MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

Informe de Valoración de Riesgos Institucionales

Tecnologías de información

Dirección General de Planificación

Departamento de Control Interno

2013

SAN JOSÉ/COSTA RICA

Contenido

Presentación

El proceso de valoración de riesgos, se ejecuta todos los años por parte de la administración activa que involucra Jerarca y titulares subordinados, atendiendo las responsabilidades legales consignadas en los artículos 14 y 18 de la Ley General de Control Interno, integrándose como una herramienta para mejorar la gestión institucional y el cumplimento de sus objetivos.

Asimismo, las Normas Técnicas para la gestión y el control de las tecnologías de Información (N-2-2007-CO-DFOE), sobre Gestión de riesgos señala que… **"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante la gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.**

Es decir, las buenas prácticas concentradas en el marco de las normas técnicas para la gestión y el control, establece que las Instituciones se alineen con la tecnología de la información para así alcanzar los mejores resultados, dando valor agregado y mitigando el riesgo, controles que constituyen esencia en la gestión de las Tecnologías de Información (TI).

Es así como, el proceso de valoración de riesgos 2013, propuso la evaluación de riesgos en los procesos que se apoyan con el uso de las tecnologías de información, bajo la integración de los componentes, Calidad de la Información, Gestión de la Seguridad, Seguridad Física y Ambiental, Infraestructura y Arquitectura, Definición de Servicios y Gestión de Proyectos, conforme lo establece dichas normas.

En este contexto, el presente informe de resultado, se integra al proceso de rendición de cuentas y al compromiso que muestra el Ministerio de Trabajo y Seguridad Social por el cumplimiento de las exigencias contenidas en la Legislación costarricense en materia de control interno.

Metodología Aplicada

La metodología utilizada es la denominada Gerencia de Riesgos que exigen las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración de Riesgos (SEVRI) D-3-2005-CO-DFOE, emitidas por la Contraloría General de la República, que involucra los componentes de un marco orientador y las actividades de identificación, análisis, evaluación, administración, revisión, documentación y comunicación de los riesgos institucionales relevantes.

El proceso para llevar a cabo el SEVRI-MTSS del 2013 consta de tres matrices, están ubicadas en un libro de Excel con tres hojas que se encuentran vinculadas entre sí, de manera que al alimentar la primera matriz, automáticamente las matrices dos y tres son enlazadas con dicha información.

El proceso SEVRI-MTSS del 2013 fue suscrito por el señor Ministro de Trabajo y Seguridad Social, Ph.D. Olman Segura Bonilla mediante circular DMT-001-2013 del 16 de julio de los corrientes; en el cual se estableció el Marco Orientador con los Lineamientos y plazos para el proceso de Valoración de Riesgos Institucional, enfocado en este período en el uso de las Tecnologías de Información.

De forma paralela, el Departamento de Control Interno se dio a la tarea de asesorar a las unidades administrativas sobre la "Aplicación de la Metodología del Sistema Específico de Valoración de Riesgos", con la finalidad de promover un ambiente de apoyo y uniformar el proceso a nivel institucional.

Tomando como referencia los lineamientos emitidos por el jerarca de este Ministerio, un nivel de riesgo institucional aceptable es el punto de gravedad del riesgo[1] que la institución está dispuesta a enfrentar. Para estos efectos, se ha determinado para el Ministerio de Trabajo y Seguridad Social que un nivel de riesgo menor al 30% es aceptable cuando el riesgo presenta vulnerabilidad baja (impacto y probabilidad baja frente a los controles existentes).

El riesgo alto no será aceptado para ninguna de las actividades que ejecuta el Ministerio de Trabajo; por lo tanto, si alguna actividad llegara a ubicarse en estos niveles, requieren establecer un plan de tratamientos de riesgos que minimicen su impacto y, por ende, mejoren su rendimiento.

1 El punto de gravedad del riesgo lo determina el resultado de probabilidad por impacto. (Alto, moderado y bajo)

El presente cuadro describe los parámetros que definió la metodología para la calificación cuantitativa y cualitativa, utilizados en el proceso de valoración de los riesgos identificados.

Cuadro 1
COSTA RICA, MTSS: Parámetro de Valoración de Riesgo, Probabilidad e Impacto, SEVRI-2013

Parámetros de Probabilidad		
Probabilidad		**Descripción**
Cualitativa	**Cuantitativa**	
Casi certeza	9-10	Se espera que ocurra en la mayoría de las circunstancias
Probable	7-8	Probablemente ocurrirá en la mayoría de las circunstancias
Moderado	5-6-	Podría ocurrir en algún momento
Poco Común	3-4	Puede ocurrir solo en circunstancias excepcionales
Improbable	1-2	Pudo ocurrir en algún momento

Parámetros de Impacto		
Impacto		**Descripción**
Cualitativa	Cuantitativa	
Insignificante	1-2	Baja pérdida financiera; impacto social menor.
Menor	3-4	Pérdida financiera media, impacto social medio
Moderado	5-6	Pérdida financiera alta, impacto social alto
Mayor	7-8	Pérdida financiera mayor, pérdida de capacidad de producción
Crítico	9-10	Enorme pérdida financiera, gran impacto a la sociedad

Fuente: MTSS, Dirección General de Planificación, Departamento Control Interno, con base en el Marco orientador SERVRI, 2013

La asignación de dichos puntajes se requieren para valorar la probabilidad (cuan posible es que ocurra un evento y que el riesgo se materialice), Impacto de riesgo (consecuencia que puede ocasionar la materialización del riesgo) y los factores de riesgo (causa) y darle el valor automáticamente muestra la cualidad del resultado.

Cuadro 2
COSTA RICA, MTSS: Parámetros para la evaluación de medidas de control, SEVRI-2013

Medidas de control		
Calificación		
Cualitativo	Cuantitativo	Descripción del control
Excelente	5	Controles que no requieren modificaciones y agregan valor a la gestión.
Muy Bueno	4	Controles apropiados pero pueden ser mejores. Su valor agregado puede mejorar.
Bueno	3	Controles apropiados parcialmente y que requieren de mejoras. Su valor agregado debe mejorar.
Regular	2	Controles no muy apropiados y requieren de mejoras. No dan valor agregado.
Deficiente	1	Controles no apropiados obstaculizan la gestión requieren ser modificados. No dan valor agregado.

Fuente: MTSS, Dirección General de Planificación, Departamento Control Interno, con base en el Marco orientador SERVRI, 2013

El resultado de una valoración de riesgos proporciona un inventario de acciones, a fin de lograr la eficiencia de los controles.

Para los niveles de riesgos altos y moderados se requiere que cada responsable de la unidad administrativa evaluada, desarrolle e implemente estrategias y planes de acción específicos para aumentar el cumplimiento y reducir los riesgos, que por sus resultados requieren prioritariamente de atención.

Cuadro 3
COSTA RICA, MTSS: Medidas para la Administración de Riesgos SEVRI-2013

Medidas para la Administración de los Riesgos	
Modificar riesgo	Opción de administración de riesgos que consiste en modificar el proyecto, función o actividad para que logre su objetivo sin verse afectado por el riesgo.
Evitar riesgo	Opción para administrar riesgos que consiste en afectar los factores de riesgo asociados a la probabilidad y/o la consecuencia de un evento, previo a que éste ocurra.
Transferir riesgo	Opción de administración de riesgos, que consiste en que un tercero soporte o comparta, parcial o totalmente, la responsabilidad y/o las consecuencias potenciales de un riesgo.
Retener riesgo	Opción de administración de riesgos que consiste en no aplicar los otros tipos de medidas (modificación, evitar, transferencia) y estar en disposición de enfrentar las eventuales consecuencias.

Fuente: MTSS, Dirección General de Planificación, Departamento Control Interno, con base en el Marco orientador SERVRI, 2013

La medidas de administración de riesgos, se determina una vez que se ha realizado el análisis considerando el nivel de riesgo obtenido, grado de influencia sobre los factores de riesgo y la eficacia y eficiencia de los controles existentes, dando orientación para establecer un tratamiento de riesgos que nos conduzca a reducir el impacto, sobre la consecución de objetivos y por ende del funcionamiento de la Institución.

Resultados del Proceso Institucional SEVRI-MTSS-2013

Los resultados que se muestran a continuación, son acompañados por la evaluación de los niveles de riesgos mediante un análisis cualitativo y cuantitativo, en términos de consecuencia y probabilidad según los eventos identificados en torno a los procesos que sostienen las tecnologías de información y sus componentes.

Se presentan los resultados institucionales, obtenidos con una participación de todas las Direcciones que integran este Ministerio, es decir, 56 instancias administrativas que han sido agrupadas en nueve Direcciones, Tres Órganos desconcentrados, y tres unidades de *Staff*, y que han cumplido con la presentación de las matrices para la valoración del riesgo.

Cabe señalar, que el Programa Nacional de Micro y Pequeña Empresa, PRONAMYPE, mediante oficio DE-PRO-115-2013 de fecha 8 de agosto, 2013 manifiesta que no ha logrado identificar riesgos evidentes que puede gestionar o administrar, ya que el programa reviste de características propias muy diferentes, en lo que corresponde a Tecnologías de Información, esto por tener la naturaleza de un "FIDEICOMISO" todos sus procesos sustantivos en este campo están vinculados directamente con los sistemas del Banco Popular, quien opera como FIDUCIARIO, por tal motivo todas las variables evaluadas están sujetas al desarrollo, gestión y seguridad de dicha Entidad. (Anexo No.1)

1. Identificación del Riesgo

La identificación del riesgo es la primera actividad del Sistema Específico de Valoración de Riesgos. En ella se logran determinar las circunstancias o eventos que podrían en algún momento, afectar los objetivos institucionales.

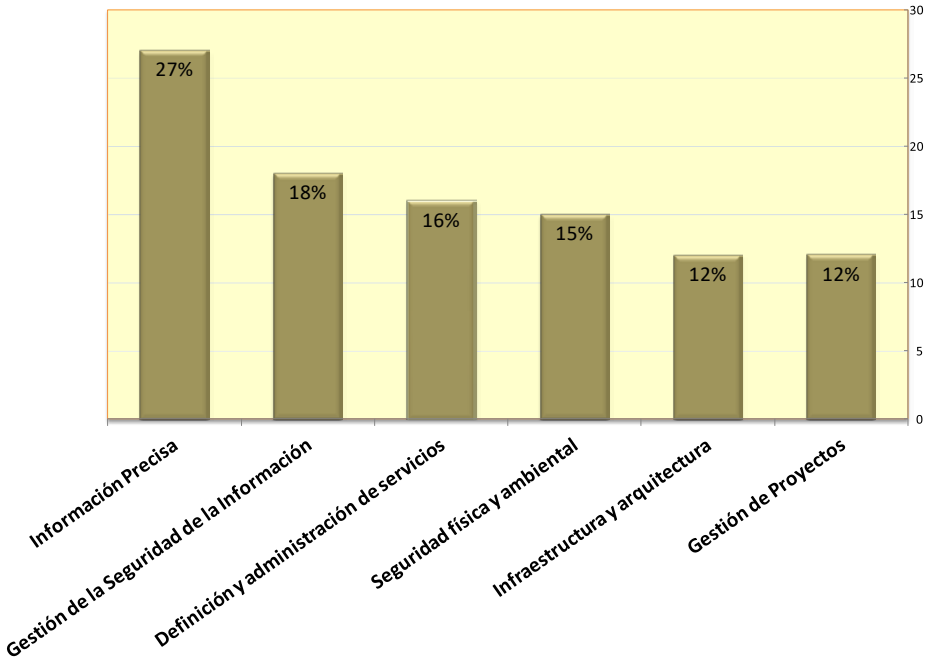
De acuerdo a la valoración realizada por las distintas unidades administrativas, los riesgos identificados con mayor frecuencia, son los que afectan la calidad de la información. En ese sentido, un 27% de las unidades administrativas lo han clasificado como riesgo bajo, el cual debe entender como aquellos que presentan una vulnerabilidad, baja y requieren comprobaciones periódicas para asegurar que se mantiene la eficiencia de las medidas de control.

Es decir, que con mayor frecuencia se han identificado en las dependencias del MTSS, posibles eventos en torno al tipo de información, asociada a la evaluación de información incompleta, excesiva y de baja calidad, que puede causar decisiones equivocadas.

Sin embargo, en igual forma en todos los componentes evaluados se presentan eventos que debilitan su funcionamiento.

El siguiente gráfico, ilustra resultados obtenidos en cada uno de los 6 componentes evaluados en la integración de las tecnologías de información y el porcentaje de riesgo obtenido en cada uno de ellos.

Gráfico 1.
COSTA RICA, MTSS Riesgos identificados en Tecnologías de Información por componente funcional, SEVRI-2013



Fuente: MTSS. Departamento de Control Interno, datos suministrados por las dependencias SEVRI 2013

1.1. Riesgo de información precisa y completa: Está referido a los eventos que se puedan presentar afectando información incompleta o excesiva y de baja calidad que puede causar decisiones equivocadas.

En este contexto el valor promedio, obtenido para los riesgos referidos a este componente es de un 27%; clasificado como riesgo bajo, como evento principal destaca la ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones en algunos sistemas que soportan las labores sustantivas del quehacer institucional.

Acompañado, de posibles eventos de información desactualizada o incorrecta, por falta de dominio sobre las herramientas tecnológicas en uso, y poco presupuesto para diseñar e

implementar programas de capacitación para los usuarios. Asimismo, se ha identificado la falta de guías o manuales de usuario para el uso de sistemas que limitan la autocapacitación.

1.2. Gestión de la seguridad de la información: Implica la identificación de eventos que afectan resguardar la confidencialidad, integridad y disponibilidad de la información, es decir, protegerla contra uso, divulgación o modificaciones no autorizadas.

Este componente presenta un valor promedio de riesgo bajo con un 18%, se requiere mejorar el compromiso en la seguridad y confidencialidad para reducir los riesgos de error en el uso de los recursos TI; acompañado de adecuadas políticas para la generación de respaldos, con mucha frecuencia los usuarios manifiestan desconocer la ubicación y periodicidad, con que se realizan respaldos de los equipos y sistemas, que podrían provocar alteraciones o pérdidas de la información registrada en la base de datos o equipos.

1.3. Definición y administración de acuerdos de servicios: Para evitar riesgos referidos a productos contratados por terceros, se deben acordar los requerimientos, los servicios ofrecidos y sus atributos, tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad en la prestación de servicios y mantenimiento.

En cuanto a los servicio TI, con un valor promedio de 16%, clasificado como bajo, según los datos aportados por las dependencias, destaca el no contar con respuesta oportuna y efectiva para las consultas de los usuarios TI, así como la atención y seguimiento de los incidentes. No se realiza una adecuada gestión de métricas, sobre los incidentes reportados o no se documentan las soluciones aplicadas, especialmente en aquellas oficinas regionales que aún carecen del sistema de incidentes o que no lo utilizan como se debe y siguen solucionando percances tecnológicos con otras iniciativas.

1.4. Seguridad física y ambiental: Este riesgo se manifiesta, cuando no exista una protección adecuada de los recursos de TI, sin establecer un ambiente físico seguro y controlado, con medidas de protección suficientes fundamentadas en políticas vigentes y análisis de riesgos.

El nivel promedio de riesgo, identificados en este componente fue de un 15% es un riesgo bajo, y las principales debilidades que detectan, están puntualizadas por la continuidad, seguridad y el control de energía eléctrica del cableado de datos y de las comunicaciones inalámbricas; este aspecto destaca con mayor intensidad en Oficinas Regionales por las instalaciones físicas que los alberga.

Un aspecto que llama la atención en este componente, es la insuficiencia de controles para el desecho y reutilización de los recursos TI, es decir, no se da una valoración oportuna a los

equipos que son desplazados por nuevas tecnologías, lo que podría provocar una subutilización del equipo o algunas de sus partes.

1.5. Riesgos en la infraestructura y arquitectura: Es la probabilidad de que no exista una estructura informática efectiva (hardware, software, redes, personas y procesos) para soportar las necesidades presentes y futuras, está asociada con los procesos que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas.

La infraestructura y arquitectura presenta la identificación de mayores riesgos, con un valor promedio de riesgo del 12%; los eventos identificados son por versiones de software desactualizados o versiones para desarrollo y producción diferentes, los recursos de la infraestructura tecnológica no son suficientes para atender las demandas de los servicios.

Por ejemplo, fallas en los equipos y servidores, suspensión o accesibilidad a internet para lograr conectividad con el sistema de casos de la Inspección, sistema de consulta laboral (Zendesk), Integra, SIGAF, compra Red, entre otros.

1.6. Gestión de Proyectos: Es el riesgo de un débil proceso de administración de los proyectos de TI de manera que no logre sus objetivos, términos de calidad, tiempo y presupuesto óptimo preestablecidos.

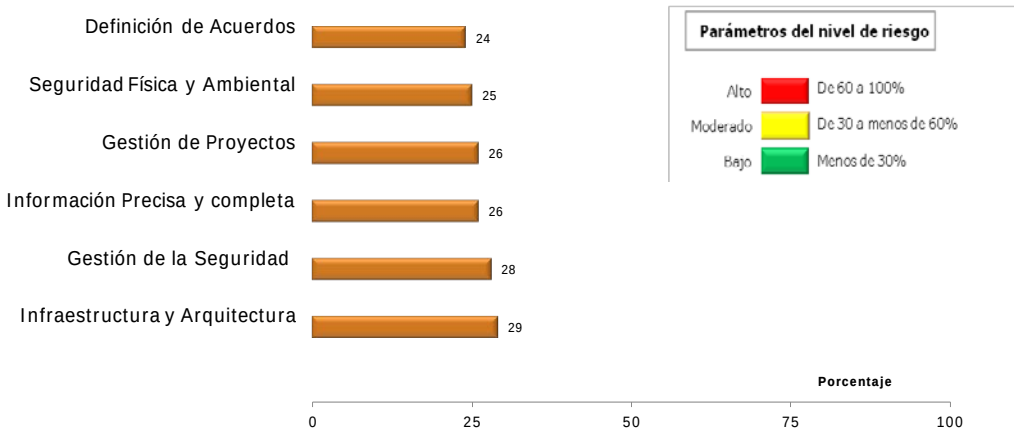
Este último componente de las tecnologías de información evaluada, obtuvo un riesgo promedio de 12% riesgo bajo, cuyo eventos posibles son el desarrollo de proyectos no alineados al Plan Estratégico, no contar con un marco de referencia para la gestión de los proyectos en cuanto a su iniciación, planificación, ejecución, control y cierre; desarrollar productos basados en requerimientos incorrectos o adquirir software sin programas fuentes.

Otro aspecto, que incide como posible evento de riesgo, son los retrasos en los procesos de contratación administrativa y la posible dificultad para definir ámbito de acción de los proveedores.

2. Nivel de Riesgo

Por otra parte, el análisis de datos permitió de manera segregada determinar el valor promedio del nivel de riesgos, obtenido por cada componente funcional en Tecnologías de Información. El nivel de riesgo, se obtiene del resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de cada proceso que se realiza.

Gráfico 2
COSTA RICA, MTSS: Nivel de Riesgo en Tecnologías de Información, por componente funcional, 2013
(Valor máximo: 100%)



Fuente: MTSS. Departamento de Control Interno, datos suministrados por las dependencias SEVRI, 2013

El gráfico 2. ilustra los resultados comentados en la fase de identificación de riesgos, utilizando datos cuantitativos determinando valores promedios de riesgos para cada uno de los componentes que integraron la evaluación en materia de Tecnologías de Información.

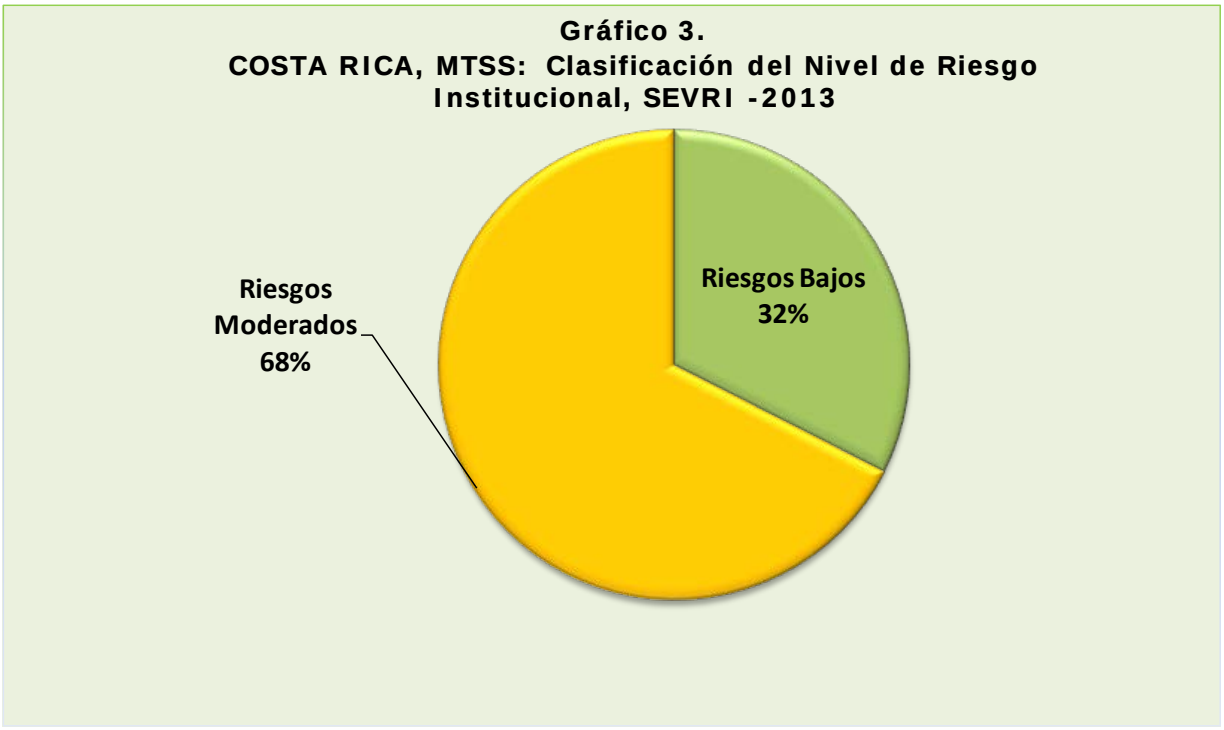
En general, los componentes se ubican en un valor promedio de riesgo entre el 24% y 29%, clasificación de riesgo bajo, es decir el riesgo presenta vulnerabilidad baja, (Impacto y Probabilidad baja versus controles existentes). Se necesita darle seguimiento constantemente con el fin de que no representen una amenaza para la institución.

3. Clasificación del Riesgo

La fase de clasificación de los riesgos en términos institucionales, se obtiene del resultado de confrontar el impacto y la probabilidad con los controles existentes aplicables, a cada dependencia que integra el Ministerio de Trabajo y Seguridad Social.

De dicho análisis y tabulación de los datos que se utilizan como insumo de información y valoración de riesgos, se obtiene el siguiente gráfico :

Gráfico 3.
COSTA RICA, MTSS: Clasificación del Nivel de Riesgo Institucional, SEVRI -2013



Fuente: MTSS. Departamento de Control Interno, datos suministrados por las dependencias SEVRI, 2013

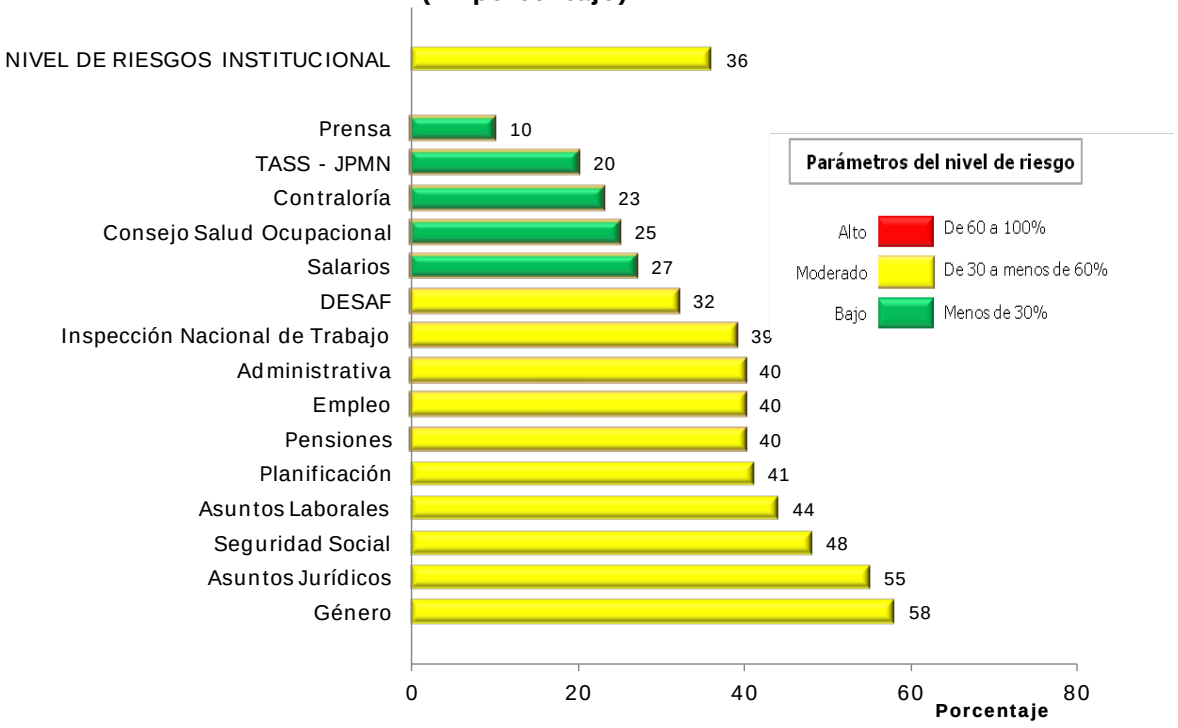
El gráfico 3. indica que el 68% de los riesgos institucionales son clasificados como moderados, que requieren de comprobaciones periódicas para asegurar que se mantienen la eficiencia de las medidas de control orientadas a minimizar el impacto. El 32% de los riesgos son bajos, por lo que se hace necesario proporcionarles seguimiento constante con el fin de que no representen una eventual amenaza para la institución.

Destaca para la evaluación de riesgos 2013, que no se presentan riesgos altos que reflejen un impacto y probabilidad alta frente a los controles existentes los cuales no son aceptables por la institución, requieren un tratamiento del riesgo que minimice su impacto y, por ende, mejore su rendimiento.

4. Evaluación del nivel de riesgos por dependencias administrativas

La identificación de dichos riesgos se acompaña con el análisis de consecuencia, según su impacto y probabilidad de ocurrencia, que define el resultado de la calificación del nivel de riesgo, el cual se presenta a continuación basado en los resultados obtenidos en cada unidad administrativa, que se agrupo según los niveles organizacionales a que corresponde.

Gráfico 4
COSTA RICA, MTSS: Nivel de riesgos, por dependencias institucionales, 2013
(En porcentaje)



Fuente: MTSS. Departamento de Control Interno, datos suministrados por las dependencias proceso SEVRI, 2013

El gráfico 4. utilizando datos cuantitativos y cualitativos muestra el nivel de riesgo en que se ubica cada dependencia, con los cuales se determinó un promedio ponderado del **36%,** equivalente moderado, el resultado institucional. El riesgo presenta vulnerabilidad moderada cuando el impacto es alto y la probabilidad es baja, o cuando el impacto es bajo con probabilidad alta frente los controles existentes.

4.1 Niveles de riesgo moderado

Destaca en el gráfico 4. la **Dirección de Asuntos Jurídicos**, con un nivel de riesgo 55% con una clasificación de riesgo moderado, obedece a las vulnerabilidades que presenta el sistema de consultas jurídicas que realizan los usuarios vía web (Zendesk), en cuanto al acceso, registro de bitácoras, respaldo de histórico de consultas, ausencia de manuales de usuarios, u otros aspectos, provocados porque actualmente, solo se cuenta con un agente autorizado para el ingreso, es decir, se comparte la misma clave de ingreso al sistema entre funcionarios de diferentes dependencias del MTSS responsables de dar consulta.

La **Dirección de Seguridad Social,** con un nivel de riesgo de 48%, riesgo moderado, determinan su resultado en la probabilidad de riesgos en la infraestructura y arquitectura efectiva para soportar las necesidades presentes y futuras, los equipos tecnológicos están obsoletos y con poca capacidad operativa con versiones de software desactualizados.

El nivel de riesgo correspondiente a la **Dirección de Asuntos Laborales**, con un 44% clasificado como riesgo moderado, está definido sobre las probabilidades de eventos que puedan afectar los datos estadísticos de los diferentes servicios que se brindan y registran en el sistema, tomando en cuenta que algunos funcionarios no tienen dominio sobre el uso de la herramienta, la ausencia de controles cruzados que comprueben la integridad de la información, acompañando de falta de presupuesto para impartir la capacitación.

La **Dirección de Nacional de Pensiones**, obtuvo un nivel de riesgo de 40% que su identificación se clasifican en probabilidades de riesgo en cuento a la infraestructura y arquitectura dado que los recursos no son suficientes para atender las demandas de los servicios, asimismo los posibles eventos en un débil proceso de administración de proyectos TI, de manera que no logre sus objetivos, términos de calidad, tiempo y presupuesto óptimo.

Por otra parte, destacan eventos en el sistema SIG, que interviene en la información precisa y exacta sobre la ubicación y proceso de expedientes, que eventualmente podrían afectar la oportunidad de los servicios en respuestas administrativas o judiciales. Acompañado de desconocimiento en las políticas de respaldo de la información, de todos los sistemas.

Tal como se ilustra en el gráfico 4. la **Dirección Nacional de Empleo**, con un resultado en el nivel de riesgo del 40%, referido por los eventos que podrían presentarse en el sistema de migraciones laborales (SIMLA), actualmente se contrataron los servicios de terceros para alimentar el sistema, se manera que los riesgos se materializan si eventualmente no se diera capacitación, seguimiento, respaldos y mantenimiento al sistema.

Asimismo, señalan posibles eventos en el SIOIE, sistema nacional de intermediación, Orientación e Información de Empleo, en cuanto a la integridad y confiabilidad de la

información que se genera, dadas las discrepancias entre los datos obtenidos por filtros dinámicos y reportes fijos; falta de dominio sobre uso de la herramienta, ausencia de controles cruzados y proceso de respaldo insuficiente.

En cuanto al programa nacional de empleo (PRONAE), que se dé un uso inadecuado al instrumento, no se brinda capacitación constante, el manual de usuario es muy general y poco amigable, que los respaldos no se estén dando con la periodicidad adecuada, no lleva al día un control de incidencias; y en cuanto a gestión de proyectos la eventualidad de un débil proceso de administración de proyectos que no logre sus objetivos.

La **Dirección de Asignaciones Familiares (DESAF**), con un resultado moderado en su nivel de riesgo del 32%, describe posibles eventos de riesgo en el control de la bitácora del sistema de patronos morosos, el cual no cuenta con manuales de usuarios y controles cruzados para garantizar la integridad de la información; en materia legal la rectitud de expedientes digitales que respaldan las prescripciones; riesgos asociados a las políticas de generación de respaldos en el control presupuestario, evaluación y demás gestión de la DESAF.

Por otro lado, se hace alguna referencia a la seguridad física y ambiental, con debilidades en la protección adecuada de los recursos TI sin establecer un ambiente físico seguro y controlado, lo cual está en proceso de administrar con la compra de los gabinetes para los servidores entre otras acciones que minimizan los riesgos.

Dirección administrativa y Financiera, con un nivel de riesgo de **40%** enfoca la identificación de riesgos en la gestión de la seguridad de la información, mediante accesos indebidos que pongan en peligro la información contenida en las bases de datos del MTSS, por falta de compromiso en la aplicación de políticas de respaldo, acceso a las instalaciones que resguardan recursos TI, debilidades en la infraestructura eléctrica, inseguridad en la red inalámbrica por falta de controles de autenticación de contraseñas, filtrado de datos web o control de descargas.

Es importante destacar la probabilidad en el riesgo de la infraestructura y arquitectura de las tecnologías, provocando que en el ciclo de desarrollo del producto, se descontinué el soporte a las versiones previas; los sistemas del MTSS se habrán obsoletos y puedan aparecer defectos del producto con limitaciones para modificar o actualizar; o que no se actualice la documentación con los cambios realizados a los componentes de la infraestructura.

El Nivel de riesgos determinado para la **Dirección Nacional de Inspección de Trabajo**, es de un 39%, obedece básicamente a probabilidades de riesgo en la información incompleta o excesiva y de baja calidad que puede causar decisiones equivocadas, provocados por una posibilidad que el sistema de casos de la Inspección de Trabajo, refleje datos o visitas inspectivas sin actualizar su estado de trámite, casos sin cerrar o creados dobles generando información incorrecta.

4.2. Niveles de riesgo bajo.

El **Departamento de Salarios**, enfoca su análisis a los posibles evento en torno al servicio de consultas salariales que ingresan mediante la página web versus su oportunidad de respuesta; no obstante, el impacto por ocurrencia a esos eventos no representa perjuicio social o perdida financiera importante en la producción Institucional, generando un nivel de riesgo del 27% clasificado como riesgo bajo.

El **Consejo de Salud Ocupacional**, realiza su análisis de riesgos entorno a la información contenida en el sitio web, asignación de perfiles de acceso y administración del proyecto; sin embargo, las probabilidades de ocurrencia han sido valoradas como poco común o improbables, acompañado de algunos controles que les permite mantener la información actualizada. Obteniendo un riesgo bajo del 25%.

El nivel de riesgos determinado en la **Contraloría de Servicios**, con 23% en condición baja, prescribe eventos de riesgo con poco impacto, tomando en cuenta que no utiliza sistemas de información específicos en sus procesos y mantienen políticas de respaldo alternas en la ejecución de sus funciones.

La participación del **Tribunal Administrativo** de la Seguridad Social del Régimen de Pensiones del Magisterio Nacional, el proceso de valoración de riesgos lo cumple entorno a la base de datos de pensiones, registro de votos y sistema de control y seguimiento de casos, procurando siempre mantener funcionarios capacitados en su uso y realizan respaldos externos cada 3 meses, calificando de poco común las probabilidades que los riesgos se materialicen dando un nivel de riesgo del 20% bajo.

Por último, en la clasificación de riesgos bajos encontramos la Oficina de **Prensa**, con un nivel de 10% posición baja, a pesar de que no utiliza sistemas o bases de datos en su función, se mantiene capacitada en ambiente Windows y realiza respaldos adicionales a las políticas institucionales.

En general, el mayor aporte para lograr un nivel de riesgo bajo lo define el impacto que pueden causar los eventos en el cumplimiento de objetivos, así como las políticas de respaldo y capacitación que procuran las unidades administrativas por iniciativa propia.

Por lo tanto, no todas las dependencias requieren establecer un plan de tratamientos de riesgos que minimicen su impacto, más bien necesitan comprobaciones periódicas para asegurar que se mantienen la eficiencia de las medidas de control y un balance adecuado entre probabilidad baja e impacto moderado de la ocurrencia de los riesgos, tal como se analiza en la fase siguiente del Sistema Específico de Valoración de Riesgos.

5. Administración de Riesgos

Una vez concluidas las fases anteriores del proceso de valoración de riesgos institucionales, con base en el análisis de probabilidad e impacto frente a los controles existentes, se determinan los riesgos que requieren un plan de actividades para su tratamiento, de manera que permita aumentar el cumplimiento de objetivos y reducir los riesgos prioritarios.

No obstante, que el riesgo institucional se ubicó en un rango promedio del 36%, considerado moderado, y no todas la dependencias requirieron establecer un plan de administración de riesgo, sin embargo, algunas, por sus resultados demandan comprobaciones periódicas para asegurar que se mantiene la eficiencia de los controles sobre los procesos y objetivos analizados.

Cuando se realiza el análisis individual, algunos riesgos clasificados moderados y altos, requieren medidas de administración, y en general se utilizará como medida atenuante la opción denominada “Modificar el riesgo”, que consiste en atacar los factores de riesgo asociados a la probabilidad y a las consecuencias de un evento antes de que ocurra.

El siguiente cuadro contiene algunas acciones de mejoras que se ha propuesto a las Direcciones que, por sus resultados en los niveles de riesgo, tienen el compromiso de minimizar:

Cuadro 4. Costa Rica, MTSS: Medidas de Administración de Riesgos de la Inspección Nacional de Inspección de Trabajo2013

Medida de Administración	Actividad para gestionar Riesgo	Instancia Responsable
Modificar Riesgo	Acciones para garantizar que el sistema de casos de la Inspección genere información actualizada.	Dirección Nacional de Inspección de Trabajo
	Mejorar el compromiso sobre las políticas de seguridad establecidas para el manejo del sistema.	
	Coordinar capacitación con el administrador del sistema sobre el desarrollo de nuevos módulos.	
	Llevar el sistema de reportes de Incidentes a Oficinas Regionales.	

Fuente: MTSS, Departamento de Control Interno, datos suministrados por Regionales de la DNI, 2013

Cuadro 5. Costa Rica, MTSS: Medidas de Administración de Riesgos DESAF, 2013

Medida de Administración	Actividad para gestionar Riesgo	Instancia Responsable
Evitar el Riesgo	Hacer revisiones aleatorias al sistema. Poner una restricción al sistema de correspondencia para que se tengan que adjuntar el archivo que contiene el documento.	DESAF Gestión
	Agregar al sistema un registro de actualizaciones de documentos.	
	Establecer un procedimiento para la asignación de permisos y accesos, con control cruzado de asignación y revisión	
	Suscribir un contrato de ejecución continua para el servicio de mantenimiento preventivo y correctivo de equipo de cómputo.	
	Hacer un proceso de contratación para la adquisición de los gabinetes.	
	Hacer un proceso de contratación para contar con cableado de red de datos que cumpla con los requerimientos establecidos a nivel internacional. Aislar los router que se encuentran en los pisos.	
	Se implementara una medida para hacer pruebas aleatorias permanentes a la supervisión de la Bitácora del sistema de patronos morosos.	Gestión de Cobro
	Ejecución de un nuevo Sistema de Información con Manuales de Usuarios.	
	Gestionar una licencia más que nos permita el acceso de todos los funcionarios a expedientes digitales de patronos morosos.	Legal
	Incorporar en el sistema de correspondencia, los archivos de toda la información generada por el Departamento de Asesoría Legal.	
	Mejorar el sistema de comunicación de las modificaciones presupuestarias para los analistas.	Presupuesto
	Contar con políticas adecuadas de respaldo de información y reportes de incidentes.	

Fuente: MTSS, Departamento de Control Interno, datos suministrados por la DESAF, proceso SEVRI, 2013

Cuadro 6. Costa Rica, MTSS: Medidas de Administración de Riesgos, Departamento de Tecnologías de Información, 2013

Medida de Administración	Actividad para gestionar Riesgo
Retener	Adquisición de software especializado que nos permita monitorear la actividad no conocida.
Transferir	Aprobación por parte de los jerarcas de las políticas de seguridad informática.
Retener	Adquisición de software de respaldos y monitoreo, así como la aplicación de las mejores prácticas para el manejo de los mismos.
Modificar	Generar propuesta para utilización de la documentación actual y establecer un plan de seguimiento de mejora.
Modificar	Reforzar el tipo de acceso al centro de computo mediante uso de controles biométricos
Modificar	Propuesta para readecuar el diseño de las instalaciones físicas del DTIC
Retener	Brindar el mantenimiento y monitoreo respectivo a la plataforma tecnológica.
Transferir	Solicitar al Departamento de Servicios generales la revisión y análisis del estado de la red eléctrica así como los ductos de cableado estructurado.
Retener	Mantener activos los contratos de firewall, antivirus y políticas de acceso
Transferir	Solicitar la aprobación del presupuesto a los jerarcas con el fin de llevar a cabo una actualización de la plataforma tecnológica
Retener	Establecer una revisión periódica de la documentación sobre la configuración de infraestructura
Transferir	Cada una de las dependencias debe coordinar con el DTIC la adquisición de cualquier solución o desarrollo informático que requieran.
Transferir	Coordinar con la proveeduría institucional la confección de los carteles de manera que se incluya de manera habitual la solicitud de lo códigos fuentes como un requisito.
Transferir	La dependencia que solicite el desarrollo debe brindar toda la documentación y requerimientos de manera clara para que no exista un mal desarrollo por falta o claridad en los requerimientos
Retener	Crear y mantener manuales de procedimientos de los diferentes procesos que se realizan en le DTIC
Retener	Establecer estándares y procedimientos para la unidad de proyectos con el fin que los marcos de referencia sean los adecuados
Transferir	Coordinar con la proveeduría institucional el cumplimiento de adecuado de las contrataciones.
Retener	Llevar un control y dar seguimiento de las acciones de los proveedores con respecto al motivo de su contratación.

Fuente: MTSS, Departamento de Control Interno, datos suministrados por Tecnologías de Información, proceso SEVRI, 2013

Cuadro 7. Costa Rica, MTSS: Medidas de Administración de Riesgos, Dirección de Asuntos Jurídicos, 2013

Medida de Administración	Actividad para gestionar Riesgo	Instancia Responsable
Modificar Riesgo	Gestionar la compra de licencias de todos los agentes (Abogados y funcionarios enlace de otras Direcciones) para el uso del Zendesk pues sólo hay un agente autorizado para uso común.	Dirección de Asuntos Jurídicos
	Gestionar una ampliación de la contratación del sistema y/o que se exija la entrega del manual de uso que no existe.	

Fuente: MTSS Departamento de Control Interno, datos suministrados por la Dirección de Asuntos Jurídicos, proceso SEVRI, 2013

Cuadro 8. Costa Rica, MTSS: Medidas de Administración de Riesgos Dirección de Seguridad Social, 2013

Medida de Administración	Actividad para gestionar Riesgo	Instancia Responsable
Transferir el Riesgo	Solicitar mediante oficio al Departamento de Gestión Humana capacitación en Excel para el uso del registro administrativo dirigido a colaboradores de la DNSS.	Dirección de Seguridad Social
Transferir Riesgo	Realizar un diagnóstico sobre el estado actual del equipo tecnológico de la DNSS, con respecto a lo que se requiere de conformidad con el quehacer de la misma.	

Fuente: MTSS, Departamento de Control Interno, datos suministrados por la Dirección de Seguridad Social proceso SEVRI, 2013

Es importante destacar que todas las Direcciones y Departamentos han definido acciones de mejora, tomando en cuenta una viabilidad y razonabilidad presupuestaria que les permita su aplicación según los riesgos prioritarios identificados, integrando de esta manera el proceso de planificación y valoración de riesgos en una actividad Institucional que refleja un mejor modelo de Planificación Operativa Institucional.

Cabe señalar que los compromisos adquiridos por las diferentes dependencias para la administración del riesgo, se encuentran a disposición en cada uno de los registros que integran el proceso en el Departamento de Control Interno.

Conclusiones

El análisis del Proceso de valoración de Riesgos 2013, ha permitido generar información institucional gracias a la participación de todas las direcciones y dependencias que integran este Ministerio, ubicándolo en un nivel de riesgo cualitativo moderado del 36%, lo que representa un punto medio de impacto y probabilidad frente a los controles existentes, clasificándose en niveles de riesgos aceptables según los parámetros definidos.

Queda excluido de los datos anteriores, el Programa Nacional de Micro y Pequeña Empresa, PRONAMYPE, que tal como se indica en Oficio DE-PRO-115-2013 de fecha 08 de agosto 2013, no ha logrado identificar riesgos ya que en lo que corresponde a Tecnologías de Información, todos sus procesos sustantivos están vinculados directamente con los sistemas del Banco Popular, quien opera como FIDUCIARIO, por tal motivo todas las variables evaluadas están sujetas al desarrollo, gestión y seguridad de dicha Entidad.

El 68% de los riesgos institucionales son clasificados como moderados, que requieren de comprobaciones periódicas para asegurar que se mantienen la eficiencia de las medidas de control orientadas a minimizar el impacto.

El 32% de los riesgos son bajos se hace necesario proporcionarles seguimiento constante con el fin de que no representen una eventual amenaza para la institución.

Destaca para la evaluación de riesgos 2013, que no se presentan riesgos alto, que reflejen un impacto y probabilidad alta frente a los controles existentes los cuales no son aceptables por la institución, requieren un tratamiento del riesgo que minimice su impacto y, por ende, mejore su rendimiento.

El Riesgo de información precisa y completa, referido a los eventos que se puedan presentar afectando información incompleta o excesiva y de baja calidad, que puedan causar decisiones equivocadas, es el riesgo que con mayor frecuencia se ha identificado, presente en un 27% de las dependencias que señalan posibles eventos en la calidad de la información.

El valor promedio obtenido para los riesgos referidos a este componente es de un 26%; clasificado como riesgo bajo y como evento principal, destaca la ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones en algunos sistemas que soportan las labores sustantivas del quehacer institucional.

Todas la Direcciones del MTSS, han obtenido valores en el nivel de riesgo moderado, sin embargo, conforme a las particularidades de cada uno de ellas en su ámbito de acción, se obtienen conclusiones diversas.

La **Dirección de Asuntos Jurídicos**, con un nivel de riesgo 55% con una clasificación de riesgo moderado, obedece a las vulnerabilidades que presenta el sistema de consultas jurídicas que realizan los usuarios vía web (Zendesk)

La Dirección de Seguridad Social, con un nivel de riesgo de 48%, riesgo moderado, determinan su resultado en la probabilidad de riesgos en la infraestructura y arquitectura efectiva para soportar las necesidades presentes y futuras

La Dirección de Asuntos Laborales, con un 44% clasificado como riesgo moderado, está definido sobre las probabilidades de eventos que puedan afectar los datos estadísticos de los diferentes servicios que se brindan y registran en el sistema.

La Dirección Nacional de Empleo, con un resultado en el nivel de riesgo del 40%, referido por los eventos que podrían presentarse en el sistema de migraciones laborales (SIMLA), posibles eventos en el SIOIE, sistema nacional de intermediación, Orientación e Información de Empleo, en cuanto a la integridad y confiabilidad de la información que se genera y en cuanto al programa nacional de empleo (PRONAE), que se dé un uso inadecuado al instrumento.

La **Dirección de Asignaciones Familiares (DESAF**), con un resultado moderado en su nivel de riesgo del 32%, entre otros, describe posibles eventos de riesgo en el control de la bitácora del sistema de patronos morosos.

Dirección administrativa y Financiera, con un nivel de riesgo de **40%** enfoca la identificación de riesgos en la gestión de la seguridad de la información; destacar la probabilidad en el riesgo de la infraestructura y arquitectura de las tecnologías, provocando que en el ciclo de desarrollo del producto, se descontinué el soporte a las versiones previas.

Dirección Nacional de Inspección de Trabajo, es de un 39%, obedece básicamente a probabilidades de riesgo en la información incompleta o excesiva y de baja calidad que puede causar decisiones equivocadas, provocados por una posibilidad que el sistema de casos de la Inspección de Trabajo.

La dependencias con niveles de riesgos bajo, que oscilan entre el 27% y 10% (Consejos de Salud Ocupacional, Salarios, Prensa, Contraloría de Servicios y Tribuna Administrativo) logran su resultado cuando definen de bajo el impacto que pueden causar los eventos en el cumplimiento de objetivos, así como las políticas de respaldo y capacitación que procuran las unidades administrativas por iniciativa propia.

Por consiguiente, el proceso de valoración de riesgos sigue respaldando la ejecución y funcionamiento en los objetivos plasmados por la institución a través de su análisis, evaluación y administración, garan tizando razonablemente su cumplimiento.