detalla el análisis de la situación actual de la institución, la evaluación de las amenazas criticas, activos y vulnerabilidades que propone esta metodología de gestión de riesgos y la que se ha realizado con ayuda conjunta con el equipo de análisis, en la que se ha asumido la responsabilidad de cada uno que lo conforma y se ha producido una estrategia de protección y planes de mitigación basados exclusivamente en los riesgos de seguridad de la institución.
A continuación se presenta los resultados obtenidos:

Atentamente,

XXXXXXXXX

Plantilla 2.20: Plantilla para comunicar el riesgo[53]

[53] Fuente: La autora

Se recomienda mantener una comunicación bidireccional de manera continua. Y garantizar las percepciones que tienen las partes involucradas sobre el riesgo, así como las percepciones de los beneficios que se pueden identificar y documentar.

2.2.6. FASE 6: MONITOREO Y REVISIÓN

Dentro de esta fase se monitorea los riesgos y sus factores lo que son los valores de los activos, los impactos, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana y mantener una visión general de la perspectiva compleja del riesgo.

2.2.6.1. Etapa 1: Monitoreo y Revisión de los factores de riesgo

En esta etapa, se encarga de monitorear las amenazas, las vulnerabilidades, las probabilidades que pueden cambiar abruptamente sin ninguna indicación. Por ende es necesario el monitoreo constante para detectar estos cambios. La organización deberá garantizar el monitoreo continuo de los siguientes aspectos:

- ✓ Activos nuevos que se han incluido en el alcance de la gestión de riesgo.
- ✓ Modificaciones necesarias de los valores de los activos como cambios de requisitos de negocio.
- ✓ Amenazas nuevas que podrían estar activas tanto fuera como dentro de la organización y que no se han evaluado
- ✓ Probabilidad que las vulnerabilidades nuevas o aumentadas puedan permitir que la amenazas exploten tantas vulnerabilidades nuevas o en cambios.
- ✓ Vulnerabilidades identificadas para determinar aquellas que se exponen a amenazas nuevas.
- ✓ El impacto aumentando de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo
- ✓ Incidentes de la seguridad de la información

A continuación se detalla una plantilla de ayuda resultante del monitoreo y revisión de los factores de riesgo:

Resultado del monitoreo y revisión de los factores de riesgo				
Nuevos activos				
Activo	**Fecha**	**Observación**		
Modificaciones realizadas				
Cambio	**Fecha**	**Observación**		
Nuevas amenazas				
Amenaza	**Fecha**	**Observación**		
Vulnerabilidades identificadas				
Vulnerabilidad	**Fecha**	**Observación**		
Nivel de riesgo				
Riesgo	**Valoración del impacto**	**Valoración de la vulnerabilidad**	**Fecha**	**Observaciones**
Incidentes de la seguridad de la información				
Incidente	**Activos afectados**	**Fecha**	**Observación**	
Fecha	**Realizado Por**		**Aprobado Por**	

Plantilla 2.21: Plantilla de Resultado de monitoreo y revisión de los factores de riesgo[54]

[54] Fuente: La autora

Se recomienda que las amenazas, vulnerabilidades o cambios nuevos en la probabilidad puedan incrementar los riesgos evaluados previamente como riesgos bajos. Los cambios importantes que afectan a la organización debería ser la razón para una revisión más específica. Por lo tanto, las actividades de monitoreo del riesgo del riesgo deberían repetirse con regularidad y las opciones seleccionadas para el tratamiento del riesgo se deberían realizar periódicamente. La organización debería revisar todos los riesgos con regularidad y cuando se presenten cambios importantes.

2.2.6.2. Etapa 2: Monitoreo, revisión y mejora de la Gestión del riesgo

En esta etapa, se encarga de gestionar el riesgo en la seguridad de la información donde se deberá monitorear, revisar y mejorar continuamente según sea necesario y adecuado. El monitoreo y la revisión continuos son necesarios para garantizar que el contexto, el resultado de la evaluación del riesgo y el tratamiento del riesgo, así como los planes de gestión siguen siendo pertinentes y adecuados para las circunstancias.

La organización deberá garantizar que el proceso de gestión del riesgo en la seguridad de la información y las actividades relacionadas aún es adecuado en las circunstancias actuales y se cumplen. Todas las mejoras acordadas para el proceso o las acciones necesarias para mejorar la conformidad con el proceso se deberían notificar a los directores correspondientes para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder.

En este proceso se deberá considerar los siguientes aspectos:

- ✓ Contexto legal y ambiental
- ✓ Contexto de competición
- ✓ Enfoque para la evaluación del riesgo
- ✓ Categorías y valor de los activos

- ✓ Criterios del impacto
- ✓ Criterios de evaluación del riesgo
- ✓ Criterios de aceptación del riesgo
- ✓ Recursos necesarios

A continuación se detalla una plantilla de resultados de monitorear, revisar y mejorar la gestión de riesgos:

Resultado del monitoreo, revisión y mejoras de la gestión de riesgos				
Contexto legal y ambiental				
Contexto	**Fecha**	**Observación**		
Contexto de competición				
Contexto	**Fecha**	**Observación**		
Enfoque para la evaluación del Riesgo				
Enfoque	**Fecha**	**Observación**		
Caracterización de los activos				
Caracterización	**Fecha**	**Observación**		
Criterios de impacto				
Criterio	**Fecha**	**Observación**		

Criterios evaluación del riesgo				
Criterio	**Fecha**	**Observación**		
Criterios de aceptación del riesgo				
Criterio	**Fecha**	**Observación**		
Recursos necesarios				
Recursos	**Fecha**	**Observación**		
Fecha		**Realizado Por**		

Plantilla 2.22: Plantilla de Resultado de monitoreo, revisión y mejora de la gestión de riesgo[55]

Se recomienda que la organización deba garantizar que los recursos para el tratamiento y la evaluación del riesgo estén disponibles continuamente para revisión del riesgo, tratar las amenazas o vulnerabilidades nuevas o con cambios asesorar a la dirección según corresponda.

2.3. PROCEDIMIENTOS DE APLICACIÓN DEL MODELO

El modelo de Gestión de riesgos y seguridad de la información propuesto, deberá ser implementado en forma secuencial y se empezará con los activos de información

[55] Fuente: La autora

más críticos que considere la institución. Este modelo implica la aplicación y pasos necesarios para analizar un sistema, identificar las amenazas, las vulnerabilidades asociadas, calcular la probabilidad de ocurrencia de esas amenazas, determinar el impacto y por último la obtención del riesgo más crítico.

Esta es una herramienta de fácil implementación en una institución militar, y que es necesaria para realizar la gestión de los riesgos.

Para implementar la metodología de Gestión de Riesgos y seguridad de la información, se ejecutarán las fases en forma secuencial empezando por la primera fase que es el Contexto Organizacional, donde se implementará todos los ajustes necesarios y cambios que aparecerán en la institución. Esta aplicación será efectiva en las áreas de tecnologías de la información y donde se pueda gestionar los riesgos más críticos.

La segunda fase es la Identificación de los riesgos, donde se encontrará, se reconocerá y se registrarán los riesgos. El propósito es identificar lo que podría suceder o que situaciones podrían existir que puedan afectar a la consecución de los objetivos de la organización.

La tercera fase es la Evaluación de los riesgos, donde se procesa todos los datos recopilados de las fases anteriores y se procederá a estimar el impacto y el riesgo al que está expuesta la organización con sus valoraciones.

La cuarta fase es el Tratamiento del Riesgo, donde se determina la lista de resultados de las anteriores fases, y se realizarán estrategias de protección y planes de mitigación.

La quinta fase es Comunicación, donde se comunicará el riesgo para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información acerca de los riesgos entre quienes toman decisiones y las otras partes involucradas.

Y como última fase es la sexta que es Monitoreo y Revisión, donde se monitorea los riesgos y sus factores, los valores de los activos, los impactos, las amenazas, las

vulnerabilidades, la probabilidad de ocurrencia con el fin de identificar todo cambio en contexto de la organización.

Al aplicar este modelo lo que se pretende es llegar a un nivel de madurez de gestión del riesgo normalizada y se pueda gestionar el riesgo como una práctica rutinaria en su negocio. Los procesos genéricos de riesgo llegarán a estar formalizados y extendidos, y los beneficios se entienden en todos los niveles de la organización. Se pretende que al aplicar este modelo llegue la institución a que su información de riesgos se utilice de forma activa para mejorar los procesos de negocio y ganar ventaja competitiva.

Se debe considerar que la gestión de riesgo es un tema de mucho interés dentro de una organización como para desempeñarla en mala forma. De allí a que se necesite evaluar y monitorear la capacidad de gestión de riesgo, comparar las prácticas internas con las mejores prácticas conocidas y extendidas, identificar las áreas de defectos que necesitan mejora, y mantenerlas en desarrollo.

Aplicando esta metodología se llegara paso a paso a niveles de madurez de la gestión del riesgo descritos a continuación:

Nivel de Madurez	Características	Metas
Nivel 1: Inicial (Fase 1) Definir el alcance al que se va a llegar a gestionar los riesgos. El éxito de gestionar el riesgo y tener una mejor forma de la seguridad de la información depende del talento de las personas involucradas en su contexto.	• Obtener de los procesos estratégicos una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. • Determinar el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados. • Determinar la identificación de contexto organizacional, en el que se desarrollará	• Obtener de los procesos estratégicos existentes de la institución, procesos agregados de valor y procesos habilitantes de apoyo que conforman la cadena de valor que se encuentran implementados en las instituciones militares. • Identificar los miembros de cada área operativa dentro de área a definir. • Considerar si tienen políticas de seguridad de la información

	el proceso de gestión de riesgos y que debe ser objeto de una revisión continua para adaptarse a las circunstancias de cada momento.	en la organización • Determinar los miembros responsables de acuerdo al criterio de la directiva de la institución a comprometerse al desarrollo y mejoramiento de los procesos al que el alcance se refiere.
Nivel 2: Identificar y Gestionar (Fase 2) Identificación de los activos de información donde se procederá a gestionarlos e incluir procesos básicos de gestión de la seguridad de la información. Los controles existentes hacen que se puedan detectar posibles incidentes de seguridad.	• Se identificará, se reconocerá y se registrarán los riesgos. • Identificar lo que podría suceder o que situaciones podrían existir que puedan afectar a la consecución de los objetivos del sistema u organización. Una vez que se identifique el riesgo, la institución debe identificar los controles existentes, tales como el diseño, características, personas, procesos y sistemas. El proceso de identificación de riesgos incluye la identificación de las causas y el origen del riesgo, hechos, situaciones o circunstancias que podrían tener un impacto material sobre los objetivos y la naturaleza de ese impacto.	• Documentar todos los activos de información sujetos a riesgo y valorizarlos • Identificar las amenazas relevantes de cada activo y valorizarlas • Identificar las vulnerabilidades que pueden ser explotadas por una amenaza y valorizarlas • Determinar los controles de seguridad de información existes ante las vulnerabilidades encontradas.
Nivel 3: Evaluar (Fase 3) Existencia de sistema de gestión de riesgos y seguridad de la información documentado y estandarizado. Se determina los incidentes para estimar el riesgo presentado	• Se procesa todos los datos recopilados en las fases anteriores con lo cual se procederá a estimar el impacto y el riesgo a que está expuesta la organización, con sus valoraciones. • Se fundamenta en estimar lo que podría ocurrir (impacto) y de lo que probablemente ocurra (riesgo).	• Identificar y valorar el impacto al que está sometido el activo por la materialización de una amenaza • Determinar las probabilidades de incidentes y su valoración. • Estimar el riesgo al que están sometidos los activos. Para cada perfil de amenaza valorar

		el riesgo estimado en base a analizarlo con el criterio de evaluación del riesgo.
Nivel 4: Tratamiento (Fase 4) Se implementa controles de seguridad de la información basados en la norma ISO 27002:2005. Donde se determinará las estrategias de protección y plan de mitigación de los riesgos gestionados.	• Se empezará el tratamiento de los riesgos con una lista de resultados de la fase 3 de los riesgos críticos obtenidos sobre los activos, se los llamará críticos a los riesgos que tengan como resultado el criterio de evaluación alto • Se realizará estrategias de protección a la organización verificando las vulnerabilidades donde se aplicaran los controles de la norma ISO 27002:2005. • Se ejecutará el plan de mitigación por lo que servirán para reducir el riesgo, retener el riesgo, evitar el riesgo o transferir el riesgo de los activos. • Se determinará lista de acciones que apoyaran el plan de mitigación de los riesgos críticos.	• Documentar las estrategias de protección que se implementaran ante las vulnerabilidades encontradas • Documentar el plan de mitigación para el tratamiento del riesgo • Documentar la lista de acciones ante el plan de mitigación.
Nivel 5: En mejora Continua (Fase 5 y Fase 6) Existe una mejora continua del modelo de gestión de riesgos y seguridad de la información, basada en la realimentación cualitativa de la gestión del riesgo	• Se comunicará el riesgo para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información, acerca de los riesgos entre quienes toman decisiones y las otras partes involucradas. • Se monitorea los riesgos y sus factores lo que son los valores de los activos, los impactos, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana y mantener una visión general de la perspectiva compleja	• Brindar seguridad del resultado de la gestión del riesgo de la organización • Recolectar información sobre el riesgo • Compartir los resultados de la evaluación del riesgo y presentar el plan para el tratamiento del riesgo • Brindar soporte para la toma de decisiones • Obtener conocimientos nuevos sobre la seguridad de la

	del riesgo.	información • Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente • Dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos • Mejorar la concienciación

Al aplicar este modelo, se recomienda tener una visión general del análisis, gestión de los riesgos y seguridad de la información al personal seleccionado para aplicarlo. Partiendo de esta premisa el departamento u centro tecnológico mejorará en su desarrollo de planes y estrategias de seguridad donde permitirá tomar decisiones a la alta gerencia para mitigar el riesgo y obtener un mejor control y gestión del mismo. Este modelo permitirá tener una mejor organización centralizada y así visualizar la realidad del área de tecnologías y una visión más clara de cuán importante y valioso es cada uno de los activos de información.

Tomando como referencia la institución militar como es la Fuerza Naval, el grado de madurez que se pretende alcanzar es hasta el nivel 5 ya que por encuestas realizadas anteriormente no tiene ningún modelo de gestión de riesgos y seguridad de la información por lo que estaría en un nivel de madurez 0.

Una vez aplicado el modelo se revisará y analizará los resultados obtenidos; y se verificará su aplicabilidad.

CAPITULO 3.

EVALUACIÓN DEL MODELO EN UN CASO DE ESTUDIO

3.1. PREPARACIÓN DEL CASO DE ESTUDIO

El objetivo es validar la aplicabilidad del modelo, y se procederá a la ejecución de cada fase. Este modelo de Gestión de riesgos y seguridad de la información se aplicará en una institución militar como es la Fuerza Naval y específicamente, en el Centro de Tecnologías de la información (CETEIQ), este departamento es un punto indispensable para la seguridad y provee información a los repartos navales que conforman la Fuerza Naval. Este ente, es el responsable de administrar, desarrollar, integrar, operar y dar soporte a la plataforma de sistemas de información, al software y hardware de los Sistemas Informáticos asignados, aplicando estándares institucionales y prácticas de control de calidad para las Tecnologías de la Información, empleando los recursos asignados en forma adecuada para dotar de tecnología de punta que sea operada por un equipo humano calificado, manteniendo la Red Naval de Datos y la seguridad de la información, a fin de contribuir al cumplimiento de la función básica de la DIRTIC [7].

Todo lo que respecta tanto a la Fuerza Naval como sus repartos de apoyo, se encuentra más detallado en el *Capítulo 1, Página 5.* El aplicar un modelo de Gestión de riesgos y seguridad de la información, contemplará muchos procesos y resultados que permitirán darse cuenta en qué grado de riesgo y seguridad de la información esta vulnerable y amenazado, y cuál será la probabilidad que se materialicen los riesgos en el Centro de Tecnologías de la información.

3.2. APLICACIÓN DEL MODELO

El modelo de gestión de riesgos y seguridad de la información propuesto, aplicará secuencialmente sus fases, se obtendrán resultados y las recomendaciones debidas. La aplicación del modelo se efectuará en el CETEIQ (Centro de tecnologías de la información Quito), departamento perteneciente a la Fuerza Naval.

3.2.1 FASE 1: CONTEXTO ORGANIZACIONAL

3.2.1.1. Etapa 1: Alcance

3.2.1.1.1. Actividad 1: Definición del Alcance

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Procesos estratégicos, agregados de valor y habilitantes de apoyo. *(Ver Anexo 1, Pg.3: DE LA FUNCIÓN BÁSICA Y OBJETIVOS ESTRATÉGICOS).*
- ❑ Misión, Visión de la institución. *(Ver Capítulo 1, Figura 1.5: Cadena de Valor)*
- ❑ Áreas operativas con miembros pertenecientes. *(Ver Anexo 1, Pg.7:* DE LA ESTRUCTURA ORGANICA DESCRIPTIVA*).*
- ❑ Políticas de seguridad de la información de la organización si lo hubiere.
  Ver Anexo 2, *DIRECTIVA SEGURIDAD INFORMATICA 12Jul2010.pdf.* Esta directiva dispuesta por la COGMAR (Comandancia General de Marina), se han elaborado y estructurado de acuerdo al estándar ISO/IEC 27002:2005.

Criterio de Salida

- ❑ Organigrama Estructural

Según el organigrama estructural del CETEIQ, se puede visualizar que se encuentra conformada en tres divisiones principales que son: división de administración y logística (que está conformada por la SECRETARIA como ente de apoyo), división de administración de recursos informáticos (que se encuentra como JEFE CBOS-IF DALTON FIGUEROA) y división de mantenimiento de sistemas informáticos (que se encuentra como JEFE SGOS-IF WILLIAN HERRERA). A la cabeza se encuentra el Jefe del Centro de Tecnologías de la información (CPCB-AD RICARDO UQUILLAS SOTO).

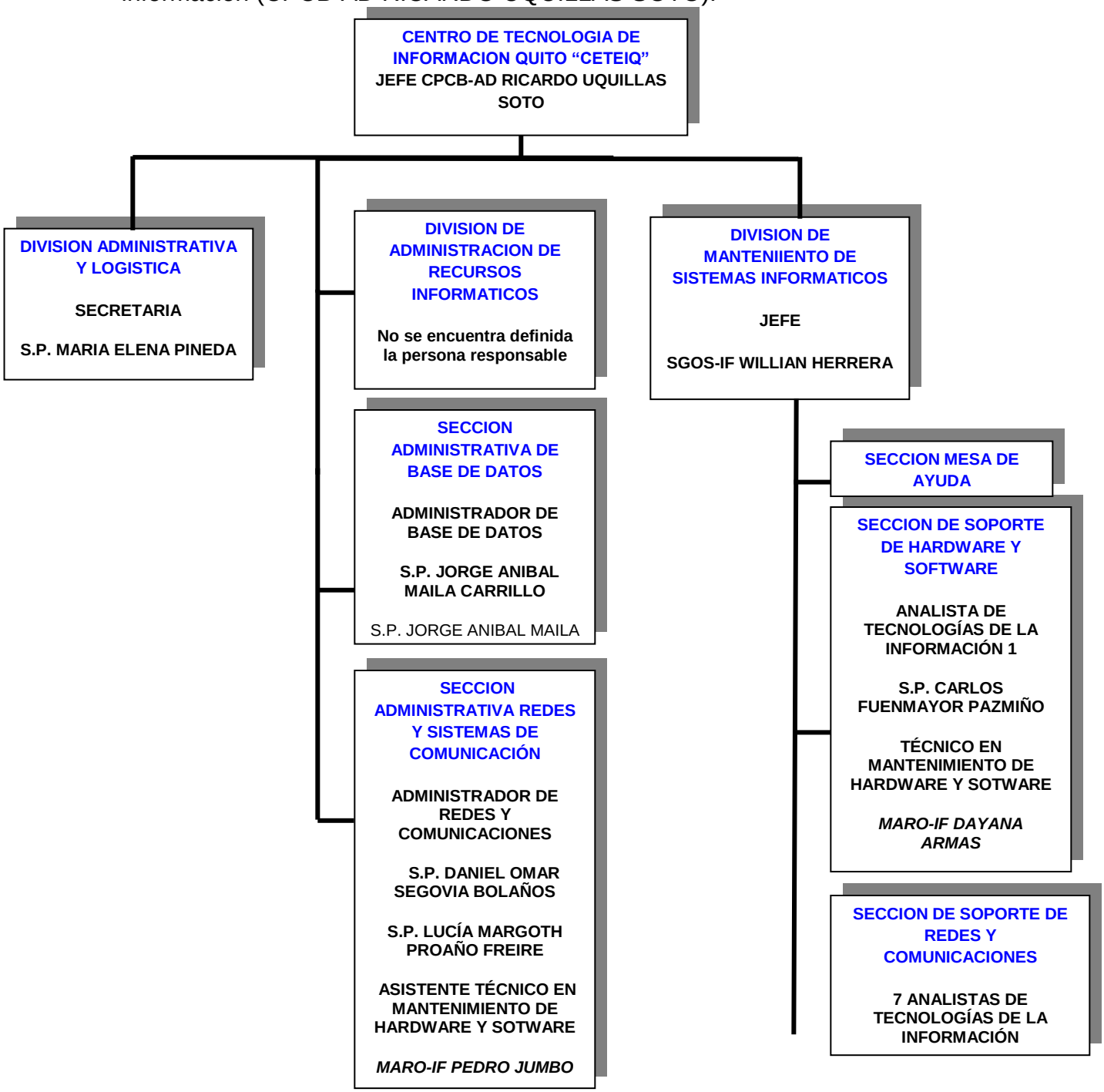

Figura 6: Estructura Orgánica[56]

Como se puede observar en la *Figura 3.1,* se visualiza que el CETEIQ, está conformada por tres divisiones principales los mismos que ayudan al manejo central de la información y reparto de comunicaciones de la Fuerza Naval en Quito

- Misión, Visión de la institución. *(Ver Capítulo 1, Figura 1.5: Cadena de Valor)*
- Procesos estratégicos, agregados de valor y de apoyo. *(Ver Anexo 1, Pg.3: DE LA FUNCIÓN BÁSICA Y OBJETIVOS ESTRATÉGICOS).*
- Miembros de aéreas operativas de procesos. *(Ver Anexo 1, Pg.7:* DE LA ESTRUCTURA ORGANICA DESCRIPTIVA*).*
- Plantilla de definición del alcance

  De acuerdo a una reunión prevista con el Jefe del Centro de Tecnologías de la Información (CETEIQ), se obtuvo el permiso para definir el alcance que tendrá la Metodología de Gestión de Riesgos y Seguridad de la información, y se pudo definir las divisiones y miembros que pertenecen a cada una de ellas, para el análisis y la gestión de riesgos.

Definición del Alcance	
REPARTO: CETEIQ	
DIVISION: ADMINISTRATIVA Y LOGISTICA	
Área: SECRETARIA	**Descripción del Área:** Ejecutar, coordinar y controlar las actividades necesarias para dar el apoyo administrativo y logístico al CETEIQ, en los temas de recursos humanos, financieros, materiales y servicios generales.
Miembros integrados:	S.P. MARIA ELENA PINEDA
DIVISION: ADMINISTRACION DE RECURSOS INFORMÁTICOS	
Área: BASE DE DATOS Y REDES Y SISTEMA	**Descripción del Área:**

[56] Fuente: CETEIQ (Centro de Tecnologías de la Información Quito)

DE COMUNICACIÓN	Administrar y garantizar la disponibilidad de la infraestructura informática, bases de datos y los sistemas de información para que cumplan con las necesidades tecnológicas de la Armada, brindando así los mejores niveles de seguridad, disponibilidad, confiabilidad y escalabilidad. Implantar, monitorear y mantener operativa la Red Naval de Datos en las áreas de jurisdicción asignadas, optimizando y racionalizando su uso.
Miembros integrados:	CBOS-IF PEDRO JUMBO CBOS-IF DAYANA ARMAS S.P. JORGE ANIBAL MAILA CARRILLO S.P. DANIEL OMAR SEGOVIA BOLAÑOS S.P. LUCÍA MARGOTH PROAÑO FREIRE
DIVISION: MANTENIMIENTO DE SISTEMAS INFORMÁTICOS	
Área: SOPORTE DE HARDWARE Y SOFTWARE, SOPORTE DE REDES Y COMUNICACIONES	**Descripción del Área:** Coordinar el apoyo y solución de los diferentes problemas de servicios de red y aplicaciones, a usuarios internos y externos. Brindar soporte técnico para solucionar los problemas de sistemas, hardware y software presentados en el nodo norte.
Miembros integrados:	SGOS-IF WILLIAN HERRERA S.P. CARLOS FUENMAYOR PAZMIÑO (técnico soporte) MARO-IF PEDRO JUMBO (técnico soporte) S.P. FABIÁN PATRICIO ESPINOSA BARRERA (administrador Proyectos) S.P. ROSA XIMENA FIALLOS COBO (Técnico) S.P. HÉCTOR PATRICIO VARGAS REINOSO (analista desarrollador) S.P. SAMMY ROBERTO RIVERA CAMPAÑA (analista desarrollador) S.P. DIANA ESTEVEZ AGUILAR (analista desarrollador) S.P. ANDREA GUADALUPE CASTRO ROSERO

	(analista desarrollador) S.P. SILVIA EUGENIA BALAREZO REVELO (desarrollador)
Observaciones: Se ha determinado la definición del alcance, el mismo que va a comprender y será de estudio para aplicar la Gestión de Riesgos y seguridad de la información será la DIVISION DE ADMINISTRACION DE RECURSOS INFORMÁTICOS, la misma que se encuentra toda la información y seguridad naval y red de datos de la Comandancia General de la Marina. Esta decisión se tomo ya que esta división es la más importante de la marina ya que se encuentra información reservada.	
Fecha: 29-07-2013	**Realizado por:** Ing. Diana Estévez
	Aprobado por: Jefe del CETEIQ

Plantilla 23: Definición del alcance[57]

3.2.1.2. Etapa 2: Contexto del Proceso de Gestión de Riesgos

3.2.1.2.1. Actividad 1: Selección de miembros responsables

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Plantilla Definición Alcance con miembros integrados de cada área. *Ver: Fase 1, E1, A1, Plantilla 3.1: Definición del Alcance.*
- ❑ Estructura Orgánica Funcional de la institución *(Ver Anexo 1, Pg.13: GUIAS FUNCIONALES INTERNAS).*

Criterio de Salida

- ❑ Determinación de personas responsables de cada proceso

  Según reunión mantenida con el Jefe del CETEIQ, se definió que habrá personas que conformarán el equipo de análisis, los mismos que se comprometerán con el

[57] Fuente: La Autora

aplicar el proceso de la metodología de gestión de riesgos, hasta el final de los resultados obtenidos.

❑ Plantilla de Equipo para el análisis de cada proceso

Equipo para el Análisis de Riesgos			
REPARTO:	CETEIQ	**DIVISIÓN:** DE ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS	
Área o proceso: Redes y comunicaciones		**Descripción del Proceso o Área:** Dentro de la División de Administración de Recursos Informáticos se encuentra el área de Redes y comunicaciones la misma que se encarga de mantener y monitorear la red naval de datos y la seguridad de la información.	
Responsables		**Participa como**	**Cargo**
CPCB-AD RICARDO UQUILLAS SOTO		Jefe del proyecto de análisis de riesgos	Jefe del CETEIQ
S.P. DANIEL OMAR SEGOVIA BOLAÑOS		Miembro principal 1	Administrador de Redes
S.P. LUCÍA MARGOTH PROAÑO FREIRE		Miembro secundario 1	Asistente de administración de redes
S.P. ESTEVEZ AGUILAR DIANA		Miembro principal 2	Analista de sistemas
S.P. JORGE ANIBAL MAILA CARRILLO		Miembro principal 3	Administrador de BDD
S.P. FABIÁN PATRICIO ESPINOSA BARRERA		Miembro secundario 2	Administrador de proyectos
Observaciones:	En la reunión mantenida con las personas de la división de Administración de recursos informáticos se definió al Jefe del proyecto y los miembros principales y secundarios responsables que conformarán el equipo. Los miembros principales serán las personas que comuniquen al Jefe del equipo todos los procesos y actividades que se finalicen en las fases de la metodología de Gestión de Riesgos y Seguridad de la información. En lo que respecta a los miembros secundarios serán respaldos de los miembros principales siempre y cuando faltaren por acciones personales o actividades que estén fuera de lo previsto; los mismos que comunicarán sus actividades y tareas ejecutadas y por ejecutar. También se llevó a cabo una capacitación para el equipo de análisis respecto al modelo de Gestión de Riesgos que se ejecutará dentro del CETEIQ, esto se dictada por la Ing. Diana		

	Estévez.		
Fecha:	29-07-2013	**Realizado Por:**	Ing. Diana Estévez
		Aprobado Por:	Jefe del CETEIQ

Plantilla 24: Equipo para el Análisis Definición del alcance[58]

3.2.1.2.2. Actividad 2: Definir la metodología de Evaluación de Riesgos

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

❑ Información de Seguridad de procesos.

No se tiene definido procesos de seguridad, solo está establecida la directiva de seguridad de la información implantada por COGMAR (Comandancia General de la Marian), *Ver Anexo 2, DIRECTIVA SEGURIDAD INFORMÁTICA 12Jul2010.pdf.*

❑ Procedimientos de gestión.

No existe documentación al respecto y tampoco se aplica ninguna metodología de gestión en el departamento de tecnología.

❑ Procesos de probabilidades de riesgos si lo tuviere.

No se encuentran definidas y no existen tampoco implementadas para ninguna metodología de gestión de riesgos, por lo que tampoco no hay datos históricos para esta gestión.

Criterio de Salida

❑ Escalas de riesgo, probabilidad e impacto

[58] Fuente: La Autora

Se aplicará la *Tabla 2.1: Escala para definir el impacto; del (Capitulo 2, Fase1, E2, A2),* para definir el impacto tomando como valores a los criterios: ALTO= 3, MEDIO= 2 y BAJO= 1.

Se aplicará la *Tabla 2.2: Escala para definir el riesgo; del (Capitulo 2, Fase1, E2, A2),* para definir el riesgo tomando como valores a los criterios: ALTO= 3, MEDIO= 2 y BAJO= 1.

Se aplicará la *Tabla 2.3: Escala para definir la probabilidad; del (Capitulo 2, Fase1, E2, A2),* para definir la probabilidad de ocurrencia tendrá como valores: MB= 1, B= 2, M= 3, A= 4 y MA= 5.

❑ Matriz de cálculo del riesgo

Se aplicará la *Tabla 2.4: Matriz para calcular el riesgo; del (Capítulo 2, Fase1, E2, A2),* para definir el cálculo del riesgo sobre la probabilidad de ocurrencia el cual tendrá valores: ALTO= 3, MEDIO= 2 y BAJO= 1.

❑ Plantilla de resultados de la metodología de evaluación del riesgo

<table>
<tr><th colspan="2">Resultado de Definir la Metodología de Evaluación del riesgo</th></tr>
<tr><td>Escala de probabilidad de ocurrencia:</td><td>MA: muy frecuente | A: frecuente | M: posible | B: poco frecuente | MB: muy poco o raro frecuente</td></tr>
<tr><td>Escala de impacto:</td><td>A: alto | M: medio | B: bajo</td></tr>
<tr><td>Escala del riesgo:</td><td>A: alto | M: medio | B: bajo</td></tr>
<tr><td>Matriz de cálculo del riesgo:</td><td>
<table>
<tr><th colspan="2" rowspan="2">RIESGO</th><th colspan="5">PROBABILIDAD</th></tr>
<tr><th>MB</th><th>B</th><th>M</th><th>A</th><th>MA</th></tr>
<tr><td rowspan="3">IMPACTO</td><td>A</td><td>M</td><td>M</td><td>A</td><td>A</td><td>A</td></tr>
<tr><td>M</td><td>B</td><td>M</td><td>M</td><td>A</td><td>A</td></tr>
<tr><td>B</td><td>B</td><td>B</td><td>B</td><td>M</td><td>M</td></tr>
</table>
</td></tr>
<tr><td>Observaciones:</td><td>Durante la reunión mantenida con el equipo de análisis se vio la necesidad de que los participantes requieran tener conocimiento en manejo de riesgos por lo que se les facilito una charla por parte de la Ing. Diana Estévez para aclarar estos temas. El equipo de análisis ha determinado los colores que se evaluarán cada criterio de definición con la calificación de: 3, 2,1 que corresponden a: Alto, medio, bajo respectivamente para el cálculo del riesgo.</td></tr>
</table>

Fecha:	02-08-2013	**Realizado Por:**	El equipo de Análisis
		Aprobado Por:	Jefe del CETEIQ

Plantilla 25: De Resultados de la metodología de evaluación del riesgo[59]

3.2.1.2.3. Actividad 3: Definir los criterios de evaluación del riesgo

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

❑ Lista de riesgos o vulnerabilidades de seguridad de la información de la organización.

Se ha pedido al Administrador de la Red del Centro de tecnologías de la información: S.P. DANIEL OMAR SEGOVIA BOLAÑOS; el detalle de las vulnerabilidades encontradas y los riesgos que se han detectado en el departamento: Ver Anexo 3, *RIESGOS O VULNERABILIDADES DEL CETEIQ*.doc

Criterio de Salida

❑ Plantilla de Definir los criterios de evaluación del riesgo

Analizando la lista otorgada dentro del Equipo de análisis se definió criterios y se especificó en cada criterio la calificación de riesgos altos, medios y bajos.

Resultado de Definir los criterios de evaluación del riesgo			
Criterios	**Bajo**	**Medio**	**Alto**
Proceso de información de datos	El riesgo será bajo siempre y cuando la calidad de los datos no se vean afectadas por cambios o instalaciones	El riesgo será medio cuando la calidad de los datos se vea afectada por cambios o instalaciones y no exista un control de por medio	El riesgo será alto cuando la calidad de los datos dentro de los cambios o instalaciones se pierdan, sean inconsistentes, duplicados, perdidos o

[59] Fuente: La Autora

			erróneos
Activos de información	el riesgo será bajo cuando el activo de información se encuentre intentos de acceso a la información, interrupción momentánea en la disponibilidad de la información, o un ente no autorizado tiene la oportunidad de observar datos que se estén utilizando en la operación de la institución	El riesgo es medio cuando se encuentra ataques masivos sobre la plataforma, o que funcionarios de la institución tengan acceso a la información a la cual no está autorizado, que haya interrupción de un día hábil en la disponibilidad de la información o que haya perdida de datos que pueden restaurar por medio de procesos de recuperación	El riesgo es alto cuando sea ha accedido y es vulnerada la información afectando así la confidencialidad, la disponibilidad y la integridad de la información y que los datos institucionales hayan sido alterados
Gestión (riesgos relacionados con la ausencia o aplicación incorrecta de métodos de gestión de las tecnologías de información y comunicaciones)	El riesgo es bajo cuando el evento no se afecte o es leve el logro de los objetivos institucionales	El riesgo es medio cuando se vea un retraso significativo en el logro de objetivos institucionales	El riesgo es alto cuando el evento impida el logro de objetivos institucionales
Operación (incumplimiento de directrices, procedimientos y metodologías y estándares en los procesos operativos de TI)	El riesgo es bajo cuando el evento afecta solo las operaciones del TI	El riesgo es medio cuando el evento provoca interrupciones intermitentes	El riesgo es alto cuando se paraliza la prestación de servicios por parte de la unidad afectando a la institución de manera considerable
Infraestructura (riesgos relacionados con fallas potenciales de la infraestructura	El riesgo es menor cuando la falla en un componente que puede ser sustituido de	El riesgo es medio cuando la falla en un componente de la infraestructura	El riesgo es alto cuando hay falla severa en un componente vital de la infraestructura

tecnológica)	inmediato por mantener equipo similar en inventario y afecta la operación por minutos o solo afecta la prestación de servicios al TI	tecnológica que afecta de manera intermitente la prestación de los servicios	tecnológica que impide la operación normal de la institución
Observaciones:	Se realizó la reunión con el equipo de análisis y analizando el listado de vulnerabilidades existentes en el departamento de infraestructura y redes se ha llegado a definir los criterios para evaluar los riesgos en el CETEIQ, esto ha sido autorizado por el Jefe del departamento; se tomo en cuenta que esta implementación de gestión de riesgos y seguridad de la información no se ha realizado nunca en el departamento así que no se tuvo datos históricos ni criterios de riesgos adicionales para definir este esquema.		
Fecha:	08-08-2013	**Realizado Por:**	Equipo de análisis
		Aprobado Por:	Jefe del CETEIQ

Plantilla 26: Plantilla de Resultado de definir los criterios de evaluación del riesgo[60]

3.2.1.2.4. Actividad 4: Definir criterios de Impacto

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Plantilla de Definir los criterios de evaluación del riesgo. *Ver Fase 1, E2, A3, Plantilla 3.4: Plantilla de Resultados de definir los criterios de evaluación del riesgo.*

Criterio de Salida

- ❑ Plantilla de Definir los criterios de impacto

[60] Fuente: La Autora

Analizando la *Plantilla 3.4 del criterio de entrada,* y considerando los aspectos que detalla esta actividad, se procedió a detallar cual serán las áreas de impacto con sus criterios altos, medios y bajos:

Resultado de Definir los criterios de impacto			
Área de impacto	**Bajo**	**Medio**	**Alto**
Activos de información	El impacto será bajo cuando los daños de un activo de información no es tan significante en operaciones diarias	El impacto será medio cuando los daños de una activo de información sean significantes en las operaciones diarias	El impacto será alto cuando la pérdida de un activo de información sea indispensable en las operaciones diarias
Operación y productividad	El impacto será bajo cuando las operaciones y productividad del TI se desgasten y no afecten a la institución	El impacto será medio cuando las operaciones y productividad del TI den una atención ineficiente o retraso en la atención a usuarios de la institución o procesos de continuidad del negocio	El impacto será alto cuando las operaciones y productividad del TI no satisfagan los requerimientos y aspectos institucionales o haya demasiadas inconformidades
Financiera	El impacto será bajo cuando sea de menos del 2% en los costos de operación del CETEIQ (por ejemplo, una semana de prórroga por cuatro miembros del personal para documentar los cambios en los planes de tratamiento, o compra de activos no representativos) El impacto será bajo cuando haya menos del 5% de pérdida anual de ingresos del CETEIQ (por ejemplo, fallos de equipos informáticos)	El impacto será medio cuando los costos operativos anuales sean de hasta 2-10% (por ejemplo, la contratación de trabajadores temporales por tres meses llevan varias veces al día) El impacto será medio desde 5-10% de pérdida anual de ingresos del CETEIQ (por ejemplo, retrasando rentables debido a la pérdida de archivos y recuperación) El impacto será medio cuando el coste financiero sea de $ 30000 mil a $ 100 000 (por ejemplo, la adición de un servidor y	El impacto será alto cuando los costos operativos anuales sean mayores del 10% (por ejemplo, añadir tiempos para la recuperación de archivos, agregar software para disuadir de nuevas intrusiones) El impacto será alto cuando haya un 10% de pérdida anual de los ingresos del CETEIQ El impacto será alto cuando el coste financiero supere los $ 100000 (por ejemplo, el sistema de sustitución o

		reutilizar activos de la asignación)	compra de un nuevo servidor, o equipamiento de data center)
Seguridad de la información	El impacto es bajo cuando existe la confidencialidad de la información no se ha perdido o no ha habido atacantes que accedan a dicha información sin debida autorización El impacto es bajo cuando la integridad de los datos no ha sido modificada por personas no autorizadas El impacto es bajo cuando la disponibilidad de la información se ha suspendido por algunas horas debido a interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema	El impacto es medio cuando existe acceso de confidencialidad de la información por personas no autorizadas y estos accesos se divulguen entro otras personas El impacto es medio cuando la integridad de los datos sea modificada siempre y cuando por personas sujetas a autorización, o es alterada por personas o procesos no autorizados El impacto es medio cuando la suspensión del servicio ha sido un día laboral por interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema	El impacto será alto cuando haya perdida de confidencialidad de información y accedan personas no autorizadas y realicen ataques El impacto será alto cuando la integridad de los datos se pierda por alteraciones, modificaciones, o manipulaciones de personas no autorizadas afectando así a la confiabilidad de la información El impacto es alto cuando sea ha suspendido por completo y por algunos días la disponibilidad en interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema y que haya ataques en la denegación del servicio
Reputación / confianza del cliente	El impacto será bajo cuando la reputación sea mínimamente afectada, poco o ningún esfuerzo o sea un gasto innecesario para recuperar	El impacto será medio cuando la reputación sea dañada, un poco de esfuerzo y los gastos necesarios para recuperar	El impacto será alto cuando la reputación sea irrevocablemente destruida o dañada

	El impacto será bajo cuando no hay cambio en la calificación o acreditación de organizaciones que autoricen la caída de menos de 1% de los clientes debido a la pérdida de confianza El impacto será bajo cuando no exista violación no pública de la Ley de Privacidad (divulgación al personal dentro de las instalaciones con la necesidad de saber - agente de confianza)	El impacto será medio cuando la reducción o advertencia de la calificación o acreditación de organizaciones que autoricen caídas de 2 a 5% en los clientes debido a la pérdida de confianza El impacto será medio cuando exista violaciones Públicas de la Ley de Privacidad: (1) la divulgación al personal dentro de las instalaciones sin la necesidad de saber, (2) cualquier persona que viola la Ley de Privacidad y revela información confidencial El impacto será medio cuando el cliente busca atención de otra fuente	El impacto será alto cuando la pérdida de la habilitación o acreditación de organizaciones de revisión tenga una caída de más de un 5% de los clientes debido a la pérdida de confianza
Observaciones:	Se realizó la reunión con el equipo de análisis y analizando el listado de los criterios de riesgos que se definió se procedió a decidir sobre los impactos posibles y los que suceden en el CETEIQ, esto ha sido autorizado por el Jefe del departamento; se tomo en cuenta que esta implementación de gestión de riesgos y seguridad de la información no se ha realizado nunca en el departamento así que no se tuvo datos históricos ni criterios de impactos adicionales para definir este esquema. Se llego a la conclusión que estos criterios en el transcurso de la gestión de riesgos podrían ser aumentados.		
Fecha:	12-08-2013	**Realizado Por:**	Equipo de análisis
		Aprobado Por:	Jefe del CETEIQ

Plantilla 27: De Resultados de definir los criterios de impacto[61]

[61] Fuente: La Autora

3.2.1.2.5. Actividad 5: Definir criterios de aceptación de riesgo

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Relacionar factores de criterios de negocio, aspectos legales, reglamentarios, operaciones, tecnológica y finanzas.

  Se realizo una reunión con el equipo de análisis y se trato este tema viendo los mejores criterios de aceptar el riesgo en el CETEIQ.

Criterio de Salida

- ❑ Plantilla de Definir los criterios de aceptación del riesgo

  Durante la reunión se definió criterios para aceptar el riesgo y ha sido aprobados por el Jefe del CETEIQ, se llego a determinar que cuando los niveles de riesgo alcancen a niveles ALTOS y MEDIOS, esos no serán aceptados y se procederá al tratamiento del mismo, siempre y cuando la gerencia lo apruebe, en cambio los riesgos de nivel BAJO, estos serán aceptados sin realizar alguna acción

Resultado de Definir los criterios de aceptación del riesgo		
Nivel de riesgo estimado	**Criterio de aceptación**	**Descripción del criterio**
Alto	Durante la etapa de tratamiento del riesgo no se aceptará y deberán ser tratados	Siempre y cuando la alta gerencia o dirección apruebe y por ende serán tratados y se ejecutará los planes de acción.
Medio	Durante la etapa de tratamiento de riesgos no se aceptarán y deberán ser tratados	Siempre y cuando la alta gerencia o dirección apruebe y por ende serán tratados y ejecutando planes de acción.
Bajo	Durante la etapa de tratamiento de	No serán sujetos a tratamiento

	riesgos se aceptarán pero estarán analizados y comunicados de sus cambios	
Observaciones:	Se realizó una reunión con el personal de equipo de análisis y se llego a la conclusión que los riesgos que tengan nivel alto y medio no serán aceptados, por lo que serán destinados a tratamiento del riesgo siempre y cuando esté aprobado por el Jefe del CETEIQ, esto quiere decir que dependerá mucho de las acciones que se tomarán los riesgos de estos niveles, En cuanto a los riesgos de nivel bajo, estos serán aceptados por el Jefe del CETEIQ y se tratará como riesgos retenidos e igual estarán en constante análisis y comunicación de sus cambios.	
Fecha:	13-08-2013	**Realizado Por:** Equipo de Análisis
		Aprobado Por: Jefe del CETEIQ

Plantilla 28: Resultado de Definición de aceptación del riesgo[62]

3.2.2 FASE 2: IDENTIFICACIÓN DE LOS RIESGOS

3.2.2.1. Etapa 1: Determinación de los Activos

3.2.2.1.1 Actividad 1: Identificación de los Activos

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Lista de activos identificados con su propietario, su responsabilidad y rendición de cuentas sobre este; hay que tomar en cuenta que este listado será identificado dentro del alcance que se determinó en la *Fase 1.*

  Según*: Ver Fase 1, E1, A1, Plantilla 3.1: Definición del alcance*; se analizó que dentro de la División de administración de recursos informáticos que está compuesta por el Área de Base de Datos y Redes y Sistemas de Comunicación,

[62] Fuente: La Autora

será el alcance para identificar los activos a analizar la gestión de riesgos y seguridad de la información.

Criterio de Salida

- Relación de activos a considerar.

  Se incluyo dentro de la plantilla de resultados las relaciones que tienen los activos.

- Plantilla de identificación de activos. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja Identificación de activos.*

RESULTADO DE LA IDENTIFICACION DE ACTIVOS

REPARTO: ESTACION NAVAL DE QUITO **DEPARTAMENTO:** CENTRO DE TECNOLOGIAS DE LA INFORMACION QUITO CETEIQ **UNIDAD RESPONSABLE:** BASE DE DATOS Y REDES Y SISTEMA DE COMUNICACIÓN

No.	Nombre del Activo	Descripción del Activo	Tipo de Activo	Detalle del Tipo de Activo	Persona Responsable del activo	Funciones principales del activo	Relación con otro activo	Cantidad
1	SWITCH	SWITCH: 3ER PISO, 3ER SWITCH PARA COGMAR CONTRATO ESMAAR-DIN-027-2001-12 CATALYST 3524 DE 24 PUERTOS 10/100 BASE-TX_ AUTOSENSING 2 PUERTOS 1000 BASE-X (GBIC) ESMAAR-FAB0604W1BG	Hardware	soporte de la red	Ing. Daniel Segovia (Administrador de red)	proporciona conexión de red al tercer y cuarto piso de la comandancia	ninguno	1
2	UPS	ANDOLAS CIA. LTDA. INCLUYE 8 BATERIAS DIRDAIAF09022975	Hardware	equipamiento auxiliar	Ing. Daniel Segovia (Administrador de red)	provee energia eléctrica en la planta baja de la comandancia y a diesel a ESNAQI	ninguno	1
3	SERVIDOR	DIRECTIVAS CHQ.22067 TECMOWARE DEL 29DIC00 FACT004685 INTEL SERVER /SERVER BOARD SBT2_CHASIS INTEL SERVER SC5000_ PROCESADOR 2 PENTIUM III XEON_ VELOCIDAD 933MHZ CAP MEMORIA MIN 256 MB (1 PASTILLA) CAP MEMORIA MAX 4 GB SDRAM_ DISCO DURO FW 18GB SCSI MARCA QUANTUM_ TOTAL SLOTS 7 CD ROM 52X IDE_ MONITOR 17" SERIE: 23-GDBK7_ TECLADO SERIE: 1S28L18250004357 Y MOUSE SERIE: S/N_ SISTEMA OPERATIVO RED HAT LINUX 7.0 SIN INSTALACION INCLUYE: CHQ.29852 COMPU EC 3DIC03 FCT.613 4NOV03 ADQ.PARTES PARA REPOTENCIAR EL SERVIDOR DEL SEC.20010108 8 2 GB RAM (KIT DE 2X512 MB) SER.632752114867 Y SER.632752114867 1.240.00 USD 2 DISCOS DUROS FIJOS DE 36GB SCSI SER.E3VAP8WB Y E3VAGEYB 640.00	Hardware	Equipo fijo	Ing. Daniel Segovia (Administrador de red)	este servidor contiene el portal de directivas de información de la fuerza naval	4	1
4	PORTAL WEB DIRECTIVAS DE INFORMACIÓN	se encuentra instalado en el servidor N.4, aplicación web de consulta de directivas	Software	Aplicación estándar del negocio	Ing. Daniel Segovia (Administrador de red)	este portal permite ingresar a los usuarios asignacion de la comandancia para visualizar todas las directivas y proedimientos que se han aprobado por la COGMAR (Comandancia General de Marina)	3	1
5	UPS	FIRMESA INDUSTRIAL 27AGT02 POWERWARE DE 9KVA_GABINETE DE 6 SLOTS0650C060 DE 1.324.00 USD 3 MODULOS ELECTRONICOS ASY DE 1.806.00	Hardware	equipamiento auxiliar	Ing. Daniel Segovia (Administrador de red)	Abastece al CETEIQ y sala de servidores de energia eléctrica y dispositivos electrico	ninguno	1

Plantilla 29: Resultado de la Identificación de Activos[63]

[63] Fuente: La Autora

Se registraron alrededor de 86 activos de información, que se clasificaron por descripción del activo, la persona responsable, funciones principales del activo, su relación con otro activo y cantidades de toda la unidad de Base de datos y redes de sistemas de comunicación parte del Centro tecnológico de información Quito CETEIQ. Esta identificación de activos, se lo exportó también de la aplicación Icron (Aplicativo Web de la Fuerza Naval), la misma que permite administrar y registrar todos los activos con sus custodios responsables de toda la Armada.

3.2.2.1.2 Actividad 2: Valoración de Activos

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Resultados de la identificación de activos *Fase 2, E1, A1, Plantilla 3.7: Resultado de la Identificación de Activos*

Criterio de Salida

- ❑ Modelo de valoración de activos.

  Se definió que se realizará el primer modelo de valoración de los activos por las características de trazabilidad, autenticidad, confidencialidad de la información, integridad de los datos, disponibilidad, ya que se concluyó que será más acorde para la valoración de los activos de información del área de infraestructura y redes del CETEIQ.

- ❑ Plantilla de valoración de los activos. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja VALORACION DE ACTIVOS (1).*

RESULTADO DE LA VALORACION DEL ACTIVO									
No.	Tipo de Activo	Nombre del Activo	Funciones principales del activo	Disponibillidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Resultado Valoracion
20	Hardware	UPS	proporciona energia eléctrica a los racks del CETEIQ, estos funciona como respaldo	8	6	5	4	3	5
22	Hardware	SWITCH	proporciona conexión de red al departamento de operaciones conecta la administración central telefónica del Estado Mayor no hay otro respaldo	10	3	4	3	4	5
27	Hardware	SWITCH	proporcion conectividad a la red informatica del CETEIQ	9	4	8	3	3	5
42	Hardware	UPS	alimenta el rack de comunicaciones	7	3	3	4	6	5
73	Hardware	DISCO EXTERNO	disco duro para reespaldos de back up de BDD	7	7	7	4	2	5
5	Hardware	UPS	Abastece al CETEIQ y sala de servidores de energia eléctrica y dispositivos electrico	10	4	0	1	5	4
28	Hardware	SWITCH	proporciona conexión de red a la red administrativa	7	2	4	3	4	4
32	Hardware	SWITCH	proporciona conexión de red a ESNAQI Estacion naval de quito planta alta	7	2	4	2	3	4
38	Hardware	UPS	provee energia eléctrica al 1er y 2do piso de la comandancia general de la marina	8	1	2	2	7	4
40	Hardware	UPS	provee energia eléctrica a los blades de IBM	7	0	4	3	7	4
49	Hardware	SWITCH	proporciona conexión de red a la planta alta de ESNAQI a usuario comandantes y capitanes	6	1	2	4	5	4
54	Hardware	VIRTUAL REPORTING SERVICES	servicio de reportes que tiene la armada para visualizacion de activos fijos y bienes no depreciables con sus custodios responsables de la armada	7	2	5	4	4	4
1	Hardware	SWITCH	proporciona conexión de red al tercer y cuarto piso de la comandancia	3	3	0	4	3	3

Plantilla 30: Resultado de la Valoración del Activo[64]

Con el Equipo de Análisis se valoró la lista de activos de la *Actividad 1,* por lo que se llego a determinar los resultados de Crítico con calificación 10 -9, Alto con calificación 8-7-6, Medio 5-4-3, Bajo 2-0, Sin efecto 0 con colores demostrativos:

Critico	Alto	Medio	Bajo	Sin Efecto
10-9	8-7-6	5-4-3	2-1	0

El tratamiento de los activos se los realizará a los que tengan como resultado critico, alto y medio.

[64] Fuente: La Autora

Para una visualización a detalle y consultas por nivel de calificación y activo se ha realizado tablas dinámicas con filtros y gráficos de barra para obtener los datos individuales por nivel de calificación obtenido, *véase Herramienta Gestión de riesgos y Seguridad de información.xls, hoja TBL DINAMICA VALORACION ACT (2):* en el eje de la y representa el nivel de valoración del activo de 0 a 10 y en el eje de las x representa la calificación que obtuvo por cada activo en este ejemplo nivel 1 y 2 que significa que los activos del área han tenido valoración baja.

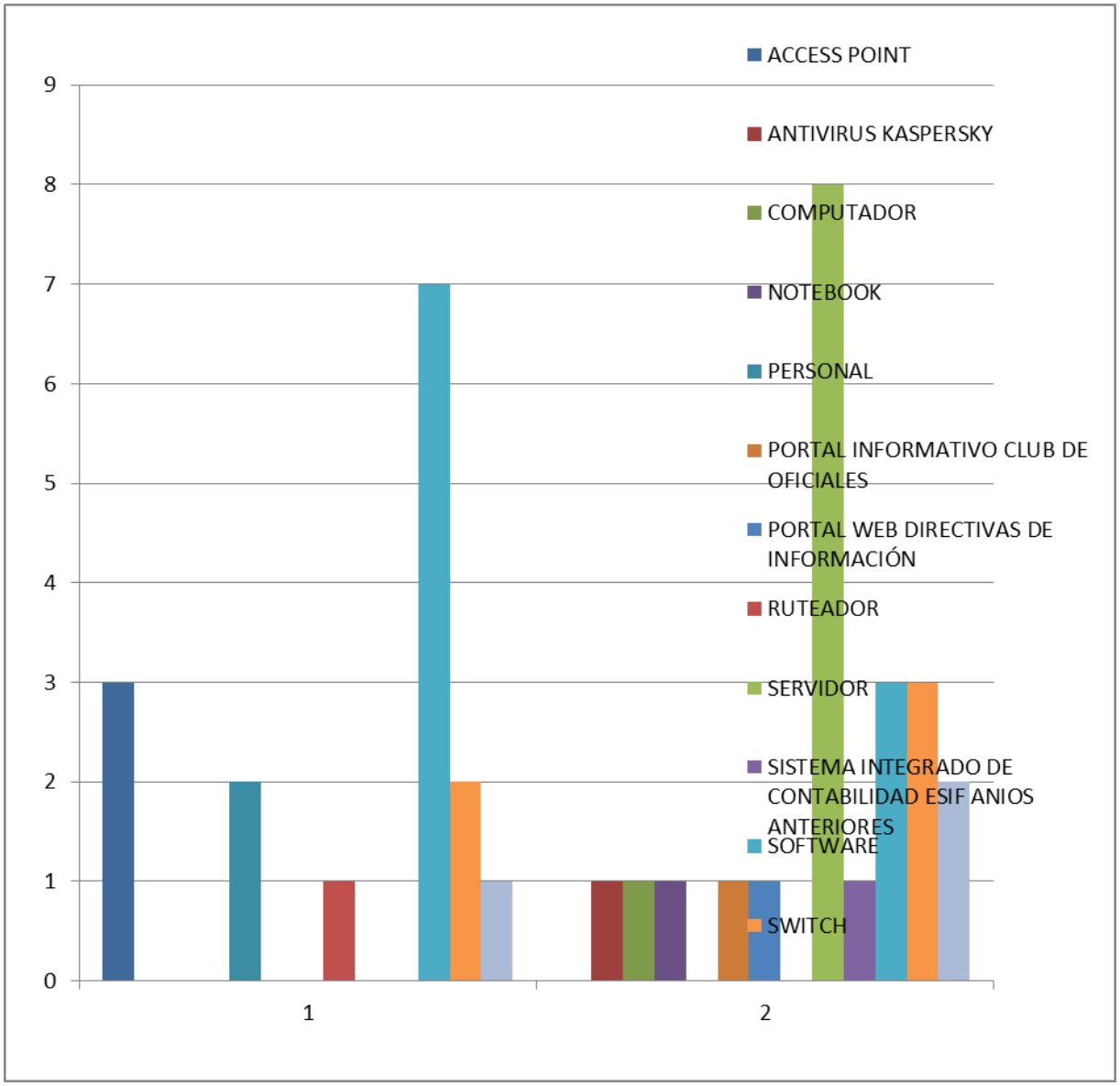

Tabla 16: Tabla dinámica de Valorar un Activo[65]

[65] Fuente: La Autora

3.2.2.2. Etapa 2: Determinación de las Amenazas

3.2.2.2.1. Actividad 1: Identificación de las amenazas

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Resultados de la identificación de activos *Fase 2, E1, A1, Plantilla 3.7: Resultado de la Identificación de Activos*
- ❑ Informes de vulnerabilidades en el producto si lo hubiere.

  No se encuentra por escrito las vulnerabilidades que existen por cada activo o área de infraestructura. Esto se detallará realizando preguntas a los custodios de cada activo y al administrador de redes del área de infraestructura.

Criterio de Salida

- ❑ Árboles de categorías de amenazas.

  Ver Figura 2.3, Figura 2.4, Figura 2.5 del Capítulo 2, Fase 2, E2, A1. Se analizó con el Equipo de análisis de la gestión de riesgos y seguridad de la información y se llegó a la conclusión que los árboles destacados en la metodologías se diferenciaran los riesgos potenciales con color rojo y los que no se encuentra amenaza alguna sin color.

- ❑ Tabla de relación entre tipo de activos y perfil de amenazas.

  Ver Tabla 2.12 del Capítulo 2, Fase 2, E2, A1. Se analizó la tabla de relación especificada en la metodología y se tomó en cuenta para los perfiles de amenaza de cada activo.

- ❑ Plantilla de identificación de amenazas.

  Se realizo la identificación de las amenazas de 45 activos que se encontraban con calificación crítico, alto y medio. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja IDENTIFICACION AMENAZAS*

RESULTADO DE LA IDENTIFICACIÓN DE LAS AMENAZAS								
No.	Tipo de Activo	Funciones del Activo	Activo	Acceso (Tipo de Amenaza)	Actor	Motivo	Resultado	Descripcion de la amenaza
75	Red	como 10 anos instalado en el	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Revelacion	
							Modificacion	Formas de compartir las unidades de red.
							Pérdida	Conexiones a internet
							Interrupción	Configuración de servidores de seguridad
						deliberada	Revelacion	
							Modificacion	Formas de compartir las unidades de red.
							Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión
							Interrupción	Configuración de servidores de seguridad
					externo	accidental	Revelacion	
							Modificacion	
							Pérdida	
							Interrupción	Conexiones a internet
						deliberada	Revelacion	
							Modificacion	
							Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión
							Interrupción	
				Actores_humanos_con_acceso_físico	interno	accidental	Revelacion	
							Modificacion	Manejo de periféricos y dispositivos especiales
							Pérdida	Explosiones, derrumbes, contaminación química, sobrecarga eléctrica
							Interrupción	Errores de administrador no intencionadas en el uso para responsabilidad de instalación y operación
						deliberada	Revelacion	Control y monitoreo sobre accesos no solo en áreas donde se encuentran los equipos informáticos sino en otras tales como áreas donde se encuentran los cableados. Además controles sobre cableados telefónicos, eléctricos, de red y de control de calefacción.
							Modificacion	
							Pérdida	
							Interrupción	Indisponibilidad del personal, ausencia por enfermedad no intencionada, guerra, alteraciones de orden público, ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueos de accesos, etc.

Plantilla 31: Resultado de identificación de las amenazas sobre activos críticos[66]

3.2.2.3. Etapa 3: Determinación de las vulnerabilidades

3.2.2.3.1 Actividad 1: Identificación de las vulnerabilidades

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Lista de amenazas conocidas *Fase2, E2, A1, Plantilla 3.9: Resultado de identificación de las amenazas sobre activos críticos.*

[66] Fuente: La Autora

Proceso que se realizó para identificar las amenazas sobre los activos críticos.

- ❑ Lista de activos crítico *Fase 2, E1, A1, Plantilla 3.7: Resultado de la Identificación de Activos.*

  Proceso que se realizo para identificar los activos críticos más importantes que se tomó para el análisis; el resultado 45 activos más críticos del CETEIQ

- ❑ Lista de controles de seguridad existentes: *Fase2, E4, A1, Plantilla 3.10: Plantilla de la identificación de controles de seguridad existentes.*

  Proceso que se realizo para identificación de controles existentes; se determino que no existe ningún control aplicable por lo que se llego a la conclusión que los controles designados por la ISO 27002:2005 serán herramientas necesarias para la seguridad de la información del CETEIQ.

Criterios de Salida

- ❑ Plantilla de resultado de identificación de vulnerabilidades.

  Se procedió con el equipo de análisis la identificación de las vulnerabilidades analizando las amenazas y propiedades del activo. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja IDENTIFICACION VULNERABILIDADES.*

RESULTADO DE LA IDENTIFICACIÓN DE LAS VULNERABILIDADES								
No.	Activo	Acceso	Actor	Motivo	Resultado	Descripcion de la amenaza	Vulnerabilidad	Descripcion de la vulnerabilidad
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Formas de compartir las unidades de red.	Red_y_comunicaciones	Unión de cables deficientes/ conexiones
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Pérdida	Conexiones a internet	Red_y_comunicaciones	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Interrupción	Configuración de servidores de seguridad	Red_y_comunicaciones	Monitoreo insuficiente de medidas de seguridad por la infraestructura
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Modificacion	Formas de compartir las unidades de red.	Red_y_comunicaciones	Punto de acceso no protegido
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión	Personal_	Falta de políticas, normas y procedimientos
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Interrupción	Configuración de servidores de seguridad	Red_y_comunicaciones	Monitoreo insuficiente de medidas de seguridad por la infraestructura
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	externo	accidental	Interrupción	Conexiones a internet	Red_y_comunicaciones	Comunicaciones móviles
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	externo	deliberada	Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión	Personal_	Entrenamiento insuficiente en seguridad
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_físico	interno	accidental	Modificacion	Manejo de periféricos y dispositivos especiales	Hardware_	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_físico	interno	accidental	Pérdida	Explosiones, derrumbes, contaminación química, sobrecarga eléctrica	Ambiente_Físico	Monitoreo insuficiente de medidas de seguridad por el medio ambiente
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_físico	interno	accidental	Interrupción	Errores de administrador no intencionadas en el uso para responsabilidad de instalación y operación	Personal_	Entrenamiento insuficiente en seguridad
		Actores_humanos_con_acceso_físico				Control y monitoreo sobre accesos no solo en áreas donde se encuentran los equipos informáticos sino en otras tales como áreas donde se encuentran los cableados. Además controles		

Plantilla 32: Plantilla de la identificación de vulnerabilidades[67]

3.2.2.3.2 Actividad 2: Valoración de las vulnerabilidades

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Lista de amenazas conocidas. *Véase Fase2, E2, A1, Plantilla 3.9: Resultado de identificación de las amenazas sobre activos críticos*
- ❑ Lista de activos críticos. *Véase Fase 2, E1, A1, Plantilla 3.7: Resultado de la Identificación de Activos*
- ❑ Lista de vulnerabilidades identificadas. *Fase 2, E4, A1, Plantilla 3.10: Plantilla de la identificación de vulnerabilidades.*

[67] Fuente: La Autora

Criterios de Salida

- ❑ Tabla valoración de las vulnerabilidades. *Ver Fase 2, E4, A2, Tabla 2.14: Tabla de valoración de las vulnerabilidades*

  El equipo de análisis reviso la tabla de valoración de las vulnerabilidades implantada en la metodología por lo que los parámetros de calificaciones será A: vulnerabilidad de alta gravedad, M: vulnerabilidad a media gravedad y B: vulnerabilidad de baja severidad

- ❑ Plantilla de resultado de identificación de vulnerabilidades con su valoración.

  Se realizo la valoración de las vulnerabilidades por cada amenaza detectada tomando como referencia la tabla de valoración de vulnerabilidades con calificación alta, media y baja. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja VALORACION VULNERABILIDADES.*

RESULTADO DE VALORACION DE LAS VULNERABILIDADES									
No.	Activo	Acceso	Actor	Motivo	Resultado	Descripcion de la amenaza	Vulnerabilidad	Descripcion de la vulnerabilidad	Valoración de la vulnerabilidad
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Formas de compartir las unidades de red.	Red_y_comunicaciones	Unión de cables deficientes/ conexiones	A
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Pérdida	Conexiones a internet	Red_y_comunicaciones	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	A
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Interrupción	Configuración de servidores de seguridad	Red_y_comunicaciones	Monitoreo insuficiente de medidas de seguridad por la infraestructura	A
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Modificacion	Formas de compartir las unidades de red.	Red_y_comunicaciones	Punto de acceso no protegido	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión	Personal_	Falta de políticas, normas y procedimientos	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Interrupción	Configuración de servidores de seguridad	Red_y_comunicaciones	Monitoreo insuficiente de medidas de seguridad por la infraestructura	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	externo	accidental	Interrupción	Conexiones a internet	Red_y_comunicaciones	Comunicaciones móviles	B
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	externo	deliberada	Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión	Personal_	Entrenamiento insuficiente en seguridad	A
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_físico	interno	accidental	Modificacion	Manejo de periféricos y dispositivos especiales	Hardware_	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_físico	interno	accidental	Pérdida	Explosiones, derrumbes, contaminación química, sobrecarga eléctrica	Ambiente_Físico	Monitoreo insuficiente de medidas de seguridad por el medio ambiente	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_físico	interno	accidental	Interrupción	Errores de administrador no intencionadas en el uso para responsabilidad de instalación y operación	Personal_	Entrenamiento insuficiente en seguridad	A
		Actores_humanos_con_acceso_físico				Control y monitoreo sobre accesos no solo en áreas donde se encuentran los equipos informáticos sino en otras tales			

Plantilla 33: Plantilla de la valoración de vulnerabilidades[68]

[68] Fuente: La Autora

3.2.2.4. Etapa 4: Determinación de los controles de seguridad

3.2.2.3.3 Actividad 1: Identificación de los controles existentes

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- Lista de procesos de gestión de seguridad de la información si lo tuviere y el listado de estado de su implementación.

  En el CETEIQ no se encuentra documentado ningún proceso de gestión de seguridad por lo q no se tiene antecedentes de esto.

- Verificación con personas responsables de la seguridad de la información.

  En el CETEIQ no se encuentra una persona única responsable de la seguridad de la información solo se dispone del administrador de redes que abarca varias actividades incluida esta pero no implementa ninguna seguridad.

Criterios de Salida

- Controles ISO/IEC 27002:2005, *Véase ANEXO 5 CONTROLES ISO 27002: 2005.pdf.* En el CETEIQ no existe la implementación de estos controles; hay un documento para controlar la seguridad de la información llamado *véase ANEXO 2 DIRECTIVA SEGURIDAD INFORMATICA 12Jul2010.pdf;* el mismo que se ha generado por el Estado Mayor de la Fuerza Naval. Esta directiva emitida están regidas con los controles ISO 27001 pero no se le presta mucha atención ni importancia en el CETEIQ para implementarla; no hay tampoco revisión por los altos mandos y exigencia de usar esta directiva. Viendo este problema con el equipo de análisis de gestión de riesgos se dispuso con el Jefe del CETEIQ seguir estos controles ISO como la Directiva dispuesta por el Estado Mayor, los mismos que se guiarán para la implementación y administración de un sistema de

gestión de seguridad de la información que ayudará a un mejor control y monitoreo de la seguridad de la información del departamento.

- Plantilla de identificación de controles de seguridad existentes. Se determino con el equipo de análisis que los controles dispuestos en la plantilla no se cumplen ni se implementan en el CETEIQ, no existe documentación de normas, estándares, procedimientos diarios, se encuentra la existencia de unas Directivas de seguridad pero tampoco son implementadas. Por lo que se llego a la conclusión que se tomaran estos controles para tener una mejor administración de la seguridad de la información. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja IDENTIFICACION CONTROLES EXIST.*

RESULTADO DE LA IDENTIFICACION DE CONTROLES DE SEGURIDAD EXISTENTES			
Dominio	Objetivos de control	Control	Cumple SI / NO
POLÍTICA DE SEGURIDAD.	Política de seguridad de la información.	Documento de política de seguridad de la información.	NO
		Revisión de la política de seguridad de la información.	NO
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	Organización interna.	Compromiso de la Dirección con la seguridad de la información.	NO
		Coordinación de la seguridad de la información.	NO
		Asignación de responsabilidades relativas a la seg. de la informac.	NO
		Proceso de autorización de recursos para el tratamiento de la	NO
		información.	NO
		Acuerdos de confidencialidad.	NO
		Contacto con las autoridades.	NO
		Contacto con grupos de especial interés.	NO
		Revisión independiente de la seguridad de la información.	NO
	Terceros	Identificación de los riesgos derivados del acceso de terceros.	NO
		Tratamiento de la seguridad en la relación con los clientes.	NO
		Tratamiento de la seguridad en contratos con terceros.	NO
GESTIÓN DE ACTIVOS.	Responsabilidad sobre los activos	Inventario de activos.	NO
		Propiedad de los activos.	NO
		Uso aceptable de los activos.	NO
	Clasificación de la información.	Directrices de clasificación.	NO
		Etiquetado y manipulado de la información.	NO

Plantilla 34: Plantilla de la identificación de controles de seguridad existentes[69]

[69] Fuente: La Autora

3.2.3 FASE 3: EVALUACIÓN DE LOS RIESGOS

3.2.3.1. Etapa 1: Determinación del impacto

3.2.3.1.1 Actividad 1: Identificación del impacto

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- Resultado de la determinación de los activos: *Fase 2, E1, A1, Plantilla 3.7: Resultado de la Identificación de Activos*
- Resultado de la determinación de las amenazas: *Fase2, E2, A1, Plantilla 3.9: Resultado de identificación de las amenazas sobre activos críticos.*
- Resultado de la determinación de las seguridades existentes: *Fase2, E3, A1, Plantilla 3.10: Plantilla de la identificación de controles de seguridad existentes*
- Resultado de la determinación de las vulnerabilidades: *Fase 2, E4, A1, Plantilla 3.11: Plantilla de la identificación de vulnerabilidades.*
- Tabla de criterios para evaluar los impactos. *Fase1, E2, A4, Plantilla 2.5, de resultados de definición de criterios de impacto).*

  Esta plantilla de resultado de criterios de impacto se la tomo de la fase 1 como dice en las observaciones se formo en una reunión con el equipo de análisis junto con el listado de los criterios de riesgos se definió los criterios de impactos posibles que suceden en el CETEIQ; la calificación del mismo tendrá A, M y B.

Criterios de Salida

- Plantilla de identificar y evaluar el impacto aplicando las características de la amenazas, tales como: revelación, modificación, destrucción- perdida, interrupción.

Se realizo la valoración e identificación del impacto por cada amenaza detectada tomando como referencia la tabla de criterios de impacto junto con calificación alta, media y baja. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja IDENTIFICAR IMPACTO.*

RESULTADO DE IDENTIFICAR Y VALORAR EL IMPACTO

No.	Activo	Acceso	Actor	Motivo	Resultado	Area de impacto	Descripcion del impacto	Valor del impacto
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Modificacion	Activos_de_Información	El impacto será alto cuando la pérdida de un activo de información sea indispensable en las operaciones diarias	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Modificacion	Operación_y_productividad	El impacto será bajo cuando las operaciones y productividad del TI se desgasten y no afecten a la institución	B
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Modificacion	Financiera	El impacto será bajo cuando sea de menos del 2% en los costos de operación del CETEIQ (por ejemplo, una semana de prórroga por cuatro miembros del personal para documentar los cambios en los planes de tratamiento, o compra de activos no representativos)	B
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Modificacion	Seguridad_de_la_Información	El impacto es medio cuando la integridad de los datos sea modificada siempre y cuando por personas sujetas a autorización, o es alterada por personas o procesos no autorizados	M
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Modificacion	Reputación_confianza_del_cliente	El impacto será medio cuando exista violaciones Públicas de la Ley de Privacidad: (1) la divulgación al personal dentro de las instalaciones sin la necesidad de saber, (2) cualquier persona que viola la Ley de Privacidad y revela información confidencial	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Pérdida	Activos_de_Información	El impacto será alto cuando la pérdida de un activo de información sea indispensable en las operaciones diarias	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Pérdida	Operación_y_productividad	El impacto será alto cuando las operaciones y productividad del TI no satisfagan los requerimientos y aspectos institucionales o haya demasiadas inconformidades	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Pérdida	Financiera	El impacto será alto cuando los costos operativos anuales sean mayores del 10% (por ejemplo, añadir tiempos para la recuperación de archivos, agregar software para disuadir de nuevas intrusiones)	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Pérdida	Seguridad_de_la_Información	El impacto es alto cuando sea ha suspendido por completo y por algunos días la disponibilidad en interrupciones del servicio debido a cortes de energía, fallos de hardware y actualizaciones del sistema y que haya ataques en la denegación del servicio	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Pérdida	Reputación_confianza_del_cliente	El impacto será medio cuando la reducción o advertencia de la calificación o acreditación de organizaciones que autoricen caídas de 2 a 5% en los clientes debido a la pérdida de confianza	M
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Interrupción	Activos_de_Información	El impacto será alto cuando la pérdida de un activo de información sea indispensable en las operaciones diarias	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Interrupción	Operación_y_productividad	El impacto será medio cuando las operaciones y productividad del TI den una atención ineficiente o retraso en la atención a usuarios de la institución o procesos de continuidad del negocio	M
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	Interno	accidental	Interrupción	Financiera	El impacto será bajo cuando sea de menos del 2% en los costos de operación del CETEIQ (por ejemplo, una semana de prórroga por cuatro miembros del personal para documentar los cambios en los planes de tratamiento, o compra de activos no representativos)	B
	CABLEADO	Actores_humanos_con_acceso_a_la_red					El impacto es medio cuando la suspensión del servicio ha sido un día laboral por interrupciones del servicio debido a cortes de energía, fallos de	

Plantilla 35: Plantilla de Resultado de identificación del impacto sobre activos críticos[70]

[70] Fuente: La Autora

3.2.3.2 Etapa 2: Determinación de la probabilidad de incidentes

3.2.3.2.1 Actividad 1: Valoración la probabilidad de incidentes

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- Resultados de la identificación de amenazas: *Fase2, E2, A1, Plantilla 3.9: Resultado de identificación de las amenazas sobre activos críticos.*
- Antecedentes: incidentes en la organización.

  El jefe del CETEIQ, solicito un informe al Ing. Daniel Segovia Administrador de la red naval de datos de las Fuerza Naval a realizar un informe de los incidentes que ocurren en el departamento de infraestructura el cual realizo un informe detallado de los antecedentes. *Ver Anexo 4, INCIDENTES DETECTADOS.pdf*).
- Resultados de la identificación y valoración de vulnerabilidades: *Fase2, E4, A2, Plantilla 3.12: Plantilla de la valoración de vulnerabilidades.*

Criterio de Salida

- Tabla de valoración de Degradación que causan las amenazas. *Ver Capitulo 2, Fase 3, E2, A1, Tabla 2.15.*

  Se tomo las dos matrices para valorar las amenazas que es la de degradación del valor del activo donde se tomo el valor por dimensión de seguridad de cada activo y la frecuencia de probabilidad de ocurrencia de la amenaza de cada activo.
- Plantilla de identificación de amenazas agregando la valoración de las mismas por cada activo.

  Se realizo la valoración de las amenazas, tomando en cuenta las dos matrices. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja VALORACION AMENAZAS.*

Se determino la calificación de la probabilidad de ocurrencia de cada amenaza y el valor de % de degradación que tiene cada amenaza por dimensión de seguridad.

RESULTADO DE VALORACION DE INCIDENTES																
No.	Activo	Acceso	Actor	Motivo	Resultado	Descripcion de la amenaza	Descripcion de la vulnerabilidad	Valoracion de la vulnerabilidad	Probabilidad ocurrencia de la amenaza	Valor probabilidad ocurrencia de la amenaza	DEGRADACION DE DIMENSIONES DE SEGURIDAD				
											C	A	I	D	T
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Formas de compartir las unidades de red.	Unión de cables deficientes/ conexiones	A	M	50			50%		
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Pérdida	Conexiones a Internet	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	A	B	10				75%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Interrupción	Configuración de servidores de seguridad	Monitoreo insuficiente de medidas de seguridad por la infraestructura	A	M	50				75%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Modificacion	Formas de compartir las unidades de red.	Punto de acceso no protegido	M	M	50			50%		
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión	Falta de politicas, normas y procedimientos	M	MB	5				100%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	deliberada	Interrupción	Configuración de servidores de seguridad	Monitoreo insuficiente de medidas de seguridad por la infraestructura	M	A	70				100%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	externo	accidental	Interrupción	Conexiones a Internet	Comunicaciones móviles	B	B	10				75%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	externo	deliberada	Pérdida	Perdida de equipos por robo, ataque destructivo, ocupación enemiga, indisponibilidad de personal, extorsión	Entrenamiento insuficiente en seguridad	A	B	10				100%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_fisico	interno	accidental	Modificacion	Manejo de periféricos y dispositivos especiales	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	M	B	10			75%		
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_fisico	interno	accidental	Pérdida	Explosiones, derrumbes, contaminación química, sobrecarga eléctrica	Monitoreo insuficiente de medidas de seguridad por el medio ambiente	M	MB	5				100%	
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_fisico	interno	accidental	Interrupción	Errores de administrador no intencionadas en el uso para responsabilidad de instalación y operación	Entrenamiento insuficiente en seguridad	A	B	10				75%	
		Actores_humanos_con_acceso_fisico				Control y monitoreo sobre accesos no solo en áreas donde									

Plantilla 36: Resultado de la valoración de identificación y valoración de las amenazas sobre activos críticos[71]

[71] Fuente: La Autora

Para una visualización a detalle y consultas por probabilidad de ocurrencia de la amenaza de cada activo se ha realizado tablas dinámicas con filtros y gráficos de barra para obtener los datos, *véase Herramienta Gestión de riesgos y Seguridad de información.xls, hoja TBL DINAMICA VALORACION AM (2):* en el eje de la y representa cuantas amenazas están valoradas, y el eje de las x son los activos.

Acceso	Otros_problemas					
Cuenta de Valor probabilidad ocurrencia de la amenaza	**Rótulos de columna**					
Rótulos de fila	**A**	**B**	**M**	**MA**	**MB**	**Total general**
AREA DE INFRAESTRUCTURA		1	2		2	5
CABLEADO ESTRUCTURADO			2			2
COMPUTADOR		1		1		2
DISCO EXTERNO			1		1	2
EQUIPO CONTROL AUTOMATICO					2	2
PERSONAL	9	2	8	4	4	27
PLANTA ENERGIA ELECTRICA		1			2	3
SERVIDOR	1	6			4	11
SWITCH		3			7	10
UPS					6	6
VIRTUAL REPORTING SERVICES		1				1
Total general	**10**	**15**	**13**	**5**	**28**	**71**

Tabla 17: Tabla dinámica de valoración de las amenazas sobre activos críticos[72]

Con esta tabla dinámica se podrá ver cuántas amenazas detectadas por calificación y acceso del activo han tenido como resultado de la valoración igualmente el grafico descrito a continuación:

[72] Fuente: La Autora

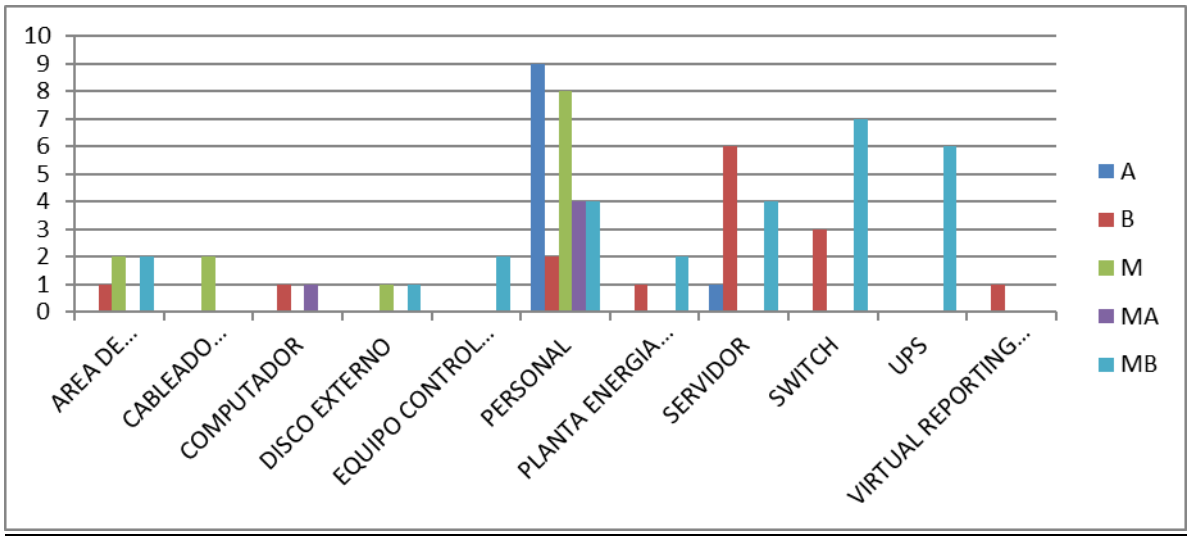

Tabla 18: Tabla dinámica de valoración de las amenazas sobre activos críticos[73]

3.2.3.3 Etapa 3: Estimación del estado del riesgo

3.2.3.3.1 Actividad 1: Estimación del riesgo

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Matriz para calcular el riesgo (*Véase FASE1, E2, A2, Tabla 2.4, Matriz para calcular el riesgo).*

  Se tomo la matriz para calcular el riesgo sobre el impacto y probabilidad de ocurrencia de la amenaza.

- ❑ Resultado de la determinación de la probabilidad de incidentes (*Véase Fase3, E2, A1, Plantilla 3.14: Resultado de la valoración de identificación y valoración de las amenazas sobre activos críticos*).

  Se tomo la plantilla de probabilidad de incidentes y se armó la matriz respectiva para aplicar el cálculo del riesgo.

[73] Fuente: La Autora

Criterios de Salida

❑ Plantilla de resultados de riesgos estimados. *Ver Fase 3, E2, A1, Plantilla 3.15: Plantilla de Resultado de la determinación de niveles de riesgo estimados.*

Se realizo la estimación de nivel de riesgo, tomando en cuenta la matriz para calcular el riesgo. *Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja CALCULO RIESGO.* A continuación se adjunta el resultado: se determino 326 riesgos con impactos de calificación alto riesgo, 724 riesgos con impactos de calificación en medio riesgo y 1410 riesgos con impactos de calificación de bajo riesgo.

RESULTADO DE RIESGOS ESTIMADOS										
No.	Activo	Acceso	Actor	Motivo	Resultado	Area de impacto	Descripcion del impacto	Valor del impacto	Probabilidad de ocurrencia de la amenaza	Nivel de Riesgo estimado
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Activos_de_información	El impacto será alto cuando la pérdida de un activo de información sea indispensable en las operaciones diarias	A	M	A
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Operación_y_productividad	El impacto será bajo cuando las operaciones y productividad del TI se desgasten y no afecten a la institución	B	M	B
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Financiera	El impacto será bajo cuando sea de menos del 2% en los costos de operación del CETEIQ (por ejemplo, una semana de prórroga por cuatro miembros del personal para documentar los cambios en los planes de tratamiento, o compra de activos no representativos)	B	M	B
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Seguridad_de_la_información	El impacto es medio cuando la integridad de los datos sea modificada siempre y cuando por personas sujetas a autorización, o es alterada por personas o procesos no autorizados	M	M	M
		Actores_humanos_con_acceso_a_la_red					El impacto será medio cuando exista violaciones Públicas de la Ley de Privacidad: (1) la divulgación al personal dentro de las instalaciones			

Plantilla 37: Plantilla de Resultado de niveles de riesgos estimados[74]

[74] Fuente: La Autora

3.2.4 FASE 4: TRATAMIENTO DE LOS RIESGOS

3.2.4.1. Etapa 1: Estrategias de Protección

3.2.4.1.1 Actividad 1: Crear estrategias de protección

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- Plantilla de resultados de valoración de las vulnerabilidades: *Fase2, E4, A2, Plantilla 3.12: Plantilla de la valoración de vulnerabilidades.*

  Se identificó en esta plantilla de resultados que 115 vulnerabilidades se encuentran con calificación A, 85 vulnerabilidades con calificación M y 292 vulnerabilidades con calificación B. Esto no quiere decir que se tomo solo las A y M; junto con el equipo de análisis se tomo la decisión que todas las vulnerabilidades detectadas en el área de redes deberán ser tratadas e implementar estrategias de protección.

- Controles ISO 27002-2005 (*Ver anexo5*). Con el equipo de análisis se verifico que hay 12 dominios los cuales se investigo la funcionalidad de sus controles para establecer las estrategias de protección.

Criterios de Salida

- Plantilla de resultado de las estrategias de protección.

  Se realizo la creación de las estrategias de protección junto con el equipo de análisis por lo que se definió lo siguiente: las estrategias que se encuentran en modo “se debe cambiar“; estas deberán ser mejoradas en el área del CETEIQ, las que se encuentran en modo esta actual estas estrategias se encuentran en el área y las que se encuentran vacías en estas no existen por lo que se van a crear en el departamento. Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja ESTRATEGIAS DE PROTECCION.

RESULTADO DE IDENTIFICAR LAS ESTRATEGIAS DE PROTECCION			
Dominio	Preguntas clave	Existe actualmente	Se debe cambiar
Politicas de seguridad	existen politicas de seguridad de la informacion que se encuentre debidamente documentada?		x
	las personas de TI, conoces claramente las politicas de seguridad implementadas?		x
	el manual de politicas de seguridad planteada abarca los requisitos del negocio ante leyes y regulaciones relevantes?	x	
	se deberia incluir mas controles de politicas de seguridad a las politicas actuales?		x
	periodicamente se revisan las politicas de seguridad impuestas por la COGMAR?		X
Aspectos organizativos de la seguridad de la informacion	existen compromisos del TI, donde existen responsabilidades para cada tarea dentro del area de infraestructura?		x
	hay coordinaciones adecuadas de actividades de seguridad de la informacion de altos mandos?		x
	estan difinidas las responsabilidades para la seguridad de la informacion?		x
	se podria mejorar la gestion de autorizaciones para nuevos recursos de tratamiento de la informacion?		x
	se revisan los acuerdos de requisitos de confidencialidad o no divulgacion y las necesidades de proteccion de la informacion?	x	
	existe periodicamente reuniones con altos medios sobre la seguridad de la informacion?	x	
	existe reuniones con proveedores ante la seguridad de la informacion?	x	
	se debe revisar las politicas para la gestion de seguridad de la informacion periodicamente?		x
	se debe revisar los objetivos de controles de seguridad impuestos por la COGMAR?		X

Plantilla 38: Plantilla de Resultado de las estrategias de protección[75]

3.2.4.2. Etapa 2: Plan de mitigación

3.2.4.2.1 Actividad 1: Crear planes de mitigación del riesgo

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

- ❑ Resultado de definir los criterios de aceptación del riesgo *((Ver Fase 1, E2, A5, Plantilla 3.6: Resultado de definición de aceptación del riesgo.)*

[75] Fuente: La Autora

Se reviso el resultado de la determinación de los niveles de riesgo y se definió que se aceptará el riesgo siempre y cuando los riesgos se encuentren con calificación baja y serán sujetos a comunicación y análisis de algún cambio que se presenten. En cambio los riesgos que tenga calificación alta y media no serán aceptados por lo que se procederá a mitigarlos siempre y cuando cumpla con los criterios de aceptación

- ❑ Resultado de la determinación de niveles de riegos estimados. (*Ver Fase 3*, *E3, A1, Plantilla 3.15: Plantilla de Resultado de la determinación de niveles de riesgo estimados*).

  El resultado de esta plantilla se determino los riesgos altos, medios y bajos. Se determinó 326 riesgos con impactos de calificación alto riesgo, 724 riesgos con impactos de calificación en medio riesgo y 1410 riesgos con impactos de calificación de bajo riesgo

- ❑ Resultado de identificar las estrategias de protección. *Ver Fase 4, E1, A1, Plantilla 3.16: Plantilla de Resultado de las estrategias de protección.*) En este resultado se lista todos los controles dispuestos por la norma ISO 27002:2005; las mismas que permitirán definir los planes de mitigación de los riesgos

Criterios de Salida

- ❑ Plantilla del resultado del tratamiento del riesgo.

  Se realizó el plan de mitigación de los riesgos con calificación alta y media por lo que con calificación baja se procedió a ponerles como aceptados. El equipo de análisis se guió en la plantilla de criterios de aceptación del riesgo. *(Ver Fase 1, E2, A5, Plantilla 3.6: Resultado de Definición de aceptación del riesgo).* Tanto los riesgos altos como medios se procedió a la mitigación del riesgo aplicando la mitigación que describe en la fase. En conclusión se llegó con el equipo de análisis que hay un activo críticos en las que se mitigo con evitar el riesgo al activo de área de infraestructura por lo que se encuentra expuesto en una área con vulnerabilidades del medio ambiente como es inundaciones y los valores de

impacto son altos, por lo que se definió que el data center del CETEIQ se recomienda estar en el segundo piso de la Fuerza Naval con todas las seguridades posibles. Con el resto de activos se procedió a reducir el riesgo. Véase Herramienta Gestión de Riesgos y Seguridad de información.xls, hoja TRATAMIENTO DEL RIESGO.

PLANTILLA DE RESULTADO DEL TRATAMIENTO DEL RIESGO														
No.	Activo	Acceso	Actor	Motivo	Resultado	Descripcion de la amenaza	Descripcion de la vulnerabilidad	Area de impacto	Descripcion del impacto	Valor del impacto	Probabilidad de ocurrencia de la amenaza	Nivel de Riesgo estimado	Tratamiento del Riesgo	Plan de mitigacion
75	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion	Formas de compartir las unidades de red.	Unión de cables deficientes/ conexiones	Activos_de_información	El impacto será alto cuando la pérdida de un activo de información sea indispensable en las operaciones diarias	A	M	A	REDUCIR	• proteccion de suministros de energia contra posible danios o interoepciones
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion			Operación_y_productividad	El impacto será bajo cuando las operaciones y productividad del TI se desgasten y no afecten a la institución	B	M	B	ACEPTAR	
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion			Financiera	El impacto será bajo cuando sea de menos del 2% en los costos de operación del CETEIQ (por ejemplo, una semana de prórroga por cuatro miembros del personal para documentar los cambios en los planes de tratamiento, o compra de activos no representativos)	B	M	B	ACEPTAR	
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion			Seguridad_de_la_información	El impacto es medio cuando la integridad de los datos sea modificada siempre y cuando por personas sujetas a autorización, o es alterada por personas o procesos no autorizados	M	M	M	REDUCIR	• Mantenimiento adecuado para garantizar su continuidad e integridad • Monitoreo periodico del entorno fisico
	CABLEADO ESTRUCTURADO	Actores_humanos_con_acceso_a_la_red	interno	accidental	Modificacion			Reputación_confianza_del_cliente	El impacto será medio cuando exista violaciones Públicas de la Ley de Privacidad: (1) la divulgación al personal dentro de las instalaciones sin la necesidad de saber, (2) cualquier persona que viola la Ley de Privacidad y revela información confidencial	M	M	M	REDUCIR	
		Actores_humanos_con_acceso_a_la_red												•Monitorear costos y volumenes de incidentes en la seguridad de la informacion • Corregir los eventos que pueden causar

Plantilla 39: Plantilla de Resultado del tratamiento del riesgo [76]

[76] Fuente: La Autora

3.2.4.2.2 Actividad 2: Crear lista de acciones

En esta actividad se procede a obtener los criterios de entrada que solicita este proceso como es:

Criterios de Entrada

❑Plantilla de Resultado de la determinación de niveles de riegos estimados *(Ver Fase 3, E3, A1, Plantilla 3.15: Plantilla de Resultado de la determinación de niveles de riesgo estimados.)*

Criterios de Salida

❑Plantilla de lista de acciones. (*Ver Plantilla 3.18 de esta actividad*).

Se realizó la lista de acciones por cada responsable del área del CETEIQ con tiempos estimados; todos los formatos y documentación que se generen serán revisados por la Jefatura del CETEIQ y aprobado por el mismo. Decidieron con el equipo de análisis que los puntos descritos se lo harán uno por uno con sus tiempos estimados. A continuación se detalla el resultado de la lista de acciones a ejecutarse por el plan de mitigación que se realizó:

Resultado de lista de acciones			
No.	**Acción**	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
1	Realizar formatos de documentación para registrar el control de acceso a los técnicos del CETEIQ cuando accedan a los servidores del data center	**Fecha de finalización**	Tiempo de duración 3 días
		Medidas de gestiones necesarias	Ninguna
2	Realizar desarrollos para que los aplicativos web tengan tablas de auditoria de accesos a los usuarios a las páginas web por hora, fecha y tipo	**Responsable**	Ingenieros Del área de desarrollo (5 personas técnicas que integran el área cada uno responsable de sus aplicaciones web.)

	de transacción a realizarse.	**Fecha de finalización**	30 días de duración
		Medidas de gestiones necesarias	El coordinador tendrá que crear sus cronogramas de trabajo por aplicativo y responsable asignado
3	Emitir reportes de registros de accesos de usuarios por fechas a los servidores del data center	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
		Fecha de finalización	Dos días
		Medidas de gestiones necesarias	Ninguna
4	Capacitar tanto al administrador como técnicos del área CETEIQ sobre políticas y procedimientos que dispone la COGMAR	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	Duración 2 meses
		Medidas de gestiones necesarias	Analizar punto a punto las políticas impuestas por la COGMAR
5	Capacitar tanto al administrador como técnicos del área CETEIQ sobre el auge en seguridad de la información	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	Duración 2 meses
		Medidas de gestiones necesarias	Contratar cursos externos para cada técnico
6	Realizar documento y plan de continuidad de gestión de la TI	**Responsable**	Jefe del CETEIQ y Administrador de red
		Fecha de finalización	3 meses
		Medidas de gestiones necesarias	Tomar referencias de la documentación de las políticas dispuestas por la COGMAR
7	Instalar herramientas para control y monitores de procedimientos y procesamiento de datos a los servidores del CETEIQ	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
		Fecha de finalización	2 semanas
		Medidas de gestiones necesarias	Los paquetes podrán ser de software libre ya que como es una

			institución pública están ligados a contratar herramientas libres
8	Tener control y documentar los accesos de conexiones tanto VPN como móviles a usuarios externos a la institución.	**Responsable**	Marinero Pedro Jumbo (Asistente Técnico)
		Fecha de finalización	3 días para tener el formato y aprobado del documento a registrar
		Medidas de gestiones necesarias	Este control será semanal
9	Revisar las políticas de seguridad de la información impuestas por la COGMAR e incluir políticas de alcance	**Responsable**	Jefe del CETEIQ y Administrador de Red
		Fecha de finalización	1 mes
		Medidas de gestiones necesarias	Ninguna
10	Establecer reuniones semanales con los técnicos del CETEIQ sobre las políticas que generen en el punto 9	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	Una vez por semana
		Medidas de gestiones necesarias	Es de vital importancia la comunicación entre el Jefe del CETEIQ y sus subordinación de las políticas de seguridad de la información
11	Control de ingreso y salida del personal de limpieza del CETEIQ	**Responsable**	Marinero Belen Armas (Asistente Técnico)
		Fecha de finalización	1 vez por semana
		Medidas de gestiones necesarias	
12	Documentar procesos de gestión de cambios	**Responsable**	Ing. Patricio Espinoza (Coordinador de aplicaciones)
		Fecha de finalización	1 mes
		Medidas de gestiones necesarias	Establecer procesos adecuados para el área de desarrollo de aplicaciones

13	Establecer ambientes separados tanto servidores para aplicación como para servidores de BDD	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
		Fecha de finalización	1 semana
		Medidas de gestiones necesarias	Coordinar con el Jefe del CETEIQ para analizar y estructurar servidores que estén aptos para una mejor estructura de aplicaciones y BDD
14	Proveer de una mejor gestión de creación de contraseñas guiarse por las políticas impuestas por COGMAR	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
		Fecha de finalización	2 semanas
		Medidas de gestiones necesarias	Coordinar con el Jefe de CETEIQ el establecimiento de contraseñas tanto para accesos a BDD, aplicaciones web, y servidores del data center
15	Tener un monitoreo de control de activos de información cuando salgan de las instalaciones del CETEIQ	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
		Fecha de finalización	A demanda
		Medidas de gestiones necesarias	Monitoreas y tener un registro de las personas que se les presta el activo y duración de entrega con firma de aceptación de responsabilidades
16	Tener monitorizada la red de datos de la fuerza naval	**Responsable**	Ing. Daniel Segovia (Administrador de la red)
		Fecha de finalización	Semanalmente
		Medidas de gestiones necesarias	El administrador de red emitirá reportes de la monitorización de la red de la fuerza naval que será verificada por el Jefe del CETEIQ

17	Capacitar al administrador de red sobre mantenimiento y configuraciones de servidores	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	1 semana
		Medidas de gestiones necesarias	Capacitarle al administrador de red junto con sus asistentes para un mejor mantenimiento y control de servidores
18	Comunicar a los usuarios de los aplicativos sobre el buen manejo de contraseñas impuestas	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	Una vez por semana
		Medidas de gestiones necesarias	Comunicar la responsabilidad que tiene cada usuario con sus contraseñas y el acceso a los aplicativos web implementadas en la fuerza naval
19	Realizar pruebas de versionamientos de aplicaciones web tanto técnico como usuario final y documentar	**Responsable**	Ing. De desarrollo del área del CETEIQ
		Fecha de finalización	Siempre que haya nuevos versionamientos
		Medidas de gestiones necesarias	El desarrollador deberá documentar los cambios realizados y a la vez registrar las pruebas tanto del mismo como del usuario con firmas de aceptación.
20	Definir los roles del personal del CETEIQ con sus funciones y responsabilidades	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	1 semana
		Medidas de gestiones necesarias	El jefe del área tendrá que definir correctamente las responsabilidades y personas que serán back up de los roles que se

			especifiquen puntualmente por cada uno
21	Registrar el control de back ups que se realicen en los servidores	**Responsable**	Ing. Jorge Maila (Administrador de BDD)
		Fecha de finalización	Diariamente
		Medidas de gestiones necesarias	Se documentara el proceso de copias de respaldo de los servidores junto con la aprobación del Jefe del Área
22	Realizar actas de compromiso al personal de TI para con la seguridad de la información	**Responsable**	Capitán Ricardo Uquillas (Jefe del CETEIQ)
		Fecha de finalización	1 semana
		Medidas de gestiones necesarias	Este punto se lo hará siempre y cuando ya hayan tenido todo el personal capacitaciones sobre la seguridad de la información y conjuntamente con el administrador de la red y el Jefe de área establecerán estas actas
23	Realizar registros de logs del administrador y operario de la información	**Responsable**	Ing. Daniel Segovia (Administrador de la red) Ing. Jorge Maila (Administrador de BDD)
		Fecha de finalización	Semanalmente
		Medidas de gestiones necesarias	Estas dos personas emitirán semanalmente un documento de registro de logs de los servidores del data center con la aprobación del Jefe del CETEIQ
24	Mantener planes de recuperación de desastres y del medio ambiente	**Responsable**	Ing. Daniel Segovia (Administrador de la red)

		Fecha de finalización	Semanalmente
		Medidas de gestiones necesarias	El administrador de red realizara planes de recuperación de desastres y analizará conjuntamente con el Jefe del CETEIQ las vulnerabilidades que se encuentra en el área de infraestructura
Observaciones: todos los puntos descritos en este documento, se realizó con la ayuda del equipo de análisis el mismo que se designó que punto por punto se lo realizará. Todas las listas de acciones tomaran un tiempo de largo plazo para mejorar la estructura y procedimientos de control de los riesgos que se especificaron en el tratamiento con sus planes de mitigación. Todos estas acciones tendrán documentación con firmas de aceptación esto es para tener un mejor control y coordinación con el personal del CETEIQ.		**Realizado Por**	Equipo de Análisis
Fecha: 18-10-2014		**Aprobado por**	Jefe del CETEIQ

Plantilla 40: Plantilla lista de acciones[77]

[77] Fuente: OCTAVE

3.2.5 FASE 5: COMUNICACIÓN

3.2.5.1. Etapa 1: Comunicar el Riesgo

El equipo de análisis reviso la información que se evaluó y analizó por lo que se procedió a comunicar y a detallar la gestión de riesgos del CETEIQ. Se tomó en cuenta que la comunicación será continua en la implementación de esta propuesta de gestión de riesgos a los altos mandos de la fuerza naval.

A continuación se detalla el informe final que se generó para comunicar el riesgo al Jefe del CETEIQ:

FUERZA NAVAL
CENTRO DE TECNOLOGIAS DE LA INFORMACION QUITO
- o -

Quito, 23 de octubre del 2013

Asunto: Informe Final de resultados de la gestión de riesgos y seguridad de la información.

Para: Capitán de Corbeta Ricardo Uquillas Soto

Dignase Señor Capitán de Corbeta Ricardo Uquillas Soto, Jefe del Centro de tecnologías de la información Quito; encontrar en este informe los resultados de la evaluación de riesgos y seguridad. Donde detalla el análisis de la situación actual de la institución, la evaluación de las amenazas criticas, activos y vulnerabilidades que

propone esta metodología de gestión de riesgos y la que se ha realizado con ayuda conjunta con el equipo de análisis, en la que se ha asumido la responsabilidad de cada uno que lo conforma y se ha producido una estrategia de protección y planes de mitigación basados exclusivamente en los riesgos de seguridad de la institución.

A continuación se presenta los resultados obtenidos:

SITUACION ACTUAL DE LA INSTITUCION:

A continuación se describe las debilidades y amenazas encontradas en el departamento del CETEIQ.

DEBILIDADES	AMENAZAS
✓ No está definida en su totalidad ni se aplica un análisis y gestión de riesgos para la seguridad de la información ✓ Falta de controles de seguridad de la información (Existen políticas pero no implementadas en su totalidad) ✓ Falta de cultura en seguridad de la información por parte de los usuarios de la red ✓ Falta de control de la información interna (Secreta, Confidencial, Uso Interno, Público, etc.). ✓ No existe auditoría y control de los registros de Seguridad ✓ Falta de metodologías estándar para una mejor Gestión de Riesgos informáticos ✓ Poco uso de herramientas en línea que	✓ Crecimiento del hacking y ataques informáticos que vulneran la seguridad ✓ Alto costos de equipos y mantenimiento de tecnologías de uso militar ✓ Acelerado desarrollo tecnológico ✓ Des actualización del personal informático ✓ Perdida de información crítica institucional ✓ Existencia de herramientas modernas y agiles para una mejor gestión informática

permita el control y evaluación de amenazas y riesgos informáticos ✓ No existen sistemas implementados para el cifrado de archivos ✓ Falta de protección de documentos o mensajes mediante permisos de acceso ✓ Los cambios en los sistemas de procesamiento de información e instalaciones no son controlados ✓ No hay un proceso de gestión para las configuraciones y los cambios ✓ No existe un modelo para asignar niveles de importancia a los componentes del entorno informático ✓ No mantiene planes de recuperación ante desastres y de reanudación de negocio	

Junto con el equipo de análisis de la gestión de riegos y apoyándose en estos detalles se describió los activos principales y primordiales del área de infraestructura con un total de 86 activos los cuales fueron calificados y a continuación se obtuvo los siguientes resultados:

Se encontraron que los activos más críticos del área de infraestructura fueron un total de 9 activos los cuales fueron calificados tanto como su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tipo de Activo	Nombre del Activo	Funciones principales del activo

Red	CABLEADO ESTRUCTURADO	este cableado tiene como 10 anos instalado en el edificio
Sitio	AREA DE INFRAESTRUCTURA	zonas de seguridad de todos los servidores y rack
Hardware	SERVIDOR	servidor que contiene el aplicativo SIGEIN (sistema de gestión institucional) de la armada e instalado una virtual de reportería del aplicativo de activos fijos, también se encuentra instalado el aplicativo de activos fijos y bienes no depreciables de la armada
Software	APLICATIVO SIGEIN	esta aplicación es una web que permite a los usuarios de la armada procesar información presupuestaria y compra de bienes y activos fijos
Software	APLICATIVO ICRON	esta aplicación es una web que permite la administración de todos los activos fijos y bienes no depreciables de la armada con el registro histórico de las personas custodias de cada uno de los bienes
Hardware	EQUIPO CONTROL AUTOMATICO	equipamiento que contiene todo el sistema de cámaras que se encuentran ubicadas dentro del centro de información de datos de la armada
Hardware	EQUIPO CONTROL AUTOMATICO	equipamiento que contiene todo el sistema de puertas para acceder al departamento de infraestructura
Personal	PERSONAL	sus funciones son mantener la red naval operativa y red de datos en mantenimiento, soporte de infraestructura
Personal	PERSONAL	oficial militar que toma decisiones para compra para equipos, proyectos en funcionamiento, administración del presupuesto del área de tecnologías y jefe de todas las divisiones del CETE IQ

Se encontraron activos con calificación alta de criticidad que fueron un total de 20 activos los cuales fueron calificados tanto como su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tipo de Activo	Nombre del Activo	Funciones principales del activo
Hardware	SERVIDOR	da servicio de DNS a toda la marina es el back up del primario
Hardware	SERVIDOR	es el servidor primario contiene el DNS controlador de dominio de Quito

Personal	PERSONAL	sus funciones son el realizar back ups de la BDD, administrar todos los procesos de las bases de información de la marina
Personal	PERSONAL	7 desarrolladores que se encargan de los aplicativos web que se encuentran instalados en los servidores de pruebas y de producción
Hardware	SERVIDOR	servidor de pruebas para aplicaciones web que se desarrollen en el CETEIQ, y base de datos
Hardware	SERVIDOR	Se encuentra el antivirus de la institución. No se encuentra respaldos de este servidor
Hardware	SERVIDOR	se encuentra el aplicativo Balance score card, y procesos de la marina y el reparto que necesita esta información es ESMAAR Escuela de servicios marinos
Software	APLICATIVO BSC Y PROCESOS INTERNOS	este aplicativo permite visualizar cuadros de mando integral y procesos para el ESMAAR
Hardware	UPS	provee de energía eléctrica al blade donde se encuentra el dominio de la fuerza naval y el DNS primario de Quito de toda la marina
Hardware	SERVIDOR	servidor que proporciona internet a todos los repartos de la fuerza naval
Hardware	SERVIDOR	servidor que contiene un portal web para servicio de información de la Dirección General de Intereses Marítimos
Software	PORTAL INFORMATIVO DIGEIM	este portal permite visualizar información relevante de la Dirección General de Intereses Marítimos
Hardware	SWITCH	proporciona conexión de red al 3er y 4to piso hace vagón de fibra
Hardware	SWITCH	proporciona conexión de red a servidores y red informática
Hardware	SWITCH	proporciona conexión de red a la oficina de la comandancia general de marina donde está la secretaria y el almirante
Hardware	DISCO EXTERNO	es de 2 teras, se encuentra información respaldada del ESMAAR, información de drivers, impresoras, laptos, pc etc.

Hardware	SUPRESOR	equipo que distribuye luz a la comandancia de la marina equipo nuevo
Hardware	COMPUTADOR	computador de trabajo del administrador BDD
Personal	PERSONAL	sus funciones son administrar y mantener el anti virus de la marina
Hardware	PLANTA ENERGIA ELECTRICA	proveer energía eléctrica cuando haya corte de luz

Se encontraron activos con calificación media que fueron un total de 16 activos los cuales fueron calificados tanto como su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tipo de Activo	Nombre del Activo	Funciones principales del activo
Hardware	UPS	proporciona energía eléctrica a los racks del CETEIQ, estos funciona como respaldo
Hardware	SWITCH	proporciona conexión de red al departamento de operaciones conecta la administración central telefónica del Estado Mayor no hay otro respaldo
Hardware	SWITCH	proporciona conectividad a la red informática del CETEIQ
Hardware	UPS	alimenta el rack de comunicaciones
Hardware	DISCO EXTERNO	disco duro para respaldos de back up de BDD
Hardware	UPS	Abastece al CETEIQ y sala de servidores de energía eléctrica y dispositivos eléctrico
Hardware	SWITCH	proporciona conexión de red a la red administrativa
Hardware	SWITCH	proporciona conexión de red a ESNAQI Estación naval de quito planta alta
Hardware	UPS	provee energía eléctrica al 1er y 2do piso de la comandancia general de la marina
Hardware	UPS	provee energía eléctrica a los blades de IBM
Hardware	SWITCH	proporciona conexión de red a la planta alta de ESNAQI a usuario comandantes y capitanes

Hardware	VIRTUAL REPORTING SERVICES	servicio de reportes que tiene la armada para visualización de activos fijos y bienes no depreciables con sus custodios responsables de la armada
Hardware	SWITCH	proporciona conexión de red al tercer y cuarto piso de la comandancia
Hardware	SWITCH	proporciona conexión de red a la Dirección General de Finanzas DIGFIN, entidad que maneja las finanzas a nivel nacional
Personal	PERSONAL	sus funciones son ser asistente del administrador de red
Personal	PERSONAL	sus funciones son ser asistente en mantenimiento y soporte a usuarios

El resto de activos fueron calificados bajas ya que no representan amenazas y vulnerabilidades en el área de infraestructura. A los activos críticos, altos y medios encontrados se realizó el análisis de amenazas, e impactos con sus vulnerabilidades detectadas.

ESTRATEGIAS DE PROTECCION ACTUAL:

Sobre las estrategias de protección actual de la institución se llego a la conclusión que algunas estrategias se encuentran impuestas pero otras no y tampoco se guían por las políticas de seguridad de información impuestas por la COGMAR

Los resultados analizados fueron:

- **Políticas de seguridad:** no se basan en las políticas actuales impuestas por la COGMAR; se recomienda guiarse de estas e incrementar de acuerdo al departamento del CETEIQ y realizar un mecanismo formal para cumplir con las políticas de seguridad, leyes y regulaciones impuestas.

- **Aspectos organizativos de la seguridad de la información:** no existe un compromiso de TI, ni responsabilidades específicamente asignadas a cada

empleado del CETEIQ. Se analizo también que debe haber una gestión de autorizaciones y coordinaciones adecuadas de actividades de la seguridad de la información.

- **Gestión de activos:** se analizo que existe una gestión de activos correctamente formada con sus responsables debidamente documentadas y con su registro histórico de los mismos.

- **Seguridad ligada a los recursos humanos:** se analizo que no existen compromisos o contratos con los empleados del CETEIQ que garanticen su compromiso con la seguridad de la información o que cumplan con las políticas plasmadas por la COGMAR.

- **Seguridad física y del entorno:** se determino que no existen controles adecuados para el acceso físico del área de infraestructura por lo que algunos activos de la información podrán tener amenazas y no hay un monitoreo y control de personal que accede a las instalaciones del CETEIQ.

- **Gestión de operaciones y comunicación:** no se coordinan los accesos al personal del CETEIQ o gestionar operaciones donde se controle la seguridad y se monitoree niveles de servicio de detección, prevención, y recuperación contra software malicioso; ni tampoco hay documentación de los sistemas contra accesos no autorizados.

- **Control de accesos:** no se establecen ni se documentan las políticas de accesos tanto a usuarios de aplicaciones como personal técnico del CETEIQ. No existe un mejoramiento de control de configuración tanto de acceso físico y lógico a los activos de información.

- **Adquisición y desarrollo de sistemas:** no existe un control de versionamientos de aplicaciones ni tampoco control de datos para pruebas y de producción ni tampoco control de respaldos de bases de datos de las aplicaciones. Se analizo

que existen algunas vulnerabilidades en las aplicaciones por lo que afectan el control de integridad de los datos.

- **Gestión de incidentes de la seguridad de la información:** no existe una gestión de incidentes en el que se pueda controlar la seguridad de la información con responsabilidades y procedimientos. Tampoco se comunica al personal del CETEIQ, sobre los eventos en la seguridad de la información.

- **Gestión de la continuidad del negocio:** no se identifica eventos de interrupciones en la institución, tampoco hay planes de continuidad del negocio ni tampoco se los prueba regularmente.

- **Cumplimiento:** no se garantiza en su totalidad la integridad de la información; no hay un control regulatorio donde los altos mandos aseguren que los procedimientos de seguridad de cada área tengan sus responsables o cumplan las políticas de seguridad.

Después de realizar la evaluación de la seguridad actual del CETEIQ se realizó un plan de mitigación con actividades que se describen a continuación:

- Realizar formatos de documentación para registrar el control de acceso a los técnicos del CETEIQ cuando accedan a los servidores del data center
- Realizar desarrollos para que los aplicativos web tengan tablas de auditoría de accesos a los usuarios a las páginas web por hora, fecha y tipo de transacción a realizarse.
- Emitir reportes de registros de accesos de usuarios por fechas a los servidores del data center
- Capacitar tanto al administrador como técnicos del área CETEIQ sobre políticas y procedimientos que dispone la COGMAR

- Capacitar tanto al administrador como técnicos del área CETEIQ sobre el auge en seguridad de la información
- Realizar documento y plan de continuidad de gestión de la TI
- Instalar herramientas para control y monitores de procedimientos y procesamiento de datos a los servidores del CETEIQ
- Tener control y documentar los accesos de conexiones tanto VPN como móviles a usuarios externos a la institución.
- Revisar las políticas de seguridad de la información impuestas por la COGMAR e incluir políticas de alcance
- Establecer reuniones semanales con los técnicos del CETEIQ sobre las políticas que se establezca
- Control de ingreso y salida del personal de limpieza del CETEIQ
- Documentar procesos de gestión de cambios
- Establecer ambientes separados tanto servidores para aplicación como para servidores de BDD
- Proveer de una mejor gestión de creación de contraseñas guiarse por las políticas impuestas por COGMAR
- Tener un monitoreo de control de activos de información cuando salgan de las instalaciones del CETEIQ
- Tener monitorizada la red de datos de la fuerza naval
- Capacitar al administrador de red sobre mantenimiento y configuraciones de servidores
- Comunicar a los usuarios de los aplicativos sobre el buen manejo de contraseñas impuestas
- Realizar pruebas de versionamientos de aplicaciones web tanto técnico como usuario final y documentar
- Definir los roles del personal del CETEIQ con sus funciones y responsabilidades
- Registrar el control de back ups que se realicen en los servidores
- Realizar actas de compromiso al personal de TI para con la seguridad de la información

- Realizar registros de logs del administrador y operario de la información
- Mantener planes de recuperación de desastres y del medio ambiente

Con todo lo detallado anteriormente, Señor Capitán reitero mis agradecimientos y atención sobre este análisis que me ha permitido realizar en el departamento del CETEIQ.

Atentamente,

ING. DIANA ESTEVEZ
ANALISTA DE SISTEMAS

Plantilla 41: Plantilla para comunicar el riesgo [78]

3.2.6 FASE 6: MONITOREO Y REVISIÓN

3.2.6.1. Etapa 1: Monitoreo y Revisión de los factores de riesgo

El equipo de análisis reviso la información para el monitoreo y revisión de los factores de riesgo y se encargo de verificar si hay activos nuevos en el área de infraestructura, alguna modificación que ocurrió durante la evaluación del análisis así como posibles vulnerabilidades encontradas como amenazas nuevas detectadas y se procedió a llenar la plantilla de ayuda; este monitoreo se lo realizará regularmente en el área de infraestructura para comunicar los riesgos posibles o nuevos que se encuentren en el área. Debido a que es la primera interacción con la aplicación de esta propuesta de gestión de riesgos y seguridad de la información y que la implementación se ha realizado sobre un proceso macro de la cadena de valor del CETEIQ, el equipo de análisis ha determinado que no se han encontrado cambios

[78] Fuente: OCTAVE

considerables en los factores de riesgo. Se recomienda tener una persona que coordine la seguridad de la información y monitoree a cada momento si hay factores de riesgo nuevos.

Resultado del monitoreo y revisión de los factores de riesgo				
Nuevos activos				
Activo	**Fecha**	**Observación**		
Ninguno	25-10-2013	No se han adquirido nuevos activos en el área de infraestructura		
Modificaciones realizadas a valores de activos				
Cambio	**Fecha**	**Observación**		
Ninguno	25-10-2013	Por el momento los activos valorados en la evaluación de la gestión de riesgos no ha sufrido cambios adicionales		
Nuevas amenazas				
Amenaza	**Fecha**	**Observación**		
Ninguna	25-10-2013	Se han detallado todas las amenazas oportunas en la evaluación de gestión de riesgos.		
Vulnerabilidades identificadas				
Vulnerabilidad	**Fecha**	**Observación**		
Ninguna	25-10-2013	Se ha detallada todas las vulnerabilidades oportunas en la evaluación de gestión de riesgos.		
Nivel de riesgo				
Riesgo	**Valoración del impacto**	**Valoración de la vulnerabilidad**	**Fecha**	**Observaciones**
Ninguna	Ninguna	Ninguna	25-10-2013	No hay factores de riesgos nuevos.
Incidentes de la seguridad de la información				

Incidente	Activos afectados	Fecha	Observación
Ninguna	Ninguna	25-10-2013	Se ha detallada todas las vulnerabilidades oportunas en la evaluación de gestión de riesgos.
Fecha	25-10-2013	**Realizado Por**	Equipo de análisis
		Aprobado Por	Jefe del CETEIQ

Plantilla 42: Plantilla de Resultado de monitoreo y revisión de los factores de riesgo[79]

3.2.6.2. Etapa 2: Monitoreo, revisión y mejora de la Gestión del riesgo

El equipo de análisis revisó la información para el monitoreo y mejora de la gestión del riesgo como es el contexto legal, contexto de competición, enfoques de la evaluación del riesgo, identificar los activos, los criterios de impacto, criterios de evaluación del riesgo, criterios de aceptación del riesgo y recursos necesarios, esto es con el objetivo de mejorar la gestión de riesgos de seguridad de la información por lo tanto, el equipo de análisis no ha registrado un cambio significativo o relevante en el monitoreo y revisión de la gestión de riesgos de seguridad de la información, debido que esta es la primera iteración sobre la implantación de esta propuesta de modelo de gestión de riesgos.

Este equipo de análisis no ha encontrado cambios de los contextos que afecten a la gestión de riesgos de seguridad, se llego un acuerdo que regularmente una persona encargada de la seguridad tendrá este monitoreo y efectuara reuniones previas para coordinar y determinar el mejoramiento de esta gestión de riesgos.

A continuación se detalla el resultado del monitoreo de esta etapa:

Resultado del monitoreo, revisión y mejoras de la gestión de riesgos
Contexto legal y ambiental

[79] Fuente: La Autora

Contexto	Fecha	Observación
Ninguno	28-10-2014	No se ha encontrado ningún cambio de contextos legales y ambientales.
Contexto de competición		
Contexto	**Fecha**	**Observación**
Ninguno	28-10-2014	No se ha encontrado ningún cambio de contexto de competición
Enfoque para la evaluación del Riesgo		
Enfoque	**Fecha**	**Observación**
Ninguno	28-10-2014	No se ha establecido ningún enfoque para la evaluación del riesgo. La aplicación del modelo es un plan piloto y con el tiempo si así lo requiera la institución se definirá algún enfoque adicional.
Caracterización de los activos		
Caracterización	**Fecha**	**Observación**
Ninguno	28-10-2014	La forma de identificar los activos está el equipo de análisis totalmente de acuerdo por lo que si hubiere algún contexto adicional se especificará
Criterios de impacto		
Criterio	**Fecha**	**Observación**
Ninguno	28-10-2014	Los criterios de impacto actualmente establecidos fueron cuando se aplicó este modelo y fueron abalizados por el equipo de análisis y aprobado por el Jefe del CETEIQ, si hubiere algún criterio que pueda ser incluido se comunicara al Jefe y al equipo de análisis.
Criterios evaluación del riesgo		
Criterio	**Fecha**	**Observación**
Ninguno	28-10-2014	Los criterios de evaluación del riesgo actualmente establecidos fueron cuando se aplicó este modelo y

		fueron abalizados por el equipo de análisis y aprobado por el Jefe del CETEIQ, si hubiere algún criterio que pueda ser incluido se comunicará al Jefe y al equipo de análisis	
Criterios de aceptación del riesgo			
Criterio	**Fecha**	**Observación**	
Ninguno	28-10-2014	Los criterios implantados al generar este modelo propuesto fueron conjuntamente realizados con el equipo de análisis y aprobado por el Jefe del CETEIQ, si hubiere criterios adicionales que faltare se comunicara al equipo de análisis para su comunicación.	
Recursos necesarios			
Recursos	**Fecha**	**Observación**	
Ninguno	28-10-2014	En la reunión con el equipo de análisis para realizar esta plantilla se definió que por el momento no se encuentran recursos adicionales si los hubieren serán comunicados al Jefe del CETEIQ	
Fecha	28-10-2014	**Realizado Por**	Equipo de Análisis
		Aprobado Por	Jefe del CETEIQ

Plantilla 43: Plantilla de Resultado de monitoreo, revisión y mejoramiento de la gestión de riesgo [80]

3.3. DISCUSIÓN DE LOS RESULTADOS

El estudio para el desarrollo de un modelo de gestión de riesgos y seguridad de la información propuesto, ha sido aplicado en un caso de estudio específico como es una institución militar la Fuerza Naval en el departamento de informática. Este

[80] Fuente: La Autora

estudio duro alrededor de un año por lo que cada uno de las fases como procesos y actividades que contiene el modelo se lo ha aplicado y se ha obtenido muchos resultados en donde se puede apreciar cuales son los activos más críticos del área de infraestructura de la institución como también cuáles son sus actuales amenazas y vulnerabilidades. A continuación se detalla las fases sus procesos y actividades y el porcentaje de finalización de cada una de ellas:

Fases, procesos y actividades	Objetivos	% de cumplimiento	Observaciones
FASE 1: CONTEXTO ORGANIZACIONAL Proceso 1: Alcance			
Actividad 1: Definición del Alcance	Obtención de los procesos estratégicos existentes de la institución, procesos agregados de valor y procesos habilitantes de apoyo que conforman la cadena de valor que se encuentran implementados en las instituciones militares. Identificar los miembros de cada área operativa dentro de área a definir. Considerar si tienen políticas de seguridad de la información en la organización	100	Los objetivos plasmados en esta actividad se completaron satisfactoriamente. Se definió el alcance para la aplicación de este modelo por lo que se realizó la gestión de riesgos solo al área de infraestructura del CETEIQ
Proceso 2: Contexto del Proceso de Gestión de Riesgos			
Actividad 1: Selección de miembros responsables	Determinar los miembros responsables de acuerdo al criterio de la directiva de la institución a comprometerse al desarrollo y mejoramiento de los procesos.	100	Los objetivos plasmados en esta actividad se completaron satisfactoriamente. En conjunto se asignaron todos los responsables que conformaron el equipo de análisis.
Actividad 2: Definir la metodología de Evaluación de Riesgos	Determinar escalas de valoración de probabilidad e impacto basándose en un enfoque cualitativo Determinar marcos de probabilidad e impacto basándose en un enfoque cualitativo Determinar el nivel de riesgo	100	Los objetivos plasmados en esta actividad se completaron satisfactoriamente. Se adoptó la metodología de evaluación de riesgos del modelo propuesto
Actividad 3: Definir los criterios de evaluación del riesgo	Definir criterios de evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la	100	Los objetivos plasmados en esta actividad se completaron satisfactoriamente. Todos los criterios se consideraron de

	organización. Permitir priorizar el riesgo teniendo en cuenta aspectos como: el valor estratégico del proceso de negocio, la criticidad de los activos, los requisitos legales y reglamentarios, importancia de la disponibilidad, confidencialidad e integridad de operaciones y del negocio y reputación de consecuencias negativas y percepciones de partes interesadas		acuerdo a la institución militar.
Actividad 4: Definir criterios de Impacto	Definir criterios de impacto del riesgo y especificarlos en términos del grado de daño.	100	Los objetivos en esta actividad se completaron. Todos los criterios se consideraron de acuerdo a la institución.
Actividad 5: Definir criterios de aceptación de riesgo	Desarrollar y especificar criterios de aceptación de riesgo que dependan con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.	100	Los objetivos plasmados en esta actividad se completaron satisfactoriamente. Con el equipo de análisis de decidió que para aceptar el riesgo serán los que tengan calificación baja previo a la aceptación y aprobación del Jefe del CETEIQ; los demás serán destinados a plan de mitigación.
FASE 2: IDENTIFICACIÓN DE LOS RIESGOS Proceso 1: Determinación de los Activos			
Actividad 1: Identificación de los Activos	Identificar los activos que componen el sistema dentro de una organización, determinando sus características, atributos y clasificación en los tipos determinados	100	Los objetivos en esta actividad se completaron con existo. Se identificaron 86 activos más importantes en el área de infraestructura
Actividad 2: Valoración de Activos	Identificar dimensiones que se va a utilizar y los criterios para valorar los activos Valorar el coste cualitativa para cada	100	Los objetivos en esta actividad se completaron con éxito por lo que se encontraron que los activos más críticos del área de infraestructura fueron un

	uno de los activos valorados		total de 9 activos, un total de 20 activos fueron de calificación alta, 16 activos con calificación media y el resto de activos tienen calificación baja.
Proceso 2: Determinación de las Amenazas			
Actividad 1: Identificación de las amenazas	Identificar las amenazas relevantes sobre cada activo	100	Los objetivos en esta actividad se completaron con éxito; se especificaron todas las amenazas por cada activo de información.
Proceso 3: Determinación de los controles de seguridad existentes			
Actividad 1: Identificación de los controles existentes	Identificar los controles existentes sobre las amenazas que se pretenden mitigar. Basándose en la norma ISO/IEC 27002:2005.	60	Los objetivos de esta actividad no se lo realizo por completo ya que no se tiene ningún control existente que se basen en la norma ISO; por lo que se especifico que no se implementa ninguno de estos
Proceso 4: Determinación de las vulnerabilidades			
Actividad 1: Identificación de las vulnerabilidades	Identificar las vulnerabilidades que pueden ser aprovechadas por una amenaza.	100	Los objetivos de esta actividad se realizaron por completo; se identificaron las vulnerabilidades por cada amenaza detectada.
Actividad 2: Valoración de las vulnerabilidades	Valorar las vulnerabilidades que pueden ser aprovechadas por una amenaza	100	El objetivo de esta actividad se realizo completamente se califico a cada vulnerabilidad detectada por calificación alta, media, baja
FASE 3: EVALUACIÓN DE LOS RIESGOS Proceso 1: Determinación del impacto			
Actividad 1: Identificación del impacto	Identificar y valorar el impacto que está sometido el activo por la materialización de una amenaza	100	El objetivo de esta actividad se cumplió con éxito; se determino cuales son los impactos por cada activo detectada y a la vez tuvo su calificación por alto, medio, bajo

Proceso 2: Determinación de la probabilidad de incidentes			
Actividad 1: Valoración la probabilidad de incidentes	Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo; y la facilidad con que las vulnerabilidades pueden ser explotadas Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.	100	Los objetivos de esta actividad se cumplieron con éxito; se determino la calificación de la probabilidad de incidentes en MA, A, M y B. Por lo que se genero tablas dinámicas para tener a detalle sobre la probabilidad de ocurrencia de una amenaza por activo de información.
Proceso 3: Estimación del estado del riesgo			
Actividad 1: Estimación del riesgo	Estimar el riesgo al que están sometidos los activos. Para cada perfil de amenaza valorar el riesgo estimado en base a analizarlo con el criterio de evaluación del riesgo	100	Los objetivos de esta actividad se cumplieron con éxito; se determino los riesgos con calificación alta, media y baja de cada uno de los activos. Se determino 326 riesgos con impactos de calificación alto riesgo, 724 riesgos con impactos de calificación en medio riesgo y 1410 riesgos con impactos de calificación de bajo riesgo.
FASE 4: TRATAMIENTO DE LOS RIESGOS Proceso 1: Estrategias de Protección			
Actividad 1: Crear estrategias de protección	Identificar y crear estrategias de protección considerando los dominios de la norma ISO 27002:2005 Realizar preguntas claves por cada dominio y estableciendo estrategias actuales; revisando las vulnerabilidades de la organización.	100	Los objetivos de esta actividad se lo cumplieron satisfactoriamente; por lo que se realizo por cada control de dominio preguntas clave para saber si no existe o se debe cambiar.
Proceso 2: Plan de mitigación			
Actividad 1: Crear planes de mitigación del riesgo	Mitigar el riesgo o aceparlo asociado del activo más crítico estableciendo controles	100	El objetivo de esta actividad se lo cumplió satisfactoriamente; En conclusión se llegó con el equipo de análisis que hay un

			activo críticos en las que se mitigo con evitar el riesgo y es el activo de área de infraestructura por lo que se encuentra expuesto en un sitio con vulnerabilidades del medio ambiente como es inundaciones y los valores de impacto son altos, por lo que se definió que el data center del CETEIQ se recomienda estar en el segundo piso de la Fuerza Naval con todas las seguridades posibles. Con el resto se redujo el riesgo.
Actividad 2: Crear lista de acciones	Crear lista de acciones que la organización lo realizará a corto o largo plazo para mitigar las amenazas de los activos críticos con responsables de cada acción	100	El objetivo de esta actividad se lo cumplió satisfactoriamente; Se realizó la lista de acciones por cada responsable del área del CETEIQ con tiempos estimados; todos los formatos y documentación que se generen serán revisados por la Jefatura del CETEIQ y aprobado por el mismo.
FASE 5: COMUNICACIÓN Proceso 1: Comunicar el Riesgo	En este proceso se encarga de que el equipo de comité de seguridad o el equipo de análisis comparta la información obtenida en las fases de la gestión del riesgo; a través de planes y coordinación entre quien toma decisiones y los interesados	100	Este proceso se cumplió satisfactoriamente por lo que el equipo de análisis reviso la información que se evaluó y analizó y se procedió a comunicar y a detallar la gestión de riesgos del CETEIQ. Se tomó en cuenta que la comunicación será continua en la implementación de esta propuesta de gestión de riesgos a los altos mandos de la fuerza naval; se genero un formato de informe que fue presentado al Jefe del CETEIQ.
FASE 6: MONITOREO Y REVISIÓN Proceso 1: Monitoreo y Revisión de los factores de riesgo	En este proceso se encarga de monitorear las amenazas, las vulnerabilidades, las probabilidades que	90	Este proceso se cumplió satisfactoriamente; equipo de análisis reviso la información para el monitoreo y

	pueden cambiar abruptamente sin ninguna indicación. Por ende es necesario el monitoreo constante para detectar estos cambios		revisión de los factores de riesgo y se encargo de verificar si hay activos nuevos en el área de infraestructura, alguna modificación que ocurrió durante la evaluación del análisis así como posibles vulnerabilidades encontradas como amenazas nuevas detectadas y se procedió a llenar la plantilla de ayuda; este monitoreo se lo realizará regularmente en el área de infraestructura para comunicar los riesgos posibles o nuevos que se encuentren en el área
Proceso 2: Monitoreo, revisión y mejora de la Gestión del riesgo	En este proceso se encarga de gestionar el riesgo en la seguridad de la información donde se deberá monitorear, revisar y mejorar continuamente según sea necesario y adecuado. El monitoreo y la revisión continuos son necesarios para garantizar que el contexto, el resultado de la evaluación del riesgo y el tratamiento del riesgo, así como los planes de gestión siguen siendo pertinentes y adecuados para las circunstancias	90	Este proceso se cumplió El equipo de análisis reviso la información para el monitoreo y mejora de la gestión del riesgo esto es con el objetivo de mejorar la gestión de riesgos de seguridad de la información por lo tanto el equipo de análisis no ha registrado un cambio significativo o relevante en el monitoreo y revisión de la gestión de riesgos de seguridad de la información
PROMEDIO DE APLICABILIDAD DEL MODELO		**97**	Se determina que un 97% alcanzo un mejoramiento en la aplicabilidad de la metodología alcanzando así en su desarrollo de planes y estrategias de seguridad en el área CETEIQ; así como también logrando tomar decisiones para mitigar el riesgo más de un 50% y

		obteniendo un mejor control y gestión de los mismos.

CAPITULO 4.

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Considerando las dos metodologías de gestión de riesgos, Magerit y Octave, se ha demostrado que se puede obtener una fusión de ellas, lo que sirve de base para el desarrollo de un nuevo modelo de gestión de riesgos y seguridad de la información, donde se logró la inclusión de los elementos importantes de cada una y se aproximo al problema de analizar los riesgos, saber cuan seguros o inseguros son los sistemas y llegar a mitigarlos.
- Se seleccionó la metodología Magerit, ya que sigue la terminología de la normativa ISO 31000; donde centra un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.
- Se seleccionó la metodología Octave, ya que permite a las organizaciones identificar, para los activos más importantes, construir planes de mitigación para hacer frente a los riesgos.
- Se determino que el área de infraestructura alcanzó un 97% de mejoramiento en su desarrollo de planes y estrategias de seguridad; por lo que ha permitido tomar decisiones para mitigar el riesgo en un 50%, obteniendo un mejor control y gestión de los mismos.
- Durante la aplicabilidad del modelo, el equipo de análisis junto al Jefe del CETEIQ tuvieron un gran proceso de aprendizaje y experiencia pero que al final se transformo en aplicar una metodología organizada y centrada, por lo que pudieron visualizar la realidad del área de tecnologías y tener una visión más de cuán importante y valioso es cada uno de los activos que conforman el área de infraestructura.
- Los criterios de probabilidad de ocurrencia de una amenaza, debe establecerse con la mayor cantidad de información, sin embargo y dado que la mayoría de los casos las organizaciones militares no cuentan con este tipo de información histórica, es necesario enfocarse en criterios

sustentados en experiencia de los participantes y es necesario que estos sean grandes conocedores de los procesos de negocio de la institución.

- La implementación del modelo propuesto se debe iniciar con la gestión de riesgos de seguridad de la información, y con la capacitación en las Normas ISO 27002:2005, puesto que el modelo propuesto se basa en esta norma para sus planes de estrategias y controles.
- El enfoque presentado en esta metodología, se puede aplicar en cualquier otra institución militar de similares características.

4.2. RECOMENDACIONES

- El CETEIQ debe constantemente revisar su plan de mitigación ya que nos encontramos en un mundo donde la tecnología avanza a pasos gigantescos, también las amenazas y riesgos crecen y deberán ser temas considerados para evitar problemas en el futuro.
- Se debe comunicar al personal CETEIQ el plan de mitigación así como también las medidas que se tomaran para el monitoreo.
- Se requiere que todos los técnicos que conforman el área de tecnologías Quito CETEIQ; se capacite en la temática de riesgos y seguridad de la información, adicionalmente es primordial que exista un compromiso y auspicio de los altos mandos que conforman los CETEINs de la Fuerza Naval para llevar a cabo este modelo a las demás áreas de tecnología que se encuentran distribuidos por el Ecuador.
- Todo el personal que conforma el CETEIQ deberá asistir a cursos de seguridad de la información para que todos tengan una visión general del tema y sepan cómo actuar ante una amenaza que presente el activo de información.
- Debido a que el área de infraestructura tiene una calificación altamente critica y puesto que se determinó evitar el riesgo, se recomienda que las misma sea transferida al segundo piso del edificio de la Fuerza Naval en donde no tendrá las amenazas del medio ambiente, entre ellas las inundaciones que últimamente le han afectado.

- Se debe dar más énfasis en el tratamiento del riesgo así como también planes de mitigación y lista de acciones que están asociados al cumplimiento de normativas legales.
- Revisar las políticas impuestas por la COGMAR e incluir más actividades que refuercen las posibles vulnerabilidades que aparezcan en el CETEIQ.

BIBLIOGRAFIA.

[1] C.C.FF.AA (Comando Conjunto de las Fuerzas Armadas), http://www.ccffaa.mil.ec (consultado enero 2013).

[2] Ejército Ecuatoriano, http://www.ejercitodelecuador.mil.ec , Visión (consultado enero 2013).

[3] Fuerza Naval, http://www.armada.mil.ec , Misión-Visión (consultado enero 2013).

[4] Fuerza Aérea, http://www. http://fuerzaaereaecuatoriana.mil.ec , Visión (consultado enero 2013).

[5] Estado Mayor de la Fuerza Naval, "Seguridad de la información", COGMAR-INF-002-2010-O; 12-Julio-2010, documento tipo Ordinario, Pag.1, http://directivas.armada.mil.ec

[6] Estado Mayor de la Fuerza Naval, "Seguridad de la información" , COGMAR-INF-002-2010-O; 12-Julio-2010, documento tipo Ordinario, ANEXO A, http://directivas.armada.mil.ec

[7] DIRTIC (Dirección de Tecnologías de la Información),http://www.dirtic.armada.mil.ec

[8] CETEIQ, "Manual de Organización del Centro de Tecnologías de la Información", documento tipo Ordinario.

[9] Fuerza Naval, PEDETIC "Programa de desarrollo de tecnologías de la información y comunicaciones", documento tipo Ordinario.

[10] Organización y transformación de los Sistemas de información en la empresa, Universidad Rey Juan Carlos, Primera Edición 2011, Pág. 285.

http://books.google.com.ec/books?id=2pqwKkqxxosC&printsec=frontcover&hl=es#v=onepage&q&f=false

[11] Ministerio de Hacienda y Administraciones Públicas, MAGERIT vs.3, Metodología de análisis y gestión de riesgos de los sistemas de información, Libro 1, Pág.7

http://administracionelectronica.gob.es/

[12] Estado Mayor de la Fuerza Naval**, "**Normar los Sistemas de Telecomunicaciones de Fuerzas Armadas y Uso del Espectro Electromagnético para la Defensa**",** COGMAR-TIC-002-2012-R**;** 7-Mayo-2012, documento tipo Reservado, Pag.5, http://directivas.armada.mil.ec

[13] Ministerio de Hacienda y Administraciones Públicas, MAGERIT vs.3, Metodología de análisis y gestión de riesgos de los sistemas de información, "Guía de técnicas", Libro 3, Pág.12

http://administracionelectronica.gob.es/

[14] Ministerio de Hacienda y Administraciones Públicas, MAGERIT vs.3, Metodología de análisis y gestión de riesgos de los sistemas de información, ”Método”, Libro 1, Pág.127

http://administracionelectronica.gob.es/

[15] Ministerio de Hacienda y Administraciones Públicas, MAGERIT vs.3, Metodología de análisis y gestión de riesgos de los sistemas de información, “Catálogo de elementos”, Libro 2, Pág.19

http://administracionelectronica.gob.es/

[16] Agencia Estatal de Meteorología, Análisis de Riesgos,

http://administracionelectronica.gob.es/recursos/pae_000005940.pdf

[17] Carnegie Mellon University, OCTAVE, Sept 17 2008 (consultado febrero 2013)

http://www.cert.org/octave/

[18] Carnegie Mellon University, OCTAVE, Catalog of Practices, Version 2.0.pdf,Octubre 2001, Pág. 9

http://www.cert.org/octave/

[19] ISO/IEC 27002:2005, Dominios y Objetivos de Control, ControlesISO27002-2005.pdf, Junio 2013.

http://www.iso27000.es/download/ControlesISO27002-2005.pdf

ANEXOS DIGITALES.

ANEXO 1

Procesos estratégicos, agregados de valor y habilitantes de apoyo

Dentro de este manual de organización se especifica la estructura organizacional del departamento CETEIQ, Ver documento adjunto: *ANEXO 1: Manual de Organización CETEIQ 2013.pdf*

ANEXO 2

Política de Seguridad de la información

En la Fuerza Naval se encuentra establecida una directiva general de seguridad de la información llamado *Ver documento adjunto: ANEXO 2: DIRECTIVA SEGURIDAD INFORMATICA 12Jul2010.pdf.* Este documento fue dispuesto por COGMAR (Comandancia General de Marina), es una política que debe seguirse en todos los repartos y unidades navales de la Fuerza Naval.

ANEXO 3

Riesgos y vulnerabilidades del CETEIQ

Dentro del CETEIQ, en lo que respecta a la administración de la red naval de datos e infraestructura informática se ha procedido a listar las vulnerabilidades y riesgos que se han venido dando durante los procesos de comunicación y seguridad de la información. *Ver documento adjunto: ANEXO 3: RIESGOS Y VULNERABILIDADES DEL CETEIQ.pdf*

ANEXO 4

Incidentes detectados

El administrador de red del CETEIQ procedió a realizar un informe al jefe de tecnologías de los incidentes detectados en su administración; cabe indicar que no hay documentado nada. *Ver documento adjunto: ANEXO 4: INCIDENTES DETECTADOS.pdf*

ANEXO 5

Controles de seguridad SGSI ISO 27002:2005

Esta norma ISO promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. *Ver documento adjunto: ANEXO 5: CONTROLES ISO 27002: 2005.pdf*

ANEXO 6

Catálogo de elementos

Determina los tipos de activos, de amenazas, seguridades ante las amenazas y vulnerabilidades de la información junto con los criterios de valoración. *Ver documento adjunto: ANEXO 6: CATALOGO DE ELEMENTOS.pdf*