MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

TEMA: "EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN EN EL PROCESO DE SEGUROS PREVISIONALES DEL ISSFA BASADA EN NORMAS ISO: 27001"

AUTORES: PORRAS CABEZAS PAULINA CECILIA

SALAZAR FLORES JORGE GIOVANNI

DIRECTOR: ING. FIDEL CASTRO, MSc.

SANGOLQUÍ

2016

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORIÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN EN EL PROCESO DE SEGUROS PREVISIONALES DEL ISSFA BASADO EN NORMAS ISO: 27001***" realizado por los señores ***PAULINA CECILIA PORRAS CABEZAS Y JORGE GIOVANNI SALAZAR FLORES***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores ***PAULINA CECILIA PORRAS CABEZAS Y JORGE GIOVANNI SALAZAR FLORES*** para que lo sustente públicamente.

Salgolquí, 02 de febrero del 2016

ING. FIDEL CASTRO MSc.

DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORIÍA DE SISTEMAS TECNOLÓGICOS

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***PAULINA CECILIA PORRAS CABEZAS*** con cédula de identidad N° 1716959471 ***Y JORGE GIOVANNI SALAZAR FLORES*** con cédula de identidad N° 1801493444, declaramos que este trabajo de titulación "***EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN EN EL PROCESO DE SEGUROS PREVISIONALES DEL ISSFA BASADO EN NORMAS ISO: 27001"*** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 02 de febrero del 2016

PAULINA PORRAS CABEZAS
C.C 1716959471

GIOVANNI SALAZAR FLORES
C.C 1801493444

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN

Nosotros, ***PAULINA CECILIA PORRAS CABEZAS Y JORGE GIOVANNI SALAZAR FLORES***, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "***EVALUACIÓN DE SEGURIDAD DE INFORMACIÓN EN EL PROCESO DE SEGUROS PREVISIONALES DEL ISSFA BASADO EN NORMAS ISO: 27001***" cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 02 de febrero del 2016

PAULINA PORRAS CABEZAS
C.C 1716959471

GIOVANNI SALAZAR FLORES
C.C 1801493444

DEDICATORIA

El presente trabajo va dedicado a Dios, pilar fundamental en mi vida, quién me dio la fuerza y sabiduría para culminar este proyecto.

A mi hija Ana Paula, fuente de inspiración razón por la cual existo y me esfuerzo cada día, quien me cedió el tiempo que le pertenecía para que yo pudiera cumplir mi sueño, te amo princesa.

A mi esposo Carlos Villavicencio, por motivarme a seguir adelante, por su paciencia y afecto durante todo este tiempo.

A mi padre Víctor, por su gran ejemplo de tenacidad, constancia. A mi madre Cecilia, por sus sabios consejos, su amor, y por cuidar de mi hija mientras realizaba mis estudios.

A mis hermanas Lorena y Sthepannie, por darme la mano cuando más lo he necesitado y por su inmenso cariño.

A todos mis familiares, abuelos, tíos, primos, suegros, cuñados, etc., que confiaron en mí, me apoyaron y pusieron su granito de arena para que pudiera cumplir mi meta.

Paulina Porras Cabezas

A Gloria América y Jorge Orlando por su cariño incondicional, a Jeannett, Erick David y Doménika por su ejemplo de comprensión y paciencia.

Giovanni Salazar Flores.

AGRADECIMIENTO

De manera especial, agradecemos al ISSFA (Instituto Nacional de Seguridad Social de las Fuerzas Armadas) y a su Director General el Gral. por darnos las facilidades necesarias para realizar la presente tesis.

Agradecemos al Ing. Fidel Castro, nuestro Director de Tesis, y la Ing. Nancy Velásquez, Oponente de Tesis, quienes con su experiencia y conocimientos supieron guiarnos para realizar el presente proyecto.

A nuestros maestros, por compartir sus conocimientos, en especial al Ing. Mario Ron B. por su amistad.

Paulina Porras Cabezas

Giovanni Salazar Flores

INDICE DE CONTENIDOS

LISTADOS DE TABLAS

LISTADO DE FIGURAS

RESUMEN

El Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA), como ente administrador de la seguridad social militar, utiliza y genera gran cantidad de información de suma importancia para la entrega con oportunidad y precisión de las prestaciones y beneficios a sus afiliados, a través de su proceso de Seguros Previsionales como parte de la cadena de valor del ISSFA. Esta información procede de diferentes fuentes y se encuentra en varios formatos para ser utilizada por los procesos de la Institución de acuerdo a su naturaleza, es así que garantizar la confidencialidad, integridad y disponibilidad de esta información se ha tornado en un problema trascendente a resolver. Es así que la Institución requiere aplicar normativas tendientes a mantener la seguridad de la información corporativa en base a marcos referenciales internacionalmente aceptados y probados, en el caso de este estudio se ha utilizado la norma ISO/IEC 27001:2005, este marco referencial habilita la ejecución de un análisis previo para determinar el estado actual de la seguridad de la información en la Institución de tal manera de obtener una línea base, en el caso del ISSFA se procedió a determinar el estado actual de los controles de seguridad aplicando un análisis de riesgos de sus activos de información basado en la norma ISO/IEC 27005, a través del cual se determinó existencias o falencias de los mismos dentro de los diversos procedimientos componentes del Proceso de Seguros Previsionales. Posteriormente se emitió un informe de la evaluación de seguridad realizada con sus respectivas recomendaciones y un plan de acción tendiente a orientar a la Institución en la implementación de los controles de la norma ISO/IEC 27002 seleccionados.

PALABRAS CLAVES:
PLAN DE ACCIÓN.
SEGURIDAD,
ACTIVO FIJO

ABSTRACT

Military Social Security is defined as the compulsory public service, promoted by the state, which includes preventive, remedial and recovery socks, legally established in a special, supportive diet dispensed in the welfare institutions, services and social assistance in favor of the military professional and military pensioners and their families, members of the armed forces and military pensioners. The ISSFA is the body set up to manage and deliver benefits to members and beneficiaries of the members universe, to which has been structured by processes in an organization, defined according to its nature, so that among the processes of the value chain the process is Prevision Insurance, which is divided into the threads Membership and Listing Management, Payroll Management and Performance Management. By the Institution defined policies to benefit their members, the financial payments made by the ISSFA several concepts in particular pension and severance must be made well in advance before the end of the month, that policy has remained in effect in over the years of life of the institution. Family safety information that was used for this evaluation is ISO / IEC 27001:2005 (Requirements) 27002:2005 (Controls) and 27005:2008 (Risks management). The result obtained in this work is the identification of risks, treatment and issue a report assessing information security, focusing on the recommendations that different stakeholders should respect and enforce. Subsequently issued an action plan to organize the implementation of projects aimed at the implementation of controls to mitigate risks. As a result of this study has two main objectives achieved, there has been laying the groundwork to maintain business continuity and by using the ISO / IEC 27001.

KEY WORDS:
THREAT
VULNERABILITY
PLANNING

CAPITULO I

PROBLEMA

1.1. Generalidades

"La Seguridad Social Militar se define como el servicio público obligatorio, promovido por el Estado, que comprende las medias preventivas, reparadoras y de recuperación, legalmente establecidas en un régimen especial, solidario, dispensadas en las instituciones de previsión, servicios y asistencia social a favor del profesional militar y el pensionado militar y su familia, los miembros de las Fuerzas Armadas y los pensionistas militares, para su bienestar y aseguramiento del nivel de vida.

La constitución de la República del Ecuador define a la Seguridad Social de las Fuerzas Armadas como un régimen especial de seguridad social que se administra en su propia ley, el organismo gestor de la Seguridad Social Militar forma parte del Sistema Nacional de Seguridad Social.

Nuestro régimen especial de protección social ampara a un colectivo de 250.000 personas dispersas en toda la Geografía Nacional. La cobertura social militar es integral pues cubre todos los riesgos profesionales a los que está expuesto el miembro de las Fuerzas Armadas. El militar ecuatoriano aporta al financiamiento de las pensiones militares, la salud y los riesgos de trabajo." (ISSFA, 2014)

La seguridad social militar es un derecho alcanzado por el colectivo de militares en servicio pasivo, consagrado en la Constitución de la República como un régimen especial, logrado a lo largo de varios años de reivindicaciones sociales de un grupo

de profesionales cuyas actividades difieren de las de otros grupos humanos con derechos similares.

La naturaleza de la profesión militar obliga a los soldados a mantener un régimen de trabajo sin horario fijo ni un lugar específico para desarrollar sus actividades, así como también a la exposición de su integridad física y su vida en pos de cumplir su misión en tiempos de paz y en tiempos de conflicto.

La cobertura de los seguros otorgados por el ISSFA a su colectivo militar, se extiende también al grupo familiar del militar en servicio activo y pasivo como a su esposa o esposo, hijos, dependientes o montepíos, en cualquier lugar en donde se encuentren.

El ISSFA financia sus derechos y beneficios en base a las aportaciones mensuales realizadas por todos los miembros de las tres fuerzas dados de alta y en servicio activo y aportaciones del estado, pero con el fin de evitar errores en el otorgamiento de derechos y actuar en derecho, exige el cumplimiento de condiciones las mismas que son controladas y verificadas por varios organismos colegiados que funcionan como parte de su estructura administrativa permanente.

Es así que la Institución ha implementado una estructura administrativa con la suficiente capacidad estratégica, táctica y operativa, para poder servir a sus afiliados con calidad, oportunidad y calidez.

La experiencia adquirida por la institución a lo largo de sus 22 años de vida ha permitido realizar una mejora continua en su forma de trabajar, de tal manera que hoy en día se otorga un gran énfasis al enfoque de la administración por procesos.

Todo el trabajo institucional se ve operativizado en base a la utilización de tecnología informática en gran escala, la misma que provee de sistemas y servicios

orientados hacia el cumplimiento de los objetivos estratégicos institucionales definidos por la alta dirección del ISSFA.

La necesidad permanente del cumplimiento legal, oportunidad en el otorgamiento de derechos, precisión en los cálculos, disponibilidad permanente de información, ubicuidad en el acceso a la misma, fidelidad en los datos procesados, así como el aparecimiento de nuevas técnicas y marcos de trabajo para poder custodiar y operar la información del negocio en forma óptima, generan nuevas oportunidades de mejora para la Institución.

Las regulaciones de la Superintendencia de Bancos y Seguros (SBS), Contraloría General del Estado (CGE), Auditoría Interna, Subsecretaria de Tecnologías de la Información del Estado, una serie de normas técnicas sobre riesgo operativo y el sentido de responsabilidad, obligan a la Institución a establecer un férreo control sobre sus operaciones y sobre todos los pagos generados.

Para este proceso es de suma importancia generar con la mayor precisión los pagos por los diferentes derechos, sin embargo la dificultad y la demora con la que la información de entrada se actualiza en las fuentes, ocasiona que en algunas oportunidades se realicen pagos indebidos con los consiguientes problemas legales posteriores, es así que con el fin de minimizar este problema, se mantienen conexiones directas con bases de datos de diferentes instituciones como son el Registro Civil, Dirección Nacional de Registro de Datos Públicos, Instituto de Seguridad Social de la Policía, Fuerzas Armadas, etc.

Como se puede deducir, la correcta ejecución de los procesos depende en gran medida de la utilización de recursos tecnológicos, lo que crea una alta dependencia de los mismos. La transmisión de información interna y externa a través de los diferentes medios de comunicaciones de datos, incrementa el riesgo de que estos sean interceptados o de alguna manera manipulados sin autorización por parte de

grupos o personas con diferentes intereses, el mismo riesgo es aplicado a la información soportada en otro tipo de medios como papel, discos compactos, equipos portátiles, etc., como ya ha ocurrido en ocasiones anteriores en varias instituciones del estado, gobierno central y gobiernos provinciales en la fecha 10 de Agosto de los años 2010, 2011, 2012.

Evidentemente la cyber seguridad es un complemento importante que debe ser implementado en forma eficaz y sistémica.

1.1.1. Visión

Alcanzar la sostenibilidad del régimen especial de seguridad social de fuerzas armadas y el otorgamiento de las prestaciones y servicios sociales con eficiencia, eficacia y calidez.

1.1.2. Misión

Proporcionar prestaciones económicas y sanitarias así como servicios sociales, con un sistema de gestión integrado, procesos ágiles y modernos, con talento humano competente y comprometido con los valores institucionales y con tecnología de última generación, para satisfacer las necesidades básicas del colectivo militar a fin de propiciar su buen vivir" (ISSFA, 2014)

1.1.3. Organigrama ISSFA

En el siguiente cuadro se describe la estructura orgánica del ISSFA a Agosto de 2013.

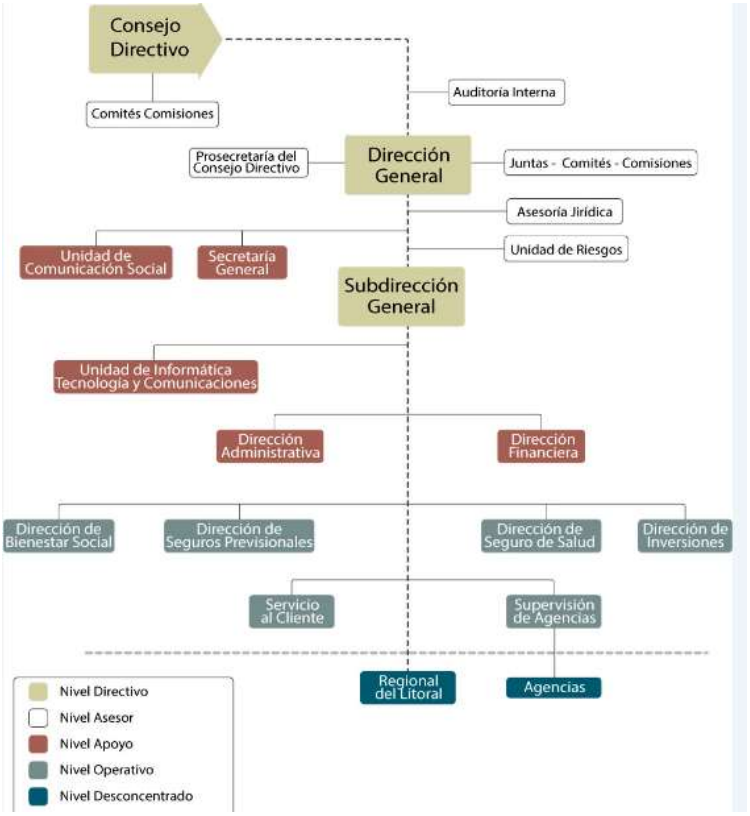


Figura 1. Estructura Orgánica ISSFA

Fuente**:** (ISSFA, 2014)

1.2. Problema

El proceso de Seguros Previsionales en el ISSFA es vital para la organización y se encuentra dentro de la cadena de valor. Es uno de los principales procesos del ISSFA y permite dar servicio al afiliado. Al momento, su funcionamiento no se encuentra controlado por normas de seguridad de información, lo cual pone en riesgo la continuidad de sus operaciones y la entrega oportuna de prestaciones a los afiliados del ISSFA, razón de ser del Instituto. Debido a la importancia y criticidad del proceso de servicios previsionales, ha sido seleccionado para la Evaluación.

Actualmente el proceso de Seguros Previsionales, seleccionado para esta evaluación, se ejecuta en forma continua, sin embargo la fecha crítica en la cual se evalúa su ejecución es a partir del día 25 de cada mes, fecha en la cual se ejecuta y verifica la exactitud del rol de pensiones. Por disposición expresa de la Dirección del ISSFA y como política mantenida desde el inicio de las operaciones de la Institución en el año 1992, las pensiones deben ser pagadas a los afiliados antes del fin de mes sobre cualquier otra prioridad.

Esta política ha mantenido la confianza del afiliado en la Institución, además de permitir solventar sus necesidades económicas en forma oportuna y planificada.

Para obtener la precisión y oportunidad mencionadas, en este proceso se utilizan a gran escala medios informáticos, comunicaciones, sistemas, intercambio de información con instituciones externas, personal especializado y cumplimiento legal, elementos que en este momento no se encuentran controlados bajo normas de seguridad de información que permitan alcanzar niveles aceptables de confidencialidad, integridad y disponibilidad de la información que utiliza y genera.

El presente trabajo es el primero de este tipo que se realiza en la institución y puede ser considerado como piloto para los demás procesos del ISSFA.

El problema es relevante para la organización ya que el Proceso de Seguros Previsionales es crítico para los afiliados de la Institución, el cual, al contar con normativas de seguridad de la información repercutirá en una mejor confianza y credibilidad en la Institución.

Inmersos en el contexto de la Institución, se puede deducir que se utiliza, procesa y genera gran cantidad de información de todo tipo y de importancia capital para la vida de ISSFA.

De acuerdo a la metodología de Gobierno por Resultados (GPR) adoptada por el ISSFA para registrar y controlar sus actividades, el proceso de Seguros Previsionales es calificado como de VITAL o ALTA importancia, (Ver tabla 1).

Tabla 1.

Calificación de importancia de procesos

Organización	No.	Proceso	Importancia	Proyectos Alineados	Indicadores			
Subdirección General >Dirección de Seguros Previsionales	P001	Afiliación Masiva de Activos	Alta	0	0	0	0	0
Subdirección General >Dirección de Seguros Previsionales	P002	Afiliación Dependientes de Activos	Alta	0	0	0	0	0
Subdirección General >Dirección de Seguros Previsionales	P005	Actualización de Datos (Seguros)	Vital	0	0	0	0	0
Subdirección General >Dirección de Seguros Previsionales	P006	Actualización de Datos (Masiva Activos)	Vital	0	0	0	0	0
Subdirección General >Dirección de Seguros Previsionales	P008	Registro de Aportes Masivo	Vital	0	0	0	0	0

Fuente: ISSFA

1.2.1. Actualización de datos (seguros) y actualización de datos masiva (activos)

Mantener actualizada la información del personal militar en servicio activo y pasivo, para que sea considerado como afiliado del Instituto de Seguridad Social de las Fuerzas Armadas, a fin de que pueda acceder a las prestaciones y servicios sociales que otorga el ISSFA.

1.2.2. Registro de aportes masivo

Registrar la información referente a las aportaciones de Ley que realizan las Fuerzas Armadas por el personal militar en servicio activo, para actualizar las cuentas individuales de los afiliados; a fin de generar de manera adecuada los procesos de cálculo de seguros.

1.2.3. Cálculo de liquidación de pensiones atrasadas

Normar los procedimientos operativos: Generación de Rol de Pensiones, Liquidación de Pensiones Atrasadas, Descuentos a Terceros (Masiva y Manual), Descuentos por Retenciones Judiciales; con la finalidad de determinar la responsabilidad de los usuarios que intervienen en dicho proceso.

Cabe indicar que existen dos agravantes, el primero es que en el ISSFA no existe ningún proceso de Gestión de Continuidad del Negocio y el segundo es que no existe aún un proceso de gestión de riesgos operativos entre los cuales se tome en cuenta a las TICs., incrementando la posibilidad de que por su alta dependencia tecnológica, este proceso pueda colapsar en algún momento dado.

La seguridad de información como proceso del negocio es inexistente, sin embargo ciertos controles si se hallan implementados los mismos que han permitido hasta este momento operar en forma ininterrumpida, lo que hace presumir que estos controles son muy eficaces.

1.3. Interrogantes de la evaluación técnica informática

Para realizar la Evaluación Técnica Informática debemos considerar varios aspectos que son importantes para conocer la situación actual de la empresa y lo que requiere a futuro. Para esto utilizamos las siguientes interrogantes.

¿Cómo se puede identificar las amenazas a las que está expuesto el Proceso de Seguros Previsionales?

Para conocer las amenazas a las que está expuesto el proceso de Seguros Previsionales, se realizará un análisis de riesgos. El cual permitirá administrar los riesgos encontrados de manera adecuada con el fin de ofrecer un mejor servicio a los afiliados.

¿Cuáles debilidades y vulnerabilidades presenta el proceso de seguros previsionales en cuanto a seguridad de la información?

La debilidad más evidente de este proceso se refiere a la falta de aplicación de normas para mantener la continuidad de sus operaciones, se desconoce el estado de los controles que se encuentran en funcionamiento y las características de los mismos.

Adicionalmente este proceso presenta una alta dependencia de recursos tecnológicos de hardware, software y comunicaciones los mismos que deben encontrase disponibles permanentemente lo que se constituye como una debilidad.

¿Cuál es la importancia de contar con normas de seguridad de la información en el proceso de seguros previsionales?

El proceso de Seguros Previsionales en el ISSFA es vital para la organización y se encuentra dentro de la cadena de valor. Su funcionamiento no se encuentra

controlado por normas de seguridad de información, lo cual pone en riesgo la continuidad de sus operaciones y la entrega oportuna de prestaciones a los afiliados del ISSFA, razón de ser del Instituto.

¿Qué medidas se tomarían para solventar los incidentes encontrados?

Considerando los resultados de la "Evaluación de Seguridad de la Información en el proceso de Seguros Previsionales del ISSFA basado en la norma ISO/IEC 2700012005" se tiene previsto realizar un plan de acción en el que se incluyan procesos, actividades, responsables, etc. con el fin de solventar las debilidades identificadas.

1.4. Objetivos

1.4.1. Objetivo general

Realizar la Evaluación de Seguridad de la Información en el proceso de Seguros Previsionales del ISSFA basado en la norma ISO/IEC 27001:2005, a fin de identificar debilidades y emitir recomendaciones dentro del proceso, lo cual permitirá garantizar la confidencialidad, integridad y disponibilidad de la información.

1.4.2. Objetivos específicos

- Analizar la información del proceso de Seguros Previsionales del ISSFA utilizando como criterio las normas ISO/IEC 27001:2005 para elaborar y ejecutar el plan de evaluación,
- Socializar los hallazgos, conclusiones, recomendaciones a fin de elaborar el informe final.
- Elaborar el Plan de acción.

Los objetivos descritos anteriormente servirán para realizar el análisis de la información del proceso de Seguros Previsionales del ISSFA tomando como base las normas ISO/IEC 27001:2005, y poder solventar las falencias encontradas utilizando el plan de acción que se tiene previsto elaborar.

1.5. Justificación

Alcanzar y mantener en el tiempo, niveles aceptados de seguridad de información en la ejecución del proceso de Seguros Previsionales garantizando la continuidad del negocio y optimizando la entrega de servicios a los afiliados.

1.6. Alcance

El presente trabajo tiene la finalidad de analizar y evaluar (auditar) la integridad, disponibilidad y confidencialidad de la información del proceso de Seguros Previsionales del ISSFA Matriz (Quito), bajo el criterio de las normas ISO/IEC 27000:2005, emitir un informe de la evaluación (auditoria) y generar un plan de acción para ser ejecutado por la Institución.

1.7. Metodología de aplicación

1.7.1. Metodología y técnicas de evaluación y auditoria.

Se requieren varios pasos para realizar una auditoría. El auditor de TICs debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos.

El proceso de auditoría exige que el auditor de TICs reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. Asimismo, la Dirección General de la Institución debe garantizar una

disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría dentro de las condiciones especiales de este trabajo académico

1.7.2. Métodos

La metodología de investigación a emplear es aplicativa, cualitativa, bibliográfica. Aplicativa por cuanto generará conocimientos para aplicaciones prácticas, está dirigida a soluciones de problemas específicos y está enfocada a intereses locales, cualitativa ya que utiliza registros narrativos de los fenómenos que son estudiados mediante técnicas de observación y bibliográfica por la necesidad de utilizar textos de referencia y material ya publicados.

1.7.3. Técnicas

Entre las técnicas a utilizar se encuentran las entrevistas, aplicación de cuestionarios a los usuarios clave tanto del proceso como de los subprocesos, observación de la ejecución de procedimientos y de documentos generados por los mismos, así como también el registro y análisis de posibles eventos de seguridad que se materialicen en el transcurso del desarrollo de este trabajo.

Estas técnicas se las empleará por la efectividad, simplicidad y precisión que se obtendrá debido al conocimiento de usuarios y del medio y posibilidad, por parte de los maestrantes, de permanecer en el sitio.

CAPITULO II

MARCO TEÓRICO

2.1. Introducción

El concepto de auditoría informática ha estado siempre ligado al de auditoría en general y al de auditoría interna en particular, y éste ha estado unido desde tiempos históricos al de contabilidad y de control de los registros y de las operaciones. Aun algunos historiadores fijan el nacimiento de la escritura como consecuencia de la necesidad de registrar y controlar operaciones.

La auditoría se desarrolla con base a normas, procedimientos y técnicas definidas formalmente por institutos establecidos a nivel nacional e internacional; por lo tanto, solo se expondrán algunos aspectos necesarios para su entendimiento; no obstante, se sugiere leer los libros listados en la bibliografía, así como la participación directa y activa en los institutos o asociaciones relacionados con el campo de la especialidad. ” (González, 2012)

2.2.Tecnologías de la información

“Se conoce como tecnología de información (TI) a la utilización de tecnología específicamente computadoras y ordenadores electrónicos - para el manejo y procesamiento de información – específicamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

Los orígenes de la TI son recientes. Aunque el nombre de tecnología de información se remonta a los años 70, su utilización en los negocios se remonta a mediados del siglo XX, durante la segunda guerra mundial. Sin embargo, ha sido en

los últimos 20 años donde ha alcanzado niveles de uso y aplicaciones tan variadas y ubicuas, que se ha convertido en un área de gran amplitud e impacto en todos los aspectos de la vida cotidiana – incluyendo la gerencia de cualquier empresa, en la cual hoy en día es casi indispensable.

Desde el surgimiento de Internet, se ha incorporado masivamente a la TI el aspecto de comunicación, con lo cual se suele hacer referencia a un tema aún más amplio, conocido como Tecnología de Información y Comunicaciones, o TIC.

El departamento o equipo que dentro de una organización ejerce las funciones de TI se encarga de estudiar, diseñar, desarrollar, implementar y administrar los sistemas de información utilizados para el manejo de datos e información de toda la organización. Estos sistemas, a su vez, comprenden aplicaciones o software, y equipos o hardware.

Llevar a cabo las tareas de la organización apoyándose en la Tecnología de información, generalmente redunda en un procesamiento más rápido y confiable de su datos. La información resultante tiene mayor movilidad y accesibilidad, y cuenta con mayor integridad, que cuando se procesa en forma manual.

Igualmente, las computadoras relevan a los empleados de numerosas actividades repetitivas y aburridas, permitiéndoles aprovechar mejor su tiempo en actividades que agregan más valor.

A medida que los precios de los equipos de computación bajan, su capacidad aumenta, y se hacen más fáciles de usar, la TI se utiliza en nuevas y variadas formas. En las empresas, sus aplicaciones son diversas. Hoy en día, la mayoría de las empresas medianas y grandes (y cada día más pequeñas y micro-empresas) utilizan la TI para gestionar casi todos los aspectos del negocio, especialmente el manejo de los registros financieros y transaccionales de las organizaciones, registros de

empleados, facturación, cobranza, pagos, compras, y mucho más.” (Gerencia.com, 2013)

2.3. Seguridad de la información

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente. (ISO 27000, 2013)

Ciberseguridad

Las noticias de cyber ataques a ciudadanos, organizaciones, empresas y, hasta, instalaciones críticas de países como plantas de energía química, centrales nucleares o fábricas de diferentes índoles se han vuelto habituales en los diferentes medios de comunicación no sólo escritos, sino radio, televisión y, naturalmente, los medios electrónicos de Internet.

La aparición de las TIC en el ámbito de las infraestructuras críticas ha derivado en la aparición de unas nuevas formas de amenaza que podrían llegar a afectar gravemente a la población, de modo que si no se gestionan adecuadamente podrían incluso llegar a aumentar el nivel de riesgo frente a ataques deliberados basados en este tipo de tecnologías.

La cyber seguridad se relaciona frecuentemente con el concepto de ciberguerra considerando el ciberespacio como el quinto dominio de la guerra junto a la tierra, mar, aire y espacio. El nuevo modelo de computación se describe en términos de nube como piedra angular de las nuevas infraestructuras tecnológicas de esta década así como las tecnologías más disruptivas de la actualidad de impacto en las ciber amenazas y, en consecuencia, en las cyber defensas (realidad aumentada, geolocalización, Web en tiempo real, Internet de las cosas,).

El Centro Criptológico Nacional en España ha desarrollado y puesto a libre disposición una serie de documentos y recursos relacionados con la seguridad de los

sistemas para aumentar el grado de concienciación y protección de las organizaciones.

En esta misma línea, la publicación por parte de OTAN de CCDCOE - National Cyber Security Framework Manual por parte del Cooperative Cyber Defence Centre of Excelence procura tomar en consideración todas las facetas que deben tenerse en cuenta en la elaboración de una estrategia nacional de seguridad cibernética, así como herramientas genuinas y asesoramiento altamente competente en este proceso para fomentar un mayor nivel de seguridad informática a nivel nacional y de cooperación internacional.

Organismos como ICANN (organismo internacional regulador de los sistemas de nombre de dominio - DNS) ha aprobado recientemente el protocolo de seguridad DNSSEC para asegurar una protección más completa de los sistemas ante los posibles agujeros en su seguridad.

Existen cada vez más legislación y publicaciones relativas a este área pero como normas de seguridad cibernética hemos querido recoger en este apartado aquellas que permiten a las organizaciones introducir o considerar por parte de proveedores aquellas técnicas en seguridad que permiten reducir al mínimo el número de ataques informáticos de seguridad que puedan lograr el éxito y que además pueden integrarse/combinarse con la serie ISO 27000 en calidad, todas ellas, de normas reconocidas y de aplicación a nivel internacional y orientadas a todo tipo de organizaciones (Instituto Español de Estudios estratégicos, s.f).

2.3.1. Seguridad física

Cuando se habla de seguridad informática existe una clara tendencia a hacer el siguiente razonamiento de forma más o menos inconsciente:

- Queremos proteger bienes de carácter informático (por ejemplo, datos confidenciales).
- Las amenazas que dichos bienes pueden sufrir proceden del medio informático (por ejemplo, copia no autorizada de esos datos).
- Por tanto, los mecanismos de protección también deben ser informáticos (por ejemplo, restricciones de acceso a dichos datos).

Así, asociamos el concepto de seguridad exclusivamente a mecanismos relativamente sofisticados de control informático, como pueden ser entrada restringida al sistema, denegación de privilegios de lectura y modificación de ficheros, cifrado de las comunicaciones, o protección de las redes mediante cortafuegos.

Como consecuencia de esta manera de pensar los sistemas informáticos quedan a merced de amenazas que no dependen para nada de su configuración: ¿de qué nos sirve tener los mejores mecanismos de control de acceso a nuestros ordenadores, o disponer de los sistemas de cifrado más actuales e invulnerables, si un simple accidente del personal de limpieza de nuestra oficina puede hacer que el equipo acabe por el suelo y que la información en él contenida quede irrecuperable? ¿O si alguna de las personas que operan en ellos se lleva a su casa ficheros con información confidencial para trabajar sobre ellos y es víctima de un robo?

La seguridad física se ocupa precisamente de los problemas de seguridad informática que, por su origen, son ajenos a los equipos y no pueden ser previstos o evitados utilizando la programación de los mismos. Es decir, de los daños que se pueden producir sin necesidad de acceder al ordenador (y muchas veces sin necesidad de enchufarlo siquiera).

Las medidas de seguridad física servirán para proteger nuestros equipos e información frente a usos inadecuados, fallos de instalación eléctrica, accidentes, robos, atentados, desastres naturales, y cualesquiera otros agentes que atenten directamente contra su integridad física (Garfinkel & Spanfford, 1996).

2.3.2. Seguridad lógica

Luego de ver como los sistemas de información puede verse afectados por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos, sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren, estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean en la Seguridad Lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y

no puedan modificar los programas ni los archivos que no correspondan.

- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información (Shared, 2011).

2.4. Introducción a la auditoria informática

2.4.1. Conceptos sobre auditoría

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

Aunque hay muchos tipos de auditoría, la expresión se utiliza generalmente para designar a la auditoría externa de estados financieros, que es una auditoría realizada por un profesional experto en contabilidad, de los libros y registros contables de una entidad, para opinar sobre la razonabilidad de la información contenida en ellos y sobre el cumplimiento de las normas contables.

"El requisito básico para la realización de una auditoría es la independencia, que comprende los siguientes puntos:

- **Independencia mental:** El estado mental que permite proporcionar una opinión sin ser afectados por influencias que comprometan el juicio

profesional y su dirección, permitiendo a una persona actuar con integridad, y ejercer objetividad y escepticismo profesional.

- **Independencia aparente:** Cuando se evitan hechos y circunstancias que sean tan importantes que un tercero juicioso e informado, con conocimiento de toda la información relevante, incluyendo cualesquiera salvaguardas que se apliquen, concluiría de manera razonable que la integridad, objetividad o escepticismo profesional del equipo auditor para atestiguar hubieran sido comprometidos.

2.4.1.1. Tipos de auditoría

AUDITORIA CONTABLE: la realizada por un profesional, experto en contabilidad, sobre los estados contables de una entidad.

AUDITORÍA ENERGÉTICA, una inspección, estudio y análisis de los flujos de energía en un edificio, proceso o sistema con el objetivo de comprender la energía dinámica del sistema bajo estudio.

AUDITORÍA JURÍDICA, profesional de derecho, con capacidad y experiencia en derecho civil o militar que realiza la revisión, examen y evaluación de los resultados de una gestión especifica o general de una institución o cuerpo, con el propósito de informar o dictaminar acerca de ellas, realizando las observaciones y recomendaciones pertinentes para mejorar su eficacia y eficiencia en su desempeño.

AUDITORÍA INFORMÁTICA, proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

AUDITORÍA MEDIOAMBIENTAL, cuantificación de los logros y la posición medioambiental de una organización.

AUDITORÍA SOCIAL, proceso que una empresa u organización realiza, con ánimo de presentar balance de su acción social y su comportamiento ético.

AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN, análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

AUDITORÍA DE INNOVACIÓN, proceso de obtención información sobre la situación actual de la empresa frente a la innovación.

AUDITORÍA POLÍTICA, revisión sistemática de los procesos y actividades, orientadas ideológicamente, de toma de decisiones de un grupo para la consecución de unos objetivos, en beneficio de todos.

AUDITORÍA ELECTORAL, la realizada a Sistemas Electorales de los diferentes países con Sistema Democrático y se realizan para darle Confiabilidad y Transparencia al Sistema.

AUDITORÍA DE ACCESIBILIDAD, revisión de la accesibilidad de un sitio web por parte de un experto.

AUDITORÍA DE MARCA, metodología para medir el valor de una marca.

AUDITORÍA DE CÓDIGO DE APLICACIONES, proceso de revisar el código de una aplicación para encontrar errores en tiempo de diseño.

AUDITORÍA SARBANES-OXLEY O AUDITORÍA SOX, revisión practicada a las firmas de auditoría de las compañías que cotizan en bolsa, de acuerdo a lo prescripto por la ley Sarbanes-Oxley.

AUDITORÍA CIENTÍFICO - TÉCNICA, realizada a Instituciones encargadas de la Investigación Científica y Técnica en las diferentes áreas del Trabajo humano.

2.4.1.2. Auditoría basada en riesgos

La constante búsqueda por la eficiencia en la aplicación de estudios de auditoría y los escasos recursos con los que los auditores cuentan para ejecutar su trabajo, ha propiciado el desarrollo de un método que permita mejorar en forma continua el proceso de auditoría, como es el análisis de riesgos, justamente para poder realizar un enfoque preciso del estudio destinando los recursos necesarios.

Este tipo de auditoría no está basada solo en el riesgo sino también en los controles internos y operativos, así como también en sus conocimientos de la empresa o del negocio. Esta decisión de determinar el tipo de riesgo puede ayudar a relacionar el análisis de costo/beneficio del control para el riesgo conocido, permitiendo que se hagan elecciones prácticas.

Los riesgos del negocio son las preocupaciones sobre los probables efectos de un evento incierto sobre el logro de objetivos establecidos.

La naturaleza de estos riesgos puede ser financiera, regulatoria u operativa, y puede también incluir riesgos derivados de tecnología específica.

Entendiendo la naturaleza del negocio los auditores pueden identificar y clasificar los tipos de riesgos que determinarán mejor el modelo de riesgo o la metodología para llevar a cabo la auditoria.

El análisis de riesgos pues, surge como una técnica importante para los auditores y no solo es aplicada para la auditoría informática sino para una amplia gama de disciplinas como por ejemplo las finanzas.

De acuerdo a BASILEA II, el riesgo de tecnología debe ser estructurado como parte del riesgo operativo u operacional, en especial en las instituciones financieras o reguladas por la Superintendecia de Bancos y Seguros, como es el caso del ISSFA.

En efecto existe varias resoluciones en las cuales la SBS dispone a sus instituciones controladas, como el ISSFA, a conformar una unidad técnica cuya misión sea la de identificar, gestionar y controlar los riesgos en la Institución como por ejemplo:

"LIBRO I.- NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY

GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO

TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS

CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO

(Incluido con resolución No JB-2005-834 de 20 de octubre del 2005)"

y varias otras como las siguientes resoluciones:

- JB-2012-2148 de 26 de abril del 2012
    - JB-2008-1202 de 23 de octubre del 2008 y renumerado con resolución No. JB-2012-2148 de 26 de abril del 2012.

En la siguiente tabla se menciona la norma descrita anteriormente, en el mismo se puede observar las referencias sobre el riesgo operativo concernientes a la información institucional y a tecnología:

Tabla 2.

Identificación de eventos fallas o insuficiencias y factores del riesgo operativo

TIPO DE EVENTOS	**FALLA O INSUFICIENCIAS**	**FACTORES DE RIESGO OPERATIVO**
	FRAUDE INTERNO	
Por Ejemplo:		
Operaciones no reveladas adecuadamente	**Mal diseño del proceso**	**Procesos**
Inadecuada utilización de información confidencial.	**Ausencia de control de perfiles de usuario**	**Tecnología de la Información**
Apropiación indebida de activos	**Inadecuada segregación de funciones.**	**Personas**
Falsificación	**Inexistencia de controles**	**Procesos**
Destrucción maliciosa de activos	**Inadecuadas medidas de seguridad**	**Procesos**
	FRAUDE EXTERNO	
Por Ejemplo:		
Robo	**Falta de seguridad física.**	**Procesos**
Emisión de Cheques sin fondo	**Inadecuada capacitación del personal.**	**Personas**
Perjuicios por intrusión o ataque de terceros.	**Falta de seguridades en Tecnología de la Información.**	**Tecnología de la Información**
	PRACTICAS DE EMPLEO Y SEGURIDAD DEL AMBIENTE DE TRABAJO	
Reclamos por compensación e indemnización del personal.	**Inadecuada contratación del personal.**	**Procesos**
Violación de las normas de salud o seguridad	**Falta de difusión y comunicación de políticas.**	**Personas**
Todo tipo de discriminación.	**Inadecuada política de administración de personal.**	**Personas**
	PRACTICAS RELACIONADAS CON CLIENTES, LOS PRODUCTOS Y EL NEGOCIO	
Mal manejo de la información confidencial de los clientes.	**Falta de definición de política y procedimientos.**	**Procesos**
Prácticas contrarias a la competencia, prácticas inadecuadas de negociación.	**Falta de definición de políticas.**	**Procesos**

Fuente: www.iso.org

Campo de auditoría informática

Algunos campos de aplicación de la auditoría informática son las siguientes:

- **Investigación científica y humanística:** Se usan las computadoras para la resolución de cálculos matemáticos, recuentos numéricos, etc. Algunas de estas operaciones:
  Resolución de ecuaciones.
  Análisis de datos de medidas experimentales, encuestas etc.
  Análisis automáticos de textos.

- **Aplicaciones técnicas:** Usa la computadora para facilitar diseños de ingeniería y de productos comerciales, trazado de planos, etc. Algunas de estas operaciones:
  Análisis y diseño de circuitos de computadora.
  Cálculo de estructuras en obras de ingeniería.
  Minería.
  Cartografía.

- **Documentación e información:** Es uno de los campos más importantes para la utilización de computadoras.

Estas se usan para el almacenamiento de grandes cantidades de datos y la recuperación controlada de los mismos en bases de datos.

Ejemplos de este campo de aplicación son:
Documentación científica y técnica.
Archivos automatizados de bibliotecas.
Bases de datos jurídicas.

- **Gestión administrativa:** Automatiza las funciones de gestión típicas de una empresa. Existen programas que realizan las siguientes actividades:

Contabilidad.
Facturación.
Control de existencias.

- **Inteligencia artificial:** Las computadoras se programan de forma que emulen el comportamiento de la mente humana. Los programas responden como previsiblemente lo haría una persona inteligente.
  Aplicaciones como:
  Reconocimiento de lenguaje natural.
  Programas de juego complejos (ajedrez).

- **Instrumentación y control:** Instrumentación electrónica, electro medicina, robots industriales, entre otros. (Rojas, 2013)

2.4.3 Normas ISO 27000

INTRODUCCIÓN

"La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC

(International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña." (ISO 27000, 2013)

A continuación se detalla de manera general las normas ISO 27000.

- ISO/IEC 27000 – Términos y Definiciones de toda la serie 27000.
- ISO/IEC 27001 – Requisitos de un Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002 – Código de práctica para la Gestión de la Seguridad de la Información.
- ISO/IEC 27003 – Guía de Implementación de SGSI.
- ISO/IEC 27004 – Métricas y técnicas de medida para determinar la eficacia de un SGSI.
- ISO/IEC 27005 – Gestión de Riesgos en Seguridad de la Información
- ISO/IEC 27006 – Requisitos para la acreditación de entidades de auditoría y certificación de SGSI.
- ISO/IEC 27007 – Guía de Auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
- ISO/IEC 27008 – Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI
- ISO/IEC 27010 – Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.
- ISO/IEC 27011 – Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

- ISO/IEC 27013 – Guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC20000-1 (gestión de servicios TI).
- ISO/IEC 27014 – Guía de gobierno corporativo de la seguridad de la información.
- ISO/IEC 27015 – Guía de SGSI orientada a organizaciones del sector financiero y de seguros.
- ISO/IEC 27016 – Guía de valoración de los aspectos financieros de la seguridad de la información.
- ISO/IEC 27017 – Guía de seguridad para Cloud Computing.
- ISO/IEC 27018– Código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.
- ISO/IEC 27019 – Guía con referencia a ISO/IEC 27002 para el proceso de control de sistemas específicos al sector de la industria de la energía.
- ISO/IEC 27031 – Guía de Continuidad del Negocio.
- ISO/IEC 27032 – Guía de Ciber seguridad.
- ISO/IEC 27033 – Guía de Seguridad en Redes – parte I a VII
- ISO/IEC 27034 – Guía de seguridad en aplicaciones informáticas– parte I a V Sin fecha prevista de publicación.
- ISO/IEC 27035 – Guía sobre la gestión de incidentes de seguridad en la información.
- ISO/IEC 27036 – Guía de seguridad en las relaciones con proveedores.
- ISO/IEC 27037 – Guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP.

- ISO/IEC 27038 – Guía de especificación para seguridad en la redacción digital.
- ISO/IEC 27039 – Guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).
- ISO/IEC 27040 – Guía para la seguridad en medios de almacenamiento.
- ISO/IEC 27041 – Guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
- ISO/IEC 27042 – Guía con directrices para el análisis e interpretación de las evidencias digitales.
- ISO/IEC 27043 – Principios y procesos de investigación
- ISO/IEC 27044 – Gestión de eventos de la seguridad de la información - Security Information and Event. Management (SIEM).
- ISO/IEC 27799 – Guía de implementación de 27002 para Salud.

Luego de detallar las normas ISO 27000, podemos indicar que las normas ISO 270001 aplican para nuestro objeto de estudio.

2.4.4. Sistema de gestión de seguridad de la información (SGSI)

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001.

Las fases que se utilizan en la Norma ISO 27001 son las siguientes:

- La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

- La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
- La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.
- La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

- **FASE DE PLANIFICACIÓN**

Esta fase está formada por los siguientes pasos:

- determinación del alcance del SGSI;
- redacción de una Política de SGSI;
- identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
- identificación de activos, vulnerabilidades y amenazas;
- evaluación de la magnitud de los riesgos;
- identificación y evaluación de opciones para el tratamiento de riesgos;
- selección de controles para el tratamiento de riesgos;
- obtención de la aprobación de la gerencia para los riesgos residuales;
- obtención de la aprobación de la gerencia para la implementación del SGSI;
- redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

- **FASE DE IMPLEMENTACIÓN**

  Esta fase incluye las siguientes actividades:

  - Redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes;
  - Implementación de un plan de tratamiento del riesgo;
  - Implementación de los controles de seguridad correspondientes;
  - determinación de cómo medir la eficacia de los controles;
  - Realización de programas de concienciación y capacitación de empleados;
  - Gestión del funcionamiento normal del SGSI;
  - Gestión de los recursos del SGSI;
  - Implementación de procedimientos para detectar y gestionar incidentes de seguridad.

- **FASE DE VERIFICACIÓN**

  Esta fase incluye lo siguiente:

  - Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
  - Revisiones periódicas de la eficacia del SGSI;
  - Medición la eficacia de los controles;
  - Revisión periódica de la evaluación de riesgos;
  - Auditorías internas planificadas;
  - Revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;

- Actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
- Mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

- **FASE DE MANTENIMIENTO Y MEJORA**

Esta fase incluye lo siguiente:

- Implementación en el SGSI de las mejoras identificadas;
- Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
- Comunicación de actividades y mejoras a todos los grupos de interés;
- Asegurar que las mejoras cumplan los objetivos previstos.

2.4.4.1. Norma ISO/IEC 27001

"La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible." (ISO 27001, 2012)

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

2.4.4.2. Documentos de ISO 27001

La norma ISO 27001 requiere los siguientes documentos:

- El alcance del SGSI;
- La política del SGSI;
- Procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas;
- Todos los demás documentos, según los controles aplicables;
- Metodología de evaluación de riesgos;
- Informe de evaluación de riesgos;
- Declaración de aplicabilidad;
- Plan de tratamiento del riesgo;
- Registros.

La cantidad y exactitud de la documentación depende del tamaño y de las exigencias de seguridad de la organización; esto significa que una docena de documentos serán suficientes para una pequeña organización, mientras que las organizaciones grandes y complejas tendrán varios cientos de documentos en su SGSI.

2.4.5. Gestión de riesgos

2.4.5.1. Normativas para la gestión y administración de riesgos

Debido a la importancia reconocida en la gestión de riesgos para las organizaciones, incluso para los países, la comunidad internacional ha respondido generando diferentes normativas referenciales orientadas a la administración de riesgos específicos o generales según su origen.

Los escándalos ocasionados por empresas de gran poder económico, han sido motivo más que suficiente para identificar la gravedad de las consecuencias económicas y sociales que la falta de proactividad en el manejo de los riesgos han originado.

Las crisis económicas que han afectado a muchos países del mundo, también al Ecuador, han obligado a mantener un monitoreo constante de todos los factores de riesgo y a adoptar ciertas normativas internacionales, en ocasiones por necesidad de las organizaciones y en ocasiones por cumplir con las regulaciones de los países con los cuales el Ecuador tiene interés en mantener relaciones comerciales o de otra índole.

Algunas de las normativas más importantes nacidas en el contexto antes descrito, son:

- **Comunicación "A" 4609 del BCRA para entidades Financieras**

Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

- **Basilea II**

Estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

- **Ley Sarbanes Oxley (SOX)**

Impulsada por el gobierno norteamericano como respuesta a los mega fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros.

- **PCI DSS**

Impulsada por las principales marcas de tarjetas de pago, este estándar busca garantizar la seguridad de los datos de titulares de tarjetas de pago en su procesado, almacenamiento y transmisión.

2.4.5.2. METODOLOGÍAS PARA LA GESTIÓN Y ANÁLISIS DE RIESGOS

- Citicus One: software comercial de Citicus, implementa el método FIRM del Foro de Seguridad de la Información;
- CRAMM: "CCTA Risk Assessment and Management Methodology" fue originalmente desarrollado para uso del gobierno de UK pero ahora es propiedad de Siemens;
- ISO TR 13335: fue el precursor de la ISO/IEC 27005;
- MAGERIT "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" está disponible tanto en español como en inglés.
- OCTAVE: "Operationally Critical Threat, Asset, and Vulnerability Evaluation" Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT;
- NIST SP 800-39 "Gestión de Riesgos de los Sistemas de Información, una perspectiva organizacional";
- NIST SP 800-30: Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información, es gratuito;

- Mehari: Método de Gestión y Análisis de Riesgos desarrollado por CLUSIF (Club de la Sécurité de l'Information Français);
- AS/NZS: Norma de Gestión de Riesgos publicada conjuntamente por Australia y Nueva Zelanda y ampliamente utilizada en todo el mundo.
- ISO 31000:2009: Gestión de riesgos - Principios y directrices, establece los principios, el marco y un proceso para la gestión del riesgo. Puede ser utilizado por cualquier organización independientemente de su tamaño, actividad o sector. El uso de ISO 31000 puede ayudar a las organizaciones a aumentar la probabilidad de alcanzar los objetivos, mejorar la identificación de oportunidades y amenazas y eficazmente asignar y utilizar los recursos para el tratamiento de riesgos.

2.4.5.3. Normas relacionadas

Un número de otras normas se refieren también a la gestión de riesgos.

- *Risk management - Vocabulary* Guía ISO 73:2009, *Gestión del riesgo - Vocabulario* complementa ISO 31000, proporcionando una colección de términos y definiciones relacionados con la gestión del riesgo.
- *ISO/IEC 31010:2009, Risk management – Risk assessment techniques* ISO / IEC 31010:2009, *Gestión del riesgo - las técnicas de evaluación de riesgos* se centra en la evaluación de riesgos. La evaluación de riesgos ayuda a los tomadores de decisiones a entender los riesgos que puedan afectar a la consecución de los objetivos, así como la adecuación de los que ya están en marcha los controles. ISO / IEC 31010:2009 se centra en los conceptos de evaluación de riesgos, los procesos y la selección de las técnicas de evaluación de riesgos.

2.4.5.4. Proceso de análisis de riesgos de la información

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, etcétera y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

Cada organización tiene una misión. En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben de estar conscientes que la administración del riesgo informático juega un rol crítico.

La meta principal de la administración del riesgo informático debería ser "proteger a la organización y su habilidad de manejar su misión" no solamente la protección de los elementos informáticos. Además, el proceso no solo debe de ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización.

Es importante recordar que el riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia. Por lo que podemos decir a grandes rasgos que la administración de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable.

El análisis de riesgo informático es un elemento que forma parte del programa de gestión de continuidad de negocio (Business Continuity Management)

En el análisis de riesgo informático es necesario identificar si existen controles que ayudan a minimizar la probabilidad de ocurrencia de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado.

Dentro de la evaluación del riesgo es necesario realizar las siguientes acciones: Calcular el impacto en caso que la amenaza se presente, tanto a nivel de riesgo no controlado como el riesgo controlado y evaluar el riesgo de tal forma que se pueda priorizar, esto se realiza de forma cuantitativa (asignando pesos) ó de forma cualitativa (matriz de riesgos)

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo. En este documento se muestran los elementos identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgo es indispensable para lograr una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización. Existen diferentes tipos de riesgos como el riesgo residual y riesgo total así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras. La fórmula para determinar el riesgo total es:

RT (Riesgo Total) = Probabilidad x Impacto Promedio

A partir de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el riesgo residual.

Como se describe en el BS ISO/IEC 27001:2005, la evaluación del riesgo incluye las siguientes actividades y acciones:

- Identificación de los activos.
- Identificación de los requisitos legales y de negocios que son relevantes para la identificación de los activos.
- Valoración de los activos identificados.
- Teniendo en cuenta los requisitos legales identificados de negocios y el impacto de una pérdida de confidencialidad, integridad y disponibilidad.

- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgo preestablecido.

Después de efectuar el análisis debemos determinar las acciones a tomar respecto a los riesgos residuales que se identificaron. Las acciones pueden ser:

- Controlar el riesgo.- Fortalecer los controles existentes y/o agregar nuevos controles.
- Eliminar el riesgo.- Eliminar el activo relacionado y con ello se elimina el riesgo.
- Compartir el riesgo.- Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.
- Aceptar el riesgo.- Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

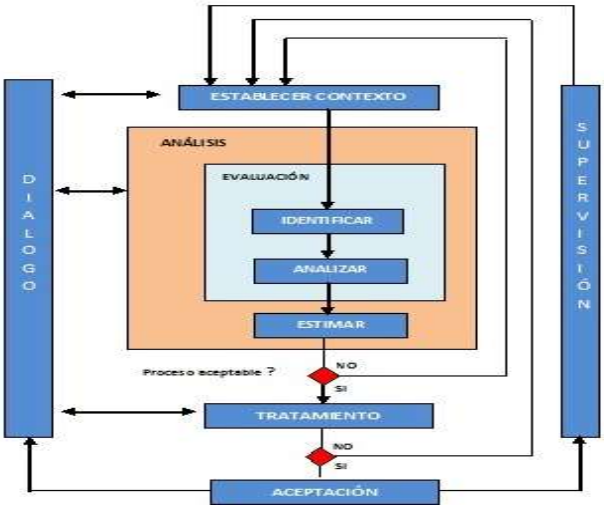


Figura 2: Esquema de estándar de gestión de riesgos ISO/IEC 27005

Fuente**:** (ISO, 2014)

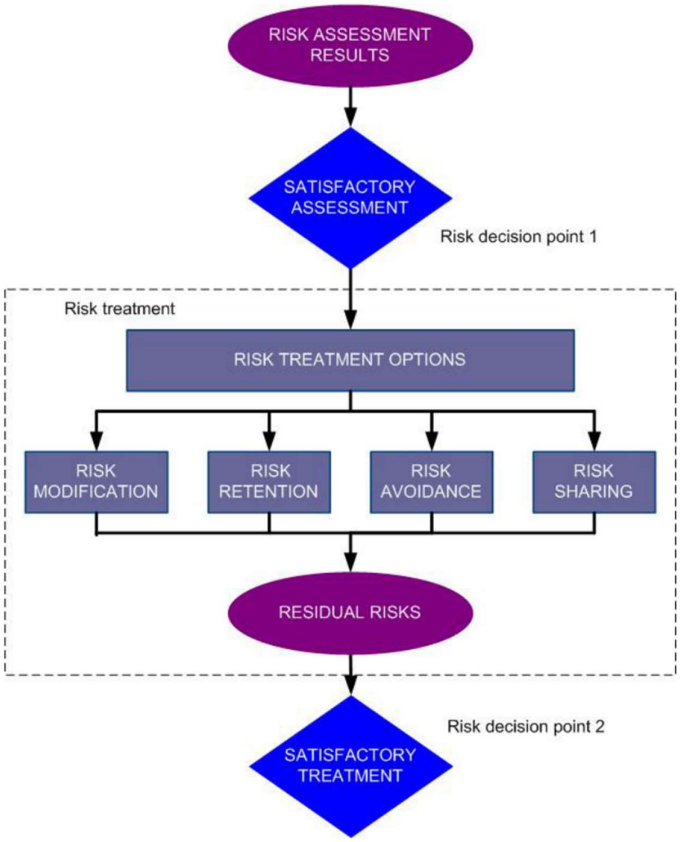


Figura 3: Tratamiento de riesgos ISO/IEC 27005

Fuente**:** (ISO, 2014)

2.5. Metodologías y/o modelos de control utilizados en la auditoría de seguridad de la información

- **BSI**

(British Standards Institution) publicó en 2006 la tercera parte de BS 7799, dedicada a la gestión de riesgos de seguridad de la información.

- **ISO 27001**

(Evolucionada a partir de BS 7799-2) indica que las organizaciones deben identificar, evaluar, tratar y gestionar los riesgos de seguridad de la información, pero no da indicaciones más detalladas de cómo realizar dicho proceso ni de cómo situar dichos riesgos en el marco de los riesgos generales de la empresa.

- **BS7799-3**

Profundiza en estos aspectos y da directrices sobre evaluación de riesgos, tratamiento de riesgos. La norma en mención no se encuentra vigente, fue reemplazada por la ISO/IEC 17799 y esta fue reemplazada por la ISO/IEC 27000:2005

- **ISA99 - ISA** Security Compliance Institute

ISA99 es el comité "Industrial Automation and Control System Security Committee" de la asociación International Society for Automation (ISA). El comité está desarrollando una serie de varios capítulos de normas e informes técnicos sobre en éste área, varios de los cuales han sido publicados como documentos ANSI (American National Standards Institute).

- **ISO 15408**

Los Criterios Comunes(CC) tienen su origen en 1990 y surgen como resultado de la armonización de los criterios sobre seguridad de productos software ya utilizados por diferentes países con el fin de que el resultado del proceso de evaluación pudiese ser aceptado en múltiples países. Los CC permiten comparar los resultados entre evaluaciones de productos independientes. Para ello, se

proporcionan un conjunto común de requisitos funcionales para los productos de TI (Tecnologías de la Información). Estos productos pueden ser hardware, software o firmware.

Con el fin de poder certificar un producto según los Criterios Comunes se deben comprobar, por parte de uno de los laboratorios independientes aprobados, numerosos parámetros de seguridad que han sido consensuados y aceptados por 22 países de todo el mundo. El proceso de evaluación incluye la certificación de que un producto software específico verifica los siguientes aspectos:

- Los requisitos del producto están definidos correctamente.
- Los requisitos están implementados correctamente.
- El proceso de desarrollo y documentación del producto cumple con ciertos requisitos previamente establecidos.

- **ISO/IEC 21827, SSE capability maturity model (SSE-CMM®)**

Estándar internacional basado en un Modelo de Madurez de Capacidades (CMM) para la Ingeniería de Seguridad de Sistemas (SSE) y desarrollado por la Asociación Internacional de Ingeniería de Seguridad de la Información (ISSEA). ISO/IEC 21827 especifica el SSE-CMM mediante la descripción de las características esenciales para alcanzar el éxito en el desarrollo del proceso de ingeniería en seguridad de una organización, incluyendo aquellas gubernamentales como comerciales o académicas. ISO/IEC 21827 no prescribe una secuencia o proceso particular, pero sí captura las prácticas que se observan en la industria. El modelo es una métrica estándar para las prácticas de la ingeniería de seguridad, que cubre:

Ciclo de vida del proyecto: incluyendo actividades de desarrollo, operación, mantenimiento y desmantelamiento

Ámbitos de la organización: incluyendo actividades de gestión, organizacionales y de ingeniería.

Interacciones concurrentes con otras disciplinas: como software y hardware de sistemas, recursos humanos, pruebas de ingeniería, gestión de sistemas, operación y mantenimiento.

Interacciones con otras organizaciones: incluyendo adquisición, gestión de sistemas, certificación, acreditación y evaluación.

Existe un interesante artículo de José Antonio Calvo-Manzano y Ana de las Heras con las sinergias de SGSI y de ISO/IEC 21827 publicado y disponible en abierto para consulta por la revista SIC.

- **NERC**

El North American Electric Reliability Corporation (NERC) ha creado diversas normas. La más ampliamente reconocida es NERC 1300 que es una modificación/actualización de NERC 1200. La última versión de NERC 1300 se denomina CIP-002-1 dentro de CIP-009-2 (CIP = Protección de Infraestructura Crítica). Estas normas se utilizan para proteger sistemas eléctricos pricipales aunque NERC ha creado estándares en otras áreas.

- **NIST**

Dentro de las publicaciones de la serie NIST destacar en este ámbito:

Publicación 800-12: ofrece un amplio panorama de la seguridad informática y de las áreas de control. También hace hincapié en la importancia de los controles de seguridad y la forma de aplicarlos. Inicialmente, este documento estaba dirigido al gobierno federal a pesar de que la mayoría de las prácticas en este documento pueden

aplicarse al sector privado. Concretamente fue escrito para aquellas personas en el gobierno federal responsable de manejar los sistemas sensibles.

- **RFC 2196**

RFC 2196 es el memorando publicado por el Internet Engineering Task Force para el desarrollo de políticas y procedimientos de seguridad de los sistemas informáticos conectados a Internet.

El RFC 2196 proporciona una visión amplia y general de seguridad de la información, incluida la seguridad de la red, respuesta a incidentes o las políticas de seguridad. El documento es muy práctico y se centra en las operaciones del día a día.

- **COBIT**

El IT Governance Institute fue establecido por ISACA (Information Systems Audit and Control Association) en 1998 para aclarar y orientar en cuestiones actuales y futuras relativas a la administración, seguridad y aseguramiento TI.

Como consecuencia de su rápida difusión internacional, ambas instituciones disponen de una amplia gama de publicaciones y productos diseñados para apoyar una gestión efectiva de las TI en el ámbito de la empresa.

Uno de sus documentos más conocidos, referencia a nivel mundial, es CobiT (Objetivos de control para tecnologías de la información y similares).

Se trata de un marco de control que apoya a las a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

Los **principios** y **habilitadores** de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público. En la Fig. 4 se describen los principios de COBIT 5.

Figura 4: Cobit

Fuente: (ISACA, 2012)

COBIT 5 une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información así como su uso en beneficio de las partes interesadas.

- **COSO-ENTERPRISE RISK MANAGEMENT / SOX**

El Committee of Sponsoring Organizations of Treadway Commission (COSO) es una iniciativa del sector privado estadounidense formada en 1985. Su objetivo principal es identificar los factores que causan informes financieros fraudulentos y hacer recomendaciones para reducir su incidencia. COSO ha establecido una definición común de controles internos, normas y criterios contra los cuales las empresas y organizaciones pueden evaluar sus sistemas de control.

Existe una relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos, que representan lo que hace falta para lograr aquellos. La relación se representa con una matriz tridimensional, en forma de cubo.

Figura 5: Diagrama COSO

Fuente: (ISACA, 2012)

Las cuatro categorías de objetivos (estrategia, operaciones, información y conformidad) están representadas por columnas verticales, los ocho componentes lo están por filas horizontales y las unidades de la entidad, por la tercera dimensión del cubo.

- **ITIL**

"IT Infrastructure Library" (ITIL) es un conjunto de publicaciones para las mejores prácticas en la gestión de servicios TI e incluye opciones que pueden ser adoptadas y adaptadas según necesidades, circunstancias y experiencia de cada proveedor de servicios.

Figura 6: Diagrama ITIL

Fuente: (ISACA, 2012)

Fue integrada en las series BS 15000 (ISO 20000 desde Diciembre 2005) con el consenso de BSI, itSMF y OGC, con el propósito de que los dos conjuntos de publicaciones formen parte de la misma estructura lógica para mejor comprensión en su publicación y difusión.

ITIL v2 (versión 2) sirve de base para el estándar ISO 20000 y consta de 7 bloques principales: “Managers Set”, “Service Support”, “Service Delivery”, “Software Support”, “Networks”, “Computer Operations” y “Environmental”.

Las áreas cubiertas por ITIL en cada documento publicado por la OGC son:

• Soporte al servicio: asegurar que el cliente (externo o interno) recibe adecuadamente un servicio, que es gestionado además de la mejor forma posible.

• Entrega del servicio: administración de los servicios de soporte y mantenimiento que se prestan al cliente.

• Planificación de la implantación: determina las ventajas de implantar ITIL en una determinada organización.

• Administración de aplicaciones: conjunto de buenas prácticas para la gestión de todo el ciclo de vida de las aplicaciones, centrándose sobre todo en definición de requisitos e implementación de soluciones.

• Administración de la infraestructura de tecnologías de la información y comunicaciones: gestión de la administración de sistemas como máquinas, redes o sistemas operativos, entre otros.

• Administración de seguridad: proceso para la implantación de requerimientos de seguridad; relaciona las áreas ITIL de soporte y entrega de servicio.

• Administración de activos de software: pautas necesarias para la gestión del software adquirido y/o de desarrollo propio.

• Entrega de servicios desde un punto de vista de negocio: fidelización de clientes, servicios de externalización y gestión del cambio, entre otros.

NIST: Serie 800

El National Institute of Standards and Technology (NIST), fundado en 1901, es un organismo federal no regulador que forma parte de la Administración de Tecnología (Technology Administration) del Departamento de Comercio (Department of Commerce) de los EE.UU.

La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de incrementar la productividad, facilitar el comercio y mejorar la calidad de vida.

CAPITULO III

PROGRAMA DE EVALUACIÓN TÉCNICA DE SEGURIDAD DE INFORMACÍON EN EL PROCESO DE SEGUROS PREVISIONALES

3.1. Proceso de seguros previsionales del ISSFA

El proceso de Seguros Previsionales en el ISSFA es vital para la organización y se encuentra dentro de la cadena de valor. Su funcionamiento no se encuentra controlado por normas de seguridad de información, lo cual pone en riesgo la continuidad de sus operaciones y la entrega oportuna de prestaciones a los afiliados del ISSFA, razón de ser del Instituto. Debido a la importancia y criticidad del proceso de servicios previsionales, ha sido seleccionado para la Evaluación y está compuesto de los siguientes subprocesos y procedimientos (Figura 7):

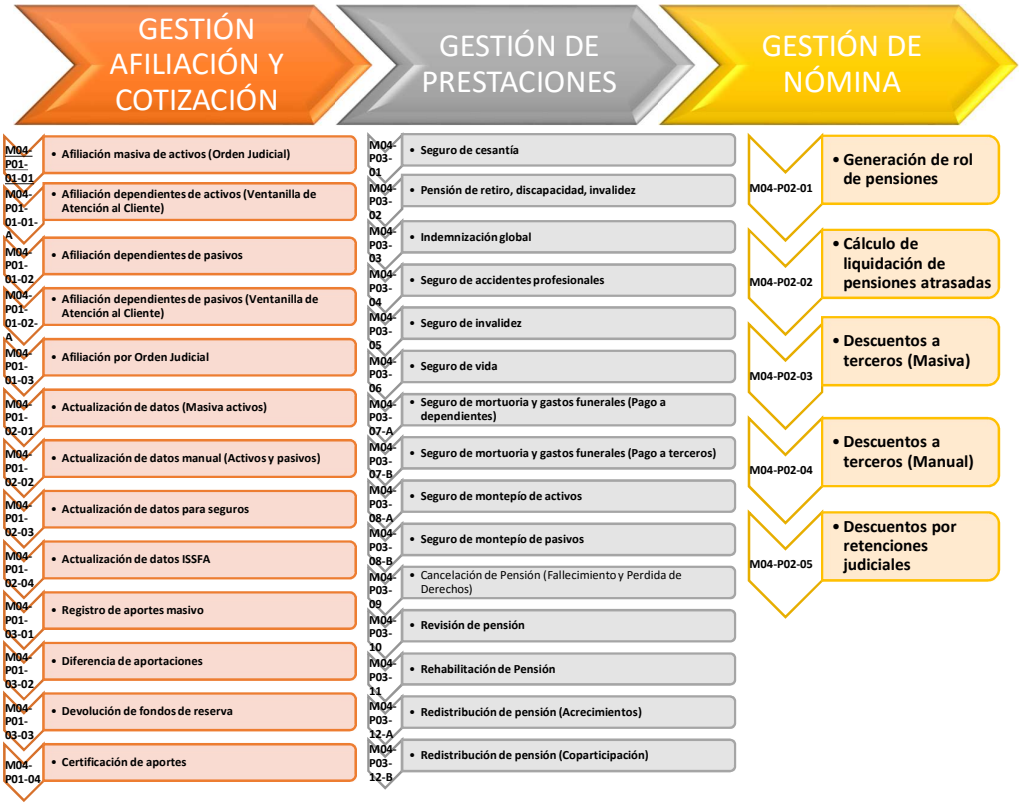


Figura 7: Proceso de Seguros Previsionales ISSFA

Fuente: Los Autores

Seguidamente se describen los procesos que conforman el macro proceso de Seguros Previsionales.

3.1.1. Gestión de afiliación y cotización

En la siguiente figura (**¡Error! No se encuentra el origen de la referencia.**Figura 8), se muestran los subprocesos que son parte del proceso GESTION DE AFILIACION Y COTIZACION.

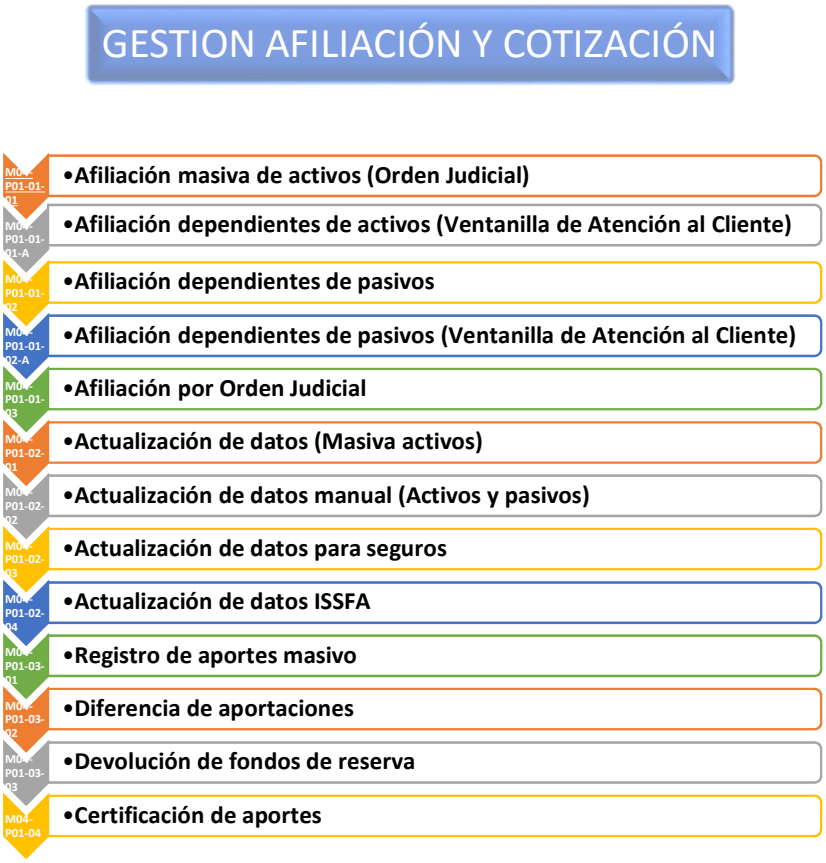


Figura 8: Proceso Gestión de Afiliación y Cotización

Fuente: Los Autores

ALCANCE

La Ley de Seguridad Social de Fuerzas Armadas, establece en su Art. 14 textualmente "La afiliación al ISSFA es obligatoria e irrenunciable y se produce inmediatamente a partir de la fecha de alta del militar en calidad de oficial o miembro de tropa."

Registrar la información referente a las aportaciones de Ley que realizan las Fuerzas Armadas por el personal militar en servicio activo, para actualizar las cuentas individuales de los afiliados; a fin de generar de manera adecuada los procesos de cálculo de seguros.

I. M04-P01-01-01 Afiliación masiva de activos (Orden judicial)

OBJETIVO

Normar los procedimientos operativos de los servicios de: afiliación de los Militares en Servicio Activo, sus dependientes, dependientes de Militares Pasivos y de derechohabientes; con la finalidad de determinar la responsabilidad de los usuarios que intervienen en dicho proceso.

ALCANCE

La Ley de Seguridad Social de Fuerzas Armadas, establece en su Art. 14 textualmente "La afiliación al ISSFA es obligatoria e irrenunciable y se produce inmediatamente a partir de la fecha de alta del militar en calidad de oficial o miembro de tropa."

II. M04-P01-01-01-A Afiliación dependientes de activos (Ventanilla de atención al cliente)

En algunos casos el titular militar afiliado, puede solicitar la afiliación de sus dependientes por múltiples motivos; para este caso la persona antes mencionada puede realizar el trámite en las ventanillas de atención al cliente de cualquiera de las agencias de todo el país. Para este propósito el usuario de Ventanilla de Atención a cliente de las diferentes agencias de todo el país deberá realizar los siguientes procedimientos:

- Recibir toda la documentación necesaria descrita en el apartado V. Políticas Generales – Entrega de Documentos, de este documento. Para empezar este trámite es necesario que el titular militar, pida a la fuerza que pertenece la Hoja de Vida Militar en la que debe constar los dependientes directos de dicha persona.
- Revisar toda la documentación entregada tomando en consideración lo descrito en el apartado V. Políticas Generales – Verificación de Documentos, de este documento.
- Ingresar en Modulo de Afiliación y Cotización de Sistema Informático y registrar datos de titular. Para el registro de datos en Modulo de Afiliación de Sistema Informático se debe tomar en cuenta las siguientes observaciones:

Escenarios:

- Se identifica quien está solicitando la afiliación: (Titular, Dependiente, Fuerzas Armadas, Otros).
- Se ingresa la cedula del militar: Continúa a Pedir Documentos.
- Se debe seleccionar la actividad a realizar.
- Se verifican los requisitos para la actividad seleccionada.

- Se ingresa los datos del solicitante, sea este el militar o no, en el caso de que el trámite sea ingresado por las Fuerzas Armadas, no se solicitara estos campos.
- Se firma la forma.
- Se solicita un número de trámite.

III. M04-P01-01-02 Afiliación dependientes de pasivos

Recepción e ingreso de documentos (Secretaria General)

Las diferentes fuerzas: Aérea, Terrestre, Marina; o el Ministerio de Defensa envían: Orden General, Hoja de Vida Militar; documentos en el que se pública la fecha en que el personal ha sido dado de Alta, dependientes (cónyuge, hijo, padres) en algunas de las fuerzas. Estas órdenes generales son receptadas en Secretaria General, en donde se registra dicha documentación en Sistema Informático.

En algunos casos las Ordenes Generales de: Marina, Fuerza Terrestre y Ministerial se la puede obtener de la página Web, las mismas tienen la siguiente información:

- Altas Militares
- Cónyuge
- Hijos
- Padres
- Bajas Militares
- Pase a Militar
- Salida de Militar
- Disponibilidad
- Ascensos

- Insubsistencia
- Rectificación de datos

Para el proceso de **Afiliación de Dependientes de Pasivos** la información relevante de las órdenes generales y hoja de vida militar es: Nombre de Titular, Cónyuge, Hijos, Padres.

- Ingresar y registrar en Sistema XNEAR los datos necesarios para un correcto seguimiento del trámite, los datos registrados son: Remitente, Fecha de Ingreso, descripción del trámite ingresado.
- El paso siguiente es grabar el trámite en Sistema XNEAR, acto seguido el sistema despliega número de trámite en pantalla de computador.
- El número de trámite desplegado en la pantalla del computador sirve para registrar dicho número en documento pre-impreso denominado formato para ingreso de documentación externa, el mismo que será adjuntado al memo de ingreso de la documentación.
- Finalmente toda la documentación ingresada es entregada a cada uno de los responsables inmediatamente después que fue registrado dicho trámite.

Verificación y Revisión de trámites en relación afiliación (Dirección de Seguros Previsionales)

- Una vez recibida la documentación, el Director de Seguros Previsionales, analizará dichos documentos y llevará un estadístico de solicitudes ingresadas por cada una de las agencias además de realizar un monitoreo continúo del trámite solicitado por el cliente a través del DAM.
- En el caso de haber solicitudes que no estén debidamente sustentada con documentos de respaldo se procederá a colocar en estado de ESPERA y se excluirá del proceso de afiliación, además se comunicara a Jefatura de

Afiliación y Cotización para que se envíe la documentación correspondiente con los debidos problemas a las diferentes fuerzas con el fin de que solucionen este inconveniente.

- De darse el caso de que los reportes en relación a solicitudes de afiliación de las diferentes agencias no tengan los documentos de sustento, es necesario que este inconveniente se comunique a Jefatura de Afiliación y Cotización para que sean ellos los encargados de comunicarse con las diferentes Jefaturas de Atención al Cliente de las Agencias, a fin de que, rectifiquen ó ratifiquen el problema encontrado.

***Evaluación las condiciones de trámite* (Jefatura de Afiliación y Cotización)**

En esta etapa las solicitudes de afiliación son evaluadas para determinar las condiciones que tiene la petición de afiliación, para finalmente delegar trámite a Revisor – Liquidador Afiliación Dependientes de Pasivos y Derechohabientes.

- El responsable de Jefatura de Afiliación y Cotización revisa la información y evalúa el tipo de afiliación que puede ser:
    - Afiliación Dependientes de Pasivos
    - Afiliación Causante, cuando el Militar ha fallecido y cualquiera de sus beneficiarios optan por la afiliación.
- Direccionar trámite a Revisor – Liquidador Afiliación Dependientes de Pasivos y Derechohabientes, con firma de responsabilidad y fecha de entrega de documentos.

***Analizar y Cargar la Información en Sistema Informático* (Revisor – Liquidador Afiliación Dependientes y Derechohabientes)**

- Receptar solicitud y documentos de respaldo proveniente de usuario Jefatura de Afiliación y Cotización.
- Ingresar en Modulo de Afiliación de Sistema Informático y cargar datos personales de titular militar.
- Concatenar información física de dependientes y titular con datos de Modulo de Afiliación y Cotización de Sistema Informático.
- Generar reporte de inconsistencia de datos cuando información de sistema es diferente a los documentos de respaldo. Entregar estos reportes con toda la documentación de respaldo a Secretaria General para envío a proveedor de información de las distintas Fuerzas y/o Ministerio de Defensa.
- Registrar afiliación Dependientes de militar pasivo. La actualización de datos solo se lo puede realizar hasta el 22 de cada mes, debido al hecho de que este procedimiento afecta a la base de datos de: Nómina, Crédito, Pensiones.
- Registrar en el Sistema BPM los trámites realizados en el Modulo de Afiliación y Cotización del Sistema Informático.
- Entregar a usuario responsable de archivo y custodia de documentos de Seguros Previsionales, todos los documentos que fueron necesarios para el registro del trámite de afiliación dependientes.

IV. M04-P01-01-02-A Afiliación dependientes de pasivos (Ventanilla de atención al cliente)

En algunos casos el militar afiliado en servicio pasivo, puede solicitar la afiliación de sus dependientes por múltiples motivos; para este caso la persona antes mencionada puede realizar el trámite en las ventanillas de atención al cliente de cualquiera de las agencias de todo el país. Los usuarios de las diferentes Ventanillas de Atención al Cliente tienen acceso al Módulo de Afiliación y Cotización del Sistema Informático, con excepción de: registro de fallecimiento de militar, actualización de datos del militar en servicio activo, derechohabientes. Para esto el

usuario de Ventanilla de Atención a cliente de las diferentes agencias de todo el país deberá realizar los siguientes procedimientos:

- Recibir toda la documentación necesaria descrita en el apartado **V. Políticas Generales – Entrega de Documentos**, de este documento. Para empezar este trámite es necesario que el militar en servicio pasivo, pida a la fuerza que pertenece la **Hoja de Vida Militar** en la que debe constar los dependientes directos de dicha persona.
- Revisar toda la documentación entregada tomando en consideración lo descrito en el apartado **V. Políticas Generales – Verificación de Documentos**, de este documento.
- Ingresar en Modulo de Afiliación y Cotización de Sistema Informático y registrar datos de militar en servicio pasivo.

Para el registro de datos en Modulo de Afiliación de Sistema Informático se debe tomar en cuenta las siguientes observaciones:

Escenarios:

- Se identifica quien está solicitando la afiliación: (Titular, Dependiente, Fuerzas Armadas, Otros).
- Se ingresa la cedula del militar*:* Continúa a Pedir Documentos.
- Se debe seleccionar la actividad a realizar.
- Se verifican los requisitos para la actividad seleccionada.
- Se ingresa los datos del solicitante, sea este el militar o no, en el caso de que el trámite sea ingresado por las Fuerzas Armadas, no se solicitara estos campos.
- Se firma la forma.
- Se solicita un número de trámite.

Formas:

Forma Principal*:* Se ingresa el número de cedula del militar, se debe seleccionar la prestación a realizar.

Requisitos: Se debe seleccionar todo los documentos que el solicitante presente de acuerdo a la lista presentada.

Pedir No Trámite: Se identifica el número de trámite que se asignó a este.

Campos:

El campo de cedula debe ser numérico y contener un número valido.

Los campos de teléfono deben tener el formato código de provincia entre paréntesis y luego el número de teléfono de 7 dígitos Ej.: (02)2532398

Los campos de replegables o combos deben ser seleccionados si estos son obligatorios.

Seguridades:

El retorno debe estar deshabilitado

El envió de la forma debe estar deshabilitado hasta seleccionar los campos requeridos y solicitar un número para el trámite.

Una vez asignado el número de trámite no se debe permitir realizar cambios en la forma.

No debe dejar enviar sin la firma al momento de firmar, debe aparecer el nombre de la persona debajo de la firma.

Este paso debe estar asignado a la persona que sea la encargada del ingreso de trámites.

- Verificar datos de titular con información de Modulo de Afiliación y Cotización de Sistema Informático.
- En el caso que algún documento entregado no esté de acuerdo a las políticas establecidas se le comunica al afiliado cual es el inconveniente para que lo solucione
- Si el Afiliado cumple con los requisitos establecidos se ingresa en el sistema la información requerida y registrar afiliación de dependientes.
- Generar reporte de carga correctos, con el fin de tener un historial de todos los trámites atendidos.
- Registrar en el Sistema BPM los trámites realizados en el Modulo de Afiliación y Cotización del Sistema Informático. Solo para usuarios de Ventanilla de Atención al Cliente de ISSFA-Quito.

Entregar a usuario responsable de archivo y custodia de documentos de Seguros Previsionales, todos los documentos que fueron necesarios para el registro del trámite de afiliación. El Revisor - Liquidador debe, disponer de los siguientes documentos para entregarlos a responsable de archivo y custodia de documentos:

- **Reporte detallado de los registros de afiliación**, reporte resumen en el cual consta el número de afiliaciones que fueron realizadas en el período al que corresponde dicho reporte. Con la correspondiente documentación de respaldo de cada trámite.
- **Reporte de Novedades Solucionadas** según tipo de afiliación
- **Reporte de carga de información por cada fuerza,** resumen de todos las afiliaciones ingresadas en módulo de afiliación en sistema informático; mensualmente.

Si el trámite fue efectivizado en las Ventanillas de Atención al Cliente de la ISSFA – Quito, el Jefe de Atención al cliente deberá realizar las siguientes actividades:

Remitirá diariamente a la Dirección de Seguros Previsionales, hasta las 16h00 de cada día la siguiente información:

- **Informe de solicitudes ingresadas**, certificando que la información ha sido analizada revisada e ingresada correctamente por el usuario de ventanilla de atención al cliente, este documento debe estar firmado por la Jefatura de Servicio al Cliente.
- **Listado con las solicitudes de afiliación ingresadas**, depuradas, corregidas, selladas y firmadas por cada Afiliado.

Si el ingreso de información para afiliación ha sido efectivizada en cualquiera de las agencias fuera de Quito, es necesario que el Jefe de Servicio al Cliente genere reportes de solicitudes ingresadas, las mismas que deben ser enviadas a Seguros Previsionales ISSFA-Quito, adjuntando los documentos de respaldo para que en dicha unidad se pueda depurar la base de datos original y evitar errores posteriores. Este envío de reportes y listado de solicitudes ingresadas debe hacerse cada 15 días para actualizar continuamente la BDD (Base de datos).

V. M04-P01-01-03 Afiliación por orden judicial

Recepción e ingreso de documentos ***(Ventanilla de Atención al Cliente / Agencias)***

- Recibir toda la documentación necesaria descrita en el apartado **V. Políticas Generales – Entrega de Documentos**, de este documento. Para empezar este

trámite es necesario que exista una **Orden Judicial** emitida por alguno de los juzgados del medio.

- Revisar toda la documentación entregada tomando en consideración lo descrito en el apartado **V. Políticas Generales – Verificación de Documentos**, de este documento.
- Si el Afiliado cumple con los requisitos establecidos se ingresa en el Modulo de Afiliación y Cotización del Sistema Informático la información requerida y se genera reportes de afiliación.
- Enviar reporte de afiliación y documentos de respaldo a usuario de Nómina.

El responsable de nómina deberá realizar las siguientes actividades:

- Verificar si el menor está afiliado.
- Ingresar retención en Modulo Informático.
- Notificar dependientes no afiliados a usuario Revisor – Liquidador Activos y Dependientes.

Analizar y Cargar la Información en Sistema Informático **(Revisor – Liquidador Afiliación Activos y Dependientes)**

- Receptar notificación y documentos de respaldo provenientes de Nómina.
- Ingresar en Modulo de Afiliación de Sistema Informático y registrar afiliación dependiente.
- Enviar documentación a Nómina para que se proceda a realizar la retención económica.
- Registrar en el Sistema BPM los trámites realizados en el Modulo de Afiliación y Cotización del Sistema Informático.

VI. M04-P01-02-01 Actualización de datos (Masiva activos)

OBJETIVO

Mantener actualizada la información del personal militar en servicio activo y pasivo, para que sea considerado como afiliado del Instituto de Seguridad Social de las Fuerzas Armadas, a fin de que pueda acceder a las prestaciones y servicios sociales que otorga el ISSFA.

ALCANCE

El presente procedimiento está dirigido a todo el personal militar en servicio activo y pasivo, de las Fuerzas Armadas; así como también a sus dependientes.

- La actualización de los datos del personal militar en servicio activo se realizará de manera constante por parte del Departamento de Afiliación y Cotización; cada vez que se emita desde el MIDENA o desde las Fuerzas (Terrestre, Naval y Aérea) las Órdenes Ministeriales u Ordenes Generales respectivamente.
- El Departamento de Afiliación y Cotización es el responsable de mantener actualizada la información del personal militar en servicio activo en el sistema informático; es el único organismo autorizado para efectuar cambios o modificaciones en la información individual de los afiliados; cualquier modificación externa será castigada de acuerdo a las normas establecidas para el efecto.
- Es responsabilidad del Departamento de Afiliación y Cotización el cruzar información con los organismos de Fuerzas Armadas, que manejan datos del personal en servicio activo (Fuerza Terrestre, Naval y Aérea; Ministerio de Defensa Nacional); con la finalidad de unificar la información de los afiliados del Sistema de Seguridad Social de Fuerzas Armadas.

VII. M04-P01-02-02 Actualización de datos manual (Activos y pasivos)

En algunos casos el titular militar afiliado activo o pasivo, puede solicitar la actualización de datos de él y/o sus dependientes por múltiples motivos; para este caso la persona antes mencionada puede realizar el trámite en las ventanillas de atención al cliente de cualquiera de las agencias de todo el país. Para este propósito el usuario de Ventanilla de Atención al cliente de las diferentes agencias de todo el país deberá realizar los siguientes procedimientos:

- Recibir toda la documentación necesaria descrita en el apartado **V. Políticas Generales – Entrega de Documentos**, de este documento; además deberá cumplir con los requisitos descritos en el Anexo 1. según sea el caso.

- Revisar toda la documentación entregada tomando en consideración lo descrito en el apartado **V. Políticas Generales – Verificación de Documentos**, de este documento.
- Si el titular activo y/o sus dependientes se encuentran habilitados para actualizar la información; es necesario ingresar en Modulo de Afiliación y Cotización de Sistema Informático y registrar todos los datos. Para el registro de datos en Modulo de Afiliación de Sistema Informático se debe tomar en cuenta las siguientes observaciones:

Escenarios:

- Se identifica quien está solicitando la actualización de datos: (Titular, Dependiente, Fuerzas Armadas, Otros).

- Se ingresa la cedula del militar*:* Continúa a Pedir Documentos.
- Se debe seleccionar la actividad a realizar.
- Se verifican los datos para la actividad seleccionada.
- Se ingresa los datos del solicitante, sea este el militar o no, en el caso de que el trámite sea ingresado por las Fuerzas Armadas, no se solicitara estos campos.
- Se firma la forma.
- Se solicita un número de trámite.

VIII. M04-P01-02-03 Actualización de datos para seguros

Recepción e ingreso de documentos ***(Ventanilla de Atención al Cliente / Agencias)***

En algunos casos el titular militar afiliado activo o pasivo, puede solicitar la actualización de datos para seguros de él y/o sus dependientes por múltiples motivos; para este caso la persona antes mencionada puede realizar el trámite en las ventanillas de atención al cliente de cualquiera de las agencias de todo el país ó en su defecto presentar toda la documentación necesario en la Fuerza a la que pertenece. Para cualquiera de los dos casos el usuario de Ventanilla de Atención a cliente de las diferentes agencias de todo el país deberá realizar los siguientes procedimientos

- Recibir toda la documentación necesaria descrita en el apartado **V. Políticas Generales – Entrega de Documentos**, de este documento; además deberá cumplir con los requisitos descritos según sea el caso.
- Revisar toda la documentación entregada tomando en consideración lo descrito en el apartado **V. Políticas Generales – Verificación de Documentos**, de este documento.

- Registrar trámite en Sistema Informático DAM y enviar documentación a Dirección de Seguros Previsionales. inmediatamente.

Verificación y Revisión de trámites en relación Actualización de Datos para Seguros (Dirección de Seguros Previsionales)

- Una vez recibida la documentación, el Director de Seguros Previsionales, analizará dichos documentos y llevará un registro de solicitudes ingresadas por cada una de las agencias además de realizar un control continuo del trámite solicitado por el cliente a través del DAM.
- En el caso de haber solicitudes que no estén debidamente sustentada con documentos de respaldo se procederá a colocar en estado de ESPERA y se excluirá del proceso de actualización de datos, además se comunicara a Jefatura de Afiliación y Cotización para que se envíe la documentación correspondiente con los debidos problemas a las diferentes fuerzas con el fin de que solucionen este inconveniente.
- De darse el caso de que los reportes en relación a solicitudes de actualización de datos de las diferentes agencias no tengan los documentos de sustento, es necesario que este inconveniente se comunique a Jefatura de Afiliación y Cotización para que sean ellos los encargados de comunicarse con las diferentes Jefaturas de Atención al Cliente de las Agencias, a fin de que, rectifiquen ó ratifiquen el problema encontrado.

Evaluación las condiciones de trámite (Jefatura de Afiliación y Cotización)

En esta etapa las solicitudes de actualización de datos son evaluadas para determinar las condiciones que tiene la petición, para finalmente delegar trámite a Revisor – Liquidador Actualización de Datos.

El responsable de Jefatura de Afiliación y Cotización revisa la información y evalúa el tipo de afiliación que puede ser:

- Actualización de Datos Manual Activos
- Actualización de Datos Manual Pasivos
- Actualización de Datos para Seguros.
- Actualización de Datos ISSFA.

Direccionar trámite a Revisor – Liquidador Actualización de Datos, con firma de responsabilidad y fecha de entrega de documentos.

Analizar y Cargar la Información en Sistema Informático **(Revisor – Liquidador Actualización de Datos para Seguros)**

- Receptar solicitud y documentos de respaldo proveniente de usuario Jefatura de Afiliación y Cotización.
- Verificar documentos de respaldo y actualizar base de datos en Modulo de Afiliación de Sistema Informático.
- Si la actualización de datos no necesita certificado de aportes, es necesario realizar los siguientes procedimientos:

    - La determinación de Potenciales Derechos
    - Otorgamiento de Derechos
    - Actualizar la base de datos del Módulo de Afiliación y Cotización del Sistema Informático, según acuerdo.
    - Pago de Beneficios.

Para el caso de que la actualización de datos necesita certificado de aportes, el usuario Revisor- Liquidador necesita seguir los siguientes procedimientos:

- Generar certificación de aportes y direccionarlos a Jefatura de Afiliación y Cotización para que se revise y sumille dicho documento.
- Al mismo tiempo el usuario Revisor – Liquidador, debe registrar el trámite en el Sistema DAM para tener un historial de los trámites realizados en esta dependencia.
- Entregar a usuario responsable de archivo y custodia de documentos de Seguros Previsionales, todos los documentos que fueron necesarios para la Actualización de Datos para Seguros.

IX. M04-P01-02-04 Actualización de datos ISSFA

El usuario Revisor – Liquidador necesita realizar los siguientes procedimientos para Actualizar los Datos que tienen relación al ISSFA:

- Procesar y Validar los documentos de acuerdo a los datos del Módulo de Afiliación del Sistema Informático.
- Generar reportes de suspensión, finalización.
- Realizar el proceso de Determinación de Potenciales Derechos.
- Ejecutar el Proceso de Otorgamiento de Derechos.
- Actualizar los datos según Acuerdo.
- Paralelamente se debe procesar la información para mantenimiento de la Base de Datos.
- Generar reportes para control de trámite

X. M04-P01-03-01 Registro de aportes masivo

OBJETIVO:

Recibir y validar que los aportes individuales y patronales recibidos desde las Fuerzas sean fidedignos.

DESCRIPCIÓN

Recibir información de aportes desde las Fuerzas. La Secretaria General del ISSFA recepta la inf0rmación de aportes desde las Fuerzas (Terrestre, Naval y Aérea), remitida a través de medios impresos, magnéticos (archivo plano). "ACT. PRINCIPAL" y resumen clasificado por numéricos de la información "ACT. PRINCIPAL". A su vez esta información se envía al Departamento de Cotización de la Dirección de Seguros Previsionales del ISSFA para su posterior ingreso al sistema.

Revisar la veracidad de la información. El liquidador de Prestaciones verificará que la información no haya sido adulterada para el efecto revisará que la información recibida desde las fuerzas no haya sufrido cambios, alteraciones o distorsiones, con la finalidad de que la información esté completamente depurada. Para el efecto, comparará la información impresa con la de lo archivos magnéticos verificando que tenga la autenticidad en el documento (Firma del Director de Personal de la Fuerza y/o Jefe de Remuneraciones y sello de la Dirección de personal de la respectiva Fuerza).

Validación de información. El liquidador de Prestaciones deberá realizar las siguientes actividades:

- Verificar que la apertura del archivo que proviene de la Fuerza, (es decir que el archivo sea idóneo), en la unidad personal del usuario (PC).
- Trasladar la información desde el archivo que proviene de la Fuerza, a:

    - Disco Local del usuario (PC), a manera de respaldo.
    - Servidores del ISSFA (SERVER, FUERZAS)

- Aperturar la información que proviene de la Fuerza, en formato *.xls.
- Validar la información, esto conlleva en cuadrar el número de afiliados con el aporte global (actividad personal-manual de validación). Imprimir resúmenes validados.
- Contar y validad, las posiciones del archivo que proviene de la fuerza, (en el formato plano *.txt)

Ingreso de las aportaciones al Sistema._ Una vez verificada la idoneidad de la información y recibido al depósito, el Liquidador de Prestaciones debe cargar automáticamente el archivo que proviene de la Fuerza, a la **Forma de Cuenta Individual, (**Sistema Informático**),** y verificar los datos en el sistema, en sus proporciones decimales y procentuales, en los respectivos fondos. De ser necesario corregir los errores provocados por inconsistencias de datos de los afiliados.

Las aportaciones a ser ingresadas son las siguientes:

- Aporte Patronal
- Aporte Individual
- Fondos de reserva

Los datos de las aportaciones sirven para alimentar la cuenta individual y así acceder el afiliado en servicio activo a los seguros correspondientes.

Efectuar el Control de Calidad de las Aportaciones.- El jefe del Departamento de Cotizaciones una vez terminado el ingreso de información de aportaciones, efectuará el control de calidad de las aportaciones en el sistemas informático; este control le sirve para depurar la información. Esta información será efectivizada cuando la Dirección Económico Financiera certifique que la Fuerza ha realizado el respectivo traspaso o depósito de fondos a la cuenta del ISSFA, una vez

realizados los asientos correspondientes. Finalmente se debe realizar las siguientes actividades:

Archivar la Información.- El liquidador de Prestaciones debe archivar la información recibida desde las Fuerzas en sus diferentes medios (impresos o magnéticos) con la finalidad de mantener un archivo físico de la información, así como el respaldo respectivo. La información documental debe ser archivada de acuerdo a las distintas técnicas de archivo, según las necesidades del Departamento de Cotización y de la Institución en general.

Además del archivo físico el usuario encargado de este proceso debe ingresar el trámite en el Sistema Documental DAM e IDM.

XI. M04-P01-03-02 Diferencia de aportaciones

OBJETIVO:

Recaudar los faltantes de las aportaciones a fin de que se generen las prestaciones reales en beneficio del Afiliado.

DESCRIPCIÓN:

Recibir los requerimiento de las Fuerzas.- El Liquidador de Prestaciones del Departamento de Cotización, receptará el oficio de requerimiento de diferencia de aportaciones por parte las Fuerzas, el cual le es entregado en la ventanilla de Recepción de Documentos; este requerimiento lo puede presentar en las mismas ventanillas de Servicio al cliente en las Agencias o en el Departamento de Cotización.

Cálculo de Aportes Faltantes.- El Liquidador de Prestaciones del Departamento de Cotización; debe detectar los problemas existentes con las

aportaciones individuales del personal militar en servicio activo. La detección de errores en las aportaciones son a consecuencia de la revisión de órdenes generales en la que les promueven al inmediato grado superior con fecha anterior a la actual, o les aportan cierto tiempo después de la fecha anterior a la actual, o les aportan cierto tiempo después de la fecha de alta. Para el cálculo de estos aportes referirse al Manual de Procedimientos PR3-P01-01.

Actualización, mantenimiento de Variables.- El estadístico Actuarial y Actuario deberán mantener un estricto control permanente de todas las variables que afecten al cálculo de aportes faltantes, de existir cambios deberán retroalimentar continuamente a la Jefatura de Cotización de dichas variaciones para que estos cálculos sean los que más se ajusten a la realidad del militar.

Notificación a la Fuerza._ El liquidador de Prestaciones del Departamento de Cotización será el encargado de elaborar un oficio dirigido al Director Personal de la Fuerza al cual adjuntará él estudia actuarial con la finalidad de que la Fuerza (Terrestre, Naval, Aérea) efectúen el pago de las aportaciones del personal afectado.

Se remite el cuadro elaborado por el departamento Actuarial con él o oficio en el que se indica el valor se debe pagar y la fecha máximo para recaudar dicho valor, en cado de no pagar en dicha fecha tope se hace el cálculo respectivo.

Para esto es necesario que este documento sea registrado en el Sistema documental DAM e IDM.

Notificar valores recibidos.- Es responsabilidad de Tesorería realizar el seguimiento de pago de los valores adecuados por parte de las diferentes fuerzas.

Registro de Aportes Faltantes-._ Una vez recibirá la información de Tesorería, el Liquidador de Prestaciones del Departamento de Cotización registra el periodo

faltante de aportes (fecha de inicio de faltante y fecha final de faltante), adicionalmente se deben registrar las variables del cálculo (haber militar, grado, tiempo de servicio).

Con estos datos se genera un archivo de aportes faltantes por cada fondo y por cada mes con su respectiva fecha de depósito, a ser ingresados en la cuenta individual del afiliado en el sistema informático. Valida que el módulo tenga el total de registros, fecha de depósito y mes que corresponde.

Validados estos datos, procede a realizar el registro de aportes faltantes en la cuenta individual.

Generación de asiento contable.- Es responsabilidad de Contabilidad el realizar el asiento contable de los valores recaudados provenientes de las distintas fuerzas, como consecuencia del pago de aportes faltantes.

XII. M04-P01-03-03 Devolución de fondos de reserva

OBJETIVO:

Garantizar la gestión oportuna de las transacciones de los fondos de reserva a los Afiliados.

DESCRIPCIÓN

Recepción de Información.- El Liquidador de Prestaciones del Departamento de Cotización para ejecutar esta actividad debe realizar las siguientes tareas:

- Receptar el archivo de Fondos de Reserva y resumen que proviene de la Fuerza, en archivo plano, (físico/sistema –mail).

Cargar las aportaciones al Sistema.- El liquidador de Prestaciones del Departamento de Cotización, ingresa las aportaciones al fondo de reserva al sistema informático con la finalidad de validar la información magnética remitida por las Fuerzas: Terrestres, Naval, Aérea.

Validar Información.- El Liquidador de Prestaciones del Departamento de Cotización, debe realizar las siguientes tareas para esta actividad:

- Verificar la apertura del archivo que proviene de la Fuerza, (es decir que el archivo sea idónea), en la unidad personal del osario (PC).
- Trasladar la información desde el archivo que proviene de la Fuerza, a:

  Unidad personal de usuario (PC), a manera de respaldo,
  Servidores del ISSFA (SERVER, FIERZAS).
  Aperturar la información que proviene de la Fuerza, en formato .xls
  Validar la información, esto conlleva en cuadrar el número de afiliados con el aporte global (actividad personal – manual de validación).
  Imprimir resúmenes validados.

- Contar y validar, las posiciones del archivo que proviene de la fuerza, (en el formato plano .txt)
- Cargar automáticamente el archivo que proviene de la Fuerza, a la Forma de cuenta individual, (SISTEMA INFORMÁTICO), y verificar los datos en el sistema, en sus proporciones decimales y porcentuales, en los respectivos fondos.

Corregir los errores.- Cargados los datos en el sistema, el Liquidador de Prestaciones efectuará el control de calidad de la información, con la finalidad de corregir errores y tener el sistema depurado.

Verificar las aportaciones.- Efectuando el control de calidad, el Jefe del Departamento de Cotizaciones, verifica las aportaciones en el sistema informático mediante una revisión al muestreo de grados y aportes, se valida al grado del aporte anterior y el grado del nuevo aporte la variación del aporte anterior con la relación al aporte actual.

Capitalizar las Aportaciones.- El sistema registra uno a uno los aportes individuales de cada afiliado, al receptar el pago de la Fuerza, el Liquidador de Prestaciones del Departamento de Cotización procesa " ***capitalización de cuenta individual"*** (en el sistema), donde el Fondo acumulado se convierte en ahorro disponible para el afiliado en caso de no tener deuda con créditos de carácter hipotecarios.

> Finalmente para completar la ejecución de esta actividad se debe obtener reporte de los afiliados que han cumplido las 36 aportaciones.

Abonos a Créditos.- Los créditos se abandonarán en forma automática o individual sea para saldar por medio de Fondos de Reserva, de acuerdo a las siguientes prioridades:

- Hipotecarios
- Quirografarios

La prioridad estará dada por el Departamento de Crédito. En caso de existir cualquier cuenta pendiente (es decir en mora), se cancelará esta primero no importa su orden dentro de los parámetros de importancia.

Generar las devoluciones.- Actualizada la información relacionada con los fondos de reserva en el sistema informática, el Liquidador de Prestaciones del Departamento de Cotización, procede a generar las devoluciones para cada cuenta o

área específica; de acuerdo a lo que dictamina el Reglamento del Fondo de Reserva del Instituto de Seguridad Social de las Fuerzas Armadas. Estas devoluciones se hacen de acuerdo a las siguientes características:

Devolución de Fondos de Reserva

Afiliados Activos, con el requisito de cumplir 36 aportaciones, se procede a la devolución de estas en forma masiva y de ser el caso dejarlo para que ganen un interés del 5% anual.

Afiliados Activos, con el requisito de cumplir las condiciones de devolución anticipada, se procede a la devolución en forma individual según el instructivo para Devoluciones Anticipadas por Situaciones Apremiantes para Fondos de Reserva y Crédito.

Afiliados Pasivos, transferencia de los saldos de fondos de reserva a la pensión.

Indemnizaciones Globales.- Los militares que pidieren la baja sin cumplir el tiempo de servicio para la obtención del beneficio de Cesantía y Pensión, según sea el caso.

Traspaso de Fondos de reserva a **FONIFA.-** El afiliado podrá dirigir sus fondos acumulados al FONIFA, para que estos sean depositados en la cuenta de ahorros, donde su dinero ganará intereses y se acumularán para ajustar la cuota básica para un préstamo hipotecario.

Abonos a Créditos Hipotecarios._ Todo el personal que posee créditos de carácter quirografario podrá abonar a pedido personal según lo que establece el Reglamento de Fondos de Reserva.

Notificar a las áreas involucradas y sacar reportes.- El Liquidador de Prestaciones del Departamento de Cotización, pone en conocimiento que la información de fondos de reserva del personal militar en servicio activo ha sido procesada y han sido generadas las devoluciones a cada área involucrada, para finalizar se debe sacar los reportes que servirán para el depósito y control de las auditorías respectivas.

Archivar la Información.- El liquidador de Prestaciones del Departamento de Cotización, archiva la información resultante del proceso en medios impresos. El archivo debe ser estructurado de acuerdo al tipo de devolución efectuado y en orden cronológico.

XIII. M04-P01-04 Certificación de aportes

OBJETIVO:

Entregar la certificación de aportes para Seguros y Afiliado conforme la información registrada en el Instituto.

DESCRIPCIÓN:

Solicitud de certificación.- El afiliado para sacar la certificación de tiempos de aportes se acerca a Cotizaciones del ISSFA con los siguientes requisitos.

- Solicitud del afiliado.
- Copia de la cédula.
- Liquidación de tiempo de servicio otorgado por Movilización.

Recepción de documentación.- Los técnicos de Servicio al Cliente, Jefes u oficinistas de Agencias a nivel nacional efectuarán las siguientes tareas en esta actividad.

Receptar del afiliado la solicitud de certificación de aportes con documentos de respaldo.

Revisar la documentación y registrar trámite en Sistemas Documental DAM e IDM.

Direccionar la solicitud y documentos de respaldo al Departamento de Cotización.

Verificación de Tiempo de Servicio.- El Liquidador de Prestaciones del Departamento de Cotización efectúa las siguientes tareas:

- Ingresa los datos del afiliado (Nombres, Número de Cédula) en el sistema informático a manera de consulta para verificar el tiempo de servicio con la documentación de respaldo.
- Verifica la cuenta individual con respecto al tiempo de servicio y genera la certificación de aportes en el sistema informático.
- Gestiona la legalización de la certificación de aportes al Jefe del Departamento de Cotización.

Nota.- Para certificación de aportes es necesario realizar las siguientes consideraciones:

Certificado de Aportes al Afiliado: Con los siguientes datos; Nombres, Celular, N.- Afiliación, Grado, Fuerza, Categoría, Enunciado del artículo 112 de la Ley del ISSFA, que textualmente dice "*El tiempo de servicio activo y efectivo del militar en las Fuerzas Armadas, se computará a partir de la fecha de su promoción como oficial o tropa, hasta la fecha de su baja, publicadas en las órdenes generales correspondientes".* Además de Tiempo de servicio, valorado en años, meses y días (cálculo por # de meses, pasado de 21 días, se considera un mes).

Antigüedad, para la posesión de un cargo en el sector público, con los siguientes datos: Nombres, Cédula, N# Afiliación, Grado, Fuerza, N# Patronal, Categoría, Tiempo de servicio, desde las fechas de alta y baja del afiliado.

Certificado para Seguros, que genera el certificado con las siguientes datos: Nombres, Cédula N# Afiliación, Grado, Fuerza N# Patronal, Categoría, tiempo de servicio, para lo cual se procede de la siguiente manera:

- Buscar la tarjeta de aportes sociales individuales (IESS), en el archivo físico.
- Añadir formato de control de aportes (Formato Excel)
- Validar la información de la carpeta individual de cada afiliado, con el sistema dentro de la ***Forma de cuenta individual.***

Certificados para Indemnización Global

Se genera el certificado con los siguientes datos: Nombres, Cédula, N.- de Afiliación, Grado, Fuerza, Categoría, para lo cual se procede de la siguiente manera:

- Buscar la tarjeta de aportes sociales individuales(IESS), archivo físico,
- Validar la información de la carpeta individual de cada afiliado, con el sistema dentro de la ***Forma de cuenta individual.***
- Se genera la liquidación de los fondos según el caso.

3.1.2. Gestión de prestaciones

Figura 9: Gestión de Prestaciones.

Fuente: Los Autores

I. M04-P03-01 Seguro de cesantía

OBJETIVO

Normar las actividades para el otorgamiento del Seguro de Cesantía el cual tiene como finalidad proteger al militar que se separa del servicio activo mediante la baja y acredita en la Institución armada un mínimo de veinte años de servicio activo y efectivo, sin abonos por tiempo de servicio ni tiempo de servicio civil.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

- El militar en servicio activo;
- El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,
- Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO IV. DEL SEGURO DE CESANTÍA Art. 50, textualmente establece.- En caso de fallecimiento del militar con derecho a cesantía, recibirán esta prestación:

La viuda, viudo o persona que mantuvo unión libre, estable y monogámica con el causante por un valor equivalente al cincuenta por ciento (50%) de la Cesantía;

Los hijos del causante por un valor equivalente al cincuenta por ciento (50%) de la Cesantía, repartido en partes iguales. En caso de no haber descendencia,

la viuda, viudo o persona que mantuvo unión libre, estable y monogámica percibirá el valor total de la Cesantía;

A falta de viuda, viudo o persona que mantuvo unión libre, estable y monogámica, el valor total de la Cesantía se prorrateará en partes iguales entre los hijos;

A falta de los anteriores el valor total de la Cesantía se repartirá por partes iguales entre los padres;

A falta de padres la Cesantía se entregará a los nietos del militar, por partes iguales; y en ausencia de nietos, el valor de la Cesantía se revertirá a favor del ISSFA.

El hijo adoptivo tiene igual derecho que los demás hijos, según lo establecido en la presente Ley.

II. M04-P03-02 Pensión de retiro, discapacidad, invalidez

OBJETIVO

Normar las actividades para el otorgamiento de la Pensión de Retiro Invalidez y Muerte el cual tiene como finalidad pagar una pensión vitalicia que garantiza al asegurado un ingreso oportuno y de cuantía suficiente que le permita mantener la estabilidad de su situación socio-económica.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

El Reglamento del Seguro de Retiro, Invalidez y Muerte del Instituto de Seguridad Social de las Fuerzas Armadas, en su CAPITULO II. DE LA COBERTURA Art. 5, textualmente establece.- El Seguro de Retiro se otorga al militar que acredita en la Institución Armada un mínimo de veinte años de servicio activo y efectivo y computado de acuerdo con el Art. 112 de la Ley.

III. M04-P03-03 Indemnización global

OBJETIVO

Normar las actividades para el otorgamiento de la indemnización global al militar que sin tener derecho a los seguros de Retiro y Cesantía se separa de la Institución y acredite un mínimo de cinco años de servicio activo y efectivo

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

- El militar en servicio activo;
- El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

- Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO II. DE LA INDEMNIZACIÓN GLOBAL Art. 82 y 83, textualmente establece.- El militar que se separe de la Institución, sin haber acreditado cinco años de servicio activo y efectivo, recibirá una indemnización global equivalente a la devolución de los aportes al Fondo de Vivienda y saldos del Fondo de Reserva capitalizados con un interés equivalente a la tasa actuarial.

En caso de muerte del asegurado, en cualquiera de las situaciones señaladas en los artículos anteriores, la indemnización global será entregada a sus derechohabientes en el orden de prelación y porcentajes establecidos en la presente Ley para el Seguro de Cesantía.

IV. M04-P03-04 Seguro de accidentes profesionales

OBJETIVO

Normar las actividades para el otorgamiento del Seguro de Accidentes Profesionales el cual tiene como finalidad entregar la prestación destinada a compensar el ingreso del militar que se incapacita por enfermedad o accidente profesional. Este seguro se hace efectivo mediante el pago de la indemnización de la discapacitación y de la pensión de discapacitación.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO VIII. DEL SEGURO DE ACCIDENTES PROFESIONALES Art. 65 y 67, textualmente establece.- Se calificará como discapacitado al militar en servicio activo que por efecto de accidente o enfermedad profesional se incapacita en actos del servicio o a consecuencia de los mismos, para desempeñar sus funciones profesionales habituales dentro de la Institución, después de haberse sometido al proceso de rehabilitación.

No tiene derecho a esta prestación el asegurado que por si o por interpuesta persona se prive la vida o se ocasione daño corporal.

M04-P03-05 Seguro de invalidez

OBJETIVO

Normar las actividades para el otorgamiento del Seguro de Invalidez el cual tiene como finalidad entregar la prestación al asegurado en servicio activo que se incapacita fuera de actos de servicio, por efecto de enfermedad común o accidente no profesional y que acredita por lo menos cinco años de servicio activo y efectivo en la Institución; esta prestación termina con la rehabilitación orgánica-funcional o con el fallecimiento del asegurado.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO II. DEL SEGURO DE INVALIDEZ Art. 19, textualmente establece.- El asegurado en servicio activo que se invalida sin haber cumplido veinte años de servicio y acredita un mínimo de cinco años de servicio activo y efectivo en la Institución, tiene derecho a una pensión equivalente al cuarenta por ciento (40%) del sueldo imponible vigente hasta la fecha de baja.

El asegurado no tiene derecho a pensión de invalidez cuando ésta sea consecuencia de la comisión de un delito tipificado en las leyes penales, por el cual el asegurado haya merecido sentencia condenatoria.

M04-P03-06 Seguro de vida

OBJETIVO

Normar las actividades para el otorgamiento del Seguro de Vida el cual tiene como finalidad entregar una prestación a los derechohabientes por la pérdida del ingreso familiar originada por el fallecimiento del militar en servicio activo, cuya cuantía se determina en la ley del ISSFA.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO VII. SEGURO DE VIDA Art. 59, textualmente establece.- El Seguro de Vida es obligatorio para el personal militar en servicio activo, aspirantes a oficiales, aspirantes a tropa y conscriptos; y, es potestativo para los militares en servicio pasivo con pensión de retiro, discapacitación o invalidez, previo el pago de la prima establecida en el Reglamento correspondiente.

M04-P03-07-A Seguro de mortuoria y gastos funerales (Pago a dependientes)

OBJETIVO

Normar las actividades para el otorgamiento de pagos por gastos funerales a personal militar activo el cual tiene como finalidad cubrir los servicios funerales, de culto, honras fúnebres y sepultura del asegurado.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO VI. DEL SEGURO DE MORTUORIA Art. 55, textualmente establece.- Tienen derecho a la Mortuoria:

La viuda o viudo;

La persona que mantuvo con el asegurado unión libre, estable y monogámica o que tuviere descendencia de dicha unión, siempre que los dos hubieren permanecido solteros durante su convivencia;

Los hijos menores de dieciocho años;

Los hijos mayores de dieciocho años incapacitados en forma total y permanente; y,

A falta de los anteriores, la madre; y en ausencia de ésta, el padre incapacitado para el trabajo y que carezca de medios de subsistencia.

La viuda, viudo o la persona con quien el asegurado mantuvo unión libre, estable y monogámica, tendrá derecho al doble de la cuota correspondiente a un hijo.

No tendrá derecho a Seguro de Mortuoria el cónyuge que a la fecha de fallecimiento del causante estuvo legalmente separado o simplemente separado por más de seis años, o cuando por sentencia judicial se estableciere que el potencial derechohabiente ha sido sindicado como autor, cómplice o encubridor de la muerte del causante.

Si el fallecido, militar en servicio activo, pensionista de Retiro, Discapacitación, Invalidez y Montepío, pensionista del Estado, aspirante a oficial o tropa y conscripto no dejaren derechohabientes y no hubieren deudos que se responsabilicen del sepelio, el ISSFA, a través de la Dirección de Bienestar Social, asumirá esta obligación e invertirá hasta la suma prevista para los gastos de funerales.

M04-P03-07-B Seguro de mortuoria y gastos funerales (Pago a terceros)

OBJETIVO

Normar las actividades para el otorgamiento de pagos por gastos funerales a personal militar pasivo el cual tiene como finalidad cubrir los servicios funerales, de culto, honras fúnebres y sepultura del asegurado.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO VI. DEL SEGURO DE MORTUORIA Art. 55, textualmente establece.- Tienen derecho a la Mortuoria:

La viuda o viudo;

La persona que mantuvo con el asegurado unión libre, estable y monogámica o que tuviere descendencia de dicha unión, siempre que los dos hubieren permanecido solteros durante su convivencia;

Los hijos menores de dieciocho años;

Los hijos mayores de dieciocho años incapacitados en forma total y permanente; y,

A falta de los anteriores, la madre; y en ausencia de ésta, el padre incapacitado para el trabajo y que carezca de medios de subsistencia.

La viuda, viudo o la persona con quien el asegurado mantuvo unión libre, estable y monogámica, tendrá derecho al doble de la cuota correspondiente a un hijo.

No tendrá derecho a Seguro de Mortuoria el cónyuge que a la fecha de fallecimiento del causante estuvo legalmente separado o simplemente separado por más de seis años, o cuando por sentencia judicial se estableciere que el potencial

derechohabiente ha sido sindicado como autor, cómplice o encubridor de la muerte del causante

M04-P03-08-A Seguro de montepío de activos

OBJETIVO

Normar las actividades para el otorgamiento del Seguro de Montepío Activos el cual tiene como finalidad entregar una pensión vitalicia a los derechohabientes del asegurado que fallece en servicio activo.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DEL SEGURO DE MUERTE Art. 31, textualmente establece.- Tienen derecho a pensión de montepío:

El viudo, la persona que mantuvo unión libre, estable y monogámica y los hijos menores de dieciocho años del asegurado fallecido;

Los hijos mayores de dieciocho años de edad incapacitados en forma total y permanente;

Los hijos solteros hasta los veinticinco años de edad, siempre que comprobaren anualmente hallarse estudiando en establecimientos reconocidos por el Estado y que no mantengan relación laboral.

El viudo incapacitado en forma total y permanente, que no goce de pensión alguna ni disponga de medios para subsistir. En este caso, tendrá los mismos derechos que se asignan a la viuda; y,

A falta de los derechohabientes mencionados en los literales anteriores, tendrá derecho la madre y a falta de ésta, el padre que carezca de medios para subsistir y esté incapacitado para el trabajo. En estos casos, la pensión de montepío será igual al cincuenta por ciento (50%) de la originada por el causante.

La viuda, viudo o conviviente tendrá derecho al doble de la pensión asignada a un hijo.

M04-P03-08-B Seguro de montepío de pasivos

OBJETIVO

Normar las actividades para el otorgamiento del Seguro de Montepío Pasivos el cual tiene como finalidad entregar una pensión vitalicia a los derechohabientes del asegurado que fallece en servicio pasivo, con pensión de retiro, discapacitación o invalidez.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DEL SEGURO DE MUERTE Art. 31, textualmente establece.- Tienen derecho a pensión de montepío:

El viudo, la persona que mantuvo unión libre, estable y monogámica y los hijos menores de dieciocho años del asegurado fallecido;

Los hijos mayores de dieciocho años de edad incapacitados en forma total y permanente;

Los hijos solteros hasta los veinticinco años de edad, siempre que comprobaren anualmente hallarse estudiando en establecimientos reconocidos por el Estado y que no mantengan relación laboral.

El viudo incapacitado en forma total y permanente, que no goce de pensión alguna ni disponga de medios para subsistir. En este caso, tendrá los mismos derechos que se asignan a la viuda; y,

A falta de los derechohabientes mencionados en los literales anteriores, tendrá derecho la madre y a falta de ésta, el padre que carezca de medios para subsistir y esté incapacitado para el trabajo. En estos casos, la pensión de montepío será igual al cincuenta por ciento (50%) de la originada por el causante.

La viuda, viudo o conviviente tendrá derecho al doble de la pensión asignada a un hijo.

M04-P03-09 Cancelación de Pensión (Fallecimiento y Pérdida de Derechos).

NO HAY INFORMACIÓN DEL PROCESO.

M04-P03-10 Revisión de pensión

OBJETIVO

Normar las actividades para la revisión de pensión el cual tiene como finalidad entregar una pensión vitalicia del asegurado que se separa del servicio activo de las Fuerzas Armadas mediante la baja, pensión que fue calculada de acuerdo a lo establecido en la Ley del ISSFA, artículo 21 del Capítulo I, Del Seguro de Retiro.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO I. DEL SEGURO DE RETIRO Art. 23, textualmente establece.- El asegurado que alcanzare el derecho a la pensión de retiro y hubiere acreditado en el IESS tiempos de servicio civiles antes de su afiliación al ISSFA, tendrán derecho a una mejora de su pensión de retiro, siempre que tales aportes hayan sido transferidos por el IESS al ISSFA.

Si los tiempos de servicio civiles los hubiere prestado con posterioridad a la obtención de la pensión de retiro, tendrá derecho a que el IESS le reconozca la mejora correspondiente.

En los dos casos, el valor de la mejora se calculará con sujeción al procedimiento establecido para el efecto, en los estatutos del IESS.

M04-P03-12-A Rehabilitación de pensión (Acrecimientos)

OBJETIVO

Normar las actividades para la redistribución de pensión (acrecimiento) a un grupo familiar, perceptor de pensión de montepío, al extinguirse el derecho de un beneficiario, su pensión acrecerá la de los demás en partes proporcionales y en relación a sus derechos de reparto inicial.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

El Reglamento de Retiro Invalidez y Muerte del Instituto de Seguridad Social de las Fuerzas Armadas, en el Artículo 55, CAPITULO II. DE LA COBERTURA, textualmente establece.- Una vez calificados los beneficiarios con derecho y determinada la cuantía de la pensión de montepío, ésta se distribuirá en la proporción de dos partes para la viuda o mujer con quien el asegurado mantuvo unión libre, estable y monogámica y una parte para cada hijo.

M04-P03-12-A Redistribución de pensión (Acrecimientos)

OBJETIVO

Normar las actividades para la redistribución de pensión (acrecimiento) a un grupo familiar, perceptor de pensión de montepío, al extinguirse el derecho de un beneficiario, su pensión acrecerá la de los demás en partes proporcionales y en relación a sus derechos de reparto inicial.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

El Reglamento de Retiro Invalidez y Muerte del Instituto de Seguridad Social de las Fuerzas Armadas, en el Artículo 55, CAPITULO II. DE LA COBERTURA, textualmente establece.- Una vez calificados los beneficiarios con derecho y determinada la cuantía de la pensión de montepío, ésta se distribuirá en la proporción de dos partes para la viuda o mujer con quien el asegurado mantuvo unión libre, estable y monogámica y una parte para cada hijo.

M04-P03-12-B Redistribución de pensión (Coparticipación)

OBJETIVO

Normar las actividades para la redistribución de pensión a un grupo familiar, perceptor de pensión de montepío, al extinguirse el derecho de un beneficiario, su pensión se distribuirá en partes proporcionales y en relación a sus derechos de reparto inicial.

ALCANCE

La ley de Seguridad Social de las Fuerzas Armadas, en su CAPITULO III. DE LA COBERTURA. Art.18, textualmente establece.- Tienen derecho a las prestaciones y servicios sociales contemplados en la presente Ley:

El militar en servicio activo;

El militar en servicio pasivo que cumple con todos los requisitos legales y es calificado como pensionista; y,

Los familiares dependientes y los derechohabientes, calificados como tales, de conformidad con la presente Ley.

El Reglamento de Retiro Invalidez y Muerte del Instituto de Seguridad Social de las Fuerzas Armadas, en el Artículo 55, CAPITULO II. DE LA COBERTURA, textualmente establece.- Una vez calificados los beneficiarios con derecho y determinada la cuantía de la pensión de montepío, ésta se distribuirá en la proporción de dos partes para la viuda o mujer con quien el asegurado mantuvo unión libre, estable y monogámica y una parte para cada hijo.

3.1.3 Gestión de nómina

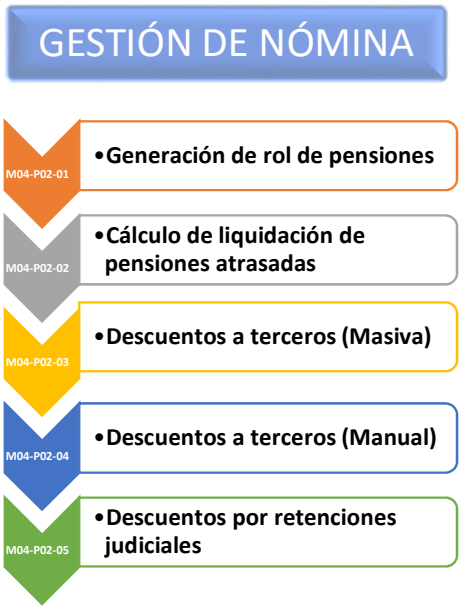


Figura 10: Proceso Gestión de Nómina

Fuente: Los Autores

I. M04-P02-01 Generación de rol de pensiones

OBJETIVO

Normar los procedimientos operativos: Generación de Rol de Pensiones, Liquidación de Pensiones Atrasadas, Descuentos a Terceros (Masiva y Manual), Descuentos por Retenciones Judiciales; con la finalidad de determinar la responsabilidad de los usuarios que intervienen en dicho proceso.

ALCANCE

Este procedimiento está dirigido para todos los clientes del Sistema de Seguridad Social de las Fuerza Armadas, pues norma el procedimiento a aplicarse en el proceso de homologación de las pensiones militares.

M04-P02-02 Cálculo de liquidación de pensiones atrasadas

OBJETIVO

Normar los procedimientos operativos del cálculo de liquidación de pensionistas de retiro; con la finalidad de automatizar informáticamente dicho proceso y reducir sustancialmente las actividades que componen dicho proceso.

ALCANCE

Este procedimiento está dirigido para todos los clientes del Sistema de Seguridad Social de las Fuerza Armadas, pues norma el procedimiento a aplicarse en el proceso de homologación de las pensiones militares.

II. M04-P02-03 Descuentos a terceros (Masiva)

Recepción de Documentos (Secretaria General / Agencias): El Usuario de Secretaria General ó Agencias receptan los oficios y archivos magnéticos, hasta el diez de cada mes. Los proveedores pueden ser:

- Asociaciones
- Cooperativas
- Clubes Deportivos
- Grupos Honoríficos
- Instituciones Militares.

Registrar trámite (Secretaria Prestaciones): Una vez receptada la documentación proveniente de Secretaria General / Agencias, el usuario de Secretaria registra trámite en sistema XNEAR, para posteriormente entregar dicha documentación, además de hoja de seguimiento a Usuario Auxiliar de Nómina.

Verificar formato de archivo magnético (Auxiliar de Nómina): Después de receptar los oficios, archivos magnéticos y hoja de seguimiento, el Auxiliar de Nómina verifica formato de archivo magnético el mismo que debe estar guardado en formato *.txt.

- En algunos casos, es necesario preparar el archivo en relación a parametrización de número de campos de las distintas columnas.
- La siguiente actividad es trasladar el archivo digital parametrizado que está en formato *.txt a Excel para finalmente grabar el mismo en el disco duro local, de acuerdo a código escogido: Fecha, tipo de descuento.

Cargar información (Auxiliar de Nómina): Cuando la información ha sido preparada en archivo digital, el paso siguiente es ingresar al Módulo Informático de Pensiones y cargar información archivada en Excel, este proceso es automático.

- En algunos casos existe la posibilidad de que en el proceso de carga de la información, los datos entregados sean inconsistente, para este efecto el Usuario de Auxiliar de Nómina procede anular la carga, y acto seguido, comunicarse con el responsable del Departamento de Sistemas y Tecnología para que solucione estos errores, y posteriormente empezar una nueva carga de información.

- Si la carga de información no genera errores, la actividad siguiente es validar esta información con documentos de respaldo y generar reportes de carga de información.

Control de Calidad de Información Cargada (Auxiliar de Nómina): El Control de Calidad se lo realiza por muestreo de datos cargados de acuerdo a oficios de proveedores y comparando con los reportes generados en la carga masiva de información por descuentos.

- De existir problemas en el control de calidad de información, el Usuario de Auxiliar de Nómina procede a corregir estas inconsistencias manualmente, ingresando en el Módulo Informático de Pensiones los descuentos de los diferentes proveedores de uno en uno.

Archivo de Documentos (Auxiliar de Nómina): Después del control de calidad de la información cargada en forma masiva por descuentos a terceros, el Usuario Auxiliar de Nómina archiva los documentos (Oficios, Archivo Magnético, Hojas de Seguimiento, Documentos de Soporte) mensualmente , mediante una encuadernación de todo los documentos de respaldo que fueron necesarios para ejecutar el trámite. La custodia de esta documentación dura por un lapso de dos años de acuerdo a lo que establece la Ley.

III. M04-P02-04 Descuentos a terceros (Manual)

Recepción de Documentos (Secretaria General / Agencias): El Usuario de Secretaria General ó Agencias receptan los oficios, hasta el diez quince de cada mes. Los proveedores pueden ser:

- Asociaciones
- Cooperativas

- Clubes Deportivos
- Grupos Honoríficos
- Instituciones Militares.

Los oficios generados por los diferentes proveedores pueden ser por:

- Descuentos Fijos
- Descuentos por Varios Períodos
- Suspensión de Descuentos Fijos
- Suspensión de Descuentos de Varios Períodos.

Registrar trámite (Secretaria Prestaciones): Una vez receptada la documentación proveniente de Secretaria General / Agencias, el usuario de Secretaria registra trámite en sistema XNEAR, para posteriormente entregar dicha documentación, además de hoja de seguimiento a Usuario Auxiliar de Nómina.

Verificar formato de archivo magnético (Auxiliar de Nómina): Después de receptar los oficios y hoja de seguimiento en XNEAR, el Auxiliar de Nómina verifica datos ingresados en solicitud de proveedor, los mismos que pueden ser: Nombres de Afiliado, Valores a ser descontados.

- Cuando el número de afiliados que necesitan ser descuento son excesivos, el Usuario Auxiliar de Nómina, explica a responsable la necesidad de que el oficio por descuentos deben ser realizados adjuntando un archivo digital, el mismo que debe ser parametrizado en formato *.txt.

- Si se da el caso de que la documentación que sustenta al trámite de descuentos a terceros, está incompleta, el Usuario Auxiliar de Nómina genera oficio a proveedor (Asociaciones, Cooperativas, Clubes

Deportivos, Grupos Honoríficos, Instituciones Militares), para que estos a su vez completen la documentación correspondientes y se pueda continuar con el proceso de trámite normal. En algunos casos esta comunicación es telefónicamente para agilitar proceso.

Ingresar Información de Descuento (Auxiliar de Nómina): Posteriormente a que el proveedor completo con la documentación faltante, la actividad siguiente es ingresar la información de descuentos (Nombres de Afiliado, Valor a descontar) en sistema informático de pensiones. Este ingreso y registro de información es en forma manual y se lo hace por cada afiliado que necesita descuento.

Finalizar trámite (Auxiliar de Nómina): Cuando la información ha sido cargada en forma manual en el Módulo Informático de Pensiones el siguiente paso es terminar trámite en Sistema XNEAR.

- Si la carga de información no genera errores, la actividad siguiente es validar esta información con documentos de respaldo y generar reportes de carga de información.

Control de Calidad de Información Cargada (Auxiliar de Nómina): El Control de Calidad se lo realiza por muestreo de datos cargados de acuerdo a oficios de proveedores y comparando con los reportes generados en la carga manual de información por descuentos.

- De existir problemas en el control de calidad de información, el Usuario de Auxiliar de Nómina procede a corregir estas inconsistencias manualmente, ingresando en el Módulo Informático de Pensiones los descuentos de los diferentes proveedores de uno en uno nuevamente.

Archivo de Documentos (Auxiliar de Nómina): Después del control de calidad de la información cargada en forma masiva por descuentos a terceros, el Usuario Auxiliar de Nómina archiva los documentos (Oficios, Hojas de Seguimiento, Documentos de Soporte) mensualmente , mediante una encuadernación de todo los documentos de respaldo que fueron necesarios para ejecutar el trámite. La custodia de esta documentación dura por un lapso de dos años de acuerdo a lo que establece la Ley.

IV. M04-P02-05 Descuentos por retenciones judiciales

Recepción de Documentos (Secretaria General / Agencias): El Usuario de Secretaria General ó Agencias receptan los oficios de los diferentes proveedores, los mismos que pueden ser por:

- Juzgados de la Niñez y Adolescencia
- Juzgados del país de todos legalmente constituidos

Registrar trámite (Secretaria Prestaciones): Una vez receptada la documentación proveniente de Secretaria General / Agencias, el usuario de Secretaria registra trámite en sistema XNEAR, para posteriormente entregar dicha documentación, además de hoja de seguimiento a Usuario Auxiliar de Nómina.

Revisar información (Auxiliar de Nómina): El Usuario Auxiliar de Nómina, una vez que recibe toda la documentación proveniente de Secretaria de Prestaciones, la actividad que realiza es revisar toda la documentación entregada en función de:

- Solicitud dirigida al ISSFA
- Documento protocolizado por firma y sello de Juez respectivo.
- Detalle del Valor a descontar.
- Nombre de Pensionista Titular.

- Además se revisa documento de respaldo como: Copias de Cédula (Beneficiario, Titular); Partida de Nacimiento (Beneficiario).

En algunos casos cuando los documentos no cumplen con los requisitos legales, el Usuario Auxiliar de Nómina, genera oficio a Beneficiario, para que estos a su vez completen la documentación correspondiente y se pueda continuar con el proceso de trámite normal. En algunos casos el beneficiario se comunica con el responsable del trámite de Retenciones Judiciales para que se le informe cuales son los documentos faltantes y su posterior entrega de los mismos.

Verificar Afiliación de Menor de Edad (Auxiliar de Nómina): Posteriormente a que el beneficiario completo con la documentación faltante, la actividad siguiente es verificar en Módulo Informático de Pensiones si el menor de edad está afiliado a la Seguridad Social de las Fuerzas Armadas.

- Si el menor de edad no se encuentra afiliado es necesario que se ejecute previamente el proceso de Afiliación **(M04-P01-01)** en el Departamento de Afiliación.

Ingresar información (Auxiliar de Nómina): Cuando se ha solucionado el inconveniente, y el menor de edad ya se encuentra afiliado en la Seguridad Social de las Fuerzas Armadas, el siguiente paso que realizará el Auxiliar de Nómina es el ingreso de datos de beneficiario y de la persona que va a cobrar la pensión en el Sistema Informático de Pensiones.

- Además de los datos personales ingresados, es necesario que se ingrese en Sistema Informático Financiero, los datos personales de persona que

va cobrar la pensión, y también el número de cuenta donde se depositaran estos valores.

Crear el Rubro de Retención (Auxiliar de Nómina): El Auxiliar de

Nómina, ayudado del Sistema Informático crea el rubro de retención, para su posterior revisión antes de generar el rol de pensiones. Estas retenciones para el rol pueden ser:

- Retenciones Judiciales
- Liquidación de Pagos Atrasados
- Modificación en Retenciones Judiciales u Órdenes Judiciales
- Bajas (Suspensión Órdenes Judiciales ó Retenciones)
- Cambio de Cuenta de Beneficiario.
- Si la carga de información no genera errores, la actividad siguiente es generar reportes de carga de información.

Control de Calidad de Información Cargada (Auxiliar de Nómina): El Control de Calidad se lo realiza por muestreo de datos cargados de acuerdo a oficios de proveedores (Juzgados) y comparando con los reportes generados en la carga manual de información por descuentos.

- De existir problemas en el control de calidad de información, el Usuario de Auxiliar de Nómina procede a corregir estas inconsistencias manualmente, ingresando en el Módulo Informático de Pensiones los descuentos de los diferentes proveedores de uno en uno nuevamente.

Archivo de Documentos (Auxiliar de Nómina): Después del control de calidad de la información cargada por descuentos debido a Retenciones Judiciales, el Usuario Auxiliar de Nómina archiva los documentos (Oficios, Hojas de Seguimiento,

Documentos de Soporte) mensualmente , mediante una encuadernación de todo los documentos de respaldo que fueron necesarios para ejecutar el trámite. La custodia de esta documentación dura por un lapso de dos años de acuerdo a lo que establece la Ley.

1.2. Conocimiento y compresión de las actividades de la gerencia de tecnologías de la información dentro del ISSFA

La UTIC del ISSFA dentro de la doctrina organizativa, es una Unidad de apoyo dependiente de la Subdirección General.

Se ha definido una estructura que cubre cuatro operaciones informáticas básicas como son:

Jefatura

Es la unidad cuya función es la de planificar, controlar, gestionar las operaciones del Departamento de IT.

Gestión de software

La función de esta unidad es la de desarrollar nuevos sistemas de software y de mantener los existentes.

Gestión de infraestructura

Esta unidad se encarga de mantener disponibles el centro de cómputo, el hardware, software básico, servidores, redes y comunicaciones, seguridad informática del ISSFA.

Gestión de información

La responsabilidad de esta unidad es la de administrar la base de datos, inteligencia de negocio y mantener aplicaciones web para el acceso a la información a través de la intranet e internet.

Figura 11: Organigrama Jefatura UTIC

Fuente: Los Autores

1.2.1. Estructura de la UTIC

La UTIC del ISSFA, además de sus funciones propias, tienen la misión de apoyar a las demás unidades de la Institución en lo referente a los componentes tecnológicos de los proyectos propuestos por estas, de tal manera que en la actualidad la carga de trabajo de IT se encuentra repartida de la siguiente manera:

1.2.1. Organigrama funcional de la institución

En el siguiente cuadro se describe la estructura orgánica del ISSFA a Agosto de 2013.

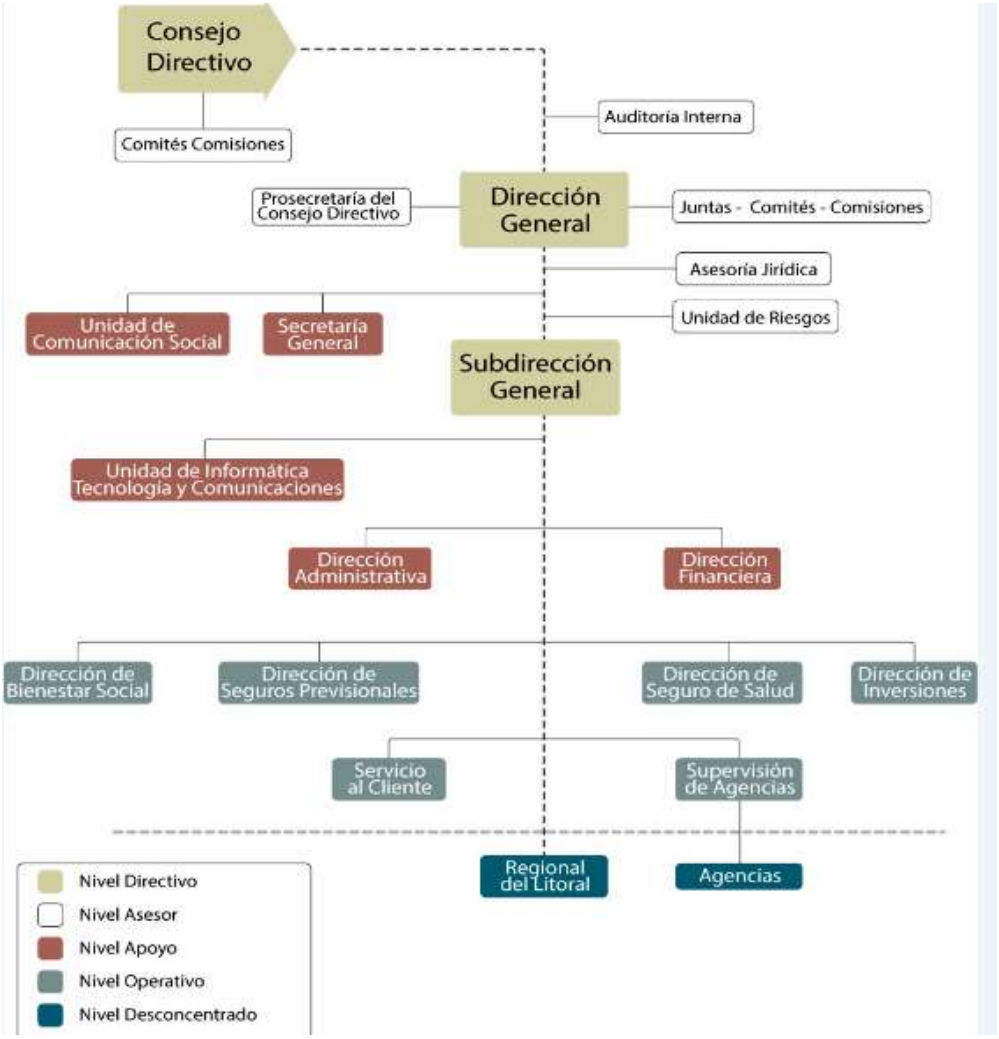


Figura 12: Estructura Orgánica ISSFA

Fuente: www.issfa.mil.ec

1.3. Aplicación de las normas ISO/ISEC: 27001

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Análisis de Riesgos Basado en ISO/IEC:27005:2012

El proceso de gestión del riesgo de la información contra del establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo. El alcance del presente documento será desarrollado hasta el tratamiento del riesgo.

En el Gráfico 5 se describe el proceso de gestión del riesgo de la seguridad de la información.

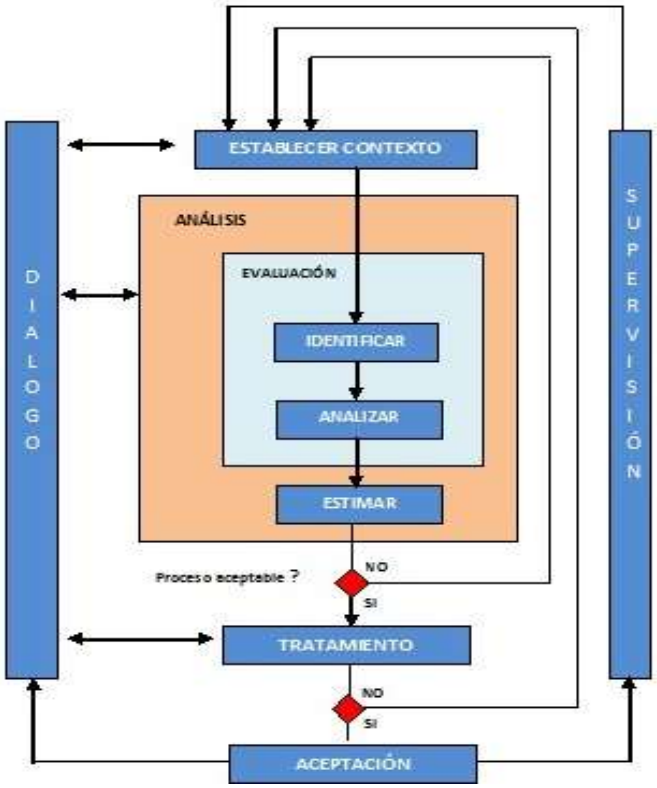


Figura 13: Proceso de gestión del riesgo de la seguridad de la información ISO/IEC 27005:2012

Fuente: Los autores

1.3.1.1. ESTABLECIMIENTO DEL CONTEXTO

En la fase de Establecimiento del Contexto, se debe considerar toda la información sobre la organización, la cual se encuentra descrita en los CAPITULOS I, II, III del presente documento.

1.3.1.1.1. Criterios básicos

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques y criterios para el tratamiento del riesgo, entre los criterios recomendados por la norma ISO/ISEC 27001 tenemos:

- Criterios de evaluación del riesgo.
- Criterios de impacto.
- Criterios de la aceptación del riesgo.

Criterios de evaluación del riesgo

"Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo de la seguridad la información de la organización, teniendo 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, asi como las obligaciones contractuales.
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.

- Las expectativas y precepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

De igual modo, los criterios de evaluación del riesgo se pueden utilizar para especificar las prioridades para el tratamiento del riesgo.

Criterios de impacto

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 de la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (partes internas o terceras partes).
- Pérdida del negocio y del valor financiero.
- Alteración de planes y fechas límites.
- Daños para la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Criterios de la aceptación del riesgo

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se debería considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) el riesgo estimado.
- Los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos, por ejemplo los riesgos que podría resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como requisito contractual.
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo, por ejemplo el riesgo que puede estar asociado con una actividad temporal o de corto plazo. Los criterios de aceptación del riesgo se deberían establecer considerando los siguientes elementos:

- Criterios del negocio.
- Aspectos legales y reglamentarios.
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios. ” (NORMA TECNICA ECUATORIANA NT INEN-ISO/IEC 27005:2012, 2013)

Para el objeto de estudio, se ha considerado los siguientes criterios básicos.

- Importancia de Subproceso BIA
- Riesgos
- Importancia de CID (Confidencialidad, Integridad, Disponibilidad).
- Criterios de aceptación (Muy alto, Alto, Medio, Bajo, Muy Bajo)
- Criterios de impacto.

Catastrófico: Paralización indefinida de al menos un proceso clave (Pensiones). Registrar pérdida superior a 78 millones (BIA 104 millones).

Mayor: Interrupción temporal de al menos un proceso clave que ocasione paralizaciones mayores a 30 días en operaciones normales de la institución. De 52 a 77,9 millones (BIA).

Moderado: Interrupción temporal de al menos un proceso clave que ocasiones paralizaciones mayores a 15 días en operaciones normales de la institución. De 26 a 51,9 millones (BIA).

Menor: Interrupción temporal de al menos un proceso clave que ocasione paralizaciones mayores a 1 día en operaciones normales de la institución. De 5 a 25,9 millones (BIA).

Insignificante: Interrupción esporádica de una actividad de un proceso de la institución. De 1 a 4,9 millones (BIA).

1.3.1.2. Valoración del riesgo

"Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del resto y los objetivos relevantes para la organización.

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los directorios priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo el cual consiste en:
- Identificación del riesgo.

- Estimación del riesgo.
- Evaluación del riesgo.

La valoración del riesgo determina el valor de los activos de información, identifica las amenazas y vulnerabilidades aplicables que existen (o que podrían existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y , finalmente, prioriza los riesgos derivados y los clasifica frente a los criterios de la evaluación de los riesgo determinados en el contexto establecido.” (NORMA TECNICA ECUATORIANA NT INEN-ISO/IEC 27005:2012, 2013)

1.3.1.2.1. Análisis del riesgo

Identificación del riesgo

“El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida.

Identificación de los activos

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software.

Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre este. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización.

Identificación de amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Algunas amenas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados. ” (NORMA TECNICA ECUATORIANA NT INEN-ISO/IEC 27005:2012, 2013)

Identificación de controles existentes

Se deberían identificar los controles existentes y los planificados. Identificar los controles existentes para evitar trabajo o costo innecesarios, pro ejemplo en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación del tratamiento del riesgo, se deberían considerar en la misma forma que aquellos ya implementados.

Para la identificación de los controles existentes o planificados, las siguientes actividades pueden ser útiles:

- Revisión de los documentos que contengan información sobre los controles (por ejemplo, los planes de implementación del tratamiento del riesgo). Si los procesos de la gestión de la seguridad de la información están bien documentos, todos los controles existentes o planificados y el estado de su implementación deberían estar disponibles.
- Verificación con las personas responsables de la seguridad de la información (por ejemplo, el funcionario a cargo de la seguridad de la información y el funcionamiento a cargo de la seguridad del sistema de información, el administrador de la instalación o el director de operaciones) y los usuarios, en cuanto a que controles están realmente implementados para el proceso de información o el sistema de información que se considera.
- Efectuar una revisión en el sitio de los controles físicos, comparando aquellos implementados con la lista de los controles que deberían estar, y verificando aquellos implementados con respecto a si funcionan correctamente de manera eficaz.
- Revisión de los resultados de las evaluaciones internas.

Identificación de las vulnerabilidades

Se deben identificar las vulnerabilidades que pueden ser explotadas por las amenazas pueden ser explotadas por las amenazas por causar daños a los activos o a la organización.

Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software o equipo de comunicaciones.
- Dependencia de partes externas.

Identificación de las consecuencias (efecto)

Identifica los daños o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de la información. El impacto de los escenarios del incidente se determina tomando en consideración los criterios del impacto que se define durante la actividad de establecimiento del contexto. Puede afectar a uno o más activos o a una parte de un activo. De este modo, los activos pueden tener valores asignados tanto para su costo financiero como para las consecuencias en el negocio, si se deterioran o se ven comprometidos. Las consecuencias pueden ser de naturaleza temporal o permanente como es el caso de la destrucción de un activo.

La organización deberían identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación.

- Pérdida de tiempo.
- Pérdida de oportunidad.
- Salud y seguridad.
- Costo financiero de las habilidades específicas para preparar el daño.
- Imagen, reputación y buen nombre." (NORMA TECNICA ECUATORIANA NT INEN-ISO/IEC 27005:2012, 2013)

1.4. Planificación del programa de evaluación

Para hacer una adecuada planeación de la Evaluación de seguridad hay que tener un profundo conocimiento y comprensión de la entidad a la que se aplicará el estudio, de esta forma, permitirá dimensionar la magnitud y características del objeto de estudio dentro del organismo a evaluar, sus sistemas, organización y equipos. Con ello podemos determinar el número y características del personal, las herramientas necesarias, el tiempo y costo, así como definir los alcances, en caso necesario, poder elaborar contratos de servicios.

1.4.1. Objetivo

Realizar la Evaluación de Seguridad de la Información en el proceso de Seguros Previsionales del ISSFA basado en la norma ISO/IEC 27001:2005, a fin de identificar debilidades y emitir recomendaciones dentro del proceso, lo cual permitirá garantizar la confidencialidad, integridad y disponibilidad de la información.

1.4.2. Alcance

El presente trabajo tiene la finalidad de analizar y evaluar la integridad, disponibilidad y confidencialidad de la información del proceso de Seguros Previsionales del ISSFA Matriz (Quito), bajo el criterio de las normas ISO/IEC

27000:2005, emitir un informe de la evaluación y generar un plan de acción para ser ejecutado por la Institución.

1.4.3. Productos a entregar

Plan de Acción de Acción resultado de la Evaluación de Seguridad de la Información en el proceso de Seguros Previsionales del ISSFA basado en la norma ISO/IEC 27001:2005.

Informe de la evaluación de los riesgos existentes a nivel de proceso y subproceso.

1.4.4. Herramientas a utilizar

Las herramientas a utilizar para la Evaluación son:

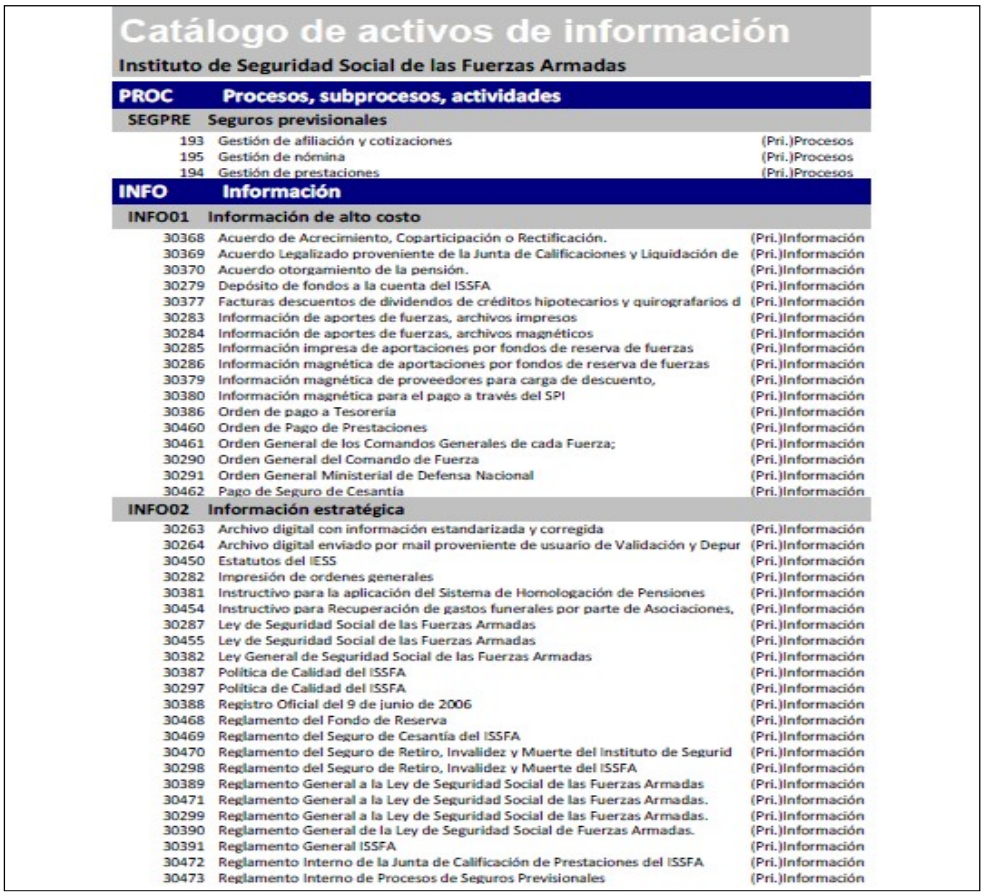
- Encuestas.
- Cuestionarios.
- Software Especializado.
- Normas INEN vigentes homologadas a la norma ISO/IEC 27001:2005.
- Normas ISO/IEC 27001:2005

1.5. Investigación de campo

1.5.1. Identificación de activos de la información

El proceso de identificación de los contenedores de información que intervienen en este proceso, se basa en el análisis de los flujos y caracterización de los tres subprocesos, utilizando la clasificación definida en la norma ISO/IEC 27005:2008. En los Gráficos 6, 7 podemos observar una muestra de los activos de la Información que se han identificado en el ISSFA. En el **ANEXO A** se detalla el catálogo de activos de la información.

Tabla 3.
Identificación de activos de la Información



Catálogo de activos de información

Instituto de Seguridad Social de las Fuerzas Armadas

PROC	**Procesos, subprocesos, actividades**	
SEGPRE	**Seguros previsionales**	
193	Gestión de afiliación y cotizaciones	(Pri.)Procesos
195	Gestión de nómina	(Pri.)Procesos
194	Gestión de prestaciones	(Pri.)Procesos
INFO	**Información**	
INFO01	**Información de alto costo**	
30368	Acuerdo de Acrecimiento, Coparticipación o Rectificación.	(Pri.)Información
30369	Acuerdo Legalizado proveniente de la Junta de Calificaciones y Liquidación de	(Pri.)Información
30370	Acuerdo otorgamiento de la pensión.	(Pri.)Información
30279	Depósito de fondos a la cuenta del ISSFA	(Pri.)Información
30377	Facturas descuentos de dividendos de créditos hipotecarios y quirografarios d	(Pri.)Información
30283	Información de aportes de fuerzas, archivos impresos	(Pri.)Información
30284	Información de aportes de fuerzas, archivos magnéticos	(Pri.)Información
30285	Información impresa de aportaciones por fondos de reserva de fuerzas	(Pri.)Información
30286	Información magnética de aportaciones por fondos de reserva de fuerzas	(Pri.)Información
30379	Información magnética de proveedores para carga de descuento,	(Pri.)Información
30380	Información magnética para el pago a través del SPI	(Pri.)Información
30386	Orden de pago a Tesorería	(Pri.)Información
30460	Orden de Pago de Prestaciones	(Pri.)Información
30461	Orden General de los Comandos Generales de cada Fuerza;	(Pri.)Información
30290	Orden General del Comando de Fuerza	(Pri.)Información
30291	Orden General Ministerial de Defensa Nacional	(Pri.)Información
30462	Pago de Seguro de Cesantía	(Pri.)Información
INFO02	**Información estratégica**	
30263	Archivo digital con información estandarizada y corregida	(Pri.)Información
30264	Archivo digital enviado por mail proveniente de usuario de Validación y Depur	(Pri.)Información
30450	Estatutos del IESS	(Pri.)Información
30282	Impresión de ordenes generales	(Pri.)Información
30381	Instructivo para la aplicación del Sistema de Homologación de Pensiones	(Pri.)Información
30454	Instructivo para Recuperación de gastos funerales por parte de Asociaciones,	(Pri.)Información
30287	Ley de Seguridad Social de las Fuerzas Armadas	(Pri.)Información
30455	Ley de Seguridad Social de las Fuerzas Armadas	(Pri.)Información
30382	Ley General de Seguridad Social de las Fuerzas Armadas	(Pri.)Información
30387	Política de Calidad del ISSFA	(Pri.)Información
30297	Política de Calidad del ISSFA	(Pri.)Información
30388	Registro Oficial del 9 de junio de 2006	(Pri.)Información
30468	Reglamento del Fondo de Reserva	(Pri.)Información
30469	Reglamento del Seguro de Cesantía del ISSFA	(Pri.)Información
30470	Reglamento del Seguro de Retiro, Invalidez y Muerte del Instituto de Segurid	(Pri.)Información
30298	Reglamento del Seguro de Retiro, Invalidez y Muerte del ISSFA	(Pri.)Información
30389	Reglamento General a la Ley de Seguridad Social de las Fuerzas Armadas	(Pri.)Información
30471	Reglamento General a la Ley de Seguridad Social de las Fuerzas Armadas.	(Pri.)Información
30299	Reglamento General a la Ley de Seguridad Social de las Fuerzas Armadas.	(Pri.)Información
30390	Reglamento General de la Ley de Seguridad Social de Fuerzas Armadas.	(Pri.)Información
30391	Reglamento General ISSFA	(Pri.)Información
30472	Reglamento Interno de la Junta de Calificación de Prestaciones del ISSFA	(Pri.)Información
30473	Reglamento Interno de Procesos de Seguros Previsionales	(Pri.)Información

CONTINÚA

30392	Reglamento Interno de Procesos de Seguros Provisionales del ISSFA	(Pri.)Información
30393	Reglamento Interno de Procesos de Seguros Provisionales del ISSFA	(Pri.)Información
30300	Reglamento interno de Procesos Seguros Previsionales del ISSFA	(Pri.)Información
30394	Reglamento Oficial 650 del 28 de Agosto del 2008	(Pri.)Información
30474	Reglamento Orgánico Funcional del ISSFA	(Pri.)Información
30412	Requerimientos de la norma ISO-9001:2000	(Pri.)Información
30316	Requerimientos de la norma ISO-9001:2000.	(Pri.)Información
INFO03	**Información personal**	
30265	Cedula militar	(Pri.)Información
30266	Certificación de aportes	(Pri.)Información
30267	Certificado de matricula y asistencia a clases en establecimientos legalmente	(Pri.)Información
30268	Certificado de no afiliación al IESS	(Pri.)Información
30269	Certificado de no afiliación al ISSPOL	(Pri.)Información
30270	Certificado de votación	(Pri.)Información
30271	Certificado para la indemnización global	(Pri.)Información
30272	Certificado para seguros	(Pri.)Información
30273	Certificado SRI de no poseer RUC	(Pri.)Información
30445	Copia de cédula de ciudadanía	(Pri.)Información
30274	Copia de Cédula de Ciudadanía (mayor de edad)	(Pri.)Información
30446	Copia de cédula de identidad	(Pri.)Información
30275	Copia de la cédula de identidad	(Pri.)Información
30276	Copia de la partida de defunción.	(Pri.)Información
30278	Declaración Juramentada del militar titular	(Pri.)Información
30374	Descuentos de Retenciones Judiciales y Ordenes Judiciales	(Pri.)Información
30452	Formulario para Requerimientos Generales	(Pri.)Información
30453	Hoja de salida de la Fuerza Terrestre	(Pri.)Información
30281	Hoja de vida militar	(Pri.)Información
30457	Liquidación del tiempo de servicio del militar con la baja otorgada por el archi	(Pri.)Información
30459	Notificación telefónica de la resolución de los Acuerdos al Afiliado	(Pri.)Información
30288	Oficio de requerimiento de diferencia de aportaciones	(Pri.)Información
30293	Original y copia de cédula del titular para el registro inicial en todos los casos.	(Pri.)Información
30463	Partida de matrimonio o sentencia de unión de hecho (Cónyuge)	(Pri.)Información
30294	Partida de matrimonio o sentencia judicial de unión de hecho emitida por un j	(Pri.)Información
30464	Partida de nacimiento	(Pri.)Información
30295	Partida de nacimiento	(Pri.)Información
30296	Poderes	(Pri.)Información
30317	Sentencia condenatoria	(Pri.)Información
30318	Solicitud afiliación de dependientes de pasivos	(Pri.)Información
30319	Solicitud de certificación de aportes	(Pri.)Información
30323	Solicitud de registro del dependiente o derechohabiente.	(Pri.)Información
30478	Solicitud de Rehabilitación de Pensión	(Pri.)Información
30479	Solicitud de Seguros	(Pri.)Información
30320	Solicitud del titular (militar activo o pasivo) requiriendo el registro del hijo.	(Pri.)Información
30321	Solicitud del titular requiriendo el registro de su cónyuge.	(Pri.)Información
30480	Solicitud dirigida al Director del ISSFA	(Pri.)Información
30322	Solicitud general de actualización de datos	(Pri.)Información
INFO04	**Información vital**	
30427	Acuerdo de Acrecimientos	(Pri.)Información
30428	Acuerdo de Coparticipación.	(Pri.)Información
30429	Acuerdo de Retiro y Cesantía	(Pri.)Información
30430	Acuerdo de Seguro de Accidentes Profesionales	(Pri.)Información
30431	Acuerdo de Seguro de Invalidez	(Pri.)Información
30432	Acuerdo de Seguro de Vida	(Pri.)Información
30324	Archivo de información proveniente de la fuerza Aérea, Naval, Terrestre	(Pri.)Información

Fuente: Los autores

1.5.2. Asignación de los activos de información a subprocesos

Una vez catalogados los activos, son asignados a cada uno de los tres subprocesos de acuerdo a su utilización.

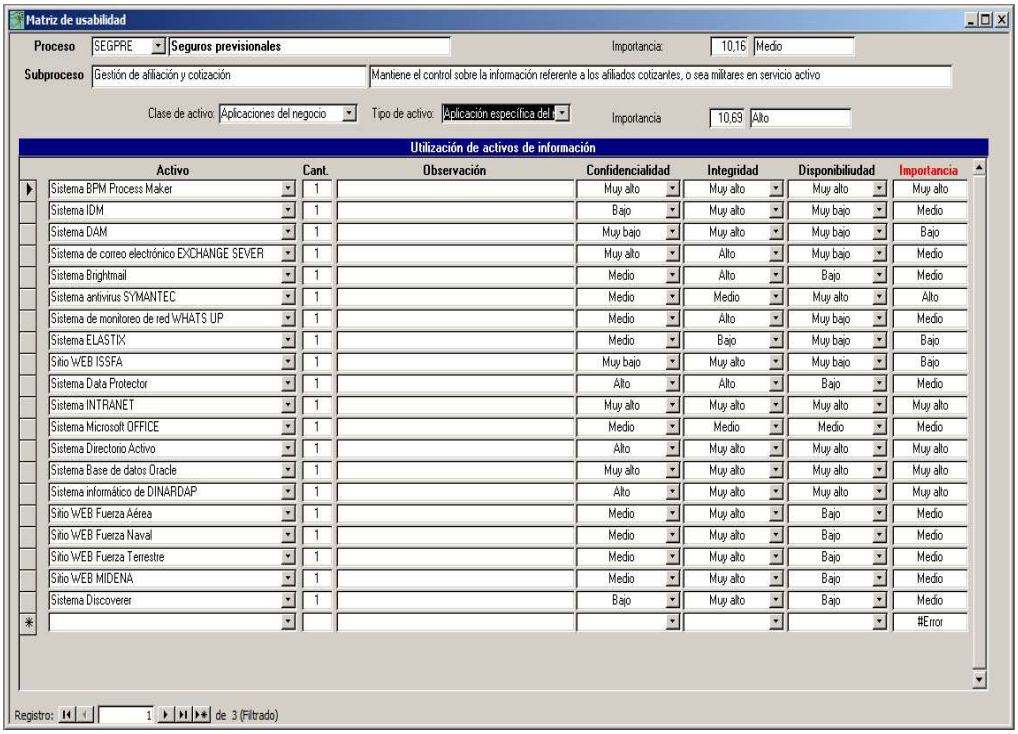


Figura 14: Asignación de los Activos de la Información a los Subprocesos

Fuente: Los Autores

En la figura 14 se puede observar el inventario de activos de información, se ha definido activos individuales y servicios TI, configurando una matriz entre los mismos y los subprocesos a los cuales se encuentran sirviendo. En donde las filas representan a los activos (Aj) y las columnas a los subprocesos (Si) para los fines prácticos se utiliza la notación de Si = (Ai1, Ai2, …, Aij, …, Aim) para denotar que el subproceso Si, está constituido por m activos.

Los posteriores incidentes de seguridad que se materialicen en un activo, tienden a comprometer al servicio y a su vez a su proceso padre, que finalmente impacta en el desempeño de la organización. El impacto de un proceso k, I(Pk), en el negocio, usualmente se determina mediante el proceso de análisis de impacto en el negocio (o BIA por sus siglas en inglés). El mismo que ha criterio de la analista puede ser heredado por sus activos dependientes para la determinación de su riesgo, es decir: I(Pk) → I(Si) → I(Aij).

Complementariamente al inventario de activos, para la valuación de riesgos es necesario disponer de los catálogos de vulnerabilidades, amenazas, efectos o consecuencias. El resultado es el documento de Análisis de Riesgos, que establece el modo de tratamiento de los riesgos y los controles ISO 27002 que van a ser implementados para cada uno de los activos, con el objetivo de cerrar las brechas de seguridad existentes.

1.5.3. Calificación de activos de información

Una vez que los activos de información han sido organizados de acuerdo a su utilización en los subprocesos a analizar, se procede a calificar sus tres dimensiones de seguridad de información como son: CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD en base a la siguiente valoración:

Tabla **4:**

Calificación de activos de la información

Calificación	Valor
Muy alto	**5**
Alto	**4**
Medio	**3**
Bajo	**2**
Muy bajo	**1**

Fuente: Los Autores

El valor de su importancia es calculado en base al promedio de la suma de los tres parámetros.

Tabla 5:

Cálculo importancia activo

C	=	Confidencialidad
I	=	Integridad
D	=	Disponibilidad
I M	=	Importancia
IM = (C+I+D) / 3		

Fuente: Los Autores

En la siguiente tabla se puede observar la calificación e importancia que se asignaron a los activos de la información. En el **ANEXO B** se describe la calificación de la importancia de activos de la información.

Tabla 6.

Calificación de Activos de la Información

Importancia de activos de información

Instituto de Seguridad Social de las Fuerzas Armadas

SEGPRE	Seguros previsionales				
AFIL	Gestión de afiliación y cotización	Confidencialidad	Integridad	Disponibilidad	Importancia
	Aplicaciones del negocio				
	Aplicación específica del negocio				
30332	Sistema antivirus SYMANTEC	Medio	Medio	Muy alto	**Alto**
30340	Sistema Base de datos Oracle	Muy alto	Muy alto	Muy alto	**Muy alto**
91	Sistema BPM Process Maker	Muy alto	Muy alto	Muy alto	**Muy alto**
30331	Sistema Brightmail	Medio	Alto	Bajo	**Medio**
92	Sistema DAM	Muy bajo	Muy alto	Muy bajo	**Bajo**
30335	Sistema Data Protector	Alto	Alto	Bajo	**Medio**
30330	Sistema de correo electrónico EXCHANGE SEVER	Muy alto	Alto	Muy bajo	**Medio**
30333	Sistema de monitoreo de red WHATS UP	Medio	Alto	Muy bajo	**Medio**
30339	Sistema Directorio Activo	Alto	Muy alto	Muy alto	**Muy alto**
30329	Sistema Discoverer	Bajo	Muy alto	Bajo	**Medio**
30334	Sistema ELASTIX	Medio	Bajo	Muy bajo	**Bajo**
90	Sistema IDM	Bajo	Muy alto	Muy bajo	**Medio**
30341	Sistema informático de DINARDAP	Alto	Muy alto	Muy alto	**Muy alto**
30336	Sistema INTRANET	Muy alto	Muy alto	Muy alto	**Muy alto**
30337	Sistema Microsoft OFFICE	Medio	Medio	Medio	**Medio**
30344	Sitio WEB Fuerza Aérea	Medio	Muy alto	Bajo	**Medio**
30343	Sitio WEB Fuerza Naval	Medio	Muy alto	Bajo	**Medio**
30342	Sitio WEB Fuerza Terrestre	Medio	Muy alto	Bajo	**Medio**
30365	Sitio WEB ISSFA	Muy bajo	Muy alto	Muy bajo	**Bajo**
30345	Sitio WEB MIDENA	Medio	Muy alto	Bajo	**Medio**
	Aplicación estándar Sistema Integrado (ERP)				
514	Interfaces - Integración	Muy alto	Muy alto	Muy alto	**Muy alto**
512	Sistema de afiliación	Muy alto	Muy alto	Muy alto	**Muy alto**
510	Sistema de ahorro FONIFA	Medio	Alto	Alto	**Alto**
30367	Sistema de contabilidad	Alto	Alto	Medio	**Alto**
30366	Sistema de control de usuarios	Muy alto	Muy alto	Bajo	**Alto**
513	Sistema de cotizaciones	Muy alto	Muy alto	Muy alto	**Muy alto**
509	Sistema de crédito	Alto	Alto	Medio	**Alto**

CONTINÚA

511	Sistema de pensiones	Muy alto	Muy alto	Muy alto	Muy alto
70	Sistema de Prestaciones	Muy alto	Muy alto	Muy alto	Muy alto
72	Sistema de Salud	Medio	Alto	Medio	Medio
30328	Sistema de servicio al cliente	Alto	Alto	Medio	Alto
30327	Sistema de tesorería	Alto	Alto	Medio	Alto
Hardware					
Equipo de procesamiento de datos					
202	Servidor antispam Brightmail	Muy bajo	Alto	Medio	Medio
201	Servidor antivirus Symantec	Muy bajo	Muy alto	Muy alto	Alto
199	Servidor aplicaciones sistema integrado	Muy alto	Muy alto	Muy alto	Muy alto
30350	Servidor BPM	Muy alto	Muy alto	Muy alto	Muy alto
30347	Servidor DAM, IDM	Muy alto	Muy alto	Muy bajo	Alto
30362	Servidor de archivos fuentes de sistema integrado	Alto	Alto	Alto	Alto
3	Servidor de base de datos ORACLE	Muy alto	Muy alto	Muy alto	Muy alto
30349	Servidor de base de datos ORACLE de pruebas	Bajo	Alto	Medio	Medio
1	Servidor de base de datos SQL Server	Muy bajo	Muy bajo	Muy alto	Bajo
2	Servidor de correo electrónico	Muy alto	Alto	Muy bajo	Medio
205	Servidor de directorio activo	Muy alto	Muy alto	Muy alto	Muy alto
7	Servidor de Intranet	Medio	Medio	Medio	Medio
5	Servidor de OAS	Medio	Medio	Medio	Medio
30348	Servidor de respaldos	Medio	Medio	Medio	Medio
30346	Servidor de telefonía	Muy alto	Bajo	Muy bajo	Medio
203	Servidor monitor de red	Medio	Medio	Bajo	Medio
6	Servidor sitio WEB del ISSFA	Medio	Medio	Medio	Medio
Equipo fijo					
108	Impresora láser	Bajo	Bajo	Alto	Medio
107	Pc de escritorio	Alto	Alto	Muy alto	Alto
110	Scanner	Muy bajo	Muy bajo	Medio	Bajo
Equipo móvil					
105	Laptop	Alto	Alto	Alto	Alto
Equipos seguridad perimetral					
198	Equipo de protección perimetral, canal de internet principal SOPHOS/ASTARO SG	Alto	Alto	Alto	Alto
204	Equipo de protección perimetral, redes telefónicas CNT, MODE SOPHOS/ASTARO	Alto	Alto	Alto	Alto
Medios para datos					
115	Cinta para respaldos de BDD LT	Medio	Alto	Medio	Medio
121	Librería de almacenamiento	Alto	Medio	Medio	Medio

CONTINÚA

120	SAN Sistema de almacenamiento	Alto	Alto	Muy alto	Alto
Periféricos para procesamiento					
30358	Impresora láser de afiliación	Medio	Medio	Alto	Medio
30359	Impresora láser de prestaciones	Medio	Medio	Alto	Medio
528	Impresora láser de tesorería	Medio	Medio	Alto	Medio
30361	Scanner de Afiliación	Medio	Medio	Bajo	Medio
30360	Scanner de Digitalización en Prestaciones	Medio	Medio	Alto	Medio
Información					
Información de alto costo					
30279	Depósito de fondos a la cuenta del ISSFA	Muy alto	Muy alto	Muy alto	Muy alto
30283	Información de aportes de fuerzas, archivos impresos	Alto	Muy alto	Bajo	Alto
30284	Información de aportes de fuerzas, archivos magnéticos	Alto	Muy alto	Muy alto	Muy alto
30285	Información impresa de aportaciones por fondos de reserva de fuerzas	Alto	Muy alto	Muy alto	Muy alto
30286	Información magnética de aportaciones por fondos de reserva de fuerzas	Alto	Muy alto	Muy alto	Muy alto
30290	Orden General del Comando de Fuerza	Alto	Muy alto	Alto	Alto
30291	Orden General Ministerial de Defensa Nacional	Muy alto	Muy alto	Alto	Muy alto
Información estratégica					
30263	Archivo digital con información estandarizada y corregida	Alto	Alto	Alto	Alto
30264	Archivo digital enviado por mail proveniente de usuario de Validación y Depuraci	Medio	Alto	Medio	Medio
30282	Impresión de ordenes generales	Muy alto	Muy alto	Medio	Alto
30287	Ley de Seguridad Social de las Fuerzas Armadas	Muy bajo	Medio	Medio	Bajo
30297	Política de Calidad del ISSFA	Bajo	Bajo	Bajo	Bajo
30298	Reglamento del Seguro de Retiro, Invalidez y Muerte del ISSFA	Bajo	Medio	Bajo	Bajo
30299	Reglamento General a la Ley de Seguridad Social de las Fuerzas Armadas.	Bajo	Medio	Bajo	Bajo
30300	Reglamento interno de Procesos Seguros Previsionales del ISSFA	Bajo	Medio	Bajo	Bajo
30316	Requerimientos de la norma ISO-9001:2000.	Bajo	Bajo	Muy bajo	Bajo
Información personal					
30265	Cedula militar	Alto	Muy alto	Medio	Alto
30266	Certificación de aportes	Alto	Muy alto	Bajo	Alto
30267	Certificado de matricula y asistencia a clases en establecimientos legalmente rec	Bajo	Muy alto	Medio	Medio
30268	Certificado de no afiliación al IESS	Alto	Alto	Alto	Alto
30269	Certificado de no afiliación al ISSPOL	Alto	Alto	Alto	Alto
30270	Certificado de votación	Bajo	Muy alto	Medio	Medio
30271	Certificado para la indemnización global	Bajo	Muy alto	Medio	Medio
30272	Certificado para seguros	Bajo	Muy alto	Medio	Medio
30273	Certificado SRI de no poseer RUC	Bajo	Muy alto	Medio	Medio
30274	Copia de Cédula de Ciudadanía (mayor de edad)	Bajo	Muy alto	Medio	Medio

30275	Copia de la cédula de identidad	Bajo	Muy alto	Medio	Medio
30276	Copia de la partida de defunción.	Bajo	Muy alto	Medio	Medio
30278	Declaración Juramentada del militar titular	Bajo	Alto	Alto	Medio
30281	Hoja de vida militar	Alto	Muy alto	Medio	Alto
30288	Oficio de requerimiento de diferencia de aportaciones	Bajo	Medio	Alto	Medio
30293	Original y copia de cédula del titular para el registro inicial en todos los casos.	Muy bajo	Muy alto	Alto	Medio
30294	Partida de matrimonio o sentencia judicial de unión de hecho emitida por un juz	Muy bajo	Muy alto	Alto	Medio
30295	Partida de nacimiento	Muy bajo	Muy alto	Alto	Medio
30296	Poderes	Muy bajo	Muy alto	Alto	Medio
Información vital					
30325	Archivo de información proveniente de la fuerza Aérea, Naval, Terrestre en form	Muy alto	Muy alto	Muy alto	Muy alto
30326	Archivo de información proveniente de la fuerza Aérea, Naval, Terrestre en form	Muy alto	Muy alto	Muy alto	Muy alto
30364	Correo electrónico institucional	Alto	Alto	Bajo	Medio
30280	Formato para ingreso de documentación externa	Muy bajo	Muy bajo	Muy bajo	Muy bajo
30289	Oficio para las fuerzas para pago de aportaciones del afiliado	Bajo	Alto	Alto	Medio
30292	Orden judicial	Bajo	Muy alto	Alto	Alto
30301	Reporte con las solicitudes de afiliación ingresadas	Alto	Alto	Alto	Alto
30302	Reporte con las solicitudes de datos actualizados	Alto	Alto	Alto	Alto
30303	Reporte de carga correctos	Bajo	Alto	Alto	Medio
30304	Reporte de carga de información por cada fuerza	Bajo	Alto	Medio	Medio
30310	Reporte de datos incorrectos	Bajo	Alto	Medio	Medio
30305	Reporte de inconsistencia de carga	Bajo	Alto	Medio	Medio
30306	Reporte de inconsistencia de datos	Bajo	Alto	Medio	Medio
30307	Reporte de novedades solucionadas	Bajo	Alto	Medio	Medio
30308	Reporte de solicitudes ingresadas	Bajo	Alto	Medio	Medio
30309	Reporte de transacción de fondos de reserva	Bajo	Alto	Medio	Medio
30311	Reporte detallado de los registros de afiliación	Bajo	Alto	Medio	Medio
30312	Reporte resumen validación	Bajo	Alto	Medio	Medio
30313	Reportes de afiliación	Bajo	Alto	Medio	Medio
30314	Reportes de datos actualizados	Bajo	Alto	Medio	Medio
30315	Reportes de los ingresos de afiliados	Bajo	Alto	Medio	Medio
Organización					
Proveedores de información					
30484	COMACO	Alto	Alto	Alto	Alto
30486	DINARDAP	Alto	Alto	Alto	Alto
30483	Fuerza Aérea	Alto	Alto	Alto	Alto
30482	Fuerza Naval	Alto	Alto	Alto	Alto

Fuente: Los Autores

1.5.4. Asignación de amenazas a activos de información

Una vez que los activos de información han sido identificados, clasificados y asignados a los procesos, se realiza una filtración de acuerdo a los parámetros de aceptación en cuanto a su importancia, es decir que para la siguiente fase de identificar y asignar sus amenazas, solo se tomarán en cuenta aquellos activos cuya calificación sea superior al parámetro definido por la Institución, en este caso se tomarán en cuenta solo los activos cuya calificación de importancia sean Muy alto y Alto.

A cada activo de información se asignará una o varias amenazas comunes y generadas por humanos, las mismas que se encuentran definidas en la ISO/IEC 27005:2008.

Los activos son protegidos de acuerdo a su importancia, determinada a partir de la calificación de sus dimensiones de seguridad (Disponibilidad, Integridad y Confidencialidad), estos están expuestos a eventos adversos o amenazas, que pueden materializarse explotando vulnerabilidades o debilidades, con determinada frecuencia o probabilidad, según la eficacia de los controles vigentes.

Figura 15: Elementos del Riesgo

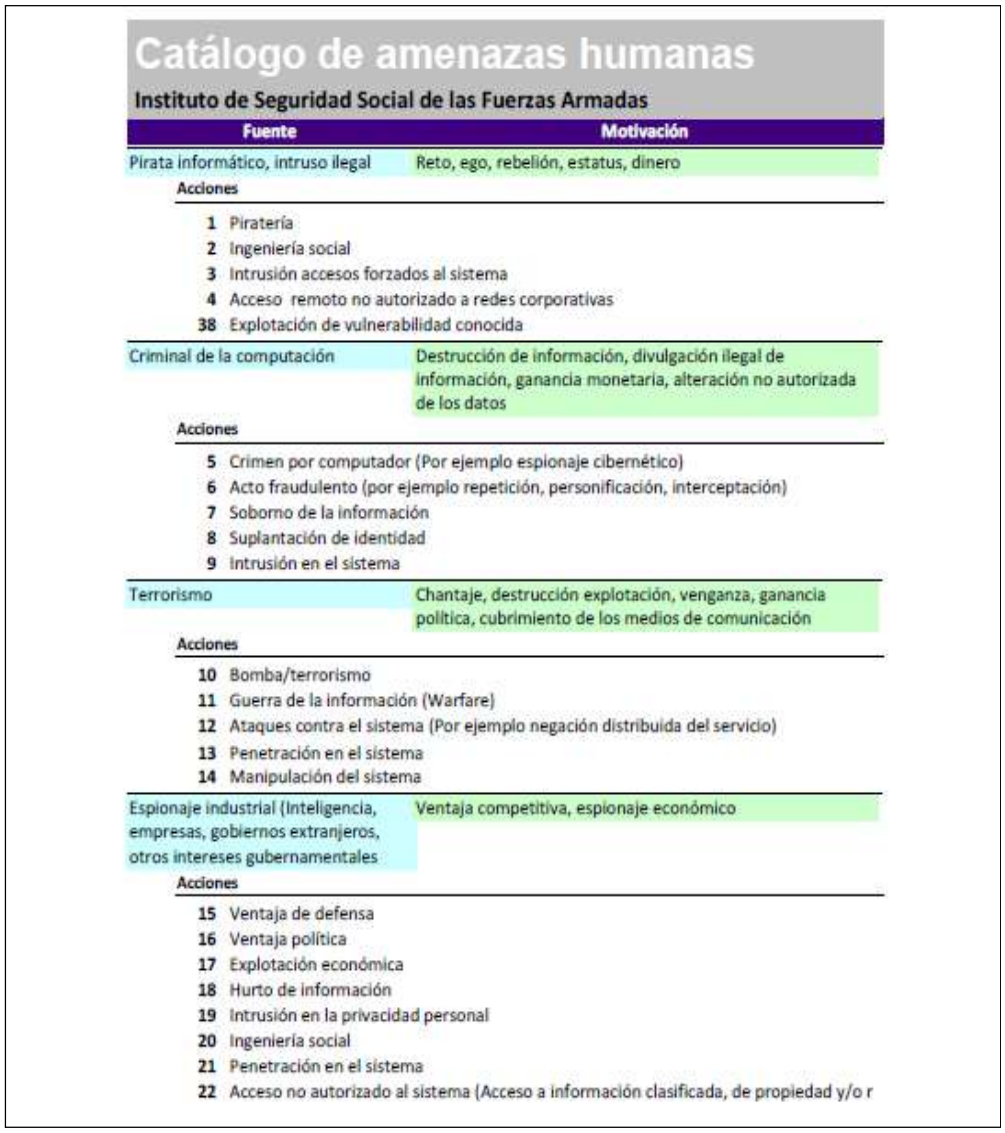
Fuente: (Secure& It, 2012)

El proceso propuesto utiliza el catálogo de amenazas y vulnerabilidades de la ISO 27005 y los controles de la ISO 27002. En el **ANEXO C** se describe el catálogo de amenazas humanas y en el **ANEXO D** el catálogo de amenazas comunes, **ANEXO E** asignación de amenazas humanas a activos de información **ANEXO F**

asignación de amenazas comunes a activos de información, **ANEXO G** catálogo de vulnerabilidades

Tabla 7.

Asignación de Amenazas humanas

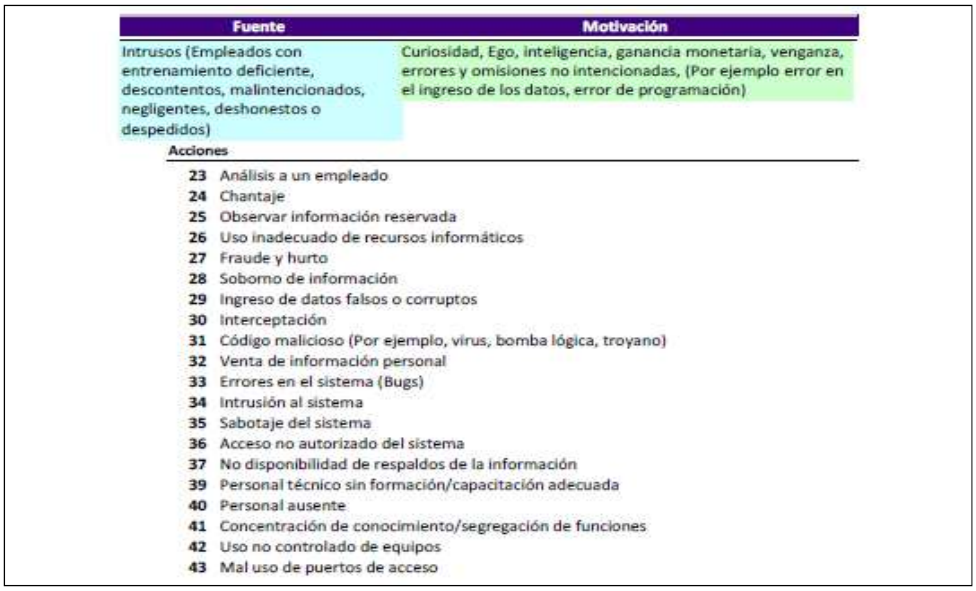


Catálogo de amenazas humanas

Instituto de Seguridad Social de las Fuerzas Armadas

Fuente	Motivación
Pirata informático, intruso ilegal	Reto, ego, rebelión, estatus, dinero
Acciones	
1 Piratería	
2 Ingeniería social	
3 Intrusión accesos forzados al sistema	
4 Acceso remoto no autorizado a redes corporativas	
38 Explotación de vulnerabilidad conocida	
Criminal de la computación	Destrucción de información, divulgación ilegal de información, ganancia monetaria, alteración no autorizada de los datos
Acciones	
5 Crimen por computador (Por ejemplo espionaje cibernético)	
6 Acto fraudulento (por ejemplo repetición, personificación, interceptación)	
7 Soborno de la información	
8 Suplantación de identidad	
9 Intrusión en el sistema	
Terrorismo	Chantaje, destrucción explotación, venganza, ganancia política, cubrimiento de los medios de comunicación
Acciones	
10 Bomba/terrorismo	
11 Guerra de la información (Warfare)	
12 Ataques contra el sistema (Por ejemplo negación distribuida del servicio)	
13 Penetración en el sistema	
14 Manipulación del sistema	
Espionaje industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses gubernamentales	Ventaja competitiva, espionaje económico
Acciones	
15 Ventaja de defensa	
16 Ventaja política	
17 Explotación económica	
18 Hurto de información	
19 Intrusión en la privacidad personal	
20 Ingeniería social	
21 Penetración en el sistema	
22 Acceso no autorizado al sistema (Acceso a información clasificada, de propiedad y/o r	

CONTINÚA



Fuente	Motivación
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad, Ego, inteligencia, ganancia monetaria, venganza, errores y omisiones no intencionadas, (Por ejemplo error en el ingreso de los datos, error de programación)

Acciones	
23	Análisis a un empleado
24	Chantaje
25	Observar información reservada
26	Uso inadecuado de recursos informáticos
27	Fraude y hurto
28	Soborno de información
29	Ingreso de datos falsos o corruptos
30	Interceptación
31	Código malicioso (Por ejemplo, virus, bomba lógica, troyano)
32	Venta de información personal
33	Errores en el sistema (Bugs)
34	Intrusión al sistema
35	Sabotaje del sistema
36	Acceso no autorizado del sistema
37	No disponibilidad de respaldos de la información
39	Personal técnico sin formación/capacitación adecuada
40	Personal ausente
41	Concentración de conocimiento/segregación de funciones
42	Uso no controlado de equipos
43	Mal uso de puertos de acceso

Fuente: Los Autores

Tabla 8:

Asignación de Amenazas comunes

Catálogo de amenazas comunes

Instituto de Seguridad Social de las Fuerzas Armadas

Tipo		Amenaza	Accidental	Deliberada	Ambiental
Daño físico					
	1	Fuego, incendio	☑	☑	☑
	2	Daño por agua	☑	☑	☑
	3	Contaminación	☑	☑	☑
	4	Accidente importante	☑	☑	☑
	5	Destrucción del equipo o los medios	☑	☑	☑
	6	Polvo, corrosión, congelamiento	☑	☑	☑
Eventos naturales					
	7	Fenómenos climáticos	☐	☐	☑
	8	Fenómenos sísmicos	☐	☐	☑
	9	Fenómenos volcánicos	☐	☐	☑
	10	Fenómenos metereológicos	☐	☐	☑
	11	Inundación	☐	☐	☑
Pérdida de los servicios esenciales					
	12	Falla en el sistema de suministro de agua o de air	☑	☐	☑
	13	Pérdida de suministro de energía eléctrica	☑	☑	☑
	14	Falla en el equipo de telecomunicaciones	☑	☐	☑
Perturbación debida a la radiación					
	15	Radiación electromagnética	☑	☑	☑
	16	Radiación térmica	☑	☑	☑
	17	Impulsos electromagnéticos	☑	☑	☑
Compromiso de la información					
	18	Interceptación de señales de interferencia compr	☐	☑	☐
	19	Espionaje remoto	☐	☑	☐
	20	Escucha encubierta	☐	☑	☐
	21	Hurto de medios o documentos	☐	☑	☐
	22	Hurto de equipo	☐	☑	☐
	23	Recuperación de medios reciclados o desechado	☐	☑	☐
	24	Divulgación	☑	☑	☐
	25	Datos provenientes de fuentes no confiables	☑	☑	☐
	26	Manipulación con hardware	☐	☑	☐
	27	Manipulación con software	☑	☑	☐
	28	Detección de la posición	☐	☑	☐
	41	Falsificación de derechos	☐	☑	☐
	42	Negación de acciones	☐	☑	☐
	43	Incumplimiento en la disponibilidad de personal	☑	☑	☑
Fallas técnicas					
	29	Fallas del equipo	☑	☐	☐

Fuente: Los Autores

Tabla 9.

Asignación de vulnerabilidades

Catálogo de vulnerabilidades

Instituto de Seguridad Social de las Fuerzas Armadas

Hardware	
1	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento
2	Ausencia de esquemas de reemplazo periódico
3	Susceptibilidad a la humedad, el polvo y la suciedad
5	Sensibilidad a la radiación electromagnética
6	Ausencia de un eficiente control de cambios en la configuración
7	Susceptibilidad a las variaciones de voltaje
9	Susceptibilidad a las variaciones de temperatura
10	Almacenamiento sin protección
11	Falta de cuidado en la disposición final
12	Copia no controlada
101	Inadecuado control de acceso a los equipos
Software	
13	Ausencia e insuficiencia de pruebas de software
14	Defectos bien conocidos en el software
15	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo
17	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
18	Ausencia de pistas de auditoria
19	Asignación errada de los derechos de acceso
20	Software ampliamente distribuido
21	En términos de tiempo, utilización de datos errados en los programas de aplicación
22	Interfaz de usuario compleja
23	Ausencia de documentación
24	Configuración incorrecta de parámetros
25	Fechas incorrectas
26	Ausencia de mecanismos de identificación y autentificación de usuario
27	Tablas de contraseñas sin protección
28	Gestión deficiente de las contraseñas
29	Habilitación de servicios innecesarios
30	Software nuevo o inmaduro
31	Especificaciones incompletas o no claras para los desarrolladores
32	Ausencia de control de cambios eficaz
33	Descarga y uso no controlados de software
34	Ausencia de copias de respaldo
35	Ausencia de protección física de la edificación, puertas y ventanas
36	Falla en la producción de informes de gestión
100	Ausencia o desactualización de software antivirus
102	Ausencia o insuficiencia de licencias de usos de software
108	Gestión deficiente de licenciamiento de software

Fuente: Los Autores

Cada amenaza de cualquier tipo asignada al activo, estará en capacidad de explotar las vulnerabilidades inherentes a este activo, con lo cual se conforma las condiciones para generar un riesgo:

Tabla 10.

Cálculo del Riesgo

A	=	Amenaza
V	=	Vulnerabilidad
R	=	Riesgo
R = A + V		

Fuente: Los Autores

En la siguiente tabla se describe una muestra de los riesgos encontrados en el Subproceso de Gestión y Afiliación.

Tabla 11. Amenazas Sub Proceso Gestión de Afiliación y Cotización

Amenaza común y vulnerabilidad por activo de información

Instituto de Seguridad Social de las Fuerzas Armadas

1	**Gestión de afiliación y cotización**			
2	Información			
63	Información vital			
30292	**Orden judicial**			
45	**Eliminación negligente de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales
94	Ausencia o deficiencia en políticas para respaldos de información	10	Interrupción, no conti	11 Interrupción de servicio
46	**Copia fraudulenta de datos**			
96	Inadecuado control de acceso a la información	3	Robo/hurto	6 Brechas en confidenciali
97	Almacenamiento no protegido	3	Robo/hurto	6 Brechas en confidenciali
30301	**Reporte con las solicitudes de afiliación ingresadas**			
45	**Eliminación negligente de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales
46	**Copia fraudulenta de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales
30302	**Reporte con las solicitudes de datos actualizados**			
45	**Eliminación negligente de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales
46	**Copia fraudulenta de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales
30325	**Archivo de información proveniente de la fuerza Aérea, Naval, Terrestre en formato .txt**			
45	**Eliminación negligente de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales
94	Ausencia o deficiencia en políticas para respaldos de información	10	Interrupción, no conti	11 Interrupción de servicio
46	**Copia fraudulenta de datos**			
96	Inadecuado control de acceso a la información	3	Robo/hurto	6 Brechas en confidenciali
97	Almacenamiento no protegido	3	Robo/hurto	6 Brechas en confidenciali
30326	**Archivo de información proveniente de la fuerza Aérea, Naval, Terrestre en formato .xls**			
45	**Eliminación negligente de datos**			
93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3	Robo/hurto	5 Problemas legales

CONTINÚA

	94	Ausencia o deficiencia en políticas para respaldos de información	10 Interrupción, no conti	11 Interrupción de servicio
	46	**Copia fraudulenta de datos**		
	96	Inadecuado control de acceso a la información	3 Robo/hurto	6 Brechas en confidenciali
	97	Almacenamiento no protegido	3 Robo/hurto	6 Brechas en confidenciali
64		Información personal		
30265		**Cedula militar**		
	1	**Fuego, incendio**		
	106	Instalación no autorizada de equipos eléctricos	2 Destrucción	36 Daños materiales.
	107	Equipos eléctricos en mal estado	2 Destrucción	11 Interrupción de servicio
	11	**Inundación**		
	56	Ubicación en un área sensible de inundación	6 Pérdida	25 Pérdida de activos
30266		**Certificación de aportes**		
	1	**Fuego, incendio**		
	106	Instalación no autorizada de equipos eléctricos	2 Destrucción	36 Daños materiales.
	107	Equipos eléctricos en mal estado	2 Destrucción	11 Interrupción de servicio
	11	**Inundación**		
	56	Ubicación en un área sensible de inundación	6 Pérdida	25 Pérdida de activos
65		Información estratégica		
30263		**Archivo digital con información estandarizada y corregida**		
	45	**Eliminación negligente de datos**		
	93	Ausencia de procesos disciplinarios definidos en el caso de inciden	3 Robo/hurto	5 Problemas legales
	94	Ausencia o deficiencia en políticas para respaldos de información	5 Deterioro	5 Problemas legales
	46	**Copia fraudulenta de datos**		
	96	Inadecuado control de acceso a la información	3 Robo/hurto	6 Brechas en confidenciali
	97	Almacenamiento no protegido	3 Robo/hurto	6 Brechas en confidenciali
30282		**Impresión de ordenes generales**		
	1	**Fuego, incendio**		
	106	Instalación no autorizada de equipos eléctricos	2 Destrucción	36 Daños materiales.
	107	Equipos eléctricos en mal estado	2 Destrucción	11 Interrupción de servicio
	11	**Inundación**		
	56	Ubicación en un área sensible de inundación	6 Pérdida	25 Pérdida de activos
	46	**Copia fraudulenta de datos**		
	96	Inadecuado control de acceso a la información	3 Robo/hurto	6 Brechas en confidenciali
	97	Almacenamiento no protegido	3 Robo/hurto	6 Brechas en confidenciali

Fuente: Los Autores

1.5.5. Análisis de riesgos

1.5.5.1. Calificación del riesgo

Una vez que el riesgo ha sido generado en base a las amenazas y vulnerabilidades, es necesario calificar el riesgo en base a la valoración de su PROBABILIDAD e IMPACTO, definida por la Institución en la siguiente tabla de rangos:

Tabla 12:

Calificación del Riesgo

Calificación		Valor = Probabilidad * Impacto	
		Desde	Hasta
Muy alto	Catastrófico	20	25
Alto	Mayor	16	20
Medio	Moderado	11	15
Bajo	Menor	6	10
Muy bajo	Insignificante	1	5

Fuente: Los Autores

El ISSFA ha definido algunos parámetros importantes que en adelante restringirán el análisis a los datos de importancia, por ejemplo:

Figura 16: Datos contextuales del Negocio
Fuente: Los Autores

Con la información obtenida en la identificación se ha realizado la valoración de riesgos, se ha determinado la frecuencia e impacto, calculado el riesgo actual, establecido los controles recomendados y determinado el riesgo residual, resultante luego de que se han definido los controles complementarios.

El Riesgo de un activo individual resulta del producto de la Probabilidad por el Impacto. La Probabilidad es el estimado de cada cuánto tiempo puede materializarse una amenaza y el Impacto es el resultado del valor por la degradación, donde la degradación es que tan perjudicado sale el activo. Las escalas de valoración para la probabilidad e impacto se ilustran en la siguiente tabla:

Tabla 13.

Escala de calificación de probabilidad e impacto

Calificación	Valor
Muy alto	5
Alto	4
Medio	3
Bajo	2
Muy bajo	1

Fuente: Los Autores

1.5.5.2. Determinación del impacto en el proceso del negocio analizado (BIA)

El impacto de un activo de información es influye en el proceso al cual sirve, determinado durante en el proceso de análisis de impacto al negocio (o Business Impact Analysis - BIA); es decir, el impacto ocasionado en el negocio por

deficiencias en un proceso, debido a un incidente o su probabilidad de ocurrencia en el activo.

La misión del BIA es determinar el impacto de los procesos en el negocio, como consecuencia de la afectación de la disponibilidad, integridad o confidencialidad de los activos de información que lo soportan. Este se ha aplicado a todas los subprocesos del Proceso de Seguros Previsionales. El proceso se ha llevado a cabo con la participación de los dueños o responsables de cada uno de los procesos, y el patrocinio de la alta dirección.

La entrada del BIA es la matriz de procesos vs. activos de información, donde se utiliza una escala de valoración del nivel de dependencia del proceso (1 a 5). El producto resultante es el informe BIA.

Tabla 14. BIA (Business Impact Analysis)

BIA (Business Impact Analysis)

Instituto de Seguridad Social de las Fuerzas Armadas

SEGPRE	Seguros previsionales	Medio											
AFIL	Gestión de afiliación y cotización	Bajo	RTO/h.		RPO/h.		Proc. Manual	Dific. Oper.	Estrat.	Impacto Finan.	Impacto Legal	Impacto Oper.
M04-P01-01-01	Afiliación masiva de activos (Orden general)	Bajo	M	49-72	M	49-72	☑	B	M	MB	B	B
M04-P01-01-01-A	Afiliación dependientes de activos (Ventanilla de atención al cliente)	Bajo	M	49-72	M	49-72	☑	B	MA	MB	MB	B
M04-P01-01-02	Afiliación dependientes de pasivos	Bajo	M	49-72	M	49-72	☑	B	A	MB	MB	B
M04-P01-01-02-A	Afiliación dependientes de pasivos (ventanilla de atención al cliente)	Bajo	M	49-72	M	49-72	☑	B	A	MB	MB	B
M04-P01-01-03	Afiliación por orden judicial	Bajo	M	49-72	M	49-72	☑	B	A	MB	MB	B
M04-P01-02-01	Actualización de datos (Masiva activos)	Medio	M	49-72	M	49-72	☐	B	A	MB	MB	B
M04-P01-02-02	Actualizaic'on de datos manual (Activos y pasivos)	Bajo	M	49-72	M	49-72	☑	B	A	MB	MB	B
M04-P01-02-03	Actualización de datos para seguros	Bajo	A	25-48	A	25-48	☑	B	A	MB	MB	B
M04-P01-02-04	Actualización de datos ISSFA	Bajo	M	49-72	B	73-96	☑	B	A	MB	MB	B
M04-P01-03-01	Registro de aportes masivo	Medio	M	49-72	MB	97-120	☑	M	A	A	MB	A
M04-P01-03-02	Diferencia de aportaciones	Medio	A	25-48	M	49-72	☑	MA	A	MA	MB	A
M04-P01-03-03	Devolución de fondos de reserva	Alto	M	49-72	M	49-72	☐	A	A	A	MB	A
M04-P01-04	Certificación de aportes	Bajo	B	73-96	B	73-96	☑	B	A	A	MB	A

Responsable del subproceso:

Ing. Miriam Quiróz
Jefe de Afiliación del ISSFA

Ing. Rothman Cornejo
Jefe de Cotización del ISSFA

NOMI	Gestión de nómina	Medio	RTO/h.		RPO/h.		Proc. Manual	Dific. Oper.	Estrat.	Impacto Finan.	Impacto Legal	Impacto Oper.
M04-P02-01	Generación de rol de pensiones	Alto	MA	0-24	MA	0-24	☑	MA	A	MA	MA	MA
M04-P02-02	Cálculo de liquidación de pensiones atrasadas	Alto	MA	0-24	M	49-72	☑	A	A	MA	A	A
M04-P02-03	Descuentos a terceros (Masiva)	Bajo	M	49-72	M	49-72	☑	M	A	MB	MB	MB
M04-P02-04	Descuentos a terceros (Manual)	Bajo	M	49-72	M	49-72	☑	M	A	MB	MB	MB

CONTINÚA

M04-P02-05	Descuentos por retenciones judiciales	Medio	MA	0-24	M	49-72	☑	M	A	M	M	M

Responsable del subproceso:

Ing. Miriam Quiróz
Jefe de Nómina

PRES	Gestión de prestaciones	Alto	RTO/h.		RPO/h.		Proc. Manual	Dific. Oper.	Estrat.	Impacto Finan.	Impacto Legal	Impacto Oper.
M04-P03-01	Seguro de cesantía	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-02	Pensión de retiro, discapacidad e invalidez	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-03	Indemnización global	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-04	Seguro de accidentes profesionales	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-05	Seguro de invalidez	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-06	Seguro de vida	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-07-A	Seguro de mortuoria y gastos funerales (Pago a dependientes)	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-07-B	Seguro de mortuoria y gastos funerales (Pago a terceros)	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-08-A	Seguro de montepío de activos	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-08-B	Seguro de montepío de pasivos	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-09	Cancelación de pensión (Fallecimientos y pérdida de derechos)	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-10	Revisión de pensión	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-11	Rehabilitación de pensión	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-12-A	Redistribución de pensión (Acrecimientos)	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA
M04-P03-12-B	Redistribución de pensión (Coparticipación)	Alto	A	25-48	A	25-48	☑	A	A	MA	MA	MA

Responsable del subproceso:

Dr. Francisco Gaona
Jefe de Prestaciones del ISSFA

Fuente: Los Autores

Para llevarse a cabo, es necesario definir las áreas de impacto, por ejemplo: Estratégico, Financiero, Legal, Operativo, existencia de un proceso manual alternativo, RTO, RPO y cualquier otra área que la Institución considere importante para su inclusión, como la Dificultades de operación y la existencia de un proceso manual.

1.5.5.3. Determinación de la probabilidad

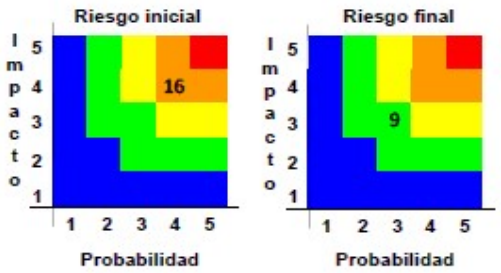
La probabilidad se determina con base en juicio experto, más aun cuando en la Institución no existen estadísticas de frecuencia, haciendo uso del catálogo de controles utilizado en la ISO 27005, calculando un promedio entre la eficiencia y eficacia del control implementado y la cantidad de controles influyentes en el riesgo al cual son aplicados.

1.5.5.4. Cálculo del riesgo

El cálculo del riesgo es el resultado de la Probabilidad por el Impacto.

Tabla 15.

Factores para determinación del riesgo



Calificación	Valor
Alto	16
Bajo	9

Fuente: Los Autores

1.5.5.5. Evaluación de riesgos

Con los resultados obtenidos en el análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable lo cual es una decisión de los dueños de los procesos, caso contrario, se define el tratamiento (retener, evitar, transferir o mitigar) y se establecen los controles necesarios. En el caso de este trabajo académico, se llegará hasta determinar un Plan de Acción el cual considerará los controles a implementar en base a una priorización definida por la Institución.

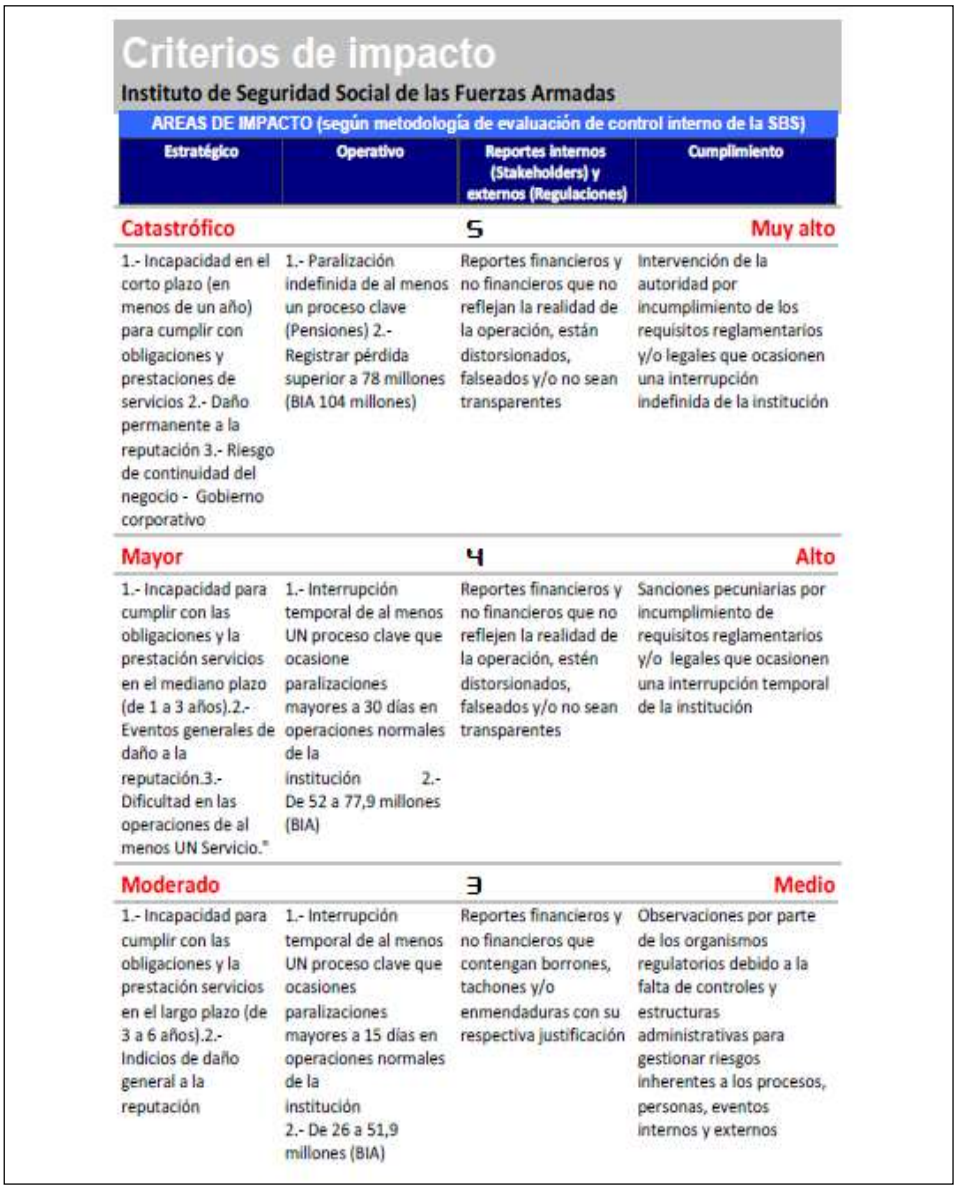
1.5.5.6. Tratamiento del riesgo

Una vez calificado el riesgo de acuerdo a los parámetros definidos por la Institución, se filtra los riesgos aptos para ser tratados, en este caso es el impacto de los riesgos calificado como MUY ALTO o CATASTROFICO y ALTO o MAYOR.

Adicionalmente se le ha asignado al riesgo una categoría referente al área de impacto definida por la Institución, seleccionada de la siguiente tabla de parámetros y debido a que el proceso por su naturaleza se encuentra posicionado en un área netamente operativa, el área de impacto para todos los riesgos es OPERATIVO.

Tabla 16.

Criterios de impacto

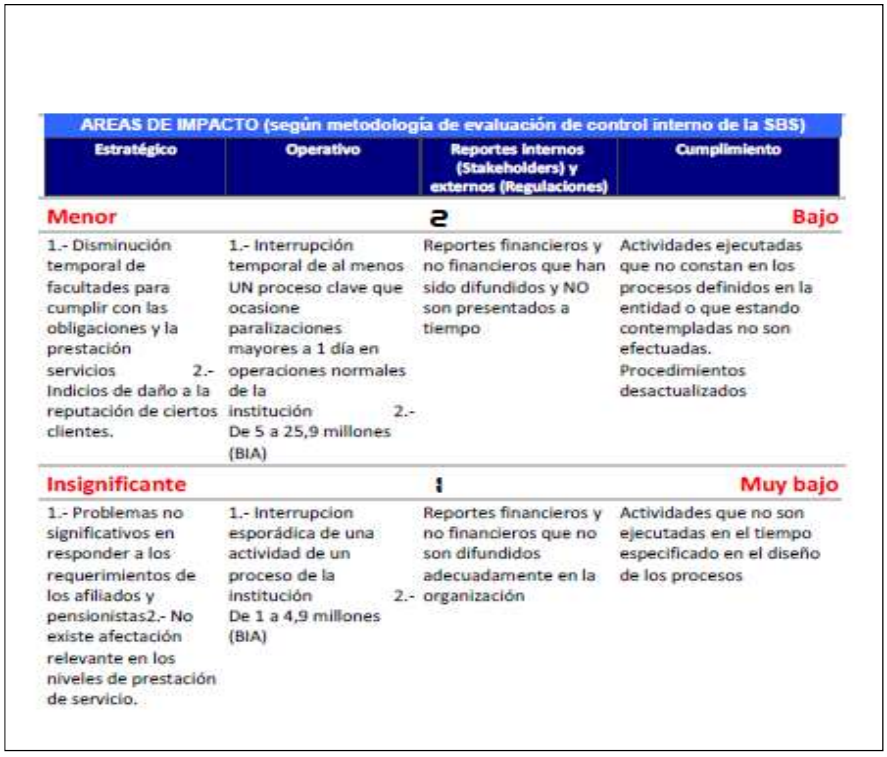


Criterios de impacto

Instituto de Seguridad Social de las Fuerzas Armadas

AREAS DE IMPACTO (según metodología de evaluación de control interno de la SBS)			
Estratégico	**Operativo**	**Reportes internos (Stakeholders) y externos (Regulaciones)**	**Cumplimiento**
Catastrófico		5	**Muy alto**
1.- Incapacidad en el corto plazo (en menos de un año) para cumplir con obligaciones y prestaciones de servicios 2.- Daño permanente a la reputación 3.- Riesgo de continuidad del negocio - Gobierno corporativo	1.- Paralización indefinida de al menos un proceso clave (Pensiones) 2.- Registrar pérdida superior a 78 millones (BIA 104 millones)	Reportes financieros y no financieros que no reflejan la realidad de la operación, están distorsionados, falseados y/o no sean transparentes	Intervención de la autoridad por incumplimiento de los requisitos reglamentarios y/o legales que ocasionen una interrupción indefinida de la institución
Mayor		4	**Alto**
1.- Incapacidad para cumplir con las obligaciones y la prestación servicios en el mediano plazo (de 1 a 3 años).2.- Eventos generales de daño a la reputación.3.- Dificultad en las operaciones de al menos UN Servicio."	1.- Interrupción temporal de al menos UN proceso clave que ocasione paralizaciones mayores a 30 días en operaciones normales de la institución 2.- De 52 a 77,9 millones (BIA)	Reportes financieros y no financieros que no reflejen la realidad de la operación, estén distorsionados, falseados y/o no sean transparentes	Sanciones pecuniarias por incumplimiento de requisitos reglamentarios y/o legales que ocasionen una interrupción temporal de la institución
Moderado		3	**Medio**
1.- Incapacidad para cumplir con las obligaciones y la prestación servicios en el largo plazo (de 3 a 6 años).2.- Indicios de daño general a la reputación	1.- Interrupción temporal de al menos UN proceso clave que ocasiones paralizaciones mayores a 15 días en operaciones normales de la institución 2.- De 26 a 51,9 millones (BIA)	Reportes financieros y no financieros que contengan borrones, tachones y/o enmendaduras con su respectiva justificación	Observaciones por parte de los organismos regulatorios debido a la falta de controles y estructuras administrativas para gestionar riesgos inherentes a los procesos, personas, eventos internos y externos

CONTINÚA



AREAS DE IMPACTO (según metodología de evaluación de control interno de la SBS)			
Estratégico	**Operativo**	**Reportes internos (Stakeholders) y externos (Regulaciones)**	**Cumplimiento**
Menor		2	**Bajo**
1.- Disminución temporal de facultades para cumplir con las obligaciones y la prestación servicios 2.- Indicios de daño a la reputación de ciertos clientes.	1.- Interrupción temporal de al menos UN proceso clave que ocasione paralizaciones mayores a 1 día en operaciones normales de la institución 2.- De 5 a 25,9 millones (BIA)	Reportes financieros y no financieros que han sido difundidos y NO son presentados a tiempo	Actividades ejecutadas que no constan en los procesos definidos en la entidad o que estando contempladas no son efectuadas. Procedimientos desactualizados
Insignificante		1	**Muy bajo**
1.- Problemas no significativos en responder a los requerimientos de los afiliados y pensionistas2.- No existe afectación relevante en los niveles de prestación de servicio.	1.- Interrupcion esporádica de una actividad de un proceso de la institución 2.- De 1 a 4,9 millones (BIA)	Reportes financieros y no financieros que no son difundidos adecuadamente en la organización	Actividades que no son ejecutadas en el tiempo especificado en el diseño de los procesos

Fuente: Los Autores

Los riesgos resultantes son los que pasan a la siguiente fase que es la de tratar los riesgos en base a la siguiente tabla de parámetros:

Tabla 17.

Parámetros para avance de fase en riesgos

Aceptar, retener
Evitar
Reducir
Transferir

Fuente: Los Autores

Para el caso de este documento académico y con el objeto de contar con los datos suficientes, se ha definido el parámetro tratamiento del riesgo como REDUCIR para todos los riesgos. Esta forma de tratamiento del riesgo permite asignar los controles de la norma ISO/IEC 27002:2005 que sean necesarios para mitigarlo y reducirlo.

1.6. Utilización de controles de la Norma ISO/IEC 27002:2005

Estos controles e encuentran definidos en la mencionada norma de la familia ISO/IEC 27000 y son ampliamente usados para implantar un SGSI o como criterios para realizar auditorías o evaluaciones técnicas de seguridad de información como en el caso de este estudio.

Tabla 18:
Controles ISO 27002

Anexo "A", controles ISO 27002

Instituto de Seguridad Social de las Fuerzas Armadas

A.5 POLITICA DE SEGURIDAD

A.5.1 POLÍTICA DE SEGURIDAD DE INFORMACIÓN

Objetivo de Control:
Brindar orientación y apoyo a la dirección en la seguridad de información de acuerdo con los requerimientos del negocio, leyes relevantes y regulaciones.

A.5.1.1 Documento de la política de seguridad de la información.

Control: Un documento de la política de seguridad debe ser aprobado por la dirección, y publicado y comunicado a todos los empleados y a partes externas relevantes.

A.5.1.2 Revisión Política de seguridad de la información

Control: La información de la política de seguridad de la información debe ser revisado a intervalos planeados o si hay cambios significativos para asegurar la conveniencia de su continuidad, adecuación y efectividad

A.6 ORGANIZACIÓN DE SEGURIDAD DE INFORMACION

A.6.1 Organización Interna.

Objetivo de control:
Gestionar la seguridad de la información dentro de la organización.

A.6.1.1 Compromiso de la dirección en la seguridad de la información.

Control: La dirección debe soportar activamente la seguridad dentro de la organización a través de directrices claras, compromiso demostrado, asignaciones expresas, y reconocimiento de las responsabilidades de la seguridad de la información

A.6.1.2 Coordinación de la seguridad de la información.

Control: Las actividades de la seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con roles relevantes y funciones de trabajo.

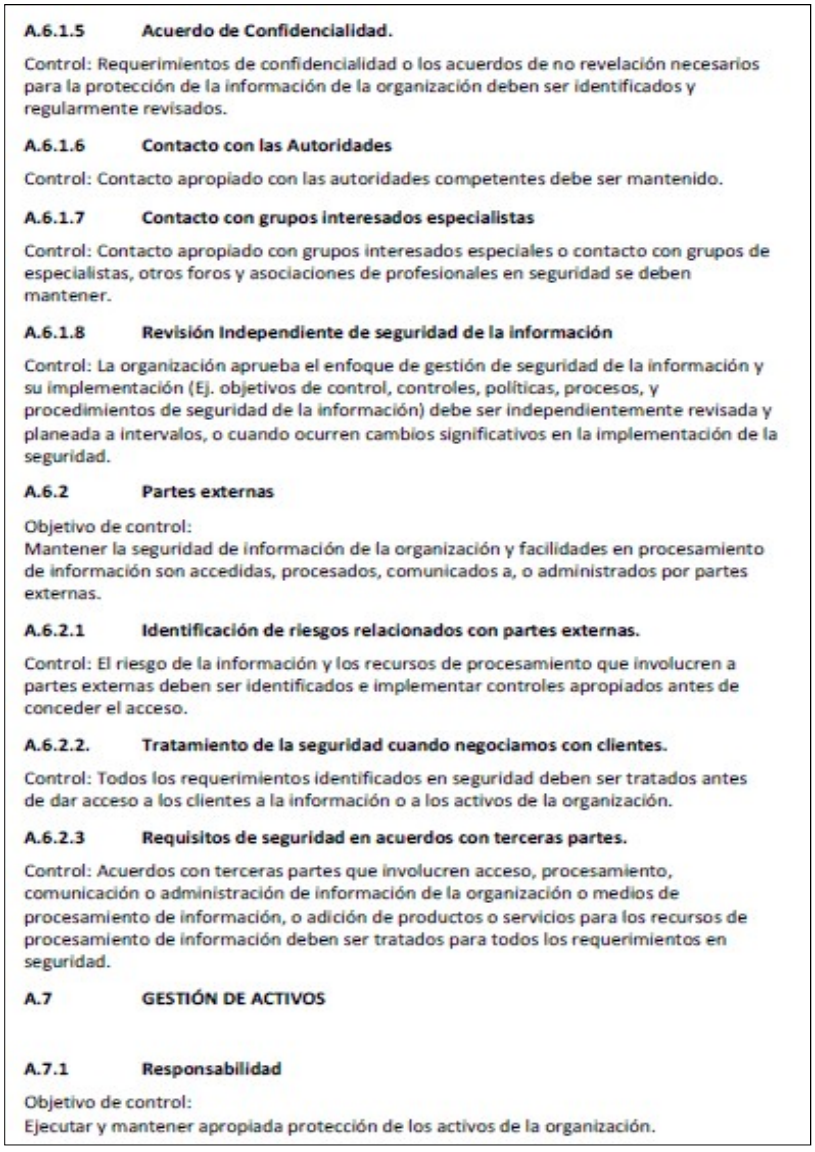
A.6.1.3 Asignación de responsabilidades de la seguridad de la información

Control: Toda la responsabilidad en seguridad de la información debe ser claramente definida.

A.6.1.4 Proceso de autorización para medios de procesamiento de la información.

Control: Un proceso de gestión de autorización para un medio de procesamiento nuevo debe ser definido e implementado.

CONTINÚA



A.6.1.5 Acuerdo de Confidencialidad.

Control: Requerimientos de confidencialidad o los acuerdos de no revelación necesarios para la protección de la información de la organización deben ser identificados y regularmente revisados.

A.6.1.6 Contacto con las Autoridades

Control: Contacto apropiado con las autoridades competentes debe ser mantenido.

A.6.1.7 Contacto con grupos interesados especialistas

Control: Contacto apropiado con grupos interesados especiales o contacto con grupos de especialistas, otros foros y asociaciones de profesionales en seguridad se deben mantener.

A.6.1.8 Revisión Independiente de seguridad de la información

Control: La organización aprueba el enfoque de gestión de seguridad de la información y su implementación (Ej. objetivos de control, controles, políticas, procesos, y procedimientos de seguridad de la información) debe ser independientemente revisada y planeada a intervalos, o cuando ocurren cambios significativos en la implementación de la seguridad.

A.6.2 Partes externas

Objetivo de control:
Mantener la seguridad de información de la organización y facilidades en procesamiento de información son accedidas, procesados, comunicados a, o administrados por partes externas.

A.6.2.1 Identificación de riesgos relacionados con partes externas.

Control: El riesgo de la información y los recursos de procesamiento que involucren a partes externas deben ser identificados e implementar controles apropiados antes de conceder el acceso.

A.6.2.2. Tratamiento de la seguridad cuando negociamos con clientes.

Control: Todos los requerimientos identificados en seguridad deben ser tratados antes de dar acceso a los clientes a la información o a los activos de la organización.

A.6.2.3 Requisitos de seguridad en acuerdos con terceras partes.

Control: Acuerdos con terceras partes que involucren acceso, procesamiento, comunicación o administración de información de la organización o medios de procesamiento de información, o adición de productos o servicios para los recursos de procesamiento de información deben ser tratados para todos los requerimientos en seguridad.

A.7 GESTIÓN DE ACTIVOS

A.7.1 Responsabilidad

Objetivo de control:
Ejecutar y mantener apropiada protección de los activos de la organización.

Fuente: Instituto de Seguridad Social de las Fuerzas Armadas

1.7. Sistema informático para el análisis de riesgos

Debido a la gran cantidad de información que un análisis de riesgos utiliza y genera, dependiendo también de la dimensión relativa del proceso a analizar, ha sido

necesario desarrollar un software especializado para gestionar los referidos datos. El resultado es la disponibilidad de información completa en tiempo real referente a cualquier riesgo y la posibilidad de modificarla o eliminarla manteniendo la consistencia del sistema, un beneficio adicional es la posibilidad de generar reportes personalizados, incluidos mapas de calor, de acuerdo a la investigación que el analista de riesgos requiera, existe la capacidad de manejar múltiples empresas y múltiples procesos llegando a definir informes de auditorías y planes, programas y proyecto de acción integrados al resto del sistema.

Este software constituye un valor agregado generado como parte de este trabajo.

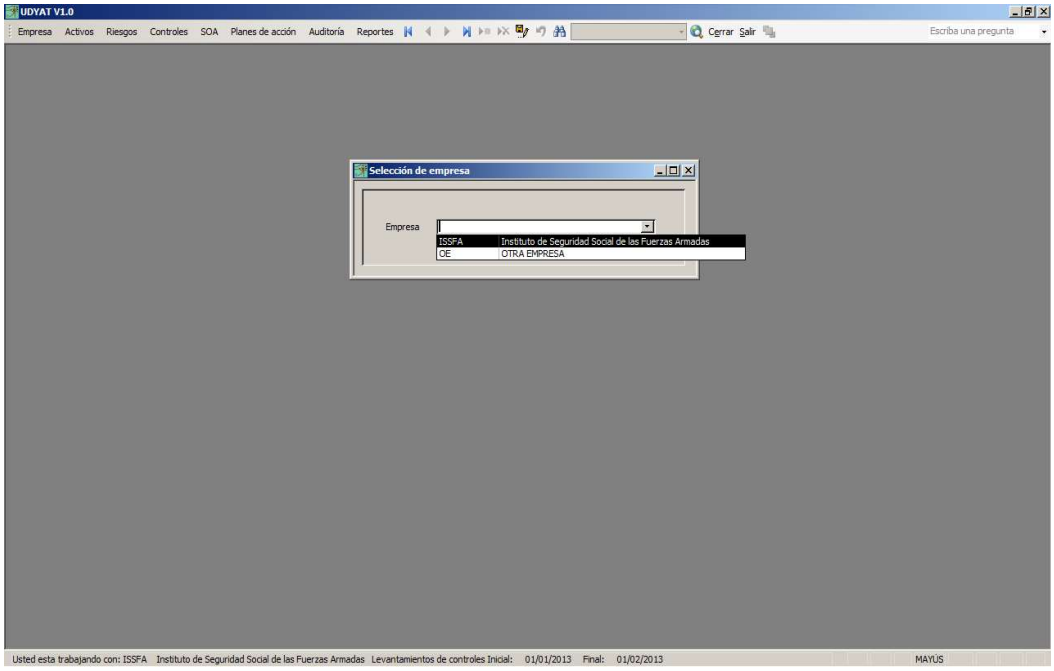


Figura 17: Pantalla de selección de empresa

Fuente: Los Autores

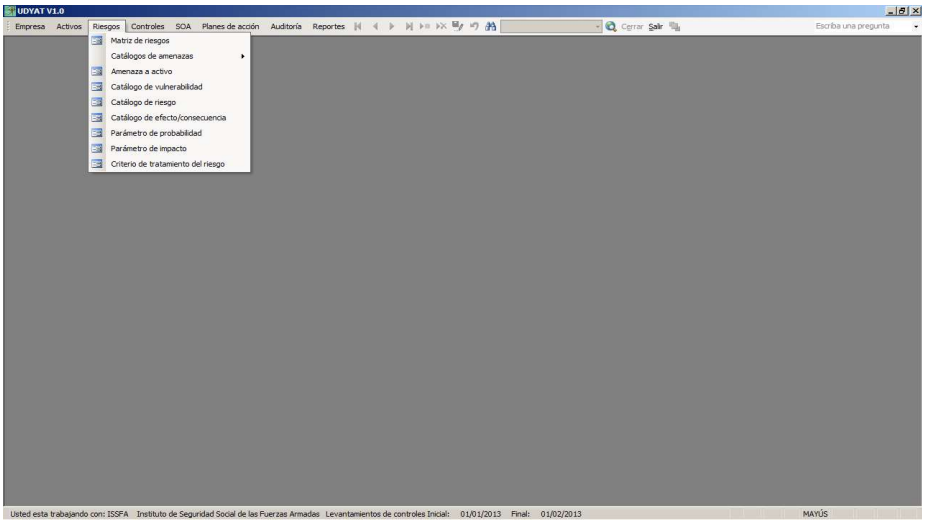


Figura 18: Menú principal del sistema

Fuente: Los Autores

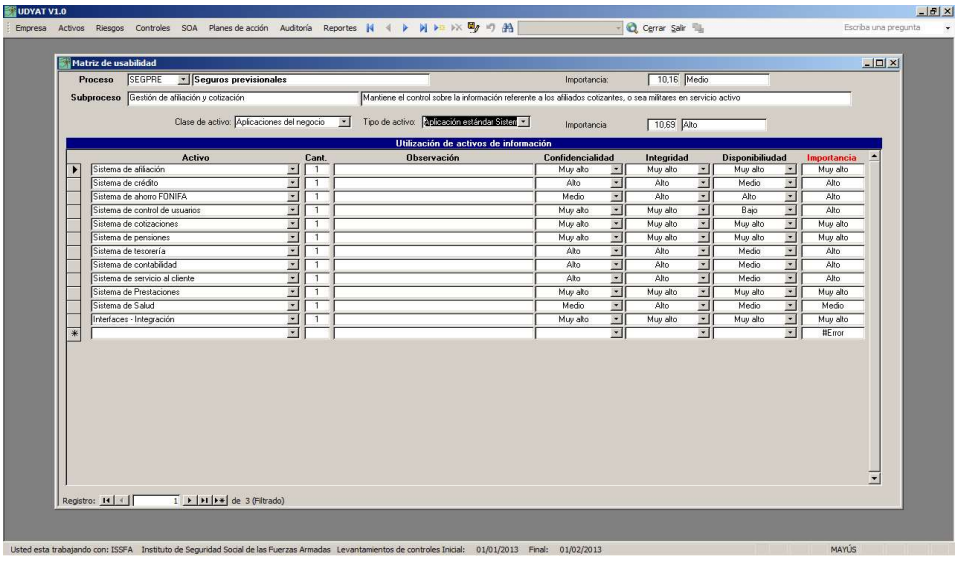


Figura 19: Uso y calificación de activos en los procesos.

Fuente: Los Autores

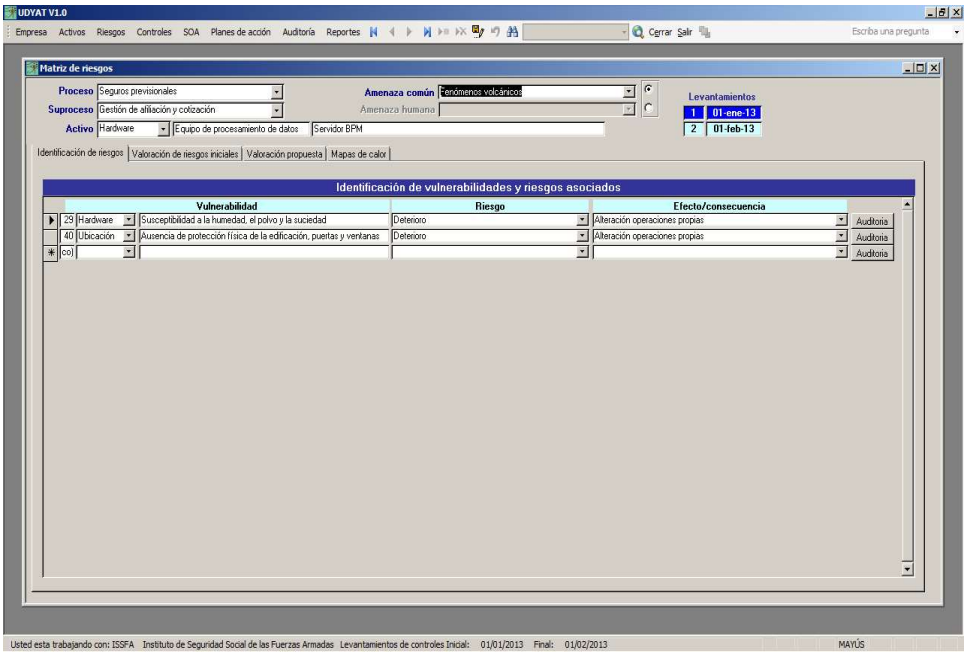


Figura 20: Definición de riesgos

Fuente: Los Autores

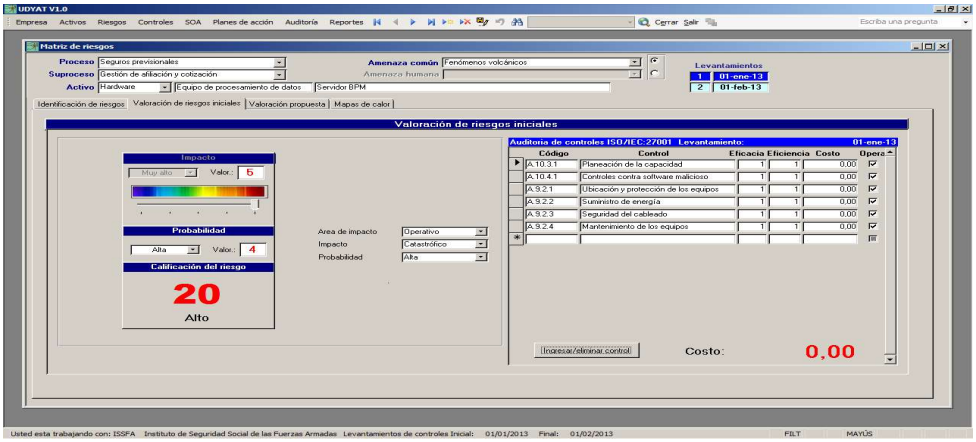
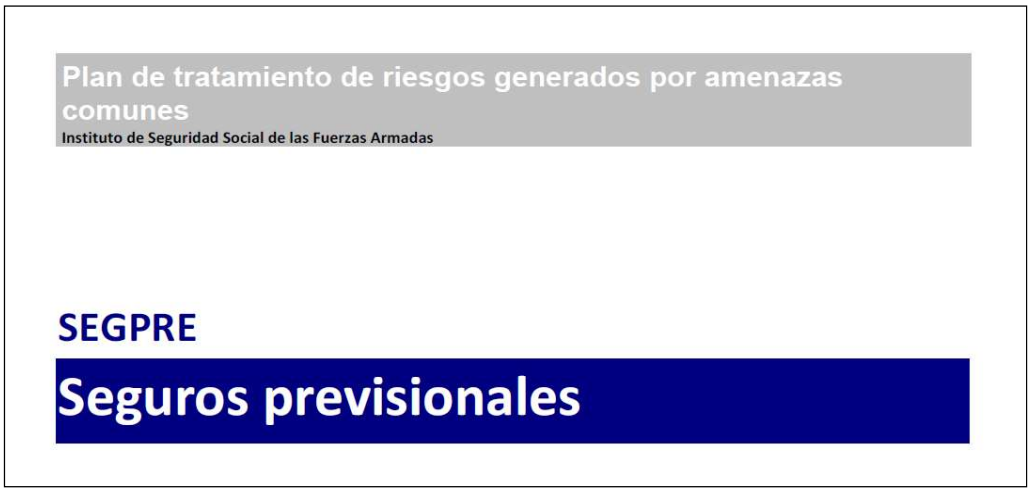


Figura 21: Análisis de riesgos

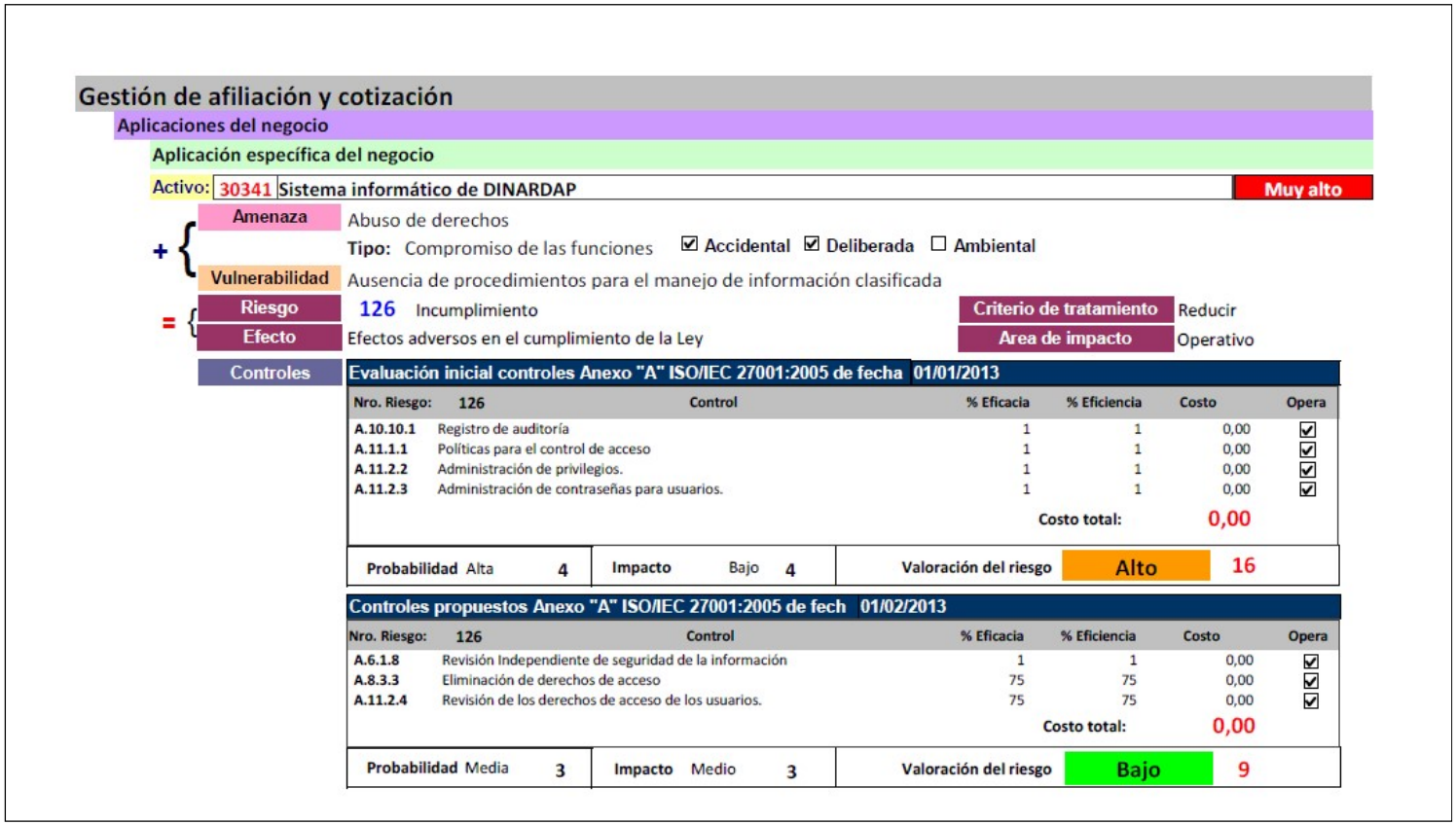
Fuente: Los Autores

1.8. Plan de tratamiento del riesgo

Con base en el informe de riesgos de TI, se ha procedido a la elaboración del plan de tratamiento de riesgos TI. Posteriormente se podrá proceder a la implementación, ejecución y monitoreo de los controles establecidos. En el **ANEXO I** se detalla plan de tratamiento de riesgos por amenazas comunes, y el **ANEXO J** el plan de tratamiento de riesgos por amenazas humanas.



CONTINÚA



Gestión de afiliación y cotización

Aplicaciones del negocio

Aplicación específica del negocio

Activo: 30341 Sistema informático de DINARDAP — **Muy alto**

Amenaza Abuso de derechos

Tipo: Compromiso de las funciones ☑ Accidental ☑ Deliberada ☐ Ambiental

Vulnerabilidad Ausencia de procedimientos para el manejo de información clasificada

Riesgo 126 Incumplimiento — **Criterio de tratamiento** Reducir

Efecto Efectos adversos en el cumplimiento de la Ley — **Area de impacto** Operativo

Controles

Evaluación inicial controles Anexo "A" ISO/IEC 27001:2005 de fecha 01/01/2013

Nro. Riesgo: 126	Control	% Eficacia	% Eficiencia	Costo	Opera
A.10.10.1	Registro de auditoría	1	1	0,00	☑
A.11.1.1	Políticas para el control de acceso	1	1	0,00	☑
A.11.2.2	Administración de privilegios.	1	1	0,00	☑
A.11.2.3	Administración de contraseñas para usuarios.	1	1	0,00	☑
			Costo total:	0,00	

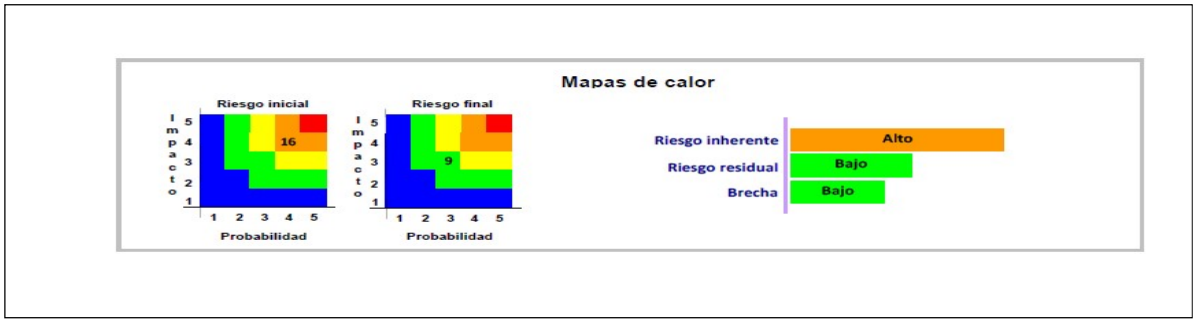
Probabilidad Alta 4	Impacto Bajo 4	Valoración del riesgo Alto 16

Controles propuestos Anexo "A" ISO/IEC 27001:2005 de fech 01/02/2013

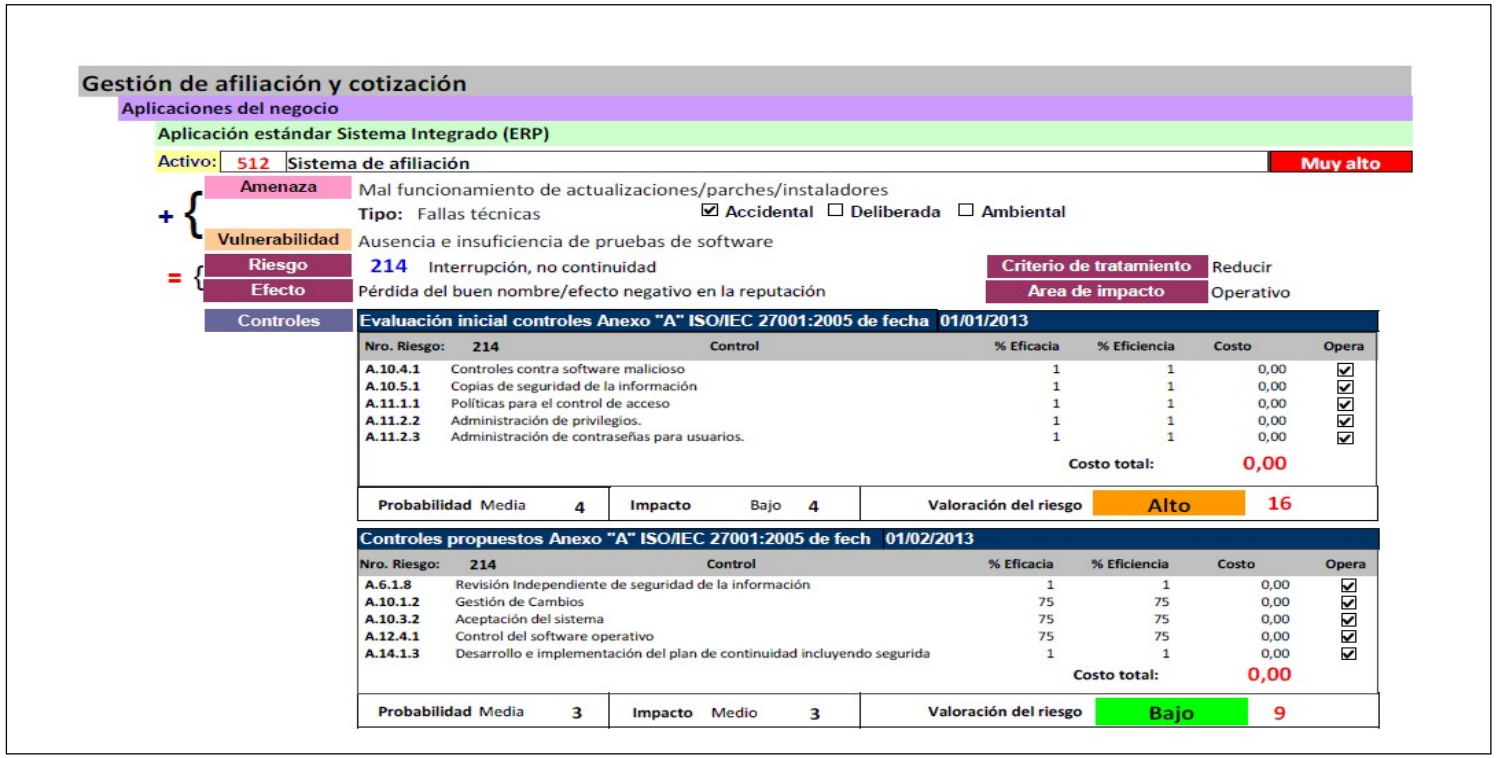
Nro. Riesgo: 126	Control	% Eficacia	% Eficiencia	Costo	Opera
A.6.1.8	Revisión Independiente de seguridad de la información	1	1	0,00	☑
A.8.3.3	Eliminación de derechos de acceso	75	75	0,00	☑
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	75	75	0,00	☑
			Costo total:	0,00	

Probabilidad Media 3	Impacto Medio 3	Valoración del riesgo Bajo 9

CONTINÚA


Mapas de calor
Riesgo inicial
Impacto
5
4
3
2
1
16
1 2 3 4 5
Probabilidad
Riesgo final
Impacto
5
4
3
2
1
9
1 2 3 4 5
Probabilidad
Riesgo inherente
Alto
Riesgo residual
Bajo
Brecha
Bajo

CONTINÚA



Gestión de afiliación y cotización

Aplicaciones del negocio

Aplicación estándar Sistema Integrado (ERP)

Activo: 512 Sistema de afiliación — **Muy alto**

Amenaza — Mal funcionamiento de actualizaciones/parches/instaladores

Tipo: Fallas técnicas — ☑ Accidental ☐ Deliberada ☐ Ambiental

Vulnerabilidad — Ausencia e insuficiencia de pruebas de software

Riesgo — 214 Interrupción, no continuidad

Efecto — Pérdida del buen nombre/efecto negativo en la reputación

Criterio de tratamiento — Reducir

Area de impacto — Operativo

Controles

Evaluación inicial controles Anexo "A" ISO/IEC 27001:2005 de fecha 01/01/2013

Nro. Riesgo:	214	Control	% Eficacia	% Eficiencia	Costo	Opera
A.10.4.1	Controles contra software malicioso		1	1	0,00	☑
A.10.5.1	Copias de seguridad de la información		1	1	0,00	☑
A.11.1.1	Políticas para el control de acceso		1	1	0,00	☑
A.11.2.2	Administración de privilegios.		1	1	0,00	☑
A.11.2.3	Administración de contraseñas para usuarios.		1	1	0,00	☑
				Costo total:	0,00	

Probabilidad	Media	4	Impacto	Bajo	4	Valoración del riesgo	Alto	16

Controles propuestos Anexo "A" ISO/IEC 27001:2005 de fech 01/02/2013

Nro. Riesgo:	214	Control	% Eficacia	% Eficiencia	Costo	Opera
A.6.1.8	Revisión Independiente de seguridad de la información		1	1	0,00	☑
A.10.1.2	Gestión de Cambios		75	75	0,00	☑
A.10.3.2	Aceptación del sistema		75	75	0,00	☑
A.12.4.1	Control del software operativo		75	75	0,00	☑
A.14.1.3	Desarrollo e implementación del plan de continuidad incluyendo segurida		1	1	0,00	☑
				Costo total:	0,00	

Probabilidad	Media	3	Impacto	Medio	3	Valoración del riesgo	Bajo	9

CONTINÚA

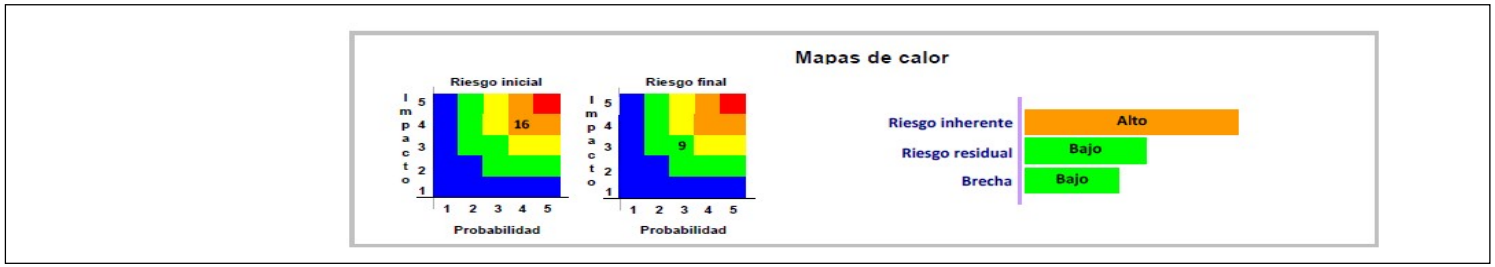


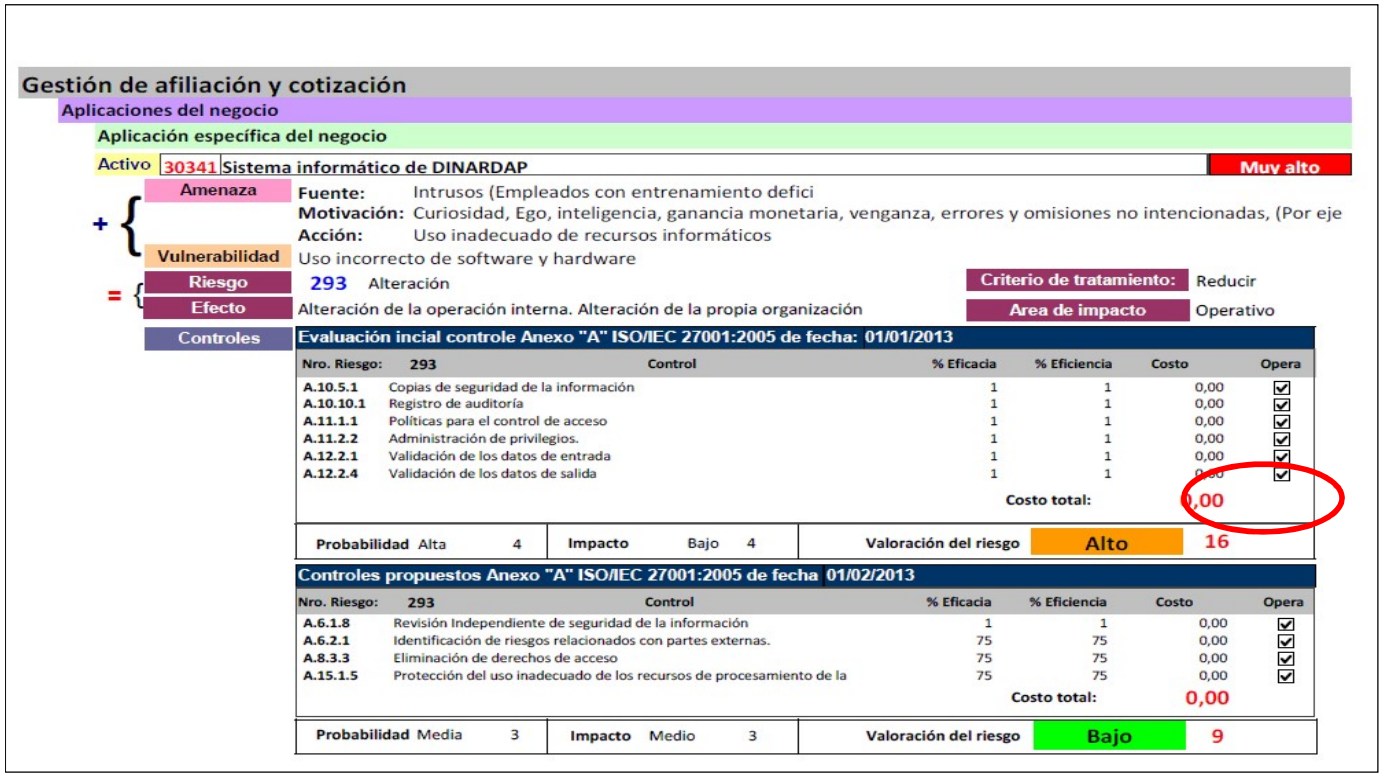
Figura 22: Plan de tratamiento de riesgos generados por amenazas comunes

Fuente: Los Autores

SEGPRE

Seguros previsionales

CONTINÚA



Gestión de afiliación y cotización

Aplicaciones del negocio

Aplicación específica del negocio

Activo | 30341 | Sistema informático de DINARDAP | **Muy alto**

Amenaza — **Fuente:** Intrusos (Empleados con entrenamiento defici
Motivación: Curiosidad, Ego, inteligencia, ganancia monetaria, venganza, errores y omisiones no intencionadas, (Por eje
Acción: Uso inadecuado de recursos informáticos

Vulnerabilidad — Uso incorrecto de software y hardware

Riesgo — 293 Alteración — **Criterio de tratamiento:** Reducir

Efecto — Alteración de la operación interna. Alteración de la propia organización — **Area de impacto** Operativo

Controles

Evaluación incial controle Anexo "A" ISO/IEC 27001:2005 de fecha: 01/01/2013

Nro. Riesgo:	293	Control	% Eficacia	% Eficiencia	Costo	Opera
A.10.5.1	Copias de seguridad de la información		1	1	0,00	☑
A.10.10.1	Registro de auditoría		1	1	0,00	☑
A.11.1.1	Políticas para el control de acceso		1	1	0,00	☑
A.11.2.2	Administración de privilegios.		1	1	0,00	☑
A.12.2.1	Validación de los datos de entrada		1	1	0,00	☑
A.12.2.4	Validación de los datos de salida		1	1	0,00	☑
				Costo total:	0,00	

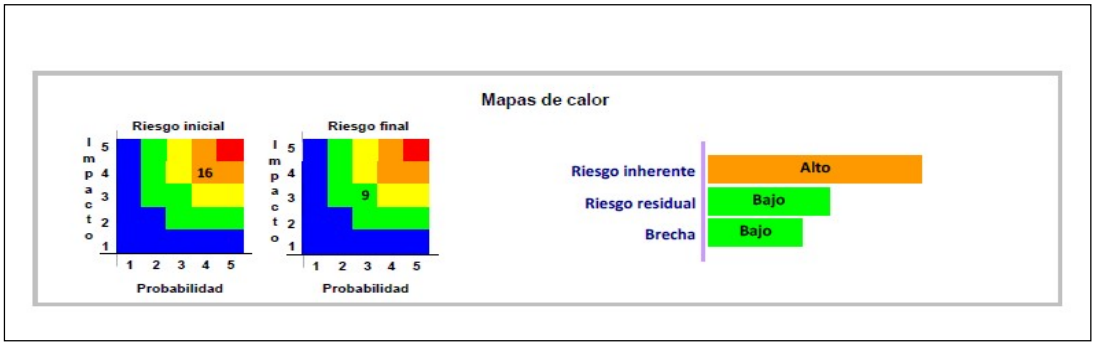
Probabilidad	Alta	4	Impacto	Bajo	4	Valoración del riesgo	Alto	16

Controles propuestos Anexo "A" ISO/IEC 27001:2005 de fecha 01/02/2013

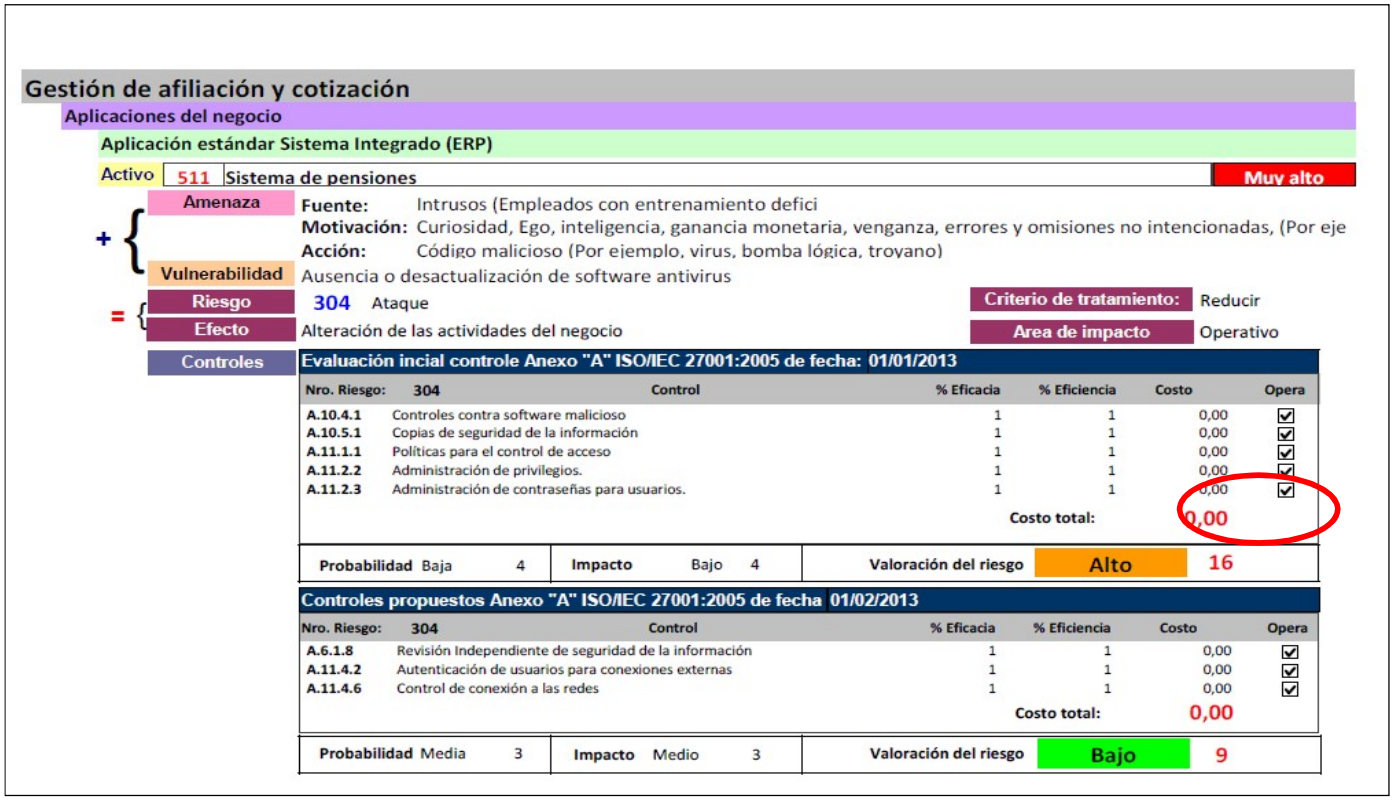
Nro. Riesgo:	293	Control	% Eficacia	% Eficiencia	Costo	Opera
A.6.1.8	Revisión Independiente de seguridad de la información		1	1	0,00	☑
A.6.2.1	Identificación de riesgos relacionados con partes externas.		75	75	0,00	☑
A.8.3.3	Eliminación de derechos de acceso		75	75	0,00	☑
A.15.1.5	Protección del uso inadecuado de los recursos de procesamiento de la		75	75	0,00	☑
				Costo total:	0,00	

Probabilidad	Media	3	Impacto	Medio	3	Valoración del riesgo	Bajo	9

CONTINÚA


Mapas de calor
Riesgo inicial
Impacto
5
4
3
2
1
16
1 2 3 4 5
Probabilidad
Riesgo final
Impacto
5
4
3
2
1
9
1 2 3 4 5
Probabilidad
Riesgo inherente
Alto
Riesgo residual
Bajo
Brecha
Bajo

CONTINÚA



Gestión de afiliación y cotización

Aplicaciones del negocio

Aplicación estándar Sistema Integrado (ERP)

Activo 511 **Sistema de pensiones** — **Muy alto**

Amenaza (+)
Fuente: Intrusos (Empleados con entrenamiento defici
Motivación: Curiosidad, Ego, inteligencia, ganancia monetaria, venganza, errores y omisiones no intencionadas, (Por eje
Acción: Código malicioso (Por ejemplo, virus, bomba lógica, troyano)

Vulnerabilidad (+) Ausencia o desactualización de software antivirus

Riesgo (=) 304 Ataque — **Criterio de tratamiento:** Reducir

Efecto (=) Alteración de las actividades del negocio — **Area de impacto** Operativo

Controles

Evaluación incial controle Anexo "A" ISO/IEC 27001:2005 de fecha: 01/01/2013

Nro. Riesgo:	304	Control	% Eficacia	% Eficiencia	Costo	Opera
A.10.4.1	Controles contra software malicioso		1	1	0,00	☑
A.10.5.1	Copias de seguridad de la información		1	1	0,00	☑
A.11.1.1	Políticas para el control de acceso		1	1	0,00	☑
A.11.2.2	Administración de privilegios.		1	1	0,00	☑
A.11.2.3	Administración de contraseñas para usuarios.		1	1	0,00	☑
				Costo total:	0,00	

Probabilidad	Baja	4	Impacto	Bajo	4	Valoración del riesgo	Alto	16

Controles propuestos Anexo "A" ISO/IEC 27001:2005 de fecha 01/02/2013

Nro. Riesgo:	304	Control	% Eficacia	% Eficiencia	Costo	Opera
A.6.1.8	Revisión Independiente de seguridad de la información		1	1	0,00	☑
A.11.4.2	Autenticación de usuarios para conexiones externas		1	1	0,00	☑
A.11.4.6	Control de conexión a las redes		1	1	0,00	☑
				Costo total:	0,00	

Probabilidad	Media	3	Impacto	Medio	3	Valoración del riesgo	Bajo	9

CONTINÚA

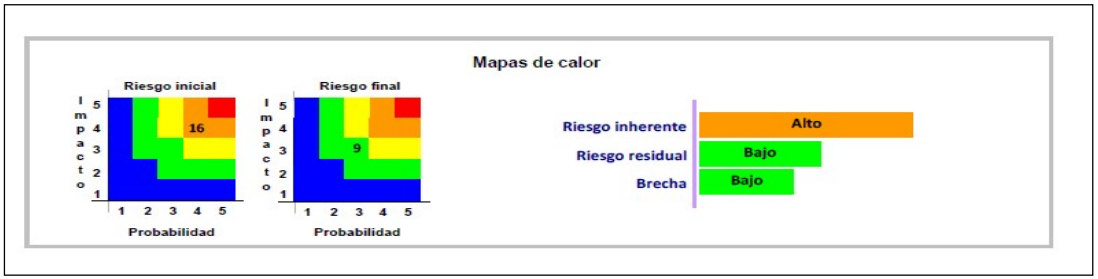


Figura 23: Plan de tratamiento de riesgos generados por amenazas humanas

Fuente: Los Autores

1.9. Declaración de aplicabilidad de controles o SOA (Statement Of Aplicability)

Un análisis adicional que se incluye en el presente trabajo, es la declaración de aplicabilidad (SOA) de los controles seleccionados y no seleccionados para la aplicación en la mitigación de los riesgos. **ANEXO K** declaración de aplicabilidad.

Tabla 19.

Declaración de Aplicabilidad de Controles (SOA)

Statement of Aplicability (SOA)

Instituto de Seguridad Social de las Fuerzas Armadas — Levantamiento: 01-feb-13

	Dominio / Objetivo de control / Control		Justificación para implementar	Justificación para NO implementar
A.5	POLITICA DE SEGURIDAD	☐		
A.5.1	POLÍTICA DE SEGURIDAD DE INFORMACIÓN	☐		
A.5.1.1	Documento de la política de seguridad de la información.	☐		No se puede recomendar la creación de una política general de información ya que el objeto de este estudio no es el de implantar un SGSI
A.5.1.2	Revisión Política de seguridad de la información	☐		No se puede revisar la política general de información ya que no existe un SGSI implantado
A.6	ORGANIZACIÓN DE SEGURIDAD DE INFORMACION	☐		
A.6.1	Organización Interna.	☐		
A.6.1.1	Compromiso de la dirección en la seguridad de la informa	☐		La Dirección General del ISSFA no tiene aun los elementos de juicio suficientes como para asumir un compromiso de este tipo. Este estudio es un insumo para que la Dirección General tome decisiones que afecten a la estructura de la seguridad de información.
A.6.1.2	Coordinación de la seguridad de la información.	☐		a Dirección General del ISSFA no tiene aun los elementos de juicio suficientes como para asumir un compromiso de este tipo. Este estudio es un insumo para que la Dirección General tome decisiones que afecten a la estructura de la seguridad de información.

Fuente: Los Autores

CAPITULO IV

INFORME FINAL DE LA EVALUACION TECNICA DE SEGURIDAD DE INFORMACION EN EL PROCESO DE SEGUROS PREVISIONALES DEL ISSFA

4.1. Alcance

La evaluación de seguridad de información está limitada a los siguientes procesos del ISSFA Matriz en Quito:

Proceso: Seguros Previsionales

Subprocesos: Gestión de Afiliación y Cotización

: Gestión de Nómina

: Gestión de Prestaciones

4.2. Enfoque

La evaluación se la ha realizado en base a riesgos y los objetivos de control tomados en cuenta son los considerados en la norma ISO/IEC 27002:2005 y son los siguientes:

- Configuración e implementación de técnicas y herramientas de seguridad lógica para restringir el acceso a programas, datos y otros recursos de información.
- Restricciones de acceso físico para garantizar que solamente el personal autorizado pueda tener acceso o utilizar los recursos de información.
- Seguridad lógica y física adecuada para los recursos de información.

- Los sistemas se desarrollan e implementan apropiadamente para proporcionar las bases que soporten el procesamiento y registro completo, exacto y válido de la información
- Los cambios a los sistemas se administran apropiadamente para minimizar la probabilidad de una interrupción, alteraciones no autorizadas y errores que impacten el procesamiento y registro completo, exacto y válido de la información.
- Los sistemas reciben mantenimiento y soporte adecuado en caso de falla.
- Los cambios a los sistemas son aprobados por los dueños de los procesos antes de su ejecución.
- Recuperación oportuna de procesos de negocio y de sistemas informáticos, en caso de una contingencia o de un desastre.
- Políticas y procedimientos de recuperación de la información.
- Respaldos de información de manera periódica.
- Control de cintas de respaldo con información histórica.
- Pruebas para la recuperación de la información.
- Identificación y clasificación de la información clave.
- La selección de proveedores es consistente con las intenciones de la gerencia.
- Medición y calificación de los niveles de servicio que está prestando el proveedor.
- Cumplimiento de los niveles de servicio de proveedores externos.
- Identificar el estatus contractual de los proveedores.
- Identificar garantías de soporte y continuidad de la operación de los sistemas que proporciona el proveedor.
- Validar el control sobre el licenciamiento en el uso de las aplicaciones principales.

INFORME FINAL DE EVAUACION

DE SEGURIDAD DE INFORMACION

Instituto de Seguridad Social de las Fuerzas Armadas

Levantamiento: 01/02/2013

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 1 NO EXISTE CONTROL EN LA ENTREGA DE INFORMACION A TERCEROS

Condición

Los proveedores o terceros en general, reciben información por parte del ISSFA, la misma que no es protegida mediante un compromiso formal firmado por las partes.

Criterio de evaluación

Código	**Control**
A.6.1.5	Acuerdo de Confidencialidad.

CONTINÚA

A.6.2.3 Requisitos de seguridad en acuerdos con terceras partes.

A.6.2.1 Identificación de riesgos relacionados con partes externas.

A.10.2.1 Entrega de servicios

A.10.2.2 Monitoreo y revisión de servicios suministrados por terceras partes

A.10.8.1 Procedimientos y políticas para el intercambio de información

A.10.8.2 Acuerdos de Intercambio

Causa

Los proveedores obtienen información institucional de todo tipo

Efecto

La información del ISSFA se encuentra en condiciones de ser difundida por terceros sin que se pueda realizar reclamos o demandas legales.

Recomendaciones

1 Para: Director General

Disponer a quien corresponda la implantación de los procedimientos necesarios para normar la entrega de la información.

2 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda, incluir criterios de seguridad de información en todos los documentos que involucren a terceros, referir a las normas internas y externas.

CONTINÚA

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 2 INEXISTENCIA DE AUDITORIAS INDEPENDIENTES DE SEGURIDAD DE INFORMACION EN EL PROCESO DE SEGUROS PREVISIONALES

Condición

Los controles de seguridad que existen en este momento no muestran suficiencia para mantener la confidencialidad, integridad y disponibilidad de la información institucional.

Criterio de evaluación

Código	**Control**
A.6.1.8	Revisión Independiente de seguridad de la información

Causa

No existe implantad una normativa o buenas prácticas para gestionar la seguridad de información, esta depende de controles insuficientes e incompletos.

Efecto

Los controles existentes no han sido auditados en forma independiente, bajo normas de seguridad de información.

CONTINÚA

Recomendaciones

5 Para: Director de Riesgos

Incluir en el plan de tratamiento de riesgos operativos, las auditorías independientes de seguridad de información generada y manipulada en este subproceso.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 3 LA INFORMACION DEL PROCESO DE SEGUROS PREVISIONALES NO SE ENCUENTRA CLASIFICADA

Condición

No se puede identificar membretes que identifiquen la clasificación de la información de la Institución que circula por diferentes medios.

Criterio de evaluación

Código **Control**

A.7.2.1 Guías de clasificación

Causa

La información no es manipulada de acuerdo a su importancia.

Efecto

Toda la información es tratada de igual manera, ocasionando falta de cuidado en información considerada importante para la Institución.

Recomendaciones

3 **Para:** **Secretario General**

Implantar normas de clasificación de la documentación generada por el presente proceso.

CONTINÚA

4 Para: <u>Jefe de la UTIC</u>

Implantar normas de clasificación de información digital, generada y recibida por este proceso, coordinar con Secretario General.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 5 NO EXISTE SEGREGACION DE FUNCIONES EN EL PERSONAL DE TECNOLOGIA INVOLUCRADOEN EL PROCESO

Condición

El personal de tecnología realiza funciones adicionales de las indicadas en sus funciones.

Criterio de evaluación

Código	**Control**
A.8.1.1	Funciones y Responsabilidades
A.8.1.3	Términos y condiciones de la relación laboral
A.8.2.1	Gestión de las responsabilidades
A.10.1.3	Separación de funciones

Causa

El personal que realiza desarrollo tiene acceso a las aplicaciones fuentes y de producción, el personal de infraestructura tienen acceso a los recursos de seguridad, debido a la falta de personal.

Efecto

El mismo personal es juez y parte.

CONTINÚA

Recomendaciones

8 Para: <u>Coordinador Administrativo Financiero</u>

Disponga el completamiento del orgánico de personal de la UTIC y facilite la segregación de funciones.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 6 NO EXISTE UN PROCESO FORMAL DE GESTION DE CAMBIOS EN LOS SISTEMAS TECNOLOGICOS

Condición

Los requerimientos de los usuarios para realizar cambios en los sistemas de información y demás recursos informáticos, no son emitidos con la aprobación de la Unidad de Planificación y Doctrina, por lo tanto los cambios no pueden ser documentados correctamente. En algunos casos no existe registro de cambios realizados.

Criterio de evaluación

Código	**Control**
A.10.1.2	Gestión de Cambios
A.10.2.3	Gestión de cambios en servicios hechos por terceras partes
A.12.5.1	Procedimientos de control de los cambios.
A.12.5.2	Revisión técnica de aplicaciones después de cambios en el sistema operativo
A.12.5.3	Restricciones en los cambios a los paquetes de software

CONTINÚA 

Causa

Los cambios en los sistemas de información y en las configuraciones de los demás

componentes tecnológicos que sirven al proceso, no son gestionados en base a las mejores prácticas para el sector. No se encuentran los registros de cambios realizados en el caso de que los sistemas deban ser mantenidos por otros desarrolladores.

Efecto

Esta condición incrementa el riesgo de que los sistemas no puedan ser mantenidos en el tiempo y pierdan paulatinamente su funcionalidad o causen problemas en el cumplimiento legal.

Recomendaciones

9 Para: Director de Seguros Previsionales

Disponga a quien corresponda que los requerimientos de cambios o nuevos desarrollos se los haga a través de la Unidad de Planificación y Doctrina.

10 Para: Director de Riesgos

Determine el riesgo operativo de tecnología que representa la falta de este control.

12 Para: Jefe de la UTIC

Diseñe un procedimiento para canalizar los requerimientos de los usuarios a través de la UPD.

Proceso Seguros previsionales

Subproceso Gestión de afiliación y cotización

Hallazgo 7 TALENTO HUMANO NO SOLICITA FUNCIONARIOS CON CONOCIMIENTOS DE SEGURIDAD

DE INFORMACION

Condición

Los funcionarios nuevos no tienen conocimientos de normas de seguridad de información. En los criterios de selección no se incluye este tipo de conocimiento.

Criterio de evaluación

Código	**Control**
A.8.1.2	Selección
A.8.2.2	Educación y formación en seguridad de la información
A.8.2.3	Proceso disciplinario

Causa

En el plan de capacitación anual no están incluidos seminarios o cursos de seguridad de información

CONTINÚA

Efecto

Los funcionarios de la Dirección de Seguros Previsionales no conocen sobre los riesgos, amenazas y vulnerabilidades de la información que ellos manejan. Tampoco conocen sobre las posibles sanciones incluso en el ámbito legal en las cuales ellos pueden incurrir.

Recomendaciones

13 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda, incluir en los planes de capacitación la inclusión de cursos y seminarios de seguridad de información para directores y usuarios.

15 Para: Director de Riesgos

Determinar la calificación del riesgo generado por la falta de capacitación

16 Para: Director de Seguros Previsionales

Realizar el seguimiento y verificar que la capacitación sea recibida por el personal a su cargo.

Proceso Seguros Previsionales

Subproceso **Gestión de afiliación y cotización**

Hallazgo 8 NO EXISTEN PROCEDIMIENTOS DE SEGURIDAD FISICA, ACCESO, AREAS SEGURAS, ETC.

Condición

Las puertas de acceso y seguridad no permanecen todo el tiempo cerradas. Han existido conato de incendio por cortocircuitos en accesorios conectados s la red eléctrica, existen electrodomésticos conectados en el área de oficinas. Vendedores ingresan a las áreas.

Criterio de evaluación

Código	**Control**
A.9.1.1	Perímetro de seguridad física
A.9.1.2	Control de acceso físico
A.9.1.3	Seguridad de oficinas, recintos e instalaciones
A.9.1.4	Protección contra amenazas externas o medioambientales.
A.9.1.5	Trabajo en áreas seguras
A.9.2.1	Ubicación y protección de los equipos

Causa

No existen manuales de seguridad que normen el acceso y permanecía de

CONTINÚA 

personal ajeno a la Dirección de Seguros Previsionales. Los funcionarios no han sido concientizados en temas de seguridad. Física. No se han realizado simulacros de desastres físicos como terremotos,

Efecto

El área física que ocupa la Dirección de Seguros Previsionales, no es 100% segura. El riesgo de incidentes de seguridad causados por amenazas externas aumenta ya que en la Planta Baja acceden todos los afiliados para realizar sus trámites.

Recomendaciones

17 Para: Coordinador Administrativo Financiero

Implante y documente los procedimientos para asegurar en forma efectiva el área de Seguros Previsionales. Concientice al personal sobre los mencionados procedimientos.

18 Para: Director de Seguros Previsionales

Supervise y coordine el aseguramiento físico de las áreas bajo su responsabilidad.

19 Para: Coordinador Administrativo Financiero

Dote de guardianía a las áreas que ocupa la Dirección de Seguros Previsionales y demás recursos que sean necesarios.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 9 LAS COPIAS DE SEGURIDAD DE LA INFORMACION NO SON ALMACENADAS FUERA DE LA INSTITUCION

Condición

No existe un sitio seguro fuera de la Institución en donde se almacenen las cintas de respaldo de la información de la base de datos corporativa.

Criterio de evaluación

Código **Control**

A.10.5.1 Copias de seguridad de la información

Causa

No se cumplen los procedimientos de seguridad existentes para almacenar las cintas en un lugar externo a la Institución.

Efecto

Se incrementa el riesgo de pérdida total de la información corporativa, ocasionada por algún desastre.

Recomendaciones

20 Para: Coordinador Administrativo Financiero

Gestione la disponibilidad de un sitio externo a la Institución con todas las

CONTINÚA

seguridades físicas, como de condiciones especiales para almacenar las cintas de backup.

21 Para: Jefe de la UTIC

Realizar el seguimiento sobre la contratación del mencionado servicio de almacenamiento y custodia y establecer el procedimiento para realizar el transporte, ingreso y retiro de las cintas, cuando el ISSFA lo necesite.

24 Para: Jefe de inventarios de activos

Implantar el procedimiento necesario para entregar a la UTIC los equipos devueltos por los usuarios, dados de baja, etc., con el fin de eliminar en forma segura la información magnética en desuso.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 10 LA INFORMACION Y SUS MEDIOS NO SON ELIMINADOS EN FORMA CORRECTA

Condición

Los medios de almacenamiento de la información tanto físicos como tecnológicos, una vez dados de baja, removidos o reutilizados, no son eliminados en forma correcta.

Criterio de evaluación

Código	**Control**
A.10.7.2	Eliminación de medios
A.10.7.3	Procedimientos para el manejo de la información

Causa

No existen procedimientos de trituración o incineración de papel, wipeado de disco duros, PENdrives, destrucción de medios de almacenamiento dañados o dados de baja, borrado de cintas, etc.

Efecto

Se incrementa el riesgo de vulnerar la confidencialidad de la información de la Institución que aparentemente se encuentra eliminada, pero que podría ser recuperada por terceros utilizando medios técnicos.

CONTINÚA

Recomendaciones

22 Para: Director de Seguros Previsionales

Disponer a quien corresponda se tramite la dotación de trituradoras o destructoras de papel, establecer un procedimiento para solicitar a la UTIC el borrado físico de los disco que contengan o hayan contenido información referente a la Dirección de seguros Previsionales.

23 Para: Jefe de la UTIC

Realizar el trámite para adquirir los recursos necesarios para realizar un borrado físico de los medios de almacenamiento magnéticos u ópticos que contengan información Institucional.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 11 EL PROCESO NO CUENTA CON UN PLAN DE CONTINUIDAD DEL NEGOCIO

Condición

Las operaciones del proceso de Seguros Previsionales, en cualquier momento pueden ser interrumpidas sin que se tenga una línea base de tiempo para poder ser recuperadas.

Criterio de evaluación

Código **Control**

A.14.1.3 Desarrollo e implementación del plan de continuidad incluyendo seguridad

A.9.2.4 Mantenimiento de los equipos

Causa

El proceso de Seguros Previsionales no cuenta con un plan global de continuidad del negocio, no se sabe como poder restablecer las operaciones y con que subprocesos, personal, otros recurso etc.

Efecto

Interrupción de entrega de cesantías, pensiones y demás derechos al afiliado.

CONTINÚA 

Recomendaciones

25 Para: Subdirector General

Disponer a quien corresponda planificar y ejecutar un Plan de Continuidad del Negocio que contemple en primera instancia al procesos de Seguros Previsionales.

26 Para: Coordinador Administrativo Financiero

Dote de los recursos necesarios para ejecutar e implementar el Plan de Continuidad del Negocio.

27 Para: Director de Seguros Previsionales

Realice el seguimiento y operativice el Plan de Continuidad del Negocio.

28 Para: Jefe de la UPD

Diseñe y controle el Plan de Continuidad del Negocio.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 12 LOS ACTIVOS DE INFORMACION NO SON DEVUELTOS EN SU TOTALIDAD EN LA

DESVINCULACION DE UN FUNCIONARIO

Condición

Los funcionarios que se separan de la Institución no reciben ni entregan todos los activos de información que manipulan en sus labores diarias o en sus proyectos. A excepción equipos de cómputo, el resto de activos no constan bajos su responsabilidad. No se entrega con claridad la autorización para la utilización de los activos de información.

Criterio de evaluación

Código	**Control**
A.8.3.2	Devolución de activos
A.8.3.3	Eliminación de derechos de acceso

Causa

No existen normas para preservar la confidencialidad, integridad y disponibilidad de la información y medios de soporte

CONTINÚA 

Efecto

Existe fuga, pérdida, destrucción, manipulación indebida, etc. de la información a cargo de los funcionarios de este proceso.

Recomendaciones

49 Para: <u>Coordinador Administrativo Financiero</u>

Disponer a quien corresponda la entrega de la totalidad de activos de información recibidos por los funcionarios.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 13 NO SE HAN REALIZADO VERIFICACIONES DE SEGURIDAD A LAS APLICACIONES EN

PRODUCCION

Condición

Las aplicaciones informáticas que sirven al subproceso de gestión de afiliación y cotización, funcionan sin el aval de un estudio técnico de penetración, hacking ético, análisis de vulnerabilidades, ingeniería social etc.

Criterio de evaluación

Código	**Control**
A.10.4.1	Controles contra software malicioso
A.12.6.1	Control de vulnerabilidades técnicas.

Causa

No existen normas de seguridad de información ni de seguridad informática para este subproceso.

Efecto

Las aplicaciones informáticas en producción pueden estar siendo vulneradas o podrán vulneradas interna o externamente en el futuro.

CONTINÚA

Recomendaciones

29 Para: Coordinador Administrativo Financiero

Dotar de los recursos necesarios para la ejecución de los test técnicos necesarios.

30 Para: Director de Seguros Previsionales

Realizar el seguimiento y operativizar los estudios.

31 Para: Jefe de la UTIC

Coordinar los aspectos técnicos informáticos.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 14 NO SE CUMPLEN PROCEDIMIENTOS FORMALES PARA RESTRINGIR EL ACCESO A LA

INFORMACION

Condición

Existen políticas informáticas tendientes a regular al acceso a la información, difundidas en los medios de correo electrónico de la Institución.

Criterio de evaluación

Código	**Control**
A.11.1.1	Políticas para el control de acceso
A.11.2.3	Administración de contraseñas para usuarios.
A.11.2.4	Revisión de los derechos de acceso de los usuarios.
A.11.3.1	Uso de contraseñas.
A.11.4.2	Autenticación de usuarios para conexiones externas
A.11.4.3	Identificación de equipos en red

Causa

Las políticas informáticas establecidas por la organización no se cumplen en su

CONTINÚA

totalidad, debido a la falta de difusión y falta de capacitación en seguridad informática.

Efecto

Acceso a información confidencial por usuarios no autorizados, riesgo de suplantación de identidad.

Recomendaciones

32 Para: Jefe de la UTIC

Elaborar planes de capacitación para los funcionarios del ISSFA, con respecto a la aplicación de las políticas establecidas.

33 Para: Coordinador Administrativo Financiero

Ejecutar las sanciones establecidas en las políticas.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 16 EL ACCESO REMOTO A LA RED DE DATOS NO SE ENCUENTRA NORMADO

Condición

No existe políticas y procedimientos para la conexión remota solicitada por los funcionario del proceso.

Criterio de evaluación

Código	**Control**
A.11.4.6	Control de conexión a las redes
A.11.6.1	Restricción de acceso a la información
A.11.7.2	Trabajo remoto

Causa

Las funciones que realizan los usuario del Proceso de Afiliación y Cotización requieren el acceso de manera remota para optimizar el tiempo de respuesta a los procedimientos, accesos que no se encuentran definidos por talento humano dentro de las funciones.

Efecto

Los accesos remotos por parte de los usuarios del proceso de Gestión de

CONTINÚA

Afiliación y Cotización, no se encuentran controlados.

Las estaciones remotas de los usuarios no cumplen con los requerimientos mínimos d **Recomendaciones**

34 Para: Jefe de la UTIC

Establecer un proceso formal para el acceso remoto a la red de datos por parte de los funcionarios del proceso de Gestión de Afiliación y Cotización. Legalizar y difundir el proceso establecido.

35 Para: Coordinador Administrativo Financiero

Incluir en las funciones del personal del proceso de Gestión de Afiliación y Cotización, la opción de teletrabajo.

36 Para: Director de Seguros Previsionales

Supervisar y dar seguimiento al cumplimientos de las políticas establecidas para teletrabajo.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 17 NO SE HAN INCORPORADO POLITICAS DE SEGURIDAD DE INFORMACION EN LA ENTREGA

DE SERVICIOS DE RED

Condición

Los controles de seguridad en los servicios de red son implementados en base a las

necesidades del trabajo cotidiano de manera informal.

Criterio de evaluación

Código	**Control**
A.10.6.1	Controles de red
A.10.6.2	Seguridad de los servicios de red.

Causa

Ausencia de políticas de seguridad informática en la entrega de servicios de red.

Efecto

Incremento del riesgo de presencia de intrusos en la red.

Interrupción de los servicios de red.

CONTINÚA

Recomendaciones

37 Para: Jefe de la UTIC

Establecer políticas de seguridad para la entrega de los servicios de red.

Legalizar y difundir las políticas establecidas.

Capacitar al personal de la UTIC sobre seguridad informática.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 18 LOS SERVICIOS DE COMUNICACIONES DE DATOS EXTERNOS NO SE ENCUENTRAN

ENCRIPTADOS

Condición

La información puede ser interceptada por intrusos arriesgando su integridad y confidencialidad.

Criterio de evaluación

Código	**Control**
A.10.8.4	Correo electrónico
A.10.9.1	Comercio electrónico
A.10.9.2	Transacciones en línea
A.12.3.1	Política en el uso de controles criptográficos
A.15.1.6	Reglamentación de los controles criptográficos

Causa

No se han implementado los recursos necesarios para encriptar la información que se tramiten mediante servicios de comunicaciones de datos externos.

CONTINÚA

Efecto

Difusión no autorizada de información.

Perdida de información.

Fraudes económicos.

Recomendaciones

38 Para: Jefe de la UTIC

Implementar una solución para la encriptación de la información transmitida a través de los canales de datos externos.Capacitar al personal de la UTIC sobre la gestión y administración de la solución

39 Para: Director de Seguros Previsionales

Dar seguimiento a la implementación de la solución de encriptación.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 19 NO EXISTE UN PROCESO DE REGISTRO DE EVENTOS O INCIDENTES DE SEGURIDAD

Condición

Falta de conocimiento sobre los incidentes de seguridad que ocurren en el proceso de Gestión

de Afiliación y Cotización.

Criterio de evaluación

Código	**Control**
A.10.10.1	Registro de auditoría
A.10.10.5	Registro de fallos
A.15.1.3	Protección de los registros de la organización
A.13.2.1	Responsabilidades y procedimientos

Causa

Falta del proceso de seguridad de información.

Desconocimiento de los usuarios sobre como actuar cuando existe un incidente de seguridad informática.

CONTINÚA 

Efecto

No se pueden tomar acciones para mitigar los fallos de seguridad informática.

Recomendaciones

40 Para: Jefe de la UTIC

Establecer el proceso para gestiones los incidentes de seguridad.

Legalizar y difundir el proceso establecido.

41 Para: Director de Seguros Previsionales

Disponer el cumplimiento del procedimiento establecido.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 20 LOS DATOS PERSONALES DE LOS AFILIADOS SE ENCUENTRAN EXPUESTOS

Condición

La información soportada en documentos impresos, puede ser revisada sin autorización por

cualquier funcionario del proceso.

Criterio de evaluación

Código **Control**

A.15.1.4 Protección de los datos y privacidad de la información personal

A.15.1.5 Protección del uso inadecuado de los recursos de procesamiento de la

Causa

No existe un procedimiento de clasificación de información que genere los niveles de

restricción a la información en documentos impresos.

Efecto

CONTINÚA

Disponibilidad de información confidencial por parte de funcionarios no autorizados.

Recomendaciones

42 Para: Director de Seguros Previsionales

Establecer el proceso para acceso a información mediante documentos impresos.

43 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda la clasificación de la información considerando su criticidad.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 21 USO DE SOFTWARE ILEGAL EN LAS ESTACIONES DE TRABAJO

Condición

Los usuarios del proceso de Gestión de Afiliación y Cotización utilizar software sin licenciamiento.

Criterio de evaluación

Código	**Control**
A.15.1.1	Identificación de la legislación aplicable
A.15.1.2	Derechos de propiedad intelectual.

Causa

No se ha regularizado el licenciamiento de software requerido por los funcionarios.

Efecto

Sanciones legales, económicas, penales a la máxima autoridad del ISFFA y al encargado de tecnología.

CONTINÚA

Recomendaciones

44 Para: Jefe de la UTIC

Realizar un proyecto de regularizar y legalizar el software que utilizan los funcionarios del

proceso de Gestión de Afiliación y Cotización.

45 Para: Coordinador Administrativo Financiero

Autorizar el proyecto de regularizar y legalizar el software que utilizan los funcionarios del proceso de Gestión de Afiliación y Cotización.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 22 LAS OPERACIONES EN EL DATA CENTER NO SE ENCUENTRAN DOCUMENTADAS

Condición

No existe documentación consistente sobre las operaciones en el Data Center.

Criterio de evaluación

Código	**Control**
A.9.2.2	Suministro de energía
A.9.2.3	Seguridad del cableado
A.10.3.1	Planeación de la capacidad
A.10.10.2	Monitoreo del uso del sistema
A.12.2.2	Control al procesamiento interno
A.12.4.1	Control del software operativo

Causa

No existe un proceso formal para documentar las operaciones en el Data Center.

Efecto

CONTINÚA

Interrupción de las actividades que realiza el personal de la UTIC por falta de documentación.

Recomendaciones

46 Para: Jefe de la UTIC

Establecer procesos para documentar las operaciones realizadas en el data center.

Proceso **Seguros previsionales**

Subproceso **Gestión de afiliación y cotización**

Hallazgo 23 AUSENCIA DE BUENAS PRACTICAS PARA EL DESARROLLO, MANTENIMIENTO Y

ADQUISICION DE LAS APLICACIONES INFORMATICAS DEL PROCESO

Condición

No se aplican formalmente estándares, normas, etc. para el desarrollo, mantenimiento de aplicaciones utilizadas en el proceso de Gestión de Afiliación y Cotización. Ausencia de un proceso formal para la adquisición de las aplicaciones por parte del usuario.

Criterio de evaluación

Código	**Control**
A.10.3.2	Aceptación del sistema
A.10.7.4	Seguridad de la documentación del sistema
A.12.2.1	Validación de los datos de entrada
A.12.5.5	Desarrollo externo de software

Causa

Falta de personal de UTIC en el área de desarrollo.

CONTINÚA

Efecto

Falta de segregación de funciones en el área de desarrollo del software lo que ocasiona tiempo de respuesta alto en requerimientos solicitados.

Incremento del riesgo en perdida de integridad de información.

Recomendaciones

47 Para: Jefe de la UTIC

Establecer un proceso para utilizar buenas prácticas para el desarrollo, mantenimiento y adquisición de las aplicaciones.

Determinar y solicitar el personal necesario para cumplir con el proceso.

48 Para: Coordinador Administrativo Financiero

Dotar del personal solicitado y requerido por la UTIC.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 24 NO EXISTE CONTROL EN LA ENTREGA DE INFORMACION A TERCEROS

Condición

Los proveedores o terceros en general, reciben información por parte del ISSFA, la misma que

no es protegida mediante un compromiso formal firmado por las partes.

Criterio de evaluación

Código	**Control**
A.6.1.5	Acuerdo de Confidencialidad.
A.6.2.1	Identificación de riesgos relacionados con partes externas.

Causa

Los proveedores obtienen información institucional de todo tipo

Efecto

La información del ISSFA se encuentra en condiciones de ser difundida por terceros sin que se pueda realizar reclamos o demandas legales.

CONTINÚA

Recomendaciones

51 Para: Director General

Disponer a quien corresponda la implantación de los procedimientos necesarios para normar

la entrega de la información.

52 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda, incluir criterios de seguridad de información en todos los documentos que involucren a terceros, referir a las normas internas y externas.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 25 INEXISTENCIA DE AUDITORIAS INDEPENDIENTES DE SEGURIDAD DE INFORMACION EN EL

PROCESO DE SEGUROS PREVISIONALES

Condición

Los controles de seguridad que existen en este momento no muestran suficiencia para mantener la confidencialidad, integridad y disponibilidad de la información institucional.

Criterio de evaluación

Código	**Control**
A.6.1.8	Revisión Independiente de seguridad de la información

Causa

No existe implantad una normativa o buenas prácticas para gestionar la seguridad de

información, esta depende de controles insuficientes e incompletos.

Efecto

Los controles existentes no han sido auditados en forma independiente, bajo normas de seguridad de información.

CONTINÚA

Recomendaciones

53 Para: Director de Riesgos

Incluir en el plan de tratamiento de riesgos operativos, las auditorías independientes de seguridad de información generada y manipulada en este subproceso.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 27 NO EXISTE SEGREGACION DE FUNCIONES EN EL PERSONAL DE TECNOLOGIA INVOLUCRADO

EN EL PROCESO

Condición

El personal de tecnología realiza funciones adicionales de las indicadas en sus funciones.

Criterio de evaluación

Código **Control**

A.8.1.3 Términos y condiciones de la relación laboral

Causa

El personal que realiza desarrollo tiene acceso a las aplicaciones fuentes y de producción, el personal de infraestructura tiene acceso a los recursos de seguridad, debido a la falta de personal.

Efecto

El mismo personal es juez y parte.

CONTINÚA

Recomendaciones

56 Para: <u>Coordinador Administrativo Financiero</u>

Disponga el completamiento del orgánico de personal de la UTIC y facilite la segregación de funciones.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 29 TALENTO HUMANO NO SOLICITA FUNCIONARIOS CON CONOCIMIENTOS DE SEGURIDAD

DE INFORMACION

Condición

Los funcionarios nuevos no tienen conocimientos de normas de seguridad de información. En

los criterios de selección no se incluye este tipo de conocimiento.

Criterio de evaluación

Código	**Control**
A.8.1.2	Selección
A.8.2.3	Proceso disciplinario

Causa

En el plan de capacitación anual no están incluidos seminarios o cursos de seguridad de información

Efecto

Los funcionarios de la Dirección de Seguros Previsionales no conocen sobre los riesgos, amenazas y vulnerabilidades de la información que ellos manejan. Tampoco

CONTINÚA

conocen sobre las posibles sanciones incluso en el ámbito legal en las cuales ellos pueden incurrir.

Recomendaciones

60 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda, incluir en los planes de capacitación la inclusión de cursos y seminarios de seguridad de información para directores y usuarios.

61 Para: Director de Riesgos

Determinar la calificación del riesgo generado por la falta de capacitación

62 Para: Director de Seguros Previsionales

Realizar el seguimiento y verificar que la capacitación sea recibida por el personal a su cargo.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 30 NO EXISTEN PROCEDIMIENTOS DE SEGURIDAD FISICA, ACCESO, AREAS SEGURAS, ETC.

Condición

Las puertas de acceso y seguridad no permanecen todo el tiempo cerradas. Han existido conato de incendio por cortocircuitos en accesorios conectados s la red eléctrica, existen electrodomésticos conectados en el área de oficinas. Vendedores ingresan a las áreas.

Criterio de evaluación

Código	**Control**
A.9.1.2	Control de acceso físico
A.9.1.4	Protección contra amenazas externas o medioambientales.
A.9.2.1	Ubicación y protección de los equipos

Causa

No existen manuales de seguridad que normen el acceso y permanecía de personal ajeno a la Dirección de Seguros Previsionales. Los funcionarios no han sido concientizados en temas de seguridad. Física. No se han realizado simulacros de desastres físicos como terremotos,

CONTINÚA 

Efecto

El área física que ocupa la Dirección de Seguros Previsionales, no es 100% segura. El riesgo de incidentes de seguridad causados por amenazas externas aumenta ya que en la Planta Baja acceden todos los afiliados para realizar sus trámites.

Recomendaciones

63 Para: Coordinador Administrativo Financiero

Implante y documente los procedimientos para asegurar en forma efectiva el área de Seguros Previsionales. Concientice al personal sobre los mencionados procedimientos.

64 Para: Director de Seguros Previsionales

Supervise y coordine el aseguramiento físico de las áreas bajo su responsabilidad.

65 Para: Coordinador Administrativo Financiero

Dote de guardianía a las áreas que ocupa la Dirección de Seguros Previsionales y demás recursos que sean necesarios.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 31 LAS COPIAS DE SEGURIDAD DE LA INFORMACION NO SON ALMACENADAS FUERA DE LA INSTITUCION

Condición

No existe un sitio seguro fuera de la Institución en donde se almacenen las cintas de respaldo de la información de la base de datos corporativa.

Criterio de evaluación

Código **Control**

A.10.5.1 Copias de seguridad de la información

Causa

No se cumplen los procedimientos de seguridad existentes para almacenar las cintas en un lugar externo a la Institución.

Efecto

Se incrementa el riesgo de pérdida total de la información corporativa, ocasionada por algún desastre.

Recomendaciones

66 **Para:** **Coordinador Administrativo Financiero**

Gestione la disponibilidad de un sitio externo a la Institución con todas las

CONTINÚA

seguridades físicas, como de condiciones especiales para almacenar las cintas de backup.

67 Para: Jefe de la UTIC

Realizar el seguimiento sobre la contratación del mencionado servicio de almacenamiento y custodia y establecer el procedimiento para realizar el transporte, ingreso y retiro de las cintas, cuando el ISSFA lo necesite.

68 Para: Jefe de inventarios de activos

Implantar el procedimiento necesario para entregar a la UTIC los equipos devueltos por los usuarios, dados de baja, etc., al fin de eliminar en forma segura la información en desuso.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 33 EL PROCESO NO CUENTA CON UN PLAN DE CONTINUIDAD DEL NEGOCIO

Condición

Las operaciones del proceso de Seguros Previsionales, en cualquier momento pueden ser interrumpidas sin que se tenga una línea base de tiempo para poder ser recuperadas.

Criterio de evaluación

Código **Control**

A.14.1.3 Desarrollo e implementación del plan de continuidad incluyendo seguridad

Causa

El proceso de Seguros Previsionales no cuenta con un plan global de continuidad del negocio, no se sabe cómo poder restablecer las operaciones y con qué subprocesos, personal, otros recurso etc.

Efecto

Interrupción de entrega de cesantías, pensiones y demás derechos al afiliado.

CONTINÚA 

Recomendaciones

71 Para: Subdirector General

Disponer a quien corresponda planificar y ejecutar un Plan de Continuidad del Negocio que contemple en primera instancia al proceso de Seguros Previsionales.

72 Para: Coordinador Administrativo Financiero

Dote de los recursos necesarios para ejecutar e implementar el Plan de Continuidad del Negocio.

73 Para: Director de Seguros Previsionales

Realice el seguimiento y operativice el Plan de Continuidad del Negocio.

74 Para: Jefe de la UPD

Diseñe y controle el Plan de Continuidad del Negocio.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 34 LOS ACTIVOS DE INFORMACION NO SON DEVUELTOS EN SU TOTALIDAD EN LA

DESVINCULACION DE UN FUNCIONARIO

Condición

Los funcionarios que se separan de la Institución no reciben ni entregan todos los activos de Información que manipulan en sus labores diarias o en sus proyectos. A excepción equipos de cómputo, el resto de activos no constan bajos su responsabilidad. No se entrega con claridad la autorización para la utilización de los activos de información.

Criterio de evaluación

Código **Control**

A.8.3.3 Eliminación de derechos de acceso

Causa

No existen normas para preservar la confidencialidad, integridad y disponibilidad de la información y medios de soporte

Efecto

Existe fuga, pérdida, destrucción, manipulación indebida, etc. de la información a cargo de los funcionarios de este proceso.

CONTINÚA

Recomendaciones

75 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda la entrega de la totalidad de activos de información recibidos por los funcionarios.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 40 NO EXISTE UN PROCESO DE REGISTRO DE EVENTOS O INCIDENTES DE SEGURIDAD

Condición

Falta de conocimiento sobre los incidentes de seguridad que ocurren en el proceso de Gestión de Afiliación y Cotización.

Criterio de evaluación

Código	**Control**
A.13.2.1	Responsabilidades y procedimientos
A.15.1.3	Protección de los registros de la organización

Causa

Falta del proceso de seguridad de información.

Desconocimiento de los usuarios sobre cómo actuar cuando existe un incidente de seguridad informática.

Efecto

No se pueden tomar acciones para mitigar los fallos de seguridad informática.

CONTINÚA

Recomendaciones

87 Para: Jefe de la UTIC

Establecer el proceso para gestiones los incidentes de seguridad.

Legalizar y difundir el proceso establecido.

88 Para: Director de Seguros Previsionales

Disponer el cumplimiento del procedimiento establecido.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 66 LOS DATOS PERSONALES DE LOS AFILIADOS SE ENCUENTRAN EXPUESTOS

Condición

La información soportada en documentos impresos, puede ser revisada sin autorización por cualquier funcionario del proceso.

Criterio de evaluación

Código **Control**

A.15.1.4 Protección de los datos y privacidad de la información personal

Causa

No existe un procedimiento de clasificación de información que genere los niveles de restricción a la información en documentos impresos.

Efecto

Disponibilidad de información confidencial por parte de funcionarios no autorizados.

Recomendaciones

145 **Para:** **Director de Seguros Previsionales**

CONTINÚA 

Establecer el proceso para acceso a información mediante documentos impresos.

146 Para: <u>Coordinador Administrativo Financiero</u>

Disponer a quien corresponda la clasificación de la información considerando su criticidad.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 67 USO DE SOFTWARE ILEGAL EN LAS ESTACIONES DE TRABAJO

Condición

Los usuarios del proceso de Gestión de Afiliación y Cotización utilizar software sin licenciamiento.

Criterio de evaluación

Código **Control**

A.15.1.1 Identificación de la legislación aplicable

Causa

No se ha regularizado el licenciamiento de software requerido por los funcionarios.

Efecto

Sanciones legales, económicas, penales a la máxima autoridad del ISFFA y al encargado de tecnología.

Recomendaciones

143 Para: Jefe de la UTIC

Realizar un proyecto de regularizar y legalizar el software que utilizan los

CONTINÚA

funcionarios del proceso de Gestión de Afiliación y Cotización.

144 Para: <u>Coordinador Administrativo Financiero</u>

Autorizar el proyecto de regularizar y legalizar el software que utilizan los funcionarios del proceso de Gestión de Afiliación y Cotización.

Proceso **Seguros previsionales**

Subproceso **Gestión de prestaciones**

Hallazgo 68 AUSENCIA DE BUENAS PRACTICAS PARA EL DESARROLLO, MANTENIMIENTO Y ADQUISICION DE LAS APLICACIONES INFORMATICAS DEL PROCESO

Condición

No se aplican formalmente estándares, normas, etc. para el desarrollo, mantenimiento de aplicaciones utilizadas en el proceso de Gestión de Afiliación y Cotización.

Ausencia de un proceso formal para la adquisición de las aplicaciones por parte del usuario.

Criterio de evaluación

Código	**Control**
A.10.7.4	Seguridad de la documentación del sistema

Causa

Falta de personal de UTIC en el área de desarrollo.

Efecto

Falta de segregación de funciones en el área de desarrollo del software lo que ocasiona tiempo de respuesta alto en requerimientos solicitados.

CONTINÚA

Incremento del riesgo en perdida de integridad de información.

Recomendaciones

141 Para: Coordinador Administrativo Financiero

Dotar del personal solicitado y requerido por la UTIC.

142 Para: Jefe de la UTIC

Establecer un proceso para utilizar buenas prácticas para el desarrollo, mantenimiento y adquisición de las aplicaciones.

Determinar y solicitar el personal necesario para cumplir con el proceso.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 45 NO EXISTE CONTROL EN LA ENTREGA DE INFORMACION A TERCEROS

Condición

Los proveedores o terceros en general, reciben información por parte del ISSFA, la misma que no es protegida mediante un compromiso formal firmado por las partes.

Criterio de evaluación

Código	**Control**
A.6.1.5	Acuerdo de Confidencialidad.
A.6.2.1	Identificación de riesgos relacionados con partes externas.

Causa

Los proveedores obtienen información institucional de todo tipo

Efecto

La información del ISSFA se encuentra en condiciones de ser difundida por terceros sin que se pueda realizar reclamos o demandas legales.

Recomendaciones

96 **Para:** **Director General**

CONTINÚA

Disponer a quien corresponda la implantación de los procedimientos necesarios para normar la entrega de la información.

97 Para: <u>Coordinador Administrativo Financiero</u>

Disponer a quien corresponda, incluir criterios de seguridad de información en todos los documentos que involucren a terceros, referir a las normas internas y externas.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 46 INEXISTENCIA DE AUDITORIAS INDEPENDIENTES DE SEGURIDAD DE INFORMACION EN EL PROCESO DE SEGUROS PREVISIONALES

Condición

Los controles de seguridad que existen en este momento no muestran suficiencia para mantener la confidencialidad, integridad y disponibilidad de la información institucional.

Criterio de evaluación

Código	**Control**
A.6.1.8	Revisión Independiente de seguridad de la información

Causa

No existe implantad una normativa o buenas prácticas para gestionar la seguridad de información, esta depende de controles insuficientes e incompletos.

Efecto

Los controles existentes no han sido auditados en forma independiente, bajo normas de seguridad de información.

CONTINÚA

Recomendaciones

98 Para: Director de Riesgos

Incluir en el plan de tratamiento de riesgos operativos, las auditorías independientes de seguridad de información generada y manipulada en este subproceso.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 48 NO EXISTE SEGREGACION DE FUNCIONES EN EL PERSONAL DE TECNOLOGIA INVOLUCRADO EN EL PROCESO

Condición

El personal de tecnología realiza funciones adicionales de las indicadas en sus funciones.

Criterio de evaluación

Código **Control**

A.8.1.3 Términos y condiciones de la relación laboral

Causa

El personal que realiza desarrollo tiene acceso a las aplicaciones fuentes y de producción, el personal de infraestructura tiene acceso a los recursos de seguridad, debido a la falta de personal.

Efecto

El mismo personal es juez y parte.

Recomendaciones

101 Para: Coordinador Administrativo Financiero

Disponga el completamiento del orgánico de personal de la UTIC y facilite la

segregación de funciones.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 50 TALENTO HUMANO NO SOLICITA FUNCIONARIOS CON CONOCIMIENTOS DE SEGURIDAD DE INFORMACION

Condición

Los funcionarios nuevos no tienen conocimientos de normas de seguridad de información. En los criterios de selección no se incluye este tipo de conocimiento.

Criterio de evaluación

Código	**Control**
A.8.1.2	Selección
A.8.2.3	Proceso disciplinario

Causa

En el plan de capacitación anual no están incluidos seminarios o cursos de seguridad de información

Efecto

Los funcionarios de la Dirección de Seguros Previsionales no conocen sobre los riesgos, amenazas y vulnerabilidades de la información que ellos manejan. Tampoco conocen sobre las posibles sanciones incluso en el ámbito legal en las cuales ellos pueden incurrir.

CONTINÚA 

Recomendaciones

105 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda, incluir en los planes de capacitación la inclusión de cursos y seminarios de seguridad de información para directores y usuarios.

106 Para: Director de Riesgos

Determinar la calificación del riesgo generado por la falta de capacitación.

107 Para: Director de Seguros Previsionales

Realizar el seguimiento y verificar que la capacitación sea recibida por el personal a su cargo.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 51 NO EXISTEN PROCEDIMIENTOS DE SEGURIDAD FISICA, ACCESO, AREAS SEGURAS, ETC.

Condición

Las puertas de acceso y seguridad no permanecen todo el tiempo cerradas. Han existido conato de incendio por cortocircuitos en accesorios conectados s la red eléctrica, existen electrodomésticos conectados en el área de oficinas. Vendedores ingresan a las áreas.

Criterio de evaluación

Código	**Control**
A.9.1.2	Control de acceso físico
A.9.1.4	Protección contra amenazas externas o medioambientales.
A.9.2.1	Ubicación y protección de los equipos

Causa

No existen manuales de seguridad que normen el acceso y permanecía de personal ajeno a la Dirección de Seguros Previsionales. Los funcionarios no han sido concientizados en temas de seguridad. Física. No se han realizado simulacros de desastres físicos como terremotos,

Efecto

CONTINÚA

El área física que ocupa la Dirección de Seguros Previsionales, no es 100% segura. El riesgo de incidentes de seguridad causados por amenazas externas aumenta ya que en la Planta Baja acceden todos los afiliados para realizar sus trámites.

Recomendaciones

108 Para: Coordinador Administrativo Financiero

Implante y documente los procedimientos para asegurar en forma efectiva el área de Seguros Previsionales. Concientice al personal sobre los mencionados procedimientos.

109 Para: Director de Seguros Previsionales

Supervise y coordine el aseguramiento físico de las áreas bajo su responsabilidad.

110 Para: Coordinador Administrativo Financiero

Dote de guardianía a las áreas que ocupa la Dirección de Seguros Previsionales y demás recursos que sean necesarios.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 52 LAS COPIAS DE SEGURIDAD DE LA INFORMACION NO SON ALMACENADAS FUERA DE LA INSTITUCION

Condición

No existe un sitio seguro fuera de la Institución en donde se almacenen las cintas de respaldo

de la información de la base de datos corporativa.

Criterio de evaluación

Código **Control**

A.10.5.1 Copias de seguridad de la información

Causa

No se cumplen los procedimientos de seguridad existentes para almacenar las cintas en un lugar externo a la Institución.

Efecto

Se incrementa el riesgo de pérdida total de la información corporativa, ocasionada por algún desastre.

Recomendaciones

111 **Para:** **Coordinador Administrativo Financiero**

CONTINÚA

Gestione la disponibilidad de un sitio externo a la Institución con todas las seguridades físicas, como de condiciones especiales para almacenar las cintas de backup.

112 Para: Jefe de la UTIC

Realizar el seguimiento sobre la contratación del mencionado servicio de almacenamiento y custodia y establecer el procedimiento para realizar el transporte, ingreso y retiro de las cintas, cuando el ISSFA lo necesite.

113 Para: Jefe de inventarios de activos

Implantar el procedimiento necesario para entregar a la UTIC los equipos devueltos por los usuarios, dados de baja, etc., con el fin de eliminar en forma segura la información en desuso.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 54 EL PROCESO NO CUENTA CON UN PLAN DE CONTINUIDAD DEL NEGOCIO

Condición

Las operaciones del proceso de Seguros Previsionales, en cualquier momento pueden ser interrumpidas sin que se tenga una línea base de tiempo para poder ser recuperadas.

Criterio de evaluación

Código **Control**

A.14.1.3 Desarrollo e implementación del plan de continuidad incluyendo seguridad

Causa

El proceso de Seguros Previsionales no cuenta con un plan global de continuidad del negocio, no se sabe como poder restablecer las operaciones y con qué subprocesos, personal, otros recurso etc.

Efecto

Interrupción de entrega de cesantías, pensiones y demás derechos al afiliado.

CONTINÚA 

Recomendaciones

116 Para: Subdirector General

Disponer a quien corresponda planificar y ejecutar un Plan de Continuidad del Negocio que contemple en primera instancia al proceso de Seguros Previsionales.

117 Para: Coordinador Administrativo Financiero

Dote de los recursos necesarios para ejecutar e implementar el Plan de Continuidad del Negocio

118 Para: Director de Seguros Previsionales

Realice el seguimiento y operativice el Plan de Continuidad del Negocio.

119 Para: Jefe de la UPD

Diseñe y controle el Plan de Continuidad del Negocio.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 55 LOS ACTIVOS DE INFORMACION NO SON DEVUELTOS EN SU TOTALIDAD EN LA DESVINCULACION DE UN FUNCIONARIO

Condición

Los funcionarios que se separan de la Institución no reciben ni entregan todos los activos de información que manipulan en sus labores diarias o en sus proyectos. A excepción equipos de cómputo, el resto de activos no constan bajos su responsabilidad. No se entrega con claridad

la autorización para la utilización de los activos de información.

Criterio de evaluación

Código **Control**

A.8.3.3 Eliminación de derechos de acceso

Causa

No existen normas para preservar la confidencialidad, integridad y disponibilidad de la información y medios de soporte

Efecto

Existe fuga, pérdida, destrucción, manipulación indebida, etc. de la información a cargo de los funcionarios de este proceso.

CONTINÚA

Recomendaciones

120 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda la entrega de la totalidad de activos de información recibidos por los funcionarios.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 61 NO EXISTE UN PROCESO DE REGISTRO DE EVENTOS O INCIDENTES DE SEGURIDAD

Condición

Falta de conocimiento sobre los incidentes de seguridad que ocurren en el proceso de Gestión de Afiliación y Cotización.

Criterio de evaluación

Código	**Control**
A.13.2.1	Responsabilidades y procedimientos
A.15.1.3	Protección de los registros de la organización

Causa

Falta del proceso de seguridad de información.

Desconocimiento de los usuarios sobre cómo actuar cuando existe un incidente de seguridad informática.

Efecto

No se pueden tomar acciones para mitigar los fallos de seguridad informática.

CONTINÚA

Recomendaciones

132 Para: Jefe de la UTIC

Establecer el proceso para gestiones los incidentes de seguridad.

Legalizar y difundir el proceso establecido.

133 Para: Director de Seguros Previsionales

Disponer el cumplimiento del procedimiento establecido.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 62 LOS DATOS PERSONALES DE LOS AFILIADOS SE ENCUENTRAN EXPUESTOS

Condición

La información soportada en documentos impresos, puede ser revisada sin autorización por cualquier funcionario del proceso.

Criterio de evaluación

Código **Control**

A.15.1.4 Protección de los datos y privacidad de la información personal

Causa

No existe un procedimiento de clasificación de información que genere los niveles de

restricción a la información en documentos impresos.

Efecto

Disponibilidad de información confidencial por parte de funcionarios no autorizados.

Recomendaciones

CONTINÚA

134 Para: Director de Seguros Previsionales

Establecer el proceso para acceso a información mediante documentos impresos.

135 Para: Coordinador Administrativo Financiero

Disponer a quien corresponda la clasificación de la información considerando su criticidad.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 63 USO DE SOFTWARE ILEGAL EN LAS ESTACIONES DE TRABAJO

Condición

Los usuarios del proceso de Gestión de Afiliación y Cotización utilizar software sin licenciamiento.

Criterio de evaluación

Código **Control**

A.15.1.1 Identificación de la legislación aplicable

Causa

No se ha regularizado el licenciamiento de software requerido por los funcionarios.

Efecto

Sanciones legales, económicas, penales a la máxima autoridad del ISFFA y al encargado de tecnología.

Recomendaciones

136 Para: Jefe de la UTIC

Realizar un proyecto de regularizar y legalizar el software que utilizan los

CONTINÚA

funcionarios del proceso de Gestión de Afiliación y Cotización.

137 Para: <u>Coordinador Administrativo Financiero</u>

Autorizar el proyecto de regularizar y legalizar el software que utilizan los funcionarios del proceso de Gestión de Afiliación y Cotización.

Proceso **Seguros previsionales**

Subproceso **Gestión de nómina**

Hallazgo 65 AUSENCIA DE BUENAS PRACTICAS PARA EL DESARROLLO, MANTENIMIENTO Y ADQUISICION DE LAS APLICACIONES INFORMATICAS DEL PROCESO

Condición

No se aplican formalmente estándares, normas, etc. para el desarrollo, mantenimiento de aplicaciones utilizadas en el proceso de Gestión de Afiliación y Cotización. Ausencia de un proceso formal para la adquisición de las aplicaciones por parte del usuario.

Criterio de evaluación

Código
Control

A.10.7.4 Seguridad de la documentación del sistema

Causa

Falta de personal de UTIC en el área de desarrollo.

Efecto

Falta de segregación de funciones en el área de desarrollo del software lo que ocasiona tiempo de respuesta alto en requerimientos solicitados. Incremento del riesgo en perdida de integridad de información.

CONTINÚA

Recomendaciones

139 Para: Coordinador Administrativo Financiero

Dotar del personal solicitado y requerido por la UTIC.

140 Para: Jefe de la UTIC

Establecer un proceso para utilizar buenas prácticas para el desarrollo, mantenimiento y adquisición de las aplicaciones. Determinar y solicitar el personal necesario para cumplir con el proceso.

Quito, DM., jueves, 17 de abril de 2014

Evaluadores de Seguridad de Información

Paulina Porras Ing., Giovanni Salazar F. Ing. Mgs.

4.3. Plan de acción

El presente plan de acción ha sido realizado tomando en cuenta la unidad de días/hombre, los tiempos de ejecución en la implantación de controles son referenciales así como el tiempo total de la ejecución del Plan.

Por criterio de los autores, los PROGRAMAS componentes del PLAN, han sido agrupados en base a la organización de dominios de la ISO/IEC 27002:2005, logrando eficiencia en la ejecución de los mismos, similar concepto ha sido aplicado

a los PROYECTOS, en los cuales se agrupan los controles incluidos tomando en cuenta su afinidad previamente definida en la norma.

Plan de acción (Plan, programas, proyectos)

Instituto de Seguridad Social de las Fuerzas Armadas — Levantamiento: 01-feb-13

	Plan, programa proyecto	Fecha inicio	Días	Fecha fin	Costo
FENIX	Seguridad de Información del ISSFA	01-may-14	3465	27-ago-23	0,00
PROG02	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	07-abr-14	170	24-sep-14	0,00
PR0201	ORGANIZACIÓN INTERNA	07-abr-14	10	24-sep-14	0,00
A.6.1.5	Acuerdo de Confidencialidad.	07-abr-14	10	17-abr-14	0,00
A.6.1.8	Revisión Independiente de seguridad de la información	07-abr-14	100	16-jul-14	0,00
PR0202	PARTES EXTERNAS	07-abr-14	40	06-jun-14	0,00
A.6.2.1	Identificación de riesgos relacionados con partes externas.	07-abr-14	40	17-may-14	0,00
A.6.2.3	Requisitos de seguridad en acuerdos con terceras partes.	07-abr-14	20	27-abr-14	0,00
PROG03	GESTION DE ACTIVOS	07-abr-14	90	06-jul-14	0,00
PR0302	CLASIFICACION DE LA INFORMACION	07-abr-14	90	07-abr-14	0,00
A.7.2.1	Guías de clasificación	07-abr-14	90	06-jul-14	0,00
PROG04	SEGURIDAD DE PERSONAL	07-abr-14	230	23-nov-14	0,00
PR0402	ANTES DEL TRABAJO	07-abr-14	40	05-ago-14	0,00
A.8.1.1	Funciones y Responsabilidades	07-abr-14	40	17-may-14	0,00
A.8.1.2	Selección	07-abr-14	40	17-may-14	0,00
A.8.1.3	Términos y condiciones de la relación laboral	07-abr-14	40	17-may-14	0,00
PR0403	DURANTE EL TRABAJO	07-abr-14	40	14-sep-14	0,00
A.8.2.1	Gestión de las responsabilidades	07-abr-14	40	17-may-14	0,00
A.8.2.2	Educación y formación en seguridad de la información	07-abr-14	90	06-jul-14	0,00
A.8.2.3	Proceso disciplinario	07-abr-14	30	07-may-14	0,00
PR0404	TERMINACION O CAMBIO DE TRABAJO	07-abr-14	30	27-may-14	0,00
A.8.3.2	Devolución de activos	07-abr-14	30	07-may-14	0,00
A.8.3.3	Eliminación de derechos de acceso	07-abr-14	20	27-abr-14	0,00

Tabla 20. Plan de Acción

CONTINÚA

	Plan, programa proyecto	Fecha inicio	Días	Fecha fin	Costo
PROG05	SEGURIDAD FISICA Y DEL ENTORNO	07-abr-14	605	03-dic-15	0,00
PR0501	AREAS SEGURAS	07-abr-14	100	20-ago-15	0,00
A.9.1.1	Perímetro de seguridad física	07-abr-14	100	16-jul-14	0,00
A.9.1.2	Control de acceso físico	07-abr-14	100	16-jul-14	0,00
A.9.1.3	Seguridad de oficinas, recintos e instalaciones	07-abr-14	100	16-jul-14	0,00
A.9.1.4	Protección contra amenazas externas o medioambientales.	07-abr-14	100	16-jul-14	0,00
A.9.1.5	Trabajo en áreas seguras	07-abr-14	100	16-jul-14	0,00
PR0502	SEGURIDAD DE LOS EQUIPOS	07-abr-14	50	21-jul-14	0,00
A.9.2.1	Ubicación y protección de los equipos	07-abr-14	50	27-may-14	0,00
A.9.2.2	Suministro de energía	07-abr-14	20	27-abr-14	0,00
A.9.2.3	Seguridad del cableado	07-abr-14	15	22-abr-14	0,00
A.9.2.4	Mantenimiento de los equipos	07-abr-14	20	27-abr-14	0,00
PROG06	GESTION DE COMUNICACIONES Y OPERACIONES	07-abr-14	930	23-oct-16	0,00
PR0601	PROCEDIMIENTO OPERACIONALES Y RESPONSABILIDADES	07-abr-14	120	03-dic-14	0,00
A.10.1.2	Gestión de Cambios	07-abr-14	120	05-ago-14	0,00
A.10.1.3	Separación de funciones	07-abr-14	120	05-ago-14	0,00
PR0602	GESTION DE SRVICIOS ENTREGADOS POR TERCERAS PARTES	07-abr-14	30	06-jul-14	0,00
A.10.2.1	Entrega de servicios	07-abr-14	30	07-may-14	0,00
A.10.2.2	Monitoreo y revisión de servicios suministrados por terceras partes	07-abr-14	30	07-may-14	0,00
A.10.2.3	Gestión de cambios en servicios hechos por terceras partes	07-abr-14	30	07-may-14	0,00
PR0603	PLANEACION Y ACEPTACION DEL SISTEMA	07-abr-14	30	06-jun-14	0,00
A.10.3.1	Planeación de la capacidad	07-abr-14	30	07-may-14	0,00
A.10.3.2	Aceptación del sistema	07-abr-14	30	07-may-14	0,00
PR0604	PROTECCION CONTRA CODIGO MALICIOSO Y DESCARGABLE	07-abr-14	30	07-may-14	0,00
A.10.4.1	Controles contra software malicioso	07-abr-14	30	07-may-14	0,00
PR0605	COPIAS DE SEGURIDAD	07-abr-14	30	07-may-14	0,00
A.10.5.1	Copias de seguridad de la información	07-abr-14	30	07-may-14	0,00

CONTINÚA

Plan, programa proyecto		Fecha inicio	Días	Fecha fin	Costo
PR0606	GESTION DE LA SEGURIDAD DE LA RED	07-abr-14	30	05-ago-14	0,00
A.10.6.1	Controles de red	07-abr-14	30	07-may-14	0,00
A.10.6.2	Seguridad de los servicios de red.	07-abr-14	90	06-jul-14	0,00
PR0607	GESTION DE LOS MEDIOS	07-abr-14	30	06-jul-14	0,00
A.10.7.2	Eliminación de medios	07-abr-14	30	07-may-14	0,00
A.10.7.3	Procedimientos para el manejo de la información	07-abr-14	30	07-may-14	0,00
A.10.7.4	Seguridad de la documentación del sistema	07-abr-14	30	07-may-14	0,00
PR0608	INTERCAMBIO DE INFORMACION	07-abr-14	40	26-jul-14	0,00
A.10.8.1	Procedimientos y políticas para el intercambio de información	07-abr-14	40	17-may-14	0,00
A.10.8.2	Acuerdos de Intercambio	07-abr-14	40	17-may-14	0,00
A.10.8.4	Correo electrónico	07-abr-14	30	07-may-14	0,00
PR0609	SEGURIDAD EN COMERCIO ELECTRONICO	07-abr-14	20	27-may-14	0,00
A.10.9.1	Comercio electrónico	07-abr-14	20	27-abr-14	0,00
A.10.9.2	Transacciones en línea	07-abr-14	30	07-may-14	0,00
PR0610	MONITOREO	07-abr-14	20	26-jul-14	0,00
A.10.10.1	Registro de auditoría	07-abr-14	20	27-abr-14	0,00
A.10.10.2	Monitoreo del uso del sistema	07-abr-14	30	07-may-14	0,00
A.10.10.5	Registro de fallos	07-abr-14	60	06-jun-14	0,00
PROG07	CONTROL DE ACCESO	07-abr-14	260	23-dic-14	0,00
PR0701	REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO	07-abr-14	20	27-abr-14	0,00
A.11.1.1	Políticas para el control de acceso	07-abr-14	20	27-abr-14	0,00
PR0702	ADMINISTRACION DE ACCESO DE USUARIOS	07-abr-14	20	17-may-14	0,00
A.11.2.3	Administración de contraseñas para usuarios.	07-abr-14	20	27-abr-14	0,00
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	07-abr-14	20	27-abr-14	0,00
PR0703	RESPONSABILIDADES DE LOS USUARIOS	07-abr-14	20	27-abr-14	0,00
A.11.3.1	Uso de contraseñas.	07-abr-14	20	27-abr-14	0,00
PR0704	CONTROL DE ACCESO A REDES	07-abr-14	10	06-jun-14	0,00

CONTINÚA

	Plan, programa proyecto	Fecha inicio	Días	Fecha fin	Costo
A.11.4.2	Autenticación de usuarios para conexiones externas	07-abr-14	10	17-abr-14	0,00
A.11.4.3	Identificación de equipos en red	07-abr-14	10	17-abr-14	0,00
A.11.4.6	Control de conexión a las redes	07-abr-14	40	17-may-14	0,00
PR0706	CONTROL DE ACCESO A LA INFORMACION Y APLICAIONES	07-abr-14	60	07-abr-14	0,00
A.11.6.1	Restricción de acceso a la información	07-abr-14	60	06-jun-14	0,00
PR0707	COMPUTACION MOVIL Y TRABAJO REMOTO	07-abr-14	60	07-abr-14	0,00
A.11.7.2	Trabajo remoto	07-abr-14	60	06-jun-14	0,00
PROG08	ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS	07-abr-14	545	04-oct-15	0,00
PR0802	PROCESAMIENTO CORRECTO DE APLICACIONES	07-abr-14	120	07-abr-14	0,00
A.12.2.1	Validación de los datos de entrada	07-abr-14	120	05-ago-14	0,00
A.12.2.2	Control al procesamiento interno	07-abr-14	60	06-jun-14	0,00
PR0803	CONTROLES CRIPTOGRAFICOS	07-abr-14	60	07-abr-14	0,00
A.12.3.1	Política en el uso de controles criptográficos	07-abr-14	60	06-jun-14	0,00
PR0804	SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA	07-abr-14	30	07-abr-14	0,00
A.12.4.1	Control del software operativo	07-abr-14	30	07-may-14	0,00
PR0805	SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE	07-abr-14	80	07-abr-14	0,00
A.12.5.1	Procedimientos de control de los cambios.	07-abr-14	80	26-jun-14	0,00
A.12.5.2	Revisión técnica de aplicaciones después de cambios en el sistema o	07-abr-14	20	27-abr-14	0,00
A.12.5.3	Restricciones en los cambios a los paquetes de software	07-abr-14	10	17-abr-14	0,00
A.12.5.5	Desarrollo externo de software	07-abr-14	120	05-ago-14	0,00
PR0806	GESTION DE VULNERABILIDADES TÉCNICAS	07-abr-14	45	07-abr-14	0,00
A.12.6.1	Control de vulnerabilidades técnicas.	07-abr-14	45	22-may-14	0,00
PROG09	GESTION DE LOS INCIDENTES DE SEGURIDAD DE LA INFOR	07-abr-14	60	06-jun-14	0,00
PR0902	GESTION DE LOS INCIDENTES DE SEGURIDAD DE INFORMAC	07-abr-14	60	07-abr-14	0,00
A.13.2.1	Responsabilidades y procedimientos	07-abr-14	60	06-jun-14	0,00
PROG10	GESTION DE CONTINUIDAD DEL NEGOCIO	07-abr-14	240	03-dic-14	0,00
PR1001	ASPECTOS DE SEGURIDAD DE INFORMACION EN CONTINUIDA	07-abr-14	240	03-dic-14	0,00

CONTINÚA

	Plan, programa proyecto	Fecha inicio	Días	Fecha fin	Costo
A.14.1.3	Desarrollo e implementación del plan de continuidad incluyendo seg	07-abr-14	240	03-dic-14	0,00
PROG11	CONFORMIDAD	07-abr-14	335	07-ene-15	0,00
PR1101	CONFORMIDAD CON LOS REQUISITOS LEGALES	07-abr-14	45	07-ene-15	0,00
A.15.1.1	Identificación de la legislación aplicable	07-abr-14	45	22-may-14	0,00
A.15.1.2	Derechos de propiedad intelectual.	07-abr-14	60	13-jun-14	0,00
A.15.1.3	Protección de los registros de la organización	07-abr-14	50	27-may-14	0,00
A.15.1.4	Protección de los datos y privacidad de la información personal	07-abr-14	100	16-jul-14	0,00
A.15.1.5	Protección del uso inadecuado de los recursos de procesamiento de l	07-abr-14	50	27-may-14	0,00
A.15.1.6	Reglamentación de los controles criptográficos	07-abr-14	30	07-may-14	0,00

Fuente: Los Autores

CAPITULO V

5.1. CONCLUSIONES

- El tránsito y transmisión de la información puede dar oportunidad para que los documentos sean interceptados, destruidos, copiados o alterados comprometiendo su integridad, disponibilidad y confidencialidad.
- El personal de de la Dirección de Seguros previsionales no cuenta con ningún tipo de entrenamiento ni capacitación en relación a seguridad de información, pudiendo ocasionar de manera involuntaria que la información que se manipula en el área sea mal utilizada.
- Los roles de acceso a la información de los sistemas informáticos son establecidos por requerimientos de la misma Dirección de Seguros Previsionales,
- La información soportada en medios físicos y digitales esta expuesta y es manipulada voluntaria o involuntariamente por personal del ISSFA sin tener la debida autorización
- Existe información generada o utilizada en el proceso de Seguros Previsionales que no tiene un propietario asignado, por lo tanto no existe un responsable de la misma.
- La información que se utiliza en el proceso de Seguros Previsionales no se encuentra clasificada de acuerdo a su criticidad.
- No se puede garantizar la continuidad de las operaciones del proceso de Seguros Previsionales ya que no existe un procedimiento para tal efecto.
- En la UTIC no se ha establecido las condiciones necesarias para segregar las funciones del personal, lo que ocasiona que el personal técnico realice operaciones de seguridad de la información las cuales no se encuentran estipuladas en sus perfiles.
- La UTIC carece de un plan de recuperación de desastres.

- El ISSFA carece del comité y del área de seguridad de información requerida para mantener los procesos de seguridad mínimos.
- Los controles de seguridad con los que cuenta el proceso de Seguros Previsionales no se encuentran documentados, básicamente estos se encuentran embebidos en los sistemas informáticos.
- El ISSFA no cuenta con licencias Office regularizadas por Microsoft.
- No existen acuerdos de Confidencialidad específicos con terceros.
- El ISSFA no realiza auditorias de seguridad de la información con entidades independientes, por lo cual no se conoce la situación actual de la Organización en cuanto a seguridad de la información.
- Las copias de seguridad de la base de datos no se almacenan en un lugar externo a la Institución.

5.2. RECOMENDACIONES

- Establecer políticas de seguridad en la infraestructura de red interna y externa, acceso físico a la información generada en medios de almacenamiento con el fin de evitar el acceso de intrusos.
- Establecer dentro del perfil de los funcionarios que laboran en la Dirección de Seguros Previsionales, contar con conocimientos básicos sobre seguridad de información.
- Los roles de acceso a la información de los sistemas informáticos, deben ser asignados de acuerdo a las funciones establecidas por Talento Humano del ISSFA.
- Establecer un control para mantener la información resguardada en un sitio con las debidas seguridades y su acceso sea con la autorización del dueño de la misma.
- Asignar un propietario a cada uno de los documentos físicos o lógicos que se manipulan en el proceso.
- Clasificar la información considerando su criticidad y establecer sus niveles de seguridad.
- Establecer un plan de continuidad del negocio para el proceso de Seguros Previsionales en coordinación con la Dirección de Riesgos del ISSFA.
- Establecer técnicamente las funciones del personal de la UTIC, implementar un procedimiento para segregar las funciones.
- Establecer un plan de recuperación de desastres para la UTIC.
- Establecer el comité y el área de seguridad de la información mínima para poder soportar los controles que el proceso de Seguros Previsionales mantiene actualmente y los que necesita establecer en forma urgente.
- Documentar y legalizar los controles de seguridad existentes, para el proceso de Seguros Previsionales.

- Regularizar el uso de software Office con el proveedor Microsoft, con el fin de evitar sanciones.
- Establecer acuerdos de Confidencialidad específicos con terceros.
- Realizar la contratación de entidades independientes capacitadas en auditoria de seguridad de la información.
- Almacenar las copias de seguridad de información en un sitio externo que cumpla con las condiciones necesarias para mantener la integridad de los soportes.

- **5.3. BIBLIOGRAFÍA**

Garfinkel, & Spanfford. (1996). *Practical Uni & Internet security.* O'Reilly & Associates.

Gerencia.com. (2013). *Qué es Tecnología de Información.* Recuperado el 12 de 9 de 2014, de http://www.degerencia.com/tema/tecnologia_de_informacion

González, g. (2012). *Informática 11 Colección Ciencia Educativa.* Nueva imagen.

Instituto Español de Estudios estratégicos. (s.f). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Instituto universitario General Gutierrez Mellado.

ISACA. (2012). *ISACA*. Recuperado el 18 de 7 de 2014, de www.isaca.org

ISO 27000. (2013). *Sistema de gestión de seguridad de información.* Recuperado el 25 de 8 de 2014, de http://www.iso27000.es/download/doc_sgsi_all.pdf

ISO 27001. (2012). *Una instroducci{on simple a los aspectos básicos*. Recuperado el 11 de 7 de 2014, de http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

ISSFA. (2014). *ISSFA*. Recuperado el 3 de 9 de 2014, de www.issfa.mil.ec

NORMA TECNICA ECUATORIANA NT INEN-ISO/IEC 27005:2012. (2013). Recuperado el 2 de 10 de 2014, de http://www.normalizacion.gob.ec

Rojas, M. (2013). *Auditoría Informática*. Recuperado el 26 de 9 de 2014, de http://es.scribd.com/doc/19505290/Auditoria-Informatica

Secure& It. (2012). *Secure& It*. Recuperado el 1 de 8 de 2014, de http://www.secureit.es/

Shared. (2011). *seguridad lógica.* Recuperado el 12 de 7 de 2014, de http://www.4shared.com/web/preview/pdf/-Q26VFvX

5.4. Listado de anexos

ANEXO A	Catalogo de activos de información
ANEXO B	Calificación de importancia de activos de información
ANEXO C	Catálogo de amenazas humanas
ANEXO D	Catálogo de amenazas comunes
ANEXO E	Asignación de amenazas humanas a activos de información
ANEXO F	Asignación de amenazas comunes a activos de información
ANEXO G	Catálogo de vulnerabilidades
ANEXO H	Controles de la norma ISO 27002
ANEXO I	Plan de tratamiento de riesgos por amenazas comunes
ANEXO J	Plan de tratamiento de riesgos por amenazas humanas
ANEXO K	Declaración de aplicabilidad