ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

UNIDAD DE GESTIÓN DE POSTGRADOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

III PROMOCIÓN

TEMA: "ANALISIS Y DISEÑO DE CONTROLES DE SEGURIDAD DE LA ADMINISTRACIÓN DE USUARIOS DEL SISTEMA ESIGEF, BASADO EN LA NORMA ISO 27002"

AUTOR: ING. FÉLIX TOMÁS PERUGACHI ALVEAR

DIRECTOR: ING. URVINA, DARIO

CODIRECTOR: ING. SOLIS, FERNANDO

SANGOLQUÍ, 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE: MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "ANÁLISIS Y DISEÑO DE CONTROLES DE SEGURIDAD DE LA ADMINISTRACIÓN DE USUARIOS DEL SISTEMA ESIGEF, BASADO EN LA NORMA ISO 27002" realizado por el señor Ing. Félix Tomás Perugachi Alvear, 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 establecido por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor Ing. Félix Tomás Perugachi Alvear para que lo sustente públicamente.

Sangolquí, 2 de diciembre del 2015

Ing. Darío Genaro Urvina López, MSc

DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

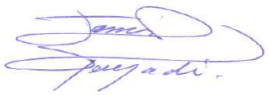
CARRERA DE: MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORÍA DE RESPONSABILIDAD

Yo, Ing. Félix Tomás Perugachi Alvear, con cédula de identidad N° 1719007385 declaro que este trabajo de titulación, "ANÁLISIS Y DISEÑO DE CONTROLES DE SEGURIDAD DE LA ADMINISTRACIÓN DE USUARIOS DEL SISTEMA ESIGEF, BASADO EN LA NORMA ISO 27002" 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, 2 de diciembre del 2015



Ing. Félix Tomás Perugachi Alvear

CC: 1719007385

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

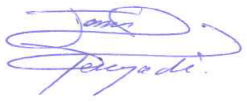
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE: MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN

Yo, Ing. Félix Tomás Perugchi Alvear, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "ANÁLISIS Y DISEÑO DE CONTROLES DE SEGURIDAD DE LA ADMINISTRACIÓN DE USUARIOS DEL SISTEMA ESIGEF, BASADO EN LA NORMA ISO 27002" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 2 de diciembre del 2015



Ing. Félix Tomás Perugachi Alvear

CC: 1719007385

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la oportunidad de estar vivo y permitirme llegar hasta este momento tan importante de mi formación profesional. A mis padres, por ser pilar fundamental y demostrarme siempre su apoyo en cada momento de mi vida. A todos mis hermanos, hermanas en especial a mi Tío Segundo Alvear, quien supo inculcar valores especiales en nuestra familia, a todos por siempre estar dispuestos a apoyarme en todo lo que he emprendido.

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos. Por esto agradezco a mi director de tesis, Ing. Dario Urvina, oponente Ing. Edgar Solis, Ing. Mario Ron y al coordinador Ing. Rubén Arroyo. A mis profesores a quienes les debo gran parte de mis conocimientos, gracias a su paciencia y enseñanza y finalmente un atento agradecimiento a esta prestigiosa institución educativa la cual abrió y abre sus puertas a personas como nosotros, preparándonos para un futuro cada vez más competitivo y formándonos como personas de bien con altos valores.

ÍNDICE

CAPÍTULO I 1
INTRODUCCIÓN 1
1.1 Introducción 1
1.2 Justificación e Importancia 2
1.3 Planteamiento del Problema 3
1.4 Formulación del problema a resolver 3
1.5 Objetivo General 3
1.6 Objetivos Específicos 3
CAPÍTULO II 5
MARCO TEÓRICO 5
2.1 Antecedentes del estado del arte 5
2.2 Normativa Legal 5
2.2.1 Delitos Informáticos 5
2.2.2 Normas de Control Interno - Contraloría General del Estado 5
2.2.3 Resumen de la Normativa Legal 6
2.3 Prevención del Fraude y Control Interno 7
2.3.1 Teoría del Fraude 7
2.3.2 Triangulo del Fraude: Oportunidad, Racionalización y Motivo 7
2.3.3 ¿Qué es Fraude? 9
2.3.4 Controles informáticos: Preventivos, Detectivos y Correctivos 12
2.4 Seguridad de la Información y Auditoría de Sistemas de Información 13
2.4.1 Seguridad de la Información 13
2.4.2 Integridad, Confidencialidad y Disponibilidad 13
2.4.3 Seguridades lógicas 14
2.4.4 Modelos de Control de Acceso 14
2.4.5 Auditoría de Sistemas de Información o Informática 17

2.5 Norma Internacional de Seguridad de la información ISO 27002 18
2.5.1 Norma Ecuatoriana NTE INEN-ISO/IEC 27002:2009 18
2.5.2 Resumen del Dominio Control de Acceso 18
2.6 Norma NTE INEN ISO/IEC 27005:2012 20
2.6.1 Análisis del riesgo 20
2.6.2 Evaluación del riesgo 24
2.6.3 Tratamiento del riesgo 24
2.6.4 Aceptación del riesgo de la seguridad de la información 27
2.6.5 Riesgo de Tecnologías de Información (TI) 27
2.7 Descripción del Sistema Nacional de las Finanzas Públicas 28
2.7.1 Código Orgánico de Planificación y Finanzas Públicas 29
2.7.2 Entidades que conforman el Presupuesto General del Estado 30
2.7.3 Acuerdo Ministerial N° 163 31
CAPÍTULO III 32
ANÁLISIS Y DISEÑO DE LOS CONTROLES DE SEGURIDAD 32
3.1 Análisis de los controles de seguridad 32
3.1.1 Administración de usuarios actual 32
3.1.2 Administración de contraseñas 33
3.2 Resumen de los casos de desvíos de fondos 34
3.3 Evaluación en la administración de usuarios realizada a una muestra 35
3.3.1 Base legal para la generación y realización de la evaluación 36
3.3.2 Selección de la muestra 36
3.3.3 Procesos de administración de usuarios a revisar 36
3.3.4 Recopilación, interpretación y análisis de resultados 40
3.4 Evaluación de riegos de los resultados basados en la norma ISO 27005 40
3.4.1 Identificación de las amenazas 41

3.4.2 Identificación de las vulnerabilidades 41
3.4.3 Probabilidad de ocurrencia 41
3.4.4 Matriz de Riesgo 41
3.5 Tabulación de resultados del nivel de madurez de los procesos revisados . 42
3.6 Diseño de controles de seguridad en base a la norma ISO 27002 43
3.6.1 Responsabilidades en la Administración de Usuarios 44
3.6.2 Controles para el proceso de registro de usuarios 46
3.6.3 Controles para el proceso de gestión de privilegios 53
3.6.4 Controles para el proceso de revisión de acceso de usuarios 55
3.6.5 Controles para el proceso de Gestión de contraseñas para usuarios 63
3.6.6 Controles para el proceso de Monitoreo del uso del sistema 65
3.6.7 Otros controles adicionales 66
3.7 Cuadro general de controles de seguridad para las instituciones 67
3.8 Nivel de madurez a implementar en las instituciones 68
CAPÍTULO IV 69
CONCLUSIONES Y RECOMENDACIONES 69
4.1 Conclusiones 69
4.2 Recomendaciones 70
BIBLIOGRAFÍA 73

ÍNDICE DE TABLAS

Tabla 1: Ejemplo de riesgo de TI 28
Tabla 2: Procesos de administración y monitoreo de usuarios a evaluar 36
Tabla 3: Procedimiento de registro de usuarios 47
Tabla 4: Procedimiento modificación de permisos 49
Tabla 5: Procedimiento para bajas de usuarios 49
Tabla 6: Relación entre elementos RBAC y sistema eSigef 54
Tabla 7: Registro reporte Talento Humano 57
Tabla 8: Registro de usuario sistema eSigef 60
Tabla 9: Registro de bajas realizadas 62
Tabla 10: Resumen controles de seguridad 67

ÍNDICE DE FIGURAS

Figura 1: Esquema de administración de usuarios 1
Figura 2: Triángulo del Fraude 8
Figura 3: Modelo de Control de Acceso Basado en Roles 17
Figura 4: Actividad para el tratamiento del riesgo 25
Figura 5: Sector Público y Presupuesto General del Estado 30
Figura 6: Ejemplo de Entidades Operativas del Ministerio de Salud 31
Figura 7: Pantalla principal de los aplicativos SINFIP 33
Figura 8: Pantalla de creación de usuarios sistema eSigef 34
Figura 9: Niveles de madurez según CMM (Cobit Madurity Model) 43
Figura 10: Formulario solicitud creación de usuarios 51
Figura 11: Comunicado de entrega de usuario y contraseña 52
Figura 12: Compromiso de confidencialidad de la información 52
Figura 13: Modelo para definición de roles 55
Figura 14: Formulario registro de usuarios temporales 56
Figura 15: Pantalla de inicio de sesión eSigef 57
Figura 16: Reporte usuarios 58
Figura 17: Búsqueda filtrado de usuarios 58
Figura 18: Búsqueda por valor o parámetro 59
Figura 19: Búsqueda por filtro activado 59
Figura 20: Resultado de la búsqueda 59
Figura 21: Exportar reporte en varios formatos 60
Figura 22: Listado de usuarios del sistema 61
Figura 23: Búsqueda por filtro o parámetro de usuarios 61
Figura 24: Desactivación de usuarios 62

RESUMEN

El presente trabajo de investigación, debido a los casos de desvíos de fondos en las entidades del sector público, tiene como objetivo realizar un análisis de estos casos, determinar sus causas y diseñar controles de seguridad adecuados según las normas de seguridad para que las entidades usuarias del sistema eSigef, que conforman el Presupuesto General del Estado, puedan adoptarlas, con el fin de poder reducir el riesgo de desvíos de fondos. Se evaluó los procesos de administración de usuarios en el uso del sistema eSigef, realizada a una muestra de instituciones, tomando como referencia la norma ISO 27002 enfocado a los Objetivos de Control: Gestión de Acceso de Usuarios: Registro de usuarios, Gestión de privilegios, Gestión de contraseñas para usuarios, Revisión de los derechos de acceso de los usuarios; y Monitoreo del uso del sistema. La metodología a seguir consistió en un estudio de los casos de desvíos de fondos desde el enfoque de la Teoría del Fraude. Posteriormente se realiza una evaluación de riesgos tomando como referencia la norma ISO 27005 y basados en estos resultados se diseñan los controles apropiados. El sistema eSigef debido al ser una herramienta necesaria para la gestión administrativa financiera gubernamental de las entidades e instituciones que conforman el Presupuesto General del Estado, constituye un sistema crítico, motivo por el cual la utilización y operación del mismo debe ser protegido ante posibles amenazas y riesgos.

ABSTRACT

The present investigation due to cases of embezzlement in the public sector entities, aims to make an analysis of these cases, determine their causes and design appropriate security controls as safety standards for user entities the eSIGEF system, comprising the General Budget of the State may adopt, in order to reduce the risk of diversion of funds. User Access Management: management processes users use the system eSIGEF conducted on a sample of institutions, with reference to the ISO 27002 focuses on Control Objectives was assessed User registration, management privileges, managing passwords for users, Review of the access rights of users; Monitoring and system usage. The methodology followed was a study of cases of embezzlement from the perspective of the theory of fraud. Subsequently, a risk

assessment is carried out by reference to the ISO 27005 standard and based on these results the appropriate controls are designed. The eSIGEF system due to be a necessary tool for government financial administration of the entities and institutions of the General State Budget, is a critical system, which is why the use and operation thereof should be protected against possible.

Palabras clave

SEGURIDAD DE LA INFORMACIÓN

RIESGO

CONTROL

FRAUDE

AUDITORÍA

CAPÍTULO I
INTRODUCCIÓN

1.1 Introducción

Debido a los casos de desvíos de fondos en las entidades del sector público surge la necesidad de realizar un análisis de los mismos, determinar sus causas y diseñar los controles adecuados según las normas internacionales para que las entidades usuarias del sistema eSigef[1], que conforman el Presupuesto General del Estado (PGE[2]), puedan adoptarlas para reducir el riesgo de desvíos de fondos.

En la figura 1 se muestra la relación que existe entre las entidades usuarias (EOD[3], UDAF[4]) y el sistema eSigef, sobre la cual se realizará el análisis de la administración de usuarios y sus procesos.

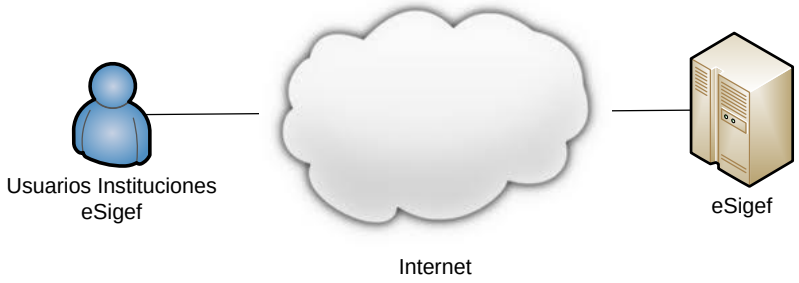


Figura 1: Esquema de administración de usuarios

Los controles de seguridad existentes en las entidades usuarias del eSigef pueden ser vulnerados por funcionarios mal intencionados que busquen su beneficio propio, por lo cual se requiere tener una gestión y control en las operaciones en dichas entidades.

El objetivo del presente trabajo es diseñar controles de seguridad basado en la norma internacional ISO 27002 y mejores prácticas de seguridad, sobre las cuales las

[1] Sistema de Gestión Financiera
[2] Presupuesto General del Estado
[3] Entidad Operativa Desconcentrada
[4] Unidades Administrativas Financieras

entidades puedan en un futuro utilizarlas para disminuir el riesgo de desvíos de fondos.

La metodología a seguir consiste en un estudio de los casos de desvíos de fondos desde el enfoque de la Teoría del Fraude. Se analizarán, en base a encuestas a una pequeña muestra, los niveles de seguridad que poseen las entidades. Posteriormente se realizará una evaluación de riesgos tomando como referencia la norma ISO 27005.

De la evaluación del riesgo, se seleccionarán los controles basado en la norma ISO 27002 y en base a esto se diseñaran los controles estándares que puedan ser aplicados en las entidades o instituciones.

1.2 Justificación e Importancia

El Código Orgánico de Planificación y Finanzas Públicas manifiesta que todas las entidades del PGE deben utilizar el sistema eSigef como el medio para su gestión financiera y como consecuencia para el funcionamiento de cada una de sus actividades.

El sistema eSigef tiene las siguientes funciones: generar, procesar y proveer información oportuna y relevante para soportar la toma de decisiones de las autoridades de las entidades del sector público; a través del sistema eSigef se maneja el PGE que para el año 2013 fue aprobado por la Asamblea Nacional con un monto de 32.366,82 millones de dólares.

Es necesario minimizar el riesgo de desvío de fondos en las instituciones del PGE por una inadecuada utilización del sistema eSigef, mejorando el control interno, de este modo las instituciones puedan mantener un control adecuado en sus recursos financieros.

El desarrollo del país depende en gran medida de las inversiones que se realizan en el campo de la educación, salud, sectores estratégicos, ciencia y tecnología que permitirá brindar un futuro promisorio al pueblo ecuatoriano, de ahí la importancia de proteger los recursos financieros que servirán para conseguir los objetivos comunes de la sociedad.

1.3 Planteamiento del Problema

Entre los principales problemas que pueden presentarse en la administración de usuarios en las entidades usuarias del sistema eSigef son:

- La falta de controles y el aprovechamiento de las debilidades de los controles de seguridad existentes.
- La falta de revisión y monitoreo por parte de la dirección en las entidades.
- La falta de concientización por parte de los usuarios respecto a normas de seguridad.

1.4 Formulación del problema a resolver

¿Cuáles son los motivos o causas de desvíos de fondos en las entidades usuarias del sistema eSigef según la teoría del fraude?

¿Cuáles son los riesgos de seguridad presentes en las operaciones y procesos que realizan las entidades usuarias en el sistema eSigef, basado en la normativa ISO 27005?

¿Cuál es el nivel de seguridad en las entidades usuarias, respecto al uso del sistema eSigef?

1.5 Objetivo General

Analizar y diseñar los controles de seguridad en los procesos de administración de usuarios del sistema eSigef basado en la norma ISO 27002, para que las instituciones usuarias del sistema puedan utilizarlas como prevención y mitigación de riesgos de fraudes y desvíos de fondos.

1.6 Objetivos Específicos

1. Analizar la información actual de los procesos de administración de usuarios.
2. Estudiar y analizar los casos de desvíos de fondos enfocado en la Teoría del Fraude.
3. Elaborar una evaluación del riesgo sobre las debilidades identificadas, en base a la norma ISO 27005.

4. Seleccionar y proponer los controles de seguridad según la norma ISO 27002 para las instituciones usuarias.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes del estado del arte

2.2 Normativa Legal

2.2.1 Delitos Informáticos

Los delitos informáticos son cualquier comportamiento criminal en que la computadora está involucrada como medio para el cometimiento del delito o como objetivo del mismo. (Leon, 2012, pág. 23)

Según (Leon, 2012, pág. 24), son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando. Son acciones de oportunidad que se aprovechan una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

Dentro del marco de delitos informáticos, se puede clasificar el fraude o desvíos de fondos como el uso de los sistemas categorizado como "instrumento o medio", y esta se evidencia con la variación en cuanto al destino de pequeñas cantidades de dinero hacia cuentas bancarias no autorizadas para pagos.

2.2.2 Normas de Control Interno - Contraloría General del Estado

La Contraloría General del Estado expidió las Normas de Control Interno para las entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos, las mismas que en la sección 100-02 "Objetivos de Control Interno", menciona lo siguiente: (Contraloría General del Estado, 2009).

El control interno de las entidades, organismo del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos para alcanzar la misión institucional, deberá contribuir al cumplimiento de los siguientes objetivos:

- Promover la eficiencia, eficacia y economía de las operaciones bajo principios éticos y de transparencia.
- Garantizar la confiabilidad, integridad y oportunidad de la información.
- Cumplir con las disposiciones legales y la normativa de la entidad para otorgar bienes y servicios públicos de calidad.
- Proteger y conservar el patrimonio público contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

Dicha norma establece un marco de trabajo integral para todas las entidades del sector público sin excepción, en la que se detallan temas de organización, auditoría, gestión de riesgos, actividades de control, entre otras, que las entidades deben realizarlas en sus diferentes áreas y departamentos, por ejemplo en las área de: Contabilidad, Tesorería, Administración Financiera, Tecnologías de Información, Talento Humano, entre otras.

En la norma 400 “Actividades de Control” indica que:

La máxima autoridad de la entidad y las servidoras y servidores responsables del control interno de acuerdo a sus competencias, establecerán políticas y procedimientos para manejar los riesgos en la consecución de los objetivos institucionales, proteger y conservar los activos y establecer políticas y procedimientos para manejar los riesgos en la consecución de los objetivos institucionales, proteger y conservar los activos y establecer los controles de acceso a los sistemas de información. (Contraloría General del Estado, 2009).

2.2.3 Resumen de la Normativa Legal

Existen normas, directrices, disposiciones, acuerdos sobre: gestión de riesgos, control interno y seguridad de la información, sin embargo muchas entidades del sector público no la ejecutan, esto puede ser por falta de conocimiento, de recursos, de concientización o falta de apoyo de las máximas autoridades.

Cabe indicar que el desconocimiento de la ley no exime de las responsabilidades que tuvieren lugar en el caso de problemas relacionados con desvíos de fondos,

fraudes u otro acto doloso; ya sea con el uso de tecnología, o actos de relación administrativa, de recursos humanos, de políticas, normas de control interno, etc.

De ahí la importancia de identificar las causas que materializaron los riesgos y provocaron desvíos de fondos desde un enfoque de la teoría de fraude, en base a estos resultados se podrá determinar y proponer las mejoras en base a controles de seguridad según la norma ISO 27002, y que en lo posterior pueda ser utilizado a fin de mejorar el control interno.

2.3 Prevención del Fraude y Control Interno

2.3.1 Teoría del Fraude

De acuerdo al Reporte a las Naciones sobre el Fraude Ocupacional y el Abuso del año 2010, la principal debilidad de control que contribuye al fraude es la falta de controles internos, el segundo motivo corresponde a burlar los controles internos existentes, y en tercer lugar son la falta de revisión de la dirección, por mencionar los más importantes. (Badillo, 7 Teorías Clave para Conocer, Comprender y Combatir el Fraude, 2012).

En el reporte indicado anteriormente también se menciona que pequeñas empresas con menos de 100 empleados poseen menos controles internos en comparación con las grandes empresas.

Las actividades de la seguridad informática y auditoría no deben estar aisladas o desentendidas, más bien deben trabajar en conjunto para detectar y prevenir los fraudes financieros que actualmente se han dado en las entidades de gobierno. (Badillo, 7 Teorías Clave para Conocer, Comprender y Combatir el Fraude, 2012).

2.3.2 Triangulo del Fraude: Oportunidad, Racionalización y Motivo

En la figura 2 se describe en qué consiste el triángulo de fraude y sus principales componentes:

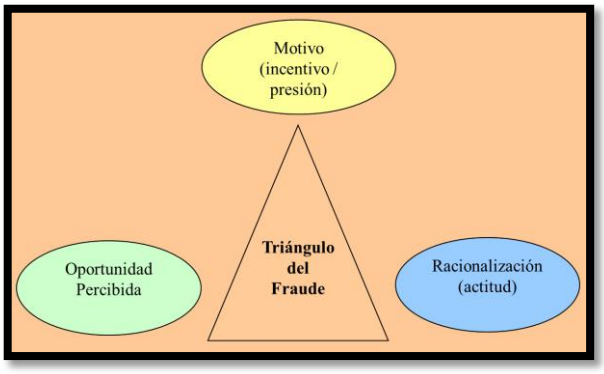


Figura 2: Triángulo del Fraude

Fuente: (DNA, 1999)

El fraude frecuentemente involucra de manera simultánea los tres elementos siguientes:

Motivo.- Presión o incentivo (necesidad, justificación, desafío) para cometer el fraude (la causa o razón). Ejemplos de motivos para cometer fraude pueden ser: alcanzar metas de desempeño (como volúmenes de venta), obtener bonos en función de resultados (incremento en las utilidades o rebaja en los costos), mantener el puesto demostrando ficticios buenos resultados, deudas personales. (Badillo, 7 Teorías Clave para Conocer, Comprender y Combatir el Fraude, 2012).

Oportunidad Percibida.- El o los perpetradores del fraude perciben que existe un entorno favorable para cometer los actos irregulares pretendidos. La oportunidad para cometer fraude se presenta cuando alguien tiene el acceso, conocimiento y tiempo para realizar sus irregulares acciones. Las debilidades del control interno o la posibilidad de ponerse de acuerdo con otros directivos o empleados para cometer fraude (colusión) son ejemplos de oportunidades para comportamientos irregulares. (Badillo, 7 Teorías Clave para Conocer, Comprender y Combatir el Fraude, 2012).

Racionalización.- Es la actitud equivocada de quien comete o planea cometer un fraude tratando de convencerse a sí mismo (y a los demás si es descubierto), consciente o inconscientemente, de que existen razones válidas que justifican su comportamiento impropio; es decir, tratar de justificar el fraude cometido. Ejemplos de racionalización para justificar el fraude cometido pueden ser: alegar baja remuneración (convencerse de que no es fraude sino una compensación salarial, un

préstamo), falta de reconocimiento en la organización (convencerse de que es una bonificación), fraude cometido por otros empleados y/o directivos (convencerse de que si otros cometen fraudes el fraude propio está justificado). (Badillo, 7 Teorías Clave para Conocer, Comprender y Combatir el Fraude, 2012).

De los anteriores conceptos se puede deducir que si bien todos juegan un papel importante para determinar las causas del cometimiento de fraudes, la **oportunidad percibida** es la más aprovechada, y tiene que ver con las debilidades de los controles internos.

"Los controles internos por sí mismos son insuficientes para prevenir plenamente el fraude ocupacional. Aunque es importante que las organizaciones cuenten con controles anti fraude estratégicos y eficaces, dichos controles internos no impedirán que se cometa todo tipo de fraude, ni detectarán todos los fraudes una vez que han comenzado. (ACFE - "Association of Certified Fraud Examiners", 2010).

La información financiera fraudulenta se define, según el informe *Treadway*, como la "conducta intencionada o descuidada, ya sea por acción u omisión, que desemboca en la distorsión de los estados financieros" (AICPA, American Institute of Certified Public Accountants, 1987).

2.3.3 ¿Qué es Fraude?

Podemos afirmar que es un engaño hacia un tercero, abuso de confianza, dolo, simulación, etc. El término "fraude" se refiere al acto intencional de la Administración, personal o terceros, que da como resultado una representación equivocada de los estados financieros (seguinfo, 2007):

Por lo general el fraude ocurre cuando una persona engaña intencionalmente a otra sobre un asunto de seguro para recibir dinero u otro beneficio que no le corresponde. Puede implicar:

- Manipulación, falsificación o alteración de registros o documentos.
- Malversación de activos.
- Supresión u omisión de los efectos de ciertas transacciones en los registros o documentos.

- Registro de transacciones sin sustancia o respaldo.
- Mala aplicación de políticas contables.

Tipos de fraude

Se considera que hay dos tipos de fraudes: el primero de ellos se realiza con la intención financiera clara de malversación de activos de la empresa. El segundo tipo de fraude, es la presentación de información financiera fraudulenta como acto intencionado encaminado a alterar las cuentas anuales (seguinfo, 2007).

- Los fraudes denominados internos son aquellos organizados por una o varias personas dentro de una institución, con el fin de obtener un beneficio propio.
- Los fraudes conocidos como externos son aquellos que se efectúan por una o varias personas para obtener un beneficio, utilizando fuentes externas como son: bancos, clientes, proveedores, etc.

Por qué hay fraudes

Se considera que hay fraudes por:

- Falta de controles adecuados
- Poco y mal personal capacitado
- Baja / alta rotación de puestos
- Documentación confusa
- Salarios bajos
- Existencia de activos de fácil conversión: bonos, pagares, etc.
- Legislación deficiente
- Actividades incompatibles entre sí

Es un hecho demostrado que evitar fraudes es responsabilidad de todos los empleados. Por ello, es importante crear una cultura empresarial encaminada a minimizar el riesgo de fraude (seguinfo, 2007).

Como se evita un fraude

La respuesta más sencilla es la de mejorar el control administrativo, implementar prácticas y políticas de control, analizar los riesgos que motiven a un fraude, tener la mejor gente posible, bien remunerada y motivada (seguinfo, 2007).

Como se detecta un fraude

Existe una infinidad de respuestas a esta pregunta las más comunes son:

- Observar, probar o revisar los riesgos específicos de control, identificar los más importantes y vigilar constantemente su adecuada administración.
- Simular operaciones.
- Revisar constantemente las conciliaciones de saldos con bancos, clientes, etc.
- Llevar a cabo pruebas de cumplimiento de la eficacia de los controles.

Concientización Anti Fraude y entrenamiento de Seguridad de la Información

Los empleados pueden presentar diferentes actividades que ayudarán a identificar potenciales fraudes. Es responsabilidad del directorio de las organizaciones dar soporte a un programa de seguridad y entrenamiento diseñado para ayudar a los empleados a identificar posibles fraudes y reportarlos a la administración.

"El personal debe tener conciencia de las acciones que necesitan para tomar ayuda preventiva contra el fraude y qué hacer cuando se sospeche o identifique alguna actividad fraudulenta. Las siguientes actividades anti fraude deben ser incorporadas en las organizaciones en la concientización y el entrenamiento el cual puede ser aplicado en cualquier organización". (Krause, 2007, pág. 558).

- Regularmente comunicar, vía concientización mensajes y entrenamiento formal, procedimientos de seguridad de la organización para descubrir a maleantes, delincuentes y actividades fraudulentas. Esto podrá ayudar a asistir en la identificación y prosecución de las personas que cometen estos actos.

- Entrenar al personal en la administración apropiada, técnica y seguridad física para proteger la seguridad, confidencialidad, y la integridad de la información.
- Establecer procedimiento que sirva para identificar personal que ha cometido crímenes contra alguna organización.
- Comunicar regularmente al personal de la organización sobre la misión, visión, valores y que actividades fraudulentas son inaceptables y no son toleradas.
- Comunicar las políticas y procedimientos de seguridad de la información al personal. La prevención del fraude empieza con una buena seguridad.
- Implementar sanciones apropiadas para actividades fraudulentas. Estas acciones pueden incluir acciones disciplinarias, civiles y criminales.
- Proporcionar cursos regulares y capacitación de los empleados y el conocimiento para explicar al personal sobre las responsabilidades de gestión en el marco del programa de seguridad, antes, durante y después de una actividad fraudulenta. (Krause, 2007)

2.3.4 Controles informáticos: Preventivos, Detectivos y Correctivos

Control Interno

Son procesos, efectuados por entidades a nivel de dirección, administración y otro personal, designado para proveer aseguramiento razonable para conseguir los siguientes objetivos (Clark, 2009, pág. 25):

- Efectividad y eficiencia en las operaciones
- Confiabilidad en los reportes financieros
- Cumplimiento de regulaciones y leyes

Conceptos claves de control interno

- El control interno es un proceso, esto significa un medio no el fin como tal.
- Los controles internos son efectuados por personas, no solo es cuestión de políticas y cuestiones de tecnología, en todos los niveles de la organización.

- Del control interno se espera proveer un aseguramiento razonable, no un aseguramiento absoluto, a una dirección de una entidad.

Controles informáticos preventivos

Ejemplo: usuarios y clave, perfil de usuarios, roles, controles biométricos, gestión de las sesiones, control intento de números de intentos fallidos, contraseñas fuertes. (Badillo, Auditoria Basada en Riesgos, 2012).

Controles informáticos detectivos

Ejemplo: Monitoreo de logs de accesos, registros de auditoría y transacciones. (Badillo, Auditoria Basada en Riesgos, 2012).

Controles informáticos correctivos

Son las acciones que se implementan para corregir un error o irregularidad detectada en los sistemas de información. (Badillo, Auditoria Basada en Riesgos, 2012).

2.4 Seguridad de la Información y Auditoría de Sistemas de Información

2.4.1 Seguridad de la Información

La seguridad de la información es la preservación de la Confidencialidad, Integridad y Disponibilidad. (Badillo, Auditoria Basada en Riesgos, 2012).

2.4.2 Integridad, Confidencialidad y Disponibilidad

Integridad

Garantía de la exactitud y completitud de la información y de sus métodos de procesamiento.

Confidencialidad

Aseguramiento de que la información es accesible solo ara aquellos autorizados de tener acceso.

Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados

2.4.3 Seguridades lógicas

Es aquella seguridad de la información alcanzada mediante controles que actúan en el campo de lo intangible: usuario, clave, perfil de usuario, firewall, cifrado, software contra código malicioso, etc.

2.4.4 Modelos de Control de Acceso

Existen tradicionalmente dos tipos básicos de controles de acceso con filosofías diametralmente opuestas:

Modelo de Control de Acceso Discrecional (DAC)

En este modelo, un usuario bien identificado (típicamente, el creador o 'propietario' del recurso) decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema. Este es el modelo habitual en buena parte de los sistemas operativos más habituales. Lo esencial es que el propietario del recurso puede cederlo a un tercero (Rodríguez Berzosa, 2012).

Modelo de Control de Acceso Mandatorio (MAC)

En este modelo, es el sistema quién protege los recursos. Todo recurso del sistema, y todo principal (usuario o entidad del sistema que represente a un usuario) tienen una etiqueta de seguridad. Esta etiqueta de seguridad sigue el modelo de clasificación de la información militar, en donde la confidencialidad de la información es lo más relevante, formando lo que se conoce como política de seguridad multinivel.

Una etiqueta de seguridad se compone de una clasificación o nivel de seguridad (número en un rango, o un conjunto de clasificaciones discretas, desde DESCLASIFICADO hasta ALTO SECRETO) y una o más categorías o compartimentos de seguridad (CONTABILIDAD, VENTAS). En este tipo de

sistemas, todas las decisiones de seguridad las impone el sistema (Rodríguez Berzosa, 2012).

Los modelos DAC y MAC son inadecuados para cubrir las necesidades de la mayor parte de las organizaciones. El modelo DAC es demasiado débil para controlar el acceso a los recursos de información de forma efectiva, en tanto que el MAC es demasiado rígido. (Rodríguez Berzosa, 2012).

Modelo de control de accesos basado en roles (RBAC)

Desde los 80 se ha propuesto el modelo de control de accesos basado en roles (RBAC), como intento de unificar los modelos clásicos DAC y MAC, consiguiendo un sistema donde el sistema impone el control de accesos, pero sin las restricciones rígidas impuestas por las etiquetas de seguridad. (Rodríguez Berzosa, 2012).

Básicamente, un rol establece un nivel de indirección entre los usuarios y los derechos de acceso, a través de un par de relaciones: asignación de roles a usuarios, y asignación de permisos y privilegios a roles. (Rodríguez Berzosa, 2012).

Las políticas de control de accesos basado en roles regulan el acceso de los usuarios a la información en términos de sus actividades y funciones de trabajo, representándose así de forma natural la estructura de las organizaciones. (Rodríguez Berzosa, 2012).

Uno de los problemas más acuciantes en la gestión de grandes sistemas de información heterogéneos es la complejidad de la administración de seguridad. La aproximación RBAC, intuitivamente, modela de forma natural la estructura de autorización en las organizaciones del mundo real, facilitando las tareas administrativas al separar la asignación de individuos a funciones o perfiles de trabajo, y la definición de políticas de acceso (definición de roles en términos de lo que pueden hacer en el sistema). (Rodríguez Berzosa, 2012).

Permiten asimismo la construcción jerárquica de estas políticas de acceso, por herencia o especialización. Así, la política de control de accesos para un supervisor de planta puede ser una especialización de la del operador de planta. Por ello, la tecnología RBAC tiene el potencial de reducir la complejidad y el coste de la

administración de seguridad en estos entornos heterogéneos. (Rodríguez Berzosa, 2012).

Además, dada la alta integración entre los roles y las responsabilidades de los usuarios, pueden seguirse los principios del mínimo privilegio y de la separación de responsabilidades. Estos principios son vitales para alcanzar el objetivo de integridad, al requerir que a un usuario no se le otorguen mayores privilegios que los necesarios para efectuar su trabajo, y que para completar una transacción de cierta seguridad (por ejemplo, la autorización de un pago) se requiera la culminación de una cadena de transacciones simples por más de un usuario. (Rodríguez Berzosa, 2012).

El modelo RBAC es hoy día ubicuo: desde sistemas de base de datos relacionales, pasando por sistemas operativos de red, cortafuegos, productos de seguridad mainframe y entornos abiertos, sistemas de Sign-On único y de seguridad web. (Rodríguez Berzosa, 2012).

La industria ha venido usando otros modelos de control de accesos, como complemento de estos tres básicos, como el modelo de capacidades, en donde parte de las decisiones de autorización se toman a partir de 'capacidades', 'derechos efectivos' o atributos de privilegio, contenidos en las credenciales que un usuario adquiere durante la autenticación. DCE, por ejemplo, incorpora este modelo en su servicio de seguridad.

A menudo estos atributos de autorización se integran en un objeto conocido como 'Certificado de Atributos de Privilegio' (PAC, por sus siglas en inglés). Un PAC es como una acreditación de visitante: Se obtiene tras prueba de identidad, está emitida por una autoridad en la que se confía, no identifica al individuo pero sí lo categoriza (e.g. 'Visitante'), es de duración limitada, y no encierra en sí mismo información de privilegios o permisos (qué puertas puedo franquear, por ejemplo). (Rodríguez Berzosa, 2012).

Como conclusión a los modelos de control de acceso lógicos el modelo que más puede ajustarse a las necesidades de un sistema de administración financiera eSigef y a la realidad de los usuarios, debería proveer las facilidades para asignar los roles a

usuarios en el cual se cumplan los requisitos y principios básicos en el otorgamiento de permisos:

- Mínimos privilegios
- Necesidad de conocer o saber
- Segregación de funciones o tareas

En la figura 3 se puede observar gráficamente el esquema del modelo de control de acceso basado en roles.

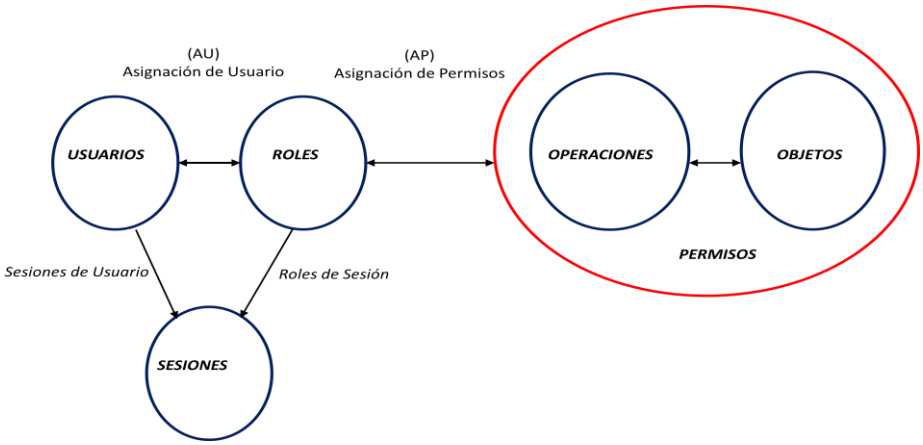


Figura 3: Modelo de Control de Acceso Basado en Roles

2.4.5 Auditoría de Sistemas de Información o Informática

Es la actividad profesional del auditor enfocada a la evaluación de la información automatizada (informática) y los sistemas de procesamiento de datos (en términos de eficiencia, efectividad y economía). (Badillo, Auditoria Basada en Riesgos, 2012).

Este tipo de auditoría está orientada a la realización de un examen para verificar el correcto funcionamiento y control de los sistemas informáticos y tecnológicos. (Badillo, Auditoria Basada en Riesgos, 2012).

Es el proceso de recolectar y evaluar evidencias para determinar si los sistemas de información y recursos relacionados, salvaguardan adecuadamente los activos, mantiene la integridad de los datos y del sistema, proveen información fiable, logran efectivamente las metas de la organización, consumen los recursos de manera eficiente, y tienen un vigor los controles internos que proveen una garantía razonable

de que se alcanzarán los objetivos del negocio, operativos y de control. (Badillo, Auditoria Basada en Riesgos, 2012).

2.5 Norma Internacional de Seguridad de la información ISO 27002

2.5.1 Norma Ecuatoriana NTE INEN-ISO/IEC 27002:2009

Esta norma para uso oficial en el Ecuador fue publicada en el 2009, y es prácticamente una adaptación de la norma internacional. En esta se describen los 11 dominios 34 objetivos de control y 133 controles.

ISO/IEC 27001 es una norma internacional publicada por ISO (*International Organization for Standarization*) que define cómo implementar y administrar el Sistema de Gestión de Seguridad de la Información. Esta norma proporciona una buena base para construir la ciberseguridad porque ofrece un catálogo de 133 controles de seguridad y la flexibilidad de aplicar solo aquellos que son realmente necesarios (según la evaluación de riesgos). (Kosutic, 2012, pág. 46)**.**

Define un marco referencial de gestión para controlar y abordar los asuntos de seguridad logrando, de esta forma, que la gestión de la seguridad sea parte de la gestión general de una organización. Es una de las principales normas en seguridad de la información existe aproximadamente 20.000 empresas certificadas por esta norma en todo el mundo (la certificación es realizada por organismos de certificación acreditados). (Kosutic, 2012, pág. 46)**.**

2.5.2 Resumen del Dominio Control de Acceso

A continuación se resumen los principales objetivos de control del dominio Control de Accesos de la Norma ITE INEN ISO/IEC 27002:2009.

Objetivo: Controlar el acceso a la información

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de la seguridad y del negocio.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

2.5.2.1 Política de control de acceso

Control: Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

2.5.2.2 Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deberían comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información.

Se debería poner atención especial, según el caso, a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

2.5.2.3 Responsabilidades de los usuarios

Objetivo: Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad. Se debería concientizar a los usuarios sobre sus responsabilidades por el

mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Es recomendable implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de información.

2.6 Norma NTE INEN ISO/IEC 27005:2012

2.6.1 Análisis del riesgo

2.6.1.1 Identificación del riesgo

El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida 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.

La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. El nivel del detalle utilizado en la identificación de los activos tendrá influencia en la cantidad total de información recolectada durante la valoración del riesgo. Este nivel se puede mejorar en iteraciones posteriores de la valoración del riesgo.

Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas.

Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado.

Identificación de los controles existentes

Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por 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, una referencia a los reportes del SGSI ya existentes debería limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades.

Identificación de las vulnerabilidades

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

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios.

Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo.

Identificación de las consecuencias

Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc.

Esta actividad 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 definen 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 por 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.

2.6.1.2 Estimación del Riesgo

Metodología para la estimación del riesgo

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias.

En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes. Posteriormente puede ser necesario realizar un análisis más específico o

cuantitativo de los riesgos importantes dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.

A continuación se describen los detalles de las metodologías para la estimación:

Estimación cualitativa:

La estimación cualitativa utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala.

Estimación cuantitativa:

La estimación cuantitativa utiliza una escala con valores numéricos (a diferencia de las escalas descriptivas utilizadas en la estimación cualitativa) tanto para las consecuencias como para la probabilidad, utilizando datos prevenientes de varias fuentes. La calidad del análisis depéndete de lo completo exacto que sean los valores numéricos, y de la validez de los modelos utilizados. En la mayoría de casos, la estimación cuantitativa utiliza datos históricos sobre los incidentes, dando como ventaja que ésta pueda relacionarse directamente con los objetivos de seguridad de la información y los intereses de la organización.

Valoración de las consecuencias

Después de identificar todos los activos bajo revisión, se deberían tener en cuenta los valores asignados a estos activos en la evaluación de las consecuencias.

El valor del impacto del negocio se puede expresar de manera cualitativa y cuantitativa, pero cualquier método para signar valor monetario en general puede suministrar más información para la toma de decisiones y, por tanto, facilitar un proceso más eficiente de toma de decisiones.

Valoración de los incidentes

Después de identificar los incidentes, es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra, utilizando técnicas de estimación cualitativas o

cuantitativas. Se deberían tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas.

Niveles de estimación del riesgo

La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo se basa en las consecuencias evaluadas y la probabilidad. Además, la estimación puede considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables, según correspondan para la evaluación del riesgo. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias.

2.6.2 Evaluación del riesgo

Los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y deberían tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones, tal como se toman en la actividad de evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo.

Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo. La agrupación de múltiples riesgos bajos o medios puede dar como resultado riesgos globales mucho más altos y es necesario tratarlos según corresponda.

2.6.3 Tratamiento del riesgo

2.6.3.1 Descripción general del tratamiento del riesgo

Existen cuatro opciones disponibles para el tratamiento del riesgo: reducción del riesgo, retención del riesgo, evitación del riesgo y transferencia del riesgo. La figura 4 ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información.

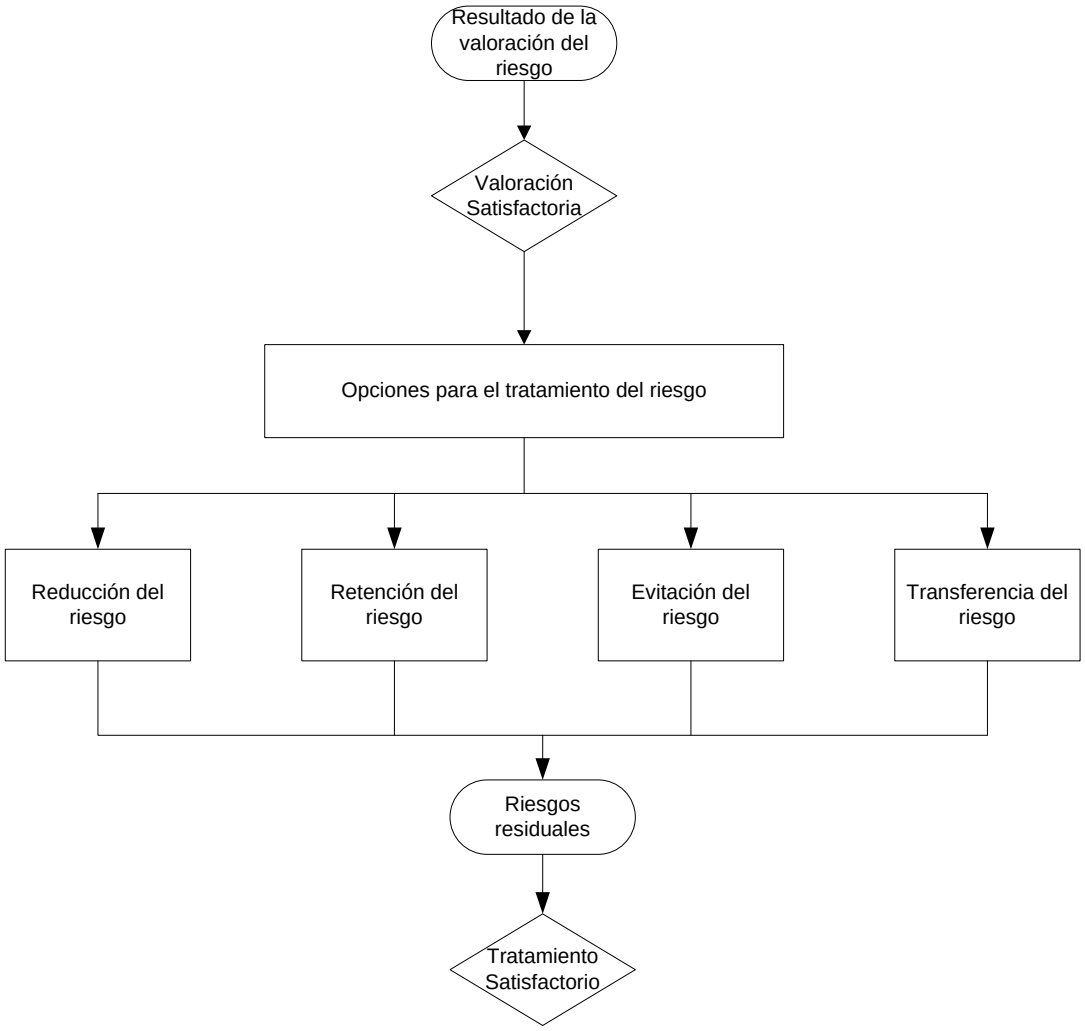


Figura 4: Actividad para el tratamiento del riesgo

Las opciones para el tratamiento del riesgo se deberían seleccionar con base al resultado de la valoración del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifica o no.

2.6.3.2 Reducción del riesgo

El nivel del riesgo se debería reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable. Se recomienda

seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo.

En esta selección se deberían tener en cuenta los criterios de aceptación del riesgo así como requisitos legales, reglamentarios y contractuales. También se deberían considerar los costos y el tiempo para la implementación de los controles, o los aspectos técnicos, ambientales y culturales. Con frecuencia es posible disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

2.6.3.3 Retención del riesgo

Si el nivel del riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.

2.6.3.4 Evitación del riesgo

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad. Por ejemplo, para los riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control.

2.6.3.5 Transferencia del riesgo

El riesgo se debería transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.

La transferencia del riesgo involucra una decisión para compartir algunos riesgos con las partes externas. La transferencia del riesgo puede crear riesgos nuevos o modificar los riesgos identificados existentes. Por lo tanto, puede ser necesario el tratamiento adicional para el riesgo.

La transferencia se puede hacer mediante un seguro que dará soporte a las consecuencias o mediante subcontratación de un asociado cuya función será monitorear el sistema de información y tomar acciones inmediatas para detener un ataque antes de que éste produzca un nivel definido de daño.

2.6.4 Aceptación del riesgo de la seguridad de la información

Se debería tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal.

Los planes para el tratamiento del riesgo deberían describir la forma en que los riesgos valorados se deben tratar, con el fin de satisfacer los criterios de aceptación del riesgo. Es importante que los directores responsables revisen y aprueben los planes propuestos para el tratamiento del riesgo y los riesgos residuales resultantes, y que registren todas las condiciones asociadas a tal aprobación.

2.6.5 Riesgo de Tecnologías de Información (TI)

Los riesgos de TI que pueden presentarse para cometer fraudes son los siguientes:

- Fallas en el hardware y/o software
- Falta de seguridades lógicas y físicas
- Indisponibilidad e integridad dudosa de los datos
- Acceso no autorizado a la información y a los sistemas
- Fallas en las telecomunicaciones
- Interrupciones de los sistemas
- Software malicioso

El riesgo es la probabilidad de que una cierta amenaza se aproveche de la vulnerabilidad de un activo o grupo de activos ocasionándoles pérdidas o daño. El impacto o gravedad relativa del riesgo, es proporcional al valor para el negocio de la pérdida o el daño, y proporcional a la frecuencia estimada de la amenaza. (Norma NTE INEN - ISO/IEC 27001), en la tabla 1 se describe como ejemplo un riesgo**.**

Tabla 1:
Ejemplo de riesgo de TI

Control de accesos lógicos a la aplicación	No existen controles de acceso adecuados para el ingreso de los usuarios, no existe una validación del usuario.
Riesgo	Acceso no autorizado a la aplicación
Probabilidad de que el evento ocurra	80%
Efecto si el evento ocurre:	Pérdida de información financiera, transacciones no autorizadas, desvíos de fondos.
Controles	Implementar controles de accesos seguros. Login biométrico, contraseñas fuertes, etc.

2.7 Descripción del Sistema Nacional de las Finanzas Públicas

Se define al Sistema Nacional de Finanzas Públicas - SINFIP como: "El conjunto de normas, políticas, instrumentos, procesos, actividades, registros y operaciones que las entidades y organismos del sector público, deben realizar con el objeto de gestionar en forma programada los ingresos, gastos y financiamiento público, con sujeción al Plan Nacional de Desarrollo y a las políticas públicas establecidas en esta ley". (Ministerio de Finanzas, 2010).

En el artículo Nro. 4 del Código Orgánico de Planificación de las Finanzas Públicas (COPLAFIP) menciona sobre el ámbito del SINFIP, en la que indica cuales son: todas las entidades, instituciones y organismos comprendidos en los artículos 225, 297 y 315 de la Constitución de la República.

En la constitución vigente en el capítulo séptimo – Administración Pública, sección primera indica que el Sector Público comprende:

Art. 225.- El sector público comprende:

- Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social.
- Las entidades que integran el régimen autónomo descentralizado.

- Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.
- Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos.

En la misma constitución en el artículo N° 297 indica que: Todo programa financiado con recursos públicos tendrá objetivos, metas y un plazo predeterminado para ser evaluado, en el marco de lo establecido en el Plan Nacional de Desarrollo.

Las instituciones y entidades que reciban o transfieran bienes o recursos públicos se someterán a las normas que las regulan y a los principios y procedimientos de transparencia, rendición de cuentas y control público.

2.7.1 Código Orgánico de Planificación y Finanzas Públicas

En el Título Preliminar - DE LAS DISPOSICIONES COMUNES A LA PLANIFICACION Y LAS FINANZAS PUBLICAS, se indica en el artículo 1:

Art. 1.- Objeto: El presente código tiene por objeto organizar, normar y vincular el Sistema Nacional Descentralizado de Planificación Participativa con el Sistema Nacional de Finanzas Públicas, y regular su funcionamiento en los diferentes niveles del sector público, en el marco del régimen de desarrollo, del régimen del buen vivir, de las garantías y los derechos constitucionales.

Las disposiciones del presente código regulan el ejercicio de las competencias de planificación y el ejercicio de la política pública en todos los niveles de gobierno, el Plan Nacional de Desarrollo, los planes de desarrollo y de ordenamiento territorial de los Gobiernos Autónomos Descentralizados, la programación presupuestaria cuatrianual del Sector Público, el Presupuesto General del Estado, los demás presupuestos de las entidades públicas; y, todos los recursos públicos y demás instrumentos aplicables a la Planificación y las Finanzas Públicas.

En el artículo 71 se indica que la rectoría del SINFIP corresponde a la Presidenta o Presidente de la República, quien la ejercerá a través del Ministerio a cargo de las finanzas públicas, en este caso le corresponde al Ministerio de Finanzas.

En el artículo N° 77 se indica en qué consiste el Presupuesto General del Estado:

El Presupuesto General del Estado es el instrumento para la determinación y gestión de los ingresos y egresos de todas las entidades que constituyen las diferentes funciones del Estado. No se consideran parte del Presupuesto General del Estado, los ingresos y egresos pertenecientes:

- Seguridad Social
- Banca pública
- Empresas públicas y
- Gobiernos Autónomos Descentralizados (GADs)

2.7.2 Entidades que conforman el Presupuesto General del Estado

En la figura 5 se muestra a las instituciones que pertenecen al PGE:

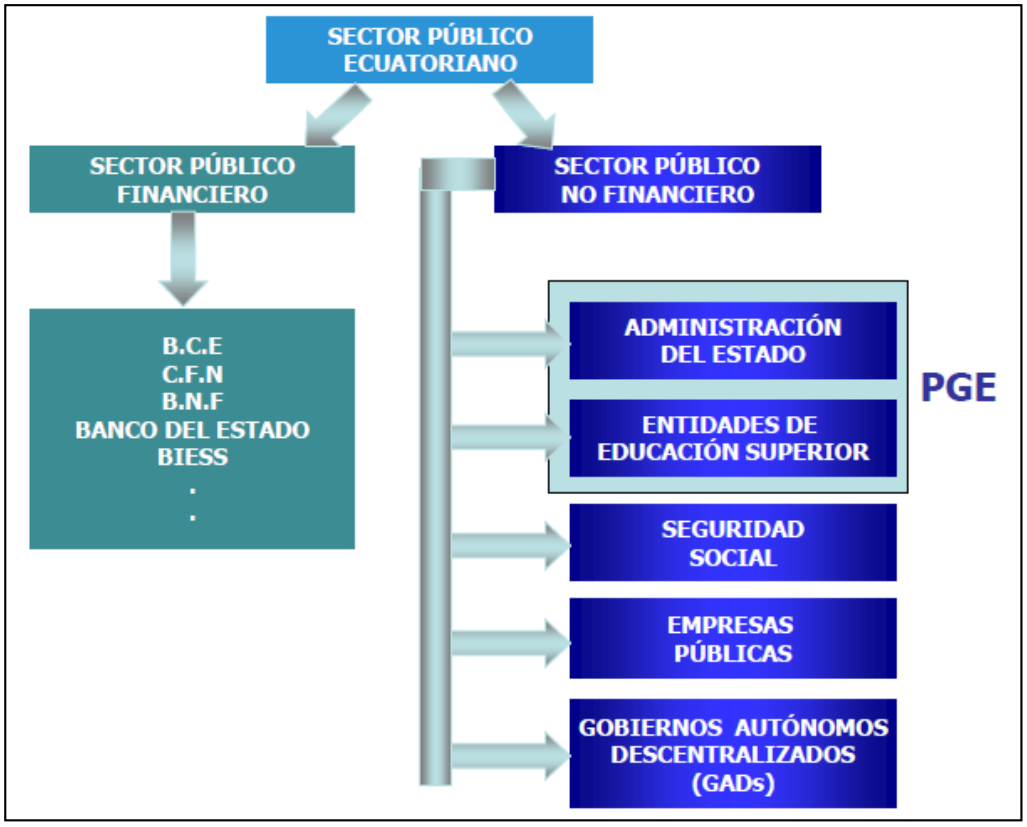


Figura 5: Sector Público y Presupuesto General del Estado

Dentro de la Administración del Estado, por ejemplo en el sector Desarrollo Social se tienen al Ministerio de Salud con las diferentes direcciones de salud, hospitales las cuales constituyen a Entidades Operativas Desconcentradas (EOD), como se indica en la figura 6:

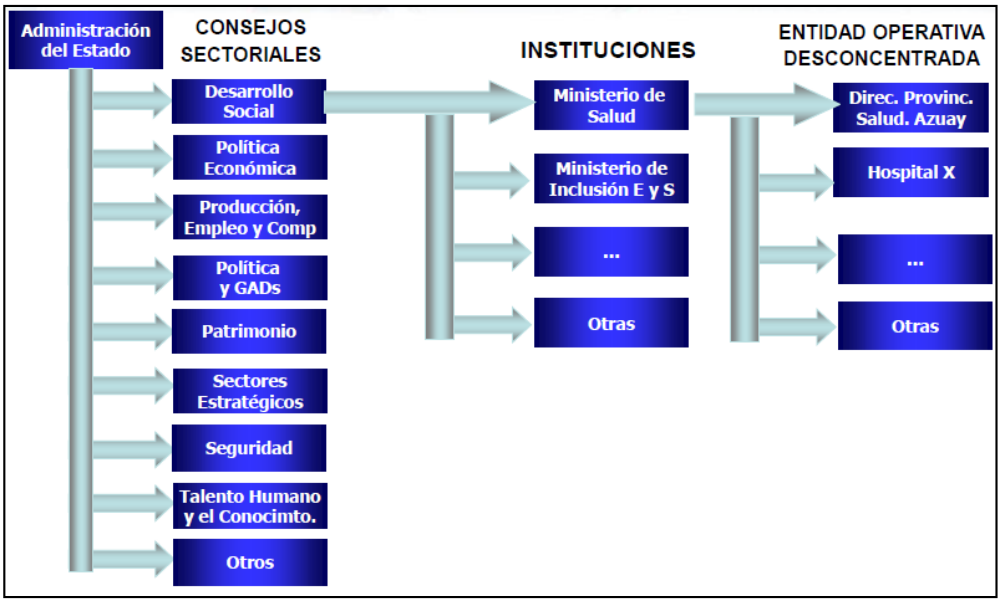


Figura 6: Ejemplo de Entidades Operativas del Ministerio de Salud

2.7.3 Acuerdo Ministerial N° 163

En este acuerdo se define lo referente a la administración de usuarios y claves para los usuarios del sistema de eSigef, permisos y perfiles para acceder a los diferentes módulos dependiendo del número de funcionarios que conformen el área de ejecución presupuestaria.

En la sección Disposiciones Generales, sección segunda se indica lo siguiente:

"El Ministerio de Finanzas realizará controles permanentes sobre el cumplimiento de esta disposición, y de presumirse la existencia de este tipo de irregularidades, pondrá en conocimiento de las autoridades de control a fin de que se determine las consecuentes responsabilidades administrativas, civiles y penales que hubiere lugar". (Ministerio de Finanzas Acuerdo Ministerial N° 163, 2008).

CAPÍTULO III
ANÁLISIS Y DISEÑO DE LOS CONTROLES DE SEGURIDAD

3.1 Análisis de los controles de seguridad

En la siguiente sección se detalla el proceso de administración de usuarios, esta información fue obtenida del sitio web www.finanzas.gob.ec, considerada como información de acceso público. En el Anexo 1 se encuentra el Acuerdo Ministerial N°163 donde se presenta a más detalle la administración de usuarios.

3.1.1 Administración de usuarios actual

Del sitio web se pudo obtener información del proceso de administración de usuarios, el cual incluyen actividades de creación, modificación y retiro de permisos para los usuarios administradores.

La Dirección Nacional del Centro de Servicios del Ministerio de Finanzas, se encarga de la administración de los administradores informáticos y financieros de las instituciones UDAFs.

En el Acuerdo Ministerial N° 163 de Ministerio de Finanzas se encuentran definidos las normas en la asignación de funciones a usuarios y claves del sistema eSigef dependiendo del número de usuarios responsables de la ejecución financiera institucional para la operación en los módulos de Presupuesto, Nómina, Tesorería y Contabilidad.

En dicho Acuerdo se define la documentación requerida para la creación de usuarios operativos dentro de cada institución, misma que debe ser respectivamente notariada a ser presentada ante el Ministerio de Finanzas:

- Formulario de “Solicitud de creación de usuarios operativos (UDAF´S/EOD’S”-FSI.AS.01”.
- Acuerdo de responsabilidad en Seguridad de la Información. A.SI.AS.01
- Acción de Personal o copia de contrato
- Copia de cédula
- Acta entrega/recepción de identificación de usuarios y compromiso de uso.

Los formularios, acuerdos y actas se encuentran en el portal del sistema esigef, como se puede apreciar en la figura 7:

Figura 7: Pantalla principal de los aplicativos SINFIP

Fuente: (eSigef, 2013)

Para el caso de los GADs y Empresas Públicas las cuales suben información financiera al sistema pero no operan en el mismo por tanto no están obligados a presentar la documentación anteriormente indicada.

Así mismo en el portal se encuentra publicado información de las funciones correspondientes a los operadores y aprobadores de los Módulos de Presupuestos, Contabilidad y de Tesorería, las mismas que son de cumplimiento obligatorio.

3.1.2 Administración de contraseñas

La administración de las contraseñas se lo realiza mediante del módulo de administración de usuarios, en el sistema se crea por defecto la contraseña con el número de cédula del funcionario, en la figura 8 se muestra una pantalla de creación de usuarios, en esta figura se puede apreciar la creación de un usuario administrador,

cabe indicar que estos administradores informáticos son los que administran a los respectivos usuarios operativos de cada entidad.

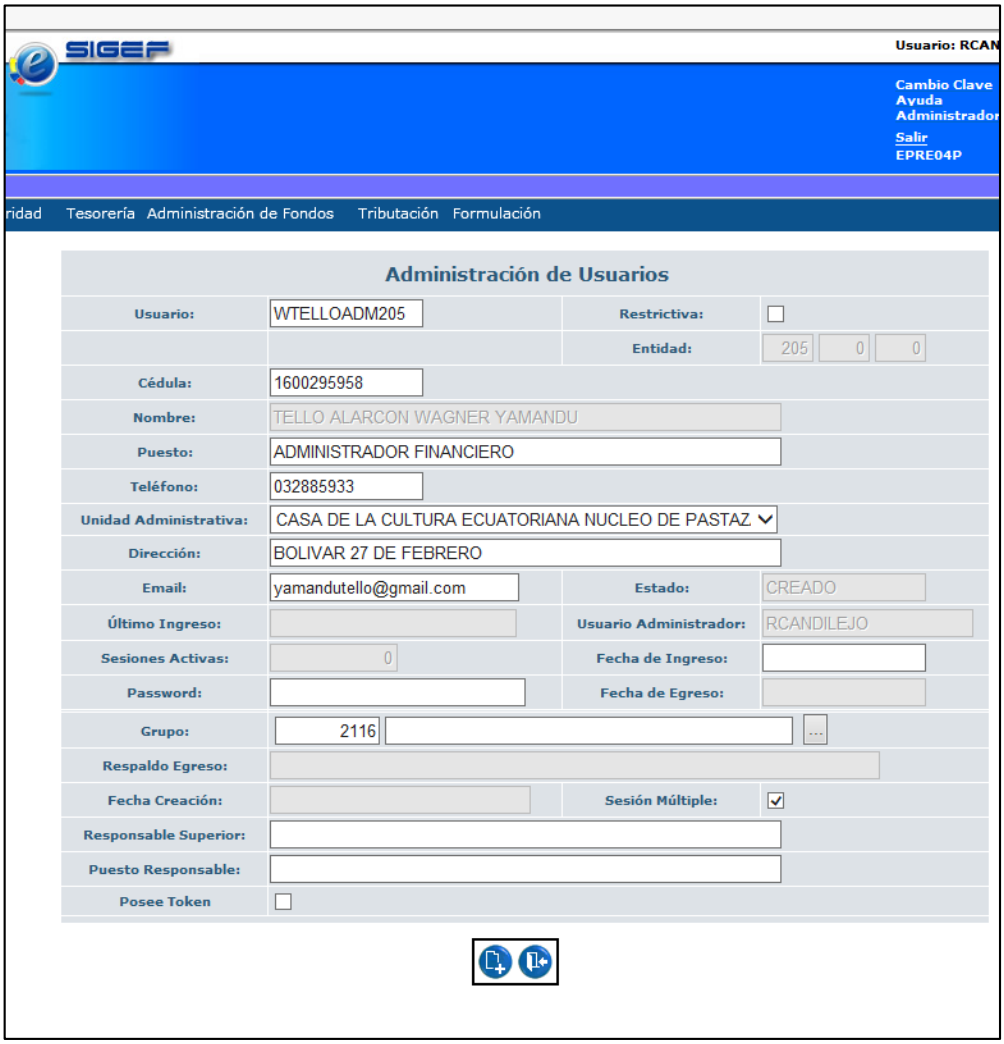


Figura 8: Pantalla de creación de usuarios sistema eSigef

Fuente: (eSigef, 2013)

3.2 Resumen de los casos de desvíos de fondos

A continuación se resumen los casos de desvíos de fondos más significativos que han ocurrido en los últimos años según información recopilada de la prensa nacional.

- **INIAP-Instituto Nacional Autónomo de Investigaciones Agropecuarias:** Recientemente se presentó un caso de presunto desvíos de fondos públicos por 628.912 dólares aproximadamente, realizada por un funcionario a otras cuentas ajenas a la institución, estos movimientos se los habría realizado el 14

y 15 de Mayo del año pasado, según argumenta la defensa de la inocencia del implicado porque le "hackearon la clave". (LaHora, 2013).

- **Ministerio del Ambiente:** Suman alrededor de 52 vinculados en proceso por desvío de fondos públicos realizados en el Ministerio del Ambiente. Los funcionarios implicados habrían facilitado sus claves del acceso al sistema eSigef con el cual desviaron 7'360.000 dólares a cuentas particulares desde el 1 hasta el 30 de mayo 2012. (Telegrafo, 2013).
- **Centro de salud N° 8 del Instituto Ecuatoriano de Seguridad Social (IESS):** El implicado en el desvío de fondos argumentó que realizó las transacciones a su cuenta puesto que se aprovechó de la clave que le confirió el Ministerio de Salud y por fallas que había encontrado en el sistema. En cinco años habría conseguido desviar 3.4 millones de dólares. Las cuentas auditadas por la Contraloría General del Estado comprenden el periodo del 1 de Septiembre del 2006 al 5 de Julio del 2011. (ElUniverso, 2012).

Como puede notarse todos estos casos de fraudes financieros son detectados después de que se han cometido los actos ilícitos, por tal motivo es de importancia proveer de controles preventivos que permitan mitigar el riesgo de fraudes.

De acuerdo a la teoría del fraude y según lo expuesto anteriormente se puede decir que ha intervenido simultáneamente los tres elementos:

Motivo: deudas de los perpetradores

Oportunidad percibida: debilidades del control interno, entorno favorable

Racionalización: justificación, convencimiento de que si otros comenten el propio está justificado

3.3 Evaluación en la administración de usuarios realizada a una muestra

En la siguiente sección se presenta la evaluación realizada a varias instituciones por medio de entrevistas a los administradores informáticos, posteriormente se detallan los lineamientos base para la elaboración de la encuesta basadas en preguntas de control de acuerdo a la norma ISO 27002.

3.3.1 Base legal para la generación y realización de la evaluación

La evaluación corresponde a una revisión cualitativa de los procesos de administración de usuarios en las entidades adscritas al sistema eSigef. Para llevar a cabo esta actividad se tomó en consideración lo establecido en el Acuerdo Ministerial N° 163, sección 2.7.3:

El Ministerio de Finanzas realizará controles permanentes sobre el cumplimiento de esta disposición (Acuerdo N° 163), y de presumirse la existencia de este tipo de irregularidades, pondrá en conocimiento de las autoridades de control a fin de que se determine las consecuentes responsabilidades administrativas, civiles y penales a que hubiere lugar. (Ministerio de Finanzas Acuerdo Ministerial N° 163, 2008).

3.3.2 Selección de la muestra

En el Anexo 2 se listan las instituciones preseleccionadas a los cuales se realizó la encuesta, esta selección fue realizada aleatoriamente y tomando en consideración la disposición de que por cada institución se debe tener a un administrador informático, el cual gestionará a los usuarios operativos de cada institución de las respectivas unidades operativas desconcentradas a las que pertenezcan.

3.3.3 Procesos de administración de usuarios a revisar

En la tabla 2 se indican los procesos de administración de usuarios que se tomarán como base para la elaboración de las encuestas, las cuales están basadas en la norma NTE INEN ISO/IEC ISO 27002.

Tabla 2:
Procesos de administración y monitoreo de usuarios a evaluar

Objetivo de Control	Controles
Gestión de acceso de usuarios	✓ Registro de usuarios ✓ Gestión de privilegios ✓ Gestión de contraseñas para usuarios ✓ Revisión de los derechos de acceso de los usuarios
Monitoreo	✓ Monitoreo del uso del sistema

A continuación se detallan los requerimientos de cada uno de estos controles:

- **Proceso de Gestión de registro de usuarios**

El proceso formal debe considerar el registro y cancelación de usuarios con el fin de conceder y revocar el acceso al sistema. Debería incluirse en el proceso lo siguiente:

- Usar una identificación única de usuario para permitir que los usuarios queden vinculados y sean responsables de las acciones.
- Verificar que el usuario tenga autorización del responsable del sistema para el uso del sistema.
- Verificar que el nivel de acceso otorgado sea adecuado para los propósitos del negocio, sea coherente con la política de seguridad, y que esté acorde a las funciones del usuario.
- Dar a los usuarios una declaración escrita de los derechos de acceso al sistema. Así como hacer firmar declaraciones que indiquen que los usuarios entienden las condiciones del uso del sistema.
- Quitar, retirar, bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, cargo, puesto o que se han desvinculado de la organización.
- Verificar, retirar o bloquear las cuentas de usuarios que no se encuentren asignadas a usuarios.

Información adicional

Se debería considerar el establecimiento de roles de acceso de usuarios basadas en los requisitos del negocio que incluyan un número de derechos en perfiles típicos de acceso.

- **Proceso de gestión de privilegios**

El proceso debería controlar y restringir la asignación de privilegios o permisos.

El proceso debería contemplar lo siguiente:

- Se debería identificar los usuarios y sus privilegios o permisos de accesos asociado al sistema.

- Se debería asignar permisos o privilegios de acuerdo a una política o modelo de control de acceso y que lo permita el sistema.
- Se debería registrar la autorización de los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización esté completo.

Información adicional

El uso no apropiado del módulo de administración de usuarios que permite dar accesos a los mismos, puede ser un factor importante de cometer errores humanos y otorgar permisos no adecuados.

- **Proceso de gestión de contraseñas para usuarios**

La asignación de contraseñas se debería controlar a través de un proceso formal, el cual debería incluir lo siguiente:

- Se debería exigir a los usuarios firmar una declaración para mantener confidenciales las contraseñas personales, esta declaración firmada se podría incluir en los términos y condiciones laborales.
- Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén obligados a cambiar al primer inicio de sesión.
- Las contraseñas temporales se debería suministrar de forma segura a los usuarios.
- Las contraseñas temporales deberían ser únicas y complejas para cada usuario.
- Las contraseñas nunca se deberían almacenar en sistemas de computador en un formato que no esté protegido.

Información adicional

Las contraseñas son un medio común de verificación de la identidad de un usuario antes de otorgar acceso al sistema de acuerdo con la autorización respectiva.

- **Proceso de revisión de los derechos de acceso de los usuarios**

Se debería contar con un proceso formal de revisión periódica de los derechos de acceso de los usuarios al sistema, el proceso debería contemplar los siguientes aspectos:

- Deberían revisarse a intervalos regulares, por ejemplo cada seis meses y después de cada cambio, por ejemplo cambio a un nivel superior o inferior, o terminación de trabajo.
- Revisar las autorizaciones realizadas en permisos de acceso privilegiadas a intervalos de tiempo más cortos, por ejemplo cada 3 meses.
- Verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados.

Información adicional

Es necesario revisar con regularidad los derechos de acceso de los usuarios para mantener un control eficaz del acceso a los datos e información del sistema.

- **Proceso de monitoreo del uso del sistema**

Se debería contar con el proceso de monitoreo de uso del sistema y se debería revisar con regularidad los resultados de las actividades de dicho monitoreo. Se debería incluir en el proceso los siguientes aspectos:

- Identificación de usuario
- Fecha y hora de accesos
- Módulos o recursos a los que se tiene acceso
- Intentos de usuarios fallidos
- Bloqueos de usuarios por intentos fallidos.

La frecuencia con la cual se revisan los resultados de las actividades de monitoreo debería depender de los riesgos más importantes que se tengan como antecedentes o sean de mayor probabilidad e impacto.

Información adicional

Es necesario el uso de procesos de monitoreo para garantizar que los usuarios únicamente ejecutan actividades autorizadas explícitamente. La revisión de los registros implica la comprensión de las amenazas enfrentadas por el sistema y la forma en que pueden originar.

3.3.4 Recopilación, interpretación y análisis de resultados

Como se indicó anteriormente las encuestas se elaboraron en base a los procesos y mejores prácticas de seguridad indicados anteriormente en la sección 3.3.3, sin embargo estas se las adecuará a la situación actual de las instituciones, puesto que existen controles que no aplican y además otros que quedan a discreción del manejo y administración interna en cada institución, por tal motivo se elaboró la encuesta en base a lo que comúnmente deberían considerarse en una administración básica de usuarios y adicionalmente se consideran temas de monitoreo y revisión.

Las entidades a las que se realizaron las encuestas se detallan en el Anexo 2, las preguntas de control se detallan en el Anexo 3. En el Anexo 4 se detallan los resultados de las encuestas realizadas a las instituciones.

En el Anexo 5 se muestran en gráficos los resultados obtenidos de las encuestas, en los cuales se puede apreciar en porcentaje las respuestas (SI/NO), en dicho Anexo se interpretan y analizan los resultados de cada pregunta y en contexto de cada proceso.

Adicionalmente se indica la información extra o adicional que los Administradores Informáticos proporcionaros, en relación a como llevan actualmente sus procesos internos.

3.4 Evaluación de riegos de los resultados basados en la norma ISO 27005

En esta sección se realiza la evaluación de riesgos que se identificaron en los resultados y análisis de las entrevistas realizadas. La norma ISO 27005 tiene en su contenido un listado de amenazas, vulnerabilidades y la metodología para realizar la valoración del riesgo en base a la probabilidad de ocurrencia, valoración de los activos y el impacto.

3.4.1 Identificación de las amenazas

En el Anexo 7 se detallan las amenazas y vulnerabilidades más importantes que se encontraron, las cuales fueron tomadas de la norma ISO 27005 la cual se adjunta en el Anexo 6.

Debido a que a lo largo del presente capítulo se ha considerado como eje principal el control de acceso al sistema y monitoreo del uso del sistema, es importante tomar en cuenta que las fuentes de las amenazas más significativas son de carácter humano, las cuales se muestran en el Anexo 8.

3.4.2 Identificación de las vulnerabilidades

En el Anexo 9 se presenta ejemplos de vulnerabilidades que se han encontrado en los resultados de las encuestas realizadas, las cuales están mayormente enfocadas en lo relacionado con las acciones que podría realizar el personal y del tipo organizacional.

3.4.3 Probabilidad de ocurrencia

Para el cálculo del riesgo, la probabilidad de ocurrencia se calcula en primer lugar por el valor del activo el cual puede tener una escala de 0 a 4, y en segundo lugar por la probabilidad de ocurrencia de que la amenaza y su relación con la fácil explotación de la vulnerabilidad correspondiente. En el Anexo 10 se detalla la metodología para la valoración del riesgo de cada proceso en la administración de usuarios del sistema eSigef.

3.4.4 Matriz de Riesgo

Como se presentó en las secciones anteriores (amenazas, vulnerabilidades y probabilidad de ocurrencia), en el Anexo 11 se resumen los principales riesgos identificados en la actual administración de usuarios que realizan las instituciones encuestadas.

3.5 Tabulación de resultados del nivel de madurez de los procesos revisados

Adicionalmente de las entrevistas realizadas se determinó el nivel de madurez de los procesos de administración de usuarios que manejan internamente. A continuación se describe en qué consiste el modelo de madurez que se utilizó:

Modelo Genérico de Madurez

0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial.- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible.- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido.- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado.- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado.- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la

empresa se adapte de manera rápida. En la figura 9, se ilustra el nivel de madurez para la evaluación de los procesos de administración de usuarios.

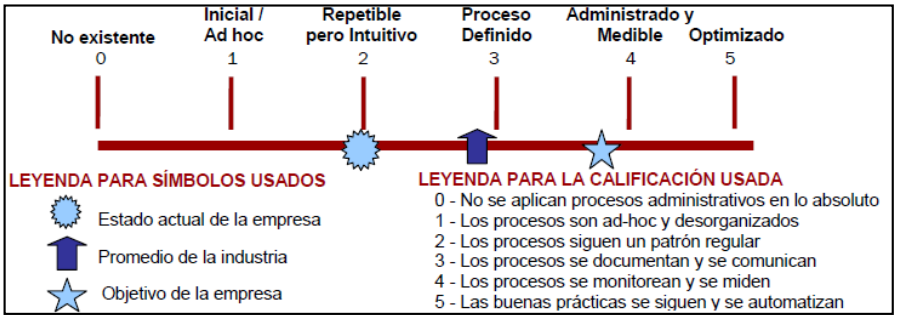


Figura 9: Niveles de madurez según CMM (Cobit Madurity Model)

Fuente: (Cobit4.1, 2007)

En el Anexo 12 se resumen el nivel de madurez obtenida de los procesos según la información que se pudo conseguir en las entrevistas realizadas:

Significado de la medición: 0 No existe, 1 Inicial, 2 Repetible, 3 Definido, 4 Administrado, 5 Optimizado.

Para la sección "Diseño de los controles de seguridad para las instituciones basado en la norma ISO 27002", se tomará en cuenta tanto el análisis de riesgo como el modelo de madurez indicado en el Anexo 12.

3.6 Diseño de controles de seguridad en base a la norma ISO 27002

Para el diseño de los controles se tomará como base la Norma Técnica Ecuatoriana NTE ISO/IEC 27002, específicamente lo relacionado en el Dominio 11 Control de Accesos. El Objetivo del Control "Gestión del acceso de usuarios" es asegurar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas, en este caso al sistema eSigef.

El objetivo del diseño de estos controles respecto a la gestión de usuarios del sistema eSigef es impedir el acceso no autorizado a la información, para lo cual se puede valer de controles mediante la aplicación de procedimientos específicos.

Como estrategia para el diseño de los controles, se priorizará los procesos de mayor riesgo, en el Anexo 13 se han ordenado los procesos según el riesgo presentado en orden descendente:

Se diseñarán los controles por cada proceso, en cada proceso se puede tener uno o varios controles, esto dependerá de las vulnerabilidades identificadas en la evaluación de riesgos y en los requerimientos de seguridad del control "*Gestión de accesos de usuarios*".

Antes de diseñar los controles es importante definir en primer lugar las responsabilidades generales que deberían considerarse para la administración de usuarios de las instituciones.

Mediante Acuerdo Ministerial N° 166 la Secretaría Nacional de la Administración Pública (SNAP), dispuso la implementación de un Esquema Gubernamental de Seguridad de la Información (EGSI) en la cual se definen responsabilidades sobre la seguridad de la información. Las responsabilidades que se definen en dicho acuerdo son:

- Comité de Seguridad de la Información
- Oficial de Seguridad de la Información
- Responsable de Seguridad de TICs

En el presente proyecto, se consideran las siguientes responsabilidades las cuales se alinean a lo indicado en Acuerdo N° 166.

3.6.1 Responsabilidades en la Administración de Usuarios

En este punto se considerará aquellas responsabilidades que deberían ser aplicadas al sistema eSigef a nivel organizacional, y en lo que respecta al nivel técnico se considerará lo que actualmente posee el sistema como tal.

3.6.1.1 Responsable de Seguridad Informática (Responsable de Seguridad de TICs-EGSI)

Tendrá las siguientes responsabilidades:

- Definir normas y procedimientos para: la gestión de accesos al sistema; la solicitud y aprobación de accesos al sistema.
- Controlar la asignación de privilegios a usuarios.

- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y uso del sistema.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.

3.6.1.2 Propietarios de la Información (Administrador Financiero-Director Financiero)

Tendrá las siguientes responsabilidades:

- Determinar los controles de accesos a nivel de procedimientos, normas y políticas internas a ser consideradas para el uso del sistema.
- Definir los eventos y actividades de usuarios a ser registrados en el sistema y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros de acuerdo a las normas internas vigentes y a sus propias necesidades o riesgos presentados.

Los Propietarios de la Información junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normatividad legal vigente.

3.6.1.3 Responsable del Área Informática (Administrador Informático)

Tendrá las siguientes responsabilidades:

- Implementar procedimientos para el registro y cancelación de acceso y derechos de acceso al sistema.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por el Propietario de la Información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes al sistema.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso al sistema.
- Otorgar acceso al sistema únicamente de acuerdo al pedido formal correspondiente y de acuerdo a las actividades dadas por el contrato de trabajo de los usuarios.
- Efectuar un control de los registros de auditoría generados por el sistema.

El Oficial de Seguridad de la Información o en su defecto quien sea designado por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre las mejoras en los procedimientos y controles que se establezcan.

Una vez definidas estas responsabilidades, a continuación se describen los controles de seguridad en las cuales cada responsable actuará en cada fase que se indique.

3.6.2 Controles para el proceso de registro de usuarios

El objetivo principal de este control es que se debería contar con un procedimiento formal para el registro, modificación y cancelación de usuarios con el fin de conceder y revocar el acceso al sistema eSigef de manera segura. A continuación se describen los controles.

3.6.2.1 Control de Altas, Bajas y Modificación de usuarios

Registro de usuario al sistema eSigef

El procedimiento para registro de usuario se detalla en la tabla 3.

Tabla 3:
Procedimiento de registro de usuarios

N°	Responsable	Actividad
1	**Área de RR.HH**	Antes del ingreso de un nuevo funcionario, el área de RR.HH. se encarga de que suscriba el "Compromiso de confidencialidad de la información" que incluirá la aceptación de las responsabilidades concernientes a: • Cuenta de usuario • Clave de acceso Ejemplo: **Usuario:** Juan Pérez **Cuenta de usuario:** jperez **Contraseña:** Tg$JpLK3!
2	**Usuario**	Completa el Formulario de solicitud de Usuarios Lo envía por e-mail o físico al Administrador Financiero, solicitando el acceso al sistema.
3	**Propietario de Información**	Recibe el formulario de solicitud, valida la solicitud y si la misma ha sido aprobada, da su conformidad y autoriza el acceso al sistema enviando un e-mail o físico de la solicitud correspondiente al Responsable de Seguridad Informática (Responsable de Seguridad de TICs-EGSI). Si la solicitud ha sido rechazado el Propietario de Información informa vía e-mail al usuario el motivo del rechazo.
4	**Responsable de Seguridad Informática**	Validará la autenticidad del nombre del Propietario de Información cotejando con el registro del personal de la institución. Si existe el nombre del Propietario de Información, envía la solicitud para creación del usuario al Responsable del Área Informática (Administrador Informático). Verifica la siguiente documentación adjunta, la cual debe ser notariada. • Acción de Personal o copia de contrato • Copia de cédula y papeleta de votación actual • Acuerdo de Confidencialidad de la Información

		En caso que la persona autorizante no se encuentre en el registro procederá al rechazo de la solicitud, comunicará al solicitante las razones del rechazo.
5	**Responsable del Área Informática**	Crea al usuario en el sistema asignándole las características solicitadas en el estándar respectivo. Asigna una contraseña que deberá estar acorde a lo dispuesto en la política de gestión de contraseñas para usuarios. Activa el cambio obligatorio de contraseña en el primer inicio de sesión.
6	**Responsable del Área Informática**	Deja constancia en sus registros de lo realizado, archiva el formulario y notifica al Responsable de Seguridad Informática por correo electrónico.
7	**Responsable de Seguridad Informática**	Entrega o envía al nuevo usuario los documentos: "Comunicación de Usuario y Clave", y el "Compromiso de Confidencialidad", conserva una copia del documento con la confirmación dada por el usuario.
8	**Propietarios de la Información**	Activa el usuario en el sistema.
9	**Usuario**	Confirma al Responsable del Área Informática e ingresa al sistema y actualiza su contraseña.

Modificación de permisos de accesos del sistema

El procedimiento modificación de permisos de usuarios se detalla en la tabla 4.

Tabla 4:
Procedimiento modificación de permisos

N°	Responsable	Actividad
1	**Propietario de la Información**	Envía al Responsable de Seguridad Informática la solicitud de edición de permisos o cambios en las funciones a realizar por los usuarios operativos.
2	**Responsable Seguridad Informática**	Valida la solicitud recibida y verifica las firmas de responsabilidad. En caso de ser rechazada dicha solicitud comunicará al Propietario de la Información. De ser aprobada la solicitud enviará al Responsable del Área Informática para que proceda con los cambios.
3	**Responsable del Área Informática**	Analizan en conjunto las características de los cambios a realizarse al usuario. Ejecuta la solicitud de modificación y comunica vía e-mail al usuario y al Responsable de Seguridad Informática.

Bajas de usuarios en el sistema eSigef

El procedimiento para bajas o cancelación de permisos de usuarios se detalla en la tabla 5.

Tabla 5:
Procedimiento para bajas de usuarios

N°	Responsable	Actividad
1	**Propietario de la Información**	Solicita la baja del usuario del sistema al Responsable de Seguridad Informática y adicionalmente notifica a Talento Humano.
2	**Responsable de Seguridad Informática**	Validará la autenticidad del nombre del Propietario de la Información. En caso que la persona autorizante no se logre validar en el registro procederá al rechazo de la solicitud. En caso de que la validación sea exitosa comunicará al Responsable del Área

		Informática para que realice la baja del usuario.
3	**Administrador del Área Informática**	Da de baja (no elimina) en el sistema la cuenta del usuario. Registra el formulario y notifica al Responsable de Seguridad Informática.
4	**Responsable de Seguridad Informática**	Notifica al Propietario de la Información
5	**Propietario de la Información**	Recibe la solicitud y la registra.

Formulario de solicitud de creación de usuarios

En la figura 10 se muestra el formulario de solicitud de creación de usuarios

DIRECCIÓN DE TICs					
ALTA / BAJA / MODIFICACIÓN DE USUARIOS					
Fecha de Solicitud:					
Persona que Solicita:					
Nombre y Apellido:					
Cargo/Área:					
Numero de cédula (1):					
Responsable de la Aprobación					
Nombre y Apellido Responsable de Área:					
Área:					
Datos Solicitud					
Concepto		**Alta**	**Baja**	**Modificación**	
Sistema (2):		**eSigef**	**eSipren**	**Spryn**	**ByE**
Perfil de Acceso (3)					
Observaciones Adicionales (4):					

Referencia de Ayuda para completar el formulario	
(1) Corresponde al número de cédula	
(2) Especificar el nombre del sistema	
(3) Especificar el perfil de acceso a asignar. Ejemplos: Operador Aprobador	
(4) De acuerdo en cada caso en particular	
	Ejecutado por: Firma:
Aprobación para ejecución	

Figura 10: Formulario solicitud creación de usuarios

3.6.2.2 Modelo acuerdo de confidencialidad

En la figura 11 se detalla el mensaje que deberá ser será enviado a cada usuario operativo en lo que respecta a la utilización de la cuenta de usuario, y en la figura 12 el compromiso de confidencialidad de la información:

Comunicación de usuario y contraseña
Apellido y Nombre: ……
Número de Cédula: …….
Por medio de la presente se le hace entrega de su cuenta de usuario y contraseña de acceso al sistema eSigef.

Cuenta de usuario: ……

Contraseña: ……

Se le comunica que:

- La clave debe ser confidencial.
- El sistema le obligará a cambiar la clave la primera vez que usted ingrese al sistema.
- Deberá ingresar una clave de 8 (ocho) caracteres de longitud.
- El sistema le obligará a cambiar la clave cada 15 días.
- El sistema no le permitirá utilizar alguna de las últimas 10 claves que haya utilizado.
- El sistema de seguridad bloqueará su cuenta luego de 3 intentos fallidos de ingreso de usuario/clave.

En caso de que usted considere necesario hacer un cambio de clave, se lo deberá notificar expresamente por medio del formulario correspondiente al Responsable

de Seguridad Informática.

Figura 11: Comunicado de entrega de usuario y contraseña

Compromiso de Confidencialidad de la Información

Por la presente ratifico haber recibido a las……: …… horas, en sobre cerrado, mi usuario y clave de acceso al sistema eSigef de [Nombre de la Institución] y me comprometo a cumplir con toda la normativa de la institución en relación a la seguridad de la información en los equipos informáticos y datos a los que tenga acceso y específicamente a:

- No divulgar cualquier información obtenida de los sistemas ni utilizarla para cualquier fin contrario a los intereses de la institución.
- Aceptar las responsabilidades sobre el uso de mi cuenta de usuario.
- No revelar ni compartir la cuenta de usuario y contraseña otorgada.
- Conservar toda información restringida o secreta en los equipos centralizados de procesamiento.

La presente también deja constancia de que deberá leer las Política, Normas y Procedimientos y salvo que en el plazo no mayor a 5 días hábiles notifique al área de Talento Humano sus objeciones específicas a cada punto definido, se entiende que usted presta conformidad a todo lo allí expresado.

El uso de su cuenta de usuario al sistema es exclusivo para usted y de acuerdo a lo definido en las normas y políticas internas.

[Nombre de la institución] deja en claro que todas las actividades de los usuarios en el sistema pueden ser monitoreadas y auditadas.

Toda información a la que acceda en el desarrollo de las tareas es de propiedad de la institución (salvo aquella que haya sido declarada como publica) y solo para su uso mientras desarrolle actividades en la misma, y deberá conservarse en los equipos de procesamiento centralizados y no en las estaciones de trabajo y otros soportes físicos.

Nombre del usuario: ……
Número de cédula: …….

Firma del usuario: ..……

Figura 12: Compromiso de confidencialidad de la información

3.6.3 Controles para el proceso de gestión de privilegios

3.6.3.1 Procedimiento de asignación de roles basados en la norma gestión de control de acceso basado en roles

Para la gestión de privilegios se ha adoptado el Modelo de Control de Accesos Basados en Roles (RBAC), como modelo para asignar los privilegios a los diferentes módulos y funciones del sistema eSigef. Este modelo es adecuado para las instituciones puesto que se acopla a la estructura que se maneja actualmente es decir al modelo basado en perfiles y roles.

Antes de realizar dicha alineación, es necesario indicar las definiciones actuales que se manejan en el esquema de funciones.

El modelo actual establece que para operar con el sistema se requiere de autorizaciones para el acceso, estos accesos se establecen por perfiles que se asocian a funciones que al relacionarse con los usuarios permiten el acceso al eSigef.

Función: La función es la asociación de uno o más perfiles que definen un esquema generalizado de permisos, operaciones y actividades que un usuario tendrá acceso.

Perfil: El perfil es el agrupamiento de los objetos (opciones o botones) a los que se tiene acceso para ejecutar una tarea específica.

Usuario: Es la persona que acceso al sistema. Al mismo que se le asignan funciones que determinan el nivel de acceso en el sistema y que pertenece a un grupo previamente definido por el modelo de gestión.

Definiciones del Modelo RBAC

- El acceso de un usuario a la información se concede por medio de roles.
- Los roles se definen de acuerdo con los puesto de trabajo según el manual de funciones de cada institución.
- Rol es una función de trabajo en las instituciones con una definición clara de las responsabilidades, acciones y la autoridad inherentes respecto de la información manejada y a la actividad que realiza.

- Los permisos se asocian con los roles y se definen con base en los niveles de autorización y de responsabilidad que correspondan al puesto de trabajo respectivo.
- Las operaciones sobre los objetos de información se definen en los permisos

En la tabla 6 se muestra la correspondencia entre los elementos del estándar RBAC y eSigef.

Tabla 6:
Relación entre elementos RBAC y sistema eSigef

RBAC	Sistema eSigef
Usuarios	Usuarios del sistema
Roles	(Operador/Aprobador, Operador, Aprobador, Consulta)
Objetos	Perfil (opciones, menú, submenú o botones)
Operaciones	Funciones (ej. 801,802,803, etc)
Permisos	N/A

En la figura 13 se detalla el modelo de definición de roles

DEFINICIÓN DEL ROL 1: APROBADOR ESIGEF	
Las funciones asignadas a este Rol deberán anexarse a la documentación del manual de puestos de cada institución.	
FUNCIONES ASIGNADAS	
☐ 601 - Total nómina	☐ 602 - Consulta nómina
☐ 603 - Operador nómina	☐ 604 - Aprobador Nómina
☐ 6057 - Aprobador de Tributacion de UDAF con UE	☐ 6057 - Aprobador de Tributacion de UDAF con UE
☐ 6058 - Consulta de Tributacion de UDAF con UE	☐ 6060 - Aprobador de Tributacion de Unidad Ejecutora
☐ 6060 - Aprobador de Tributacion de Unidad Ejecutora	☐ 6062 - Operador de Tributacion de Unidad Ejecutora
☐ 607 - Aprobador Reformas Web	☐ 632 - Operador - Aprobador General de Unidad Ejecutora
☐ 6074 - Consulta de UDAF con UE Subsidios	☐ 6075 - Aprobador de UDAF con UE Subsidios
☐ 6076 - Operador de UDAF con UE Subsidios	☐ 633 - Operador - Aprobador General de UDAF con UE
☐ 634 - Operador General de Unidad Ejecutora	☐ 635 - Operador General de UDAF con UE

Figura 13: Modelo para definición de roles

Definido este esquema o modelo de control de acceso basado en roles, cada institución definirá con claridad los roles dentro del área responsable de la ejecución financiera, para lo cual podrá valerse del siguiente formato para la definición con sus respectivas funciones de cada rol.

En la definición de los roles descritos anteriormente, se debe tomar en cuenta las consideraciones dispuestas en los manuales, procedimientos y directrices emitidos por el Ministerio de Finanzas.

3.6.4 Controles para el proceso de revisión de acceso de usuarios

3.6.4.1 Procedimiento de registro y seguimiento de cuentas de usuarios temporales en el sistema eSigef

El objetivo de este control es mantener un registro y seguimiento de aquellas cuentas que temporalmente se encuentran asignadas a un funcionario operativo encargado por algún período de tiempo.

Por acuerdo ministerial solo existirá un usuario Administrador Informático (Responsable del Área Informática) el cual administrará, gestionará y será responsable de los usuarios operativos que se encuentren en el sistema, por tal

motivo dicho administrador mantendrá un control y registro de los usuarios temporales del sistema. Para tal control se podrá utilizar el formato de la figura 14 para el registro de usuarios temporales:

FORMULARIO DE REGISTRO DE USUARIOS TEMPORALES DEL SISTEMA					
Datos del Funcionario				Fecha de registro:	
Número de Cédula:	1234567890			30-11-2015	
Nombre y Apellido	Carlos Perez				
Cargo / Área	Especialista Contabilidad				
Sistema	eSigef___	Spryn ___	ByE ___	eSiprem_____	Otros _X__
Aplicación	Tesorería/Contabilidad/				
Cuentas de usuario utilizadas	Usuario_lectura				
Nivel de Acceso	Lectura/Consulta				
Fecha de revocación de acceso:	30-12-2015				
Justificación y detalle de las actividades y funciones a realizar con la cuenta asignada en el sistema y aplicación.					
Se requiere tener acceso lectura de las diferentes cédulas presupuestarias de la institución. Nota: En caso de no tener fecha límite de revocación de acceso al sistema, indicar en esta sección los motivos o justificación.					
Solicitante: Nombre:	Revisado: Propietario de Información			Ejecutado Responsable del Área Informática	

Figura 14: Formulario registro de usuarios temporales

3.6.4.2 Procedimiento de revisión periódica de cuentas de usuarios desvinculados de la institución y activos en el sistema eSigef

El objetivo de este control es minimizar el riesgo de mantener usuarios activos en el sistema eSigef y que hayan sido desvinculados de la institución. El riesgo de tener accesos no autorizados al sistema puede ocasionar que se realicen transacciones no autorizadas días posteriores que el funcionario haya salido de la institución.

El Administrador Financiero solicitará vía correo electrónico al Administrador Informático, una revisión y depuración quincenal de los usuarios del sistema eSigef.

El Administrador Informático solicitará a Talento Humano las bajas o salidas de personal de la última semana. Para una primera revisión y depuración se solicitará el reporte total de los empleados o nómina activos o pasivos, indicando número de cédula, nombre, cargo, entre otros datos importantes de los usuarios.

El Administrador Informático manejará su registro con el formato, tabla 7, de ejemplo para el reporte entregado por Talento Humano:

Tabla 7:
Registro reporte Talento Humano

Cédula	**Nombre del empleado**	**Puesto/Cargo**	**Sucursal**	**Fecha de ingreso**	**Fecha de Salida**
1234567890	Juan Carlos Pérez Pérez	Servidor Público 5	Guayaquil	01/05/2012	13/03/2014

El Administrador Informático realizará la obtención del reporte de usuarios activos en el sistema, como se indica a continuación:

En la figura 15 se muestra la pantalla inicial de ingreso, que el Administrador Informático debe ingresar.

Figura 15: Pantalla de inicio de sesión eSigef

Fuente: (eSigef, 2013)

Una vez ingresado al sistema se debe dirigir a la sección de reportes para obtener un listado de los usuarios del sistema, figura 16:

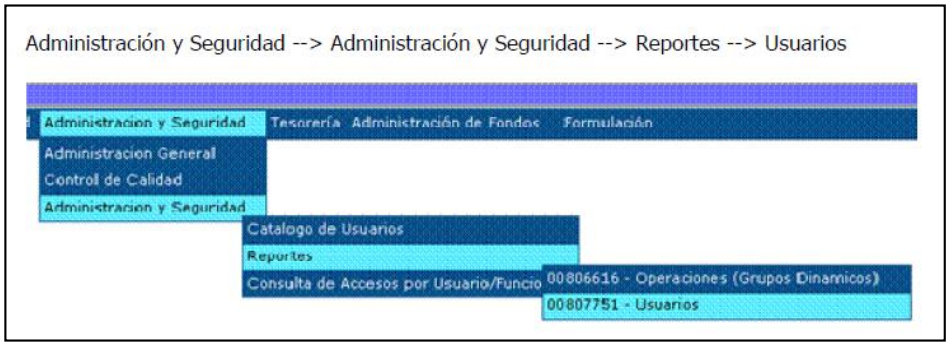


Figura 16: Reporte usuarios

Fuente: (eSigef, 2013)

Una vez seleccionada esta opción se tendrá la siguiente pantalla, con las opciones de filtrado para obtener el reporte de usuarios, figura 17:

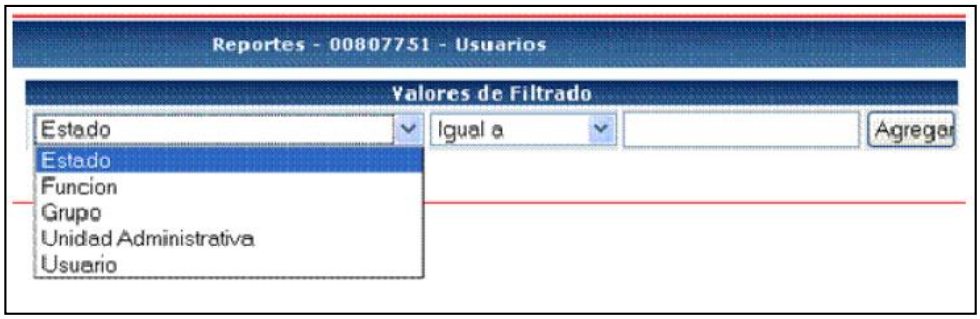


Figura 17: Búsqueda filtrado de usuarios

Fuente: (eSigef, 2013)

Para la revisión de los usuarios activos, se seleccionará la opción “Estado” la cual permitirá identificar a usuarios en estado: Activado o Desactivado como se indica en la figura 18:

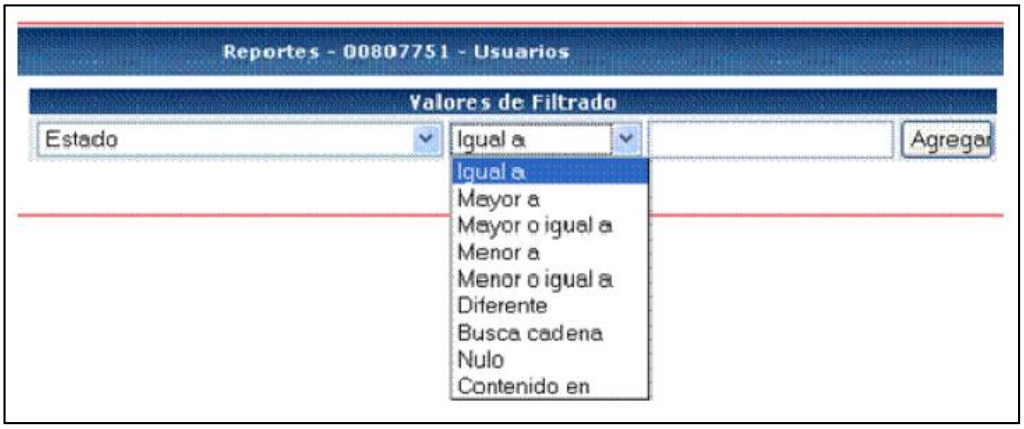


Figura 18: Búsqueda por valor o parámetro

Fuente: (eSigef, 2013)

En este caso se seleccionará el filtro “Igual a”: ACTIVADO, y se hará clic en el botón agregar, el cual aplicará el filtro, figura 19:

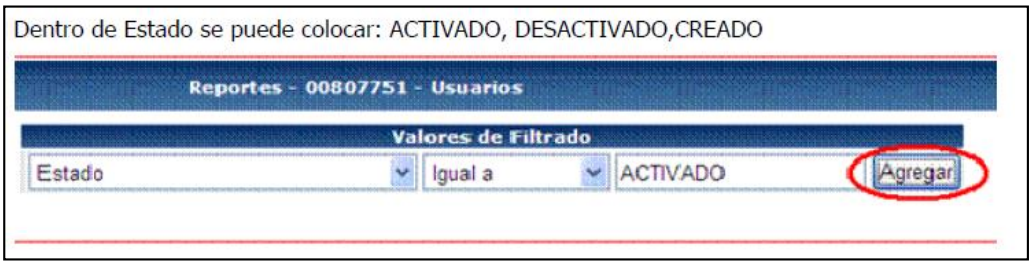


Figura 19: Búsqueda por filtro activado

Fuente: (eSigef, 2013)

En la figura 20 se muestra la operación realizada anteriormente:

Figura 20: Resultado de la búsqueda

Fuente: (eSigef, 2013)

Luego se podrá seleccionar el formato del archivo para el reporte: pdf, Excel o archivo plano, luego se debe presionar el botón “Continuar”, figura 21:

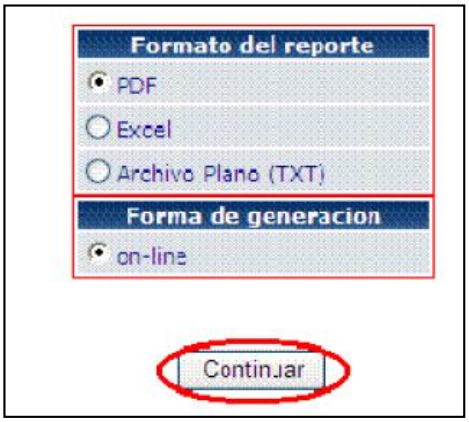


Figura 21: Exportar reporte en varios formatos

Fuente: (eSigef, 2013)

El Administrador Informático manejará en su registro un formato similar a lo indicado en la tabla 8.

Tabla 8:
Registro de usuario sistema eSigef

Código de Usuario	**Nombre**	**Login**	**Rol o Perfil**	**Estado**	**Fecha de creación**	**Fecha último acceso al aplicativo**
123	Juan Carlos Pérez Pérez	jperez	Analista Presupuesto	Activo	10/05/2012	13/03/2014

El Administrador Informático una vez que cuente con ambos reportes: a) Reporte de funcionarios pasivos de la última semana, y b) Reporte de usuarios activos del sistema eSigef, procederá a realizar una verificación manual uno a uno verificando el Reporte a) contra el Reporte b). En caso de existir algún usuario activo en el sistema y que conste como empleado o funcionario pasivo o desvinculado de la institución, procederá a realizar la desactivación o baja del mismo en el sistema.

El Administrador Informático realizará las siguientes actividades para desactivar al usuario:

Ingresará al Catálogo de usuarios, en el cual se mostrará el listado de usuarios activos del sistema, y mediante la herramienta de búsqueda, se localizará al usuario como se indica en la figura 22:

Figura 22: Listado de usuarios del sistema

Fuente: (eSigef, 2013)

En el campo usuario, seleccionar el operador a “igual” ingresar el valor (cuenta del usuario) y dar clic en aplicar criterios, como se muestra en la figura 23:

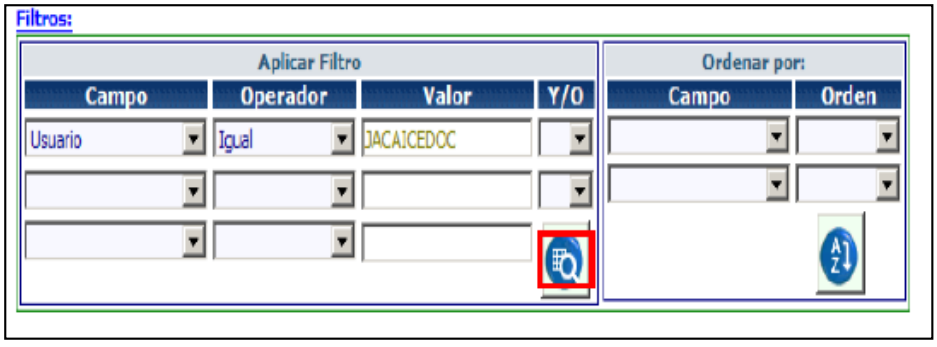


Figura 23: Búsqueda por filtro o parámetro de usuarios

Fuente: (eSigef, 2013)

Posteriormente el Administrador Informático deberá seleccionar la opción de "Desactivar" para dar de baja al funcionario desvinculado de la institución, como se indica en la figura 24:

Figura 24: Desactivación de usuarios

Fuente: (eSigef, 2013)

Para completar el procedimiento el Administrador Informático deberá mantener un registro de las bajas realizadas, este registro podrá ser sujeto de revisión por parte del Oficial de Seguridad de la Información de cada entidad. El registro de control podrá tener el siguiente formato, tabla 9:

Tabla 9:
Registro de bajas realizadas

Fecha de Revisión:	14 Marzo 2014	**Hora de Revisión inicio:**	18:25
		Hora de Revisión fin:	18:40
Nombre del Funcionario	**Existe en el sistema**	**Estado**	**Acción realizada**
Pérez Pérez Juan Pablo	NO	-	-
Caicedo Cárdenas José Alberto	SI	Activo	Desactivado
Borja Chávez Felipe Juan	SI	Desactivo	-

……..			
Realizado por: Nombre Administrador Informático		**Revisado por:** Nombre Responsable de Seguridad de TICs	
Observaciones:		**Observaciones:**	

El Administrador Informático, previa revisión por parte del Responsable de Seguridad de TICs, enviará el formato de revisión realizada al Administrador Financiero con copia al Oficial de Seguridad de la Información y Talento Humano.

Finalmente el Administrador Informático subirá el registro o bitácora de revisiones enseguida termine el proceso, con el siguiente formato de nombre: *NombreInstitución_Revision_Periódica_DiaMesAño.xlsx.*

3.6.5 Controles para el proceso de Gestión de contraseñas para usuarios

A continuación se describen dos controles que deben implementar las instituciones

3.6.5.1 Obligaciones de los usuarios

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de contraseñas:

- No se deben revelar las contraseñas a otras personas, incluyendo a los jefes inmediatos y a los administradores del sistema.
- No se debe llevar un registro de contraseñas, a menos que un método seguro haya sido aprobado por el Oficial de Seguridad de la Información.
- Las contraseñas generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las contraseñas deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas contraseñas o el sistema (en ese caso, se debe informar un incidente de seguridad de acuerdo a los procedimientos internos de la institución).
- Se deben escoger contraseñas seguras de la siguiente forma:
    - utilizando al menos ocho caracteres;
    - utilizando al menos un carácter numérico;

  - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;
  - utilizando al menos un carácter especial;
  - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;
  - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
  - no se deben usar nuevamente las últimas tres contraseñas.
- Se deben cambiar las contraseñas cada 3 meses.
- Se deben cambiar las contraseñas en el primer ingreso al sistema eSigef.
- Las contraseñas no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- No se deben utilizar las mismas contraseñas personales para fines privados y para fines personales.

3.6.5.2 Gestión de la contraseña del usuario

Cuando se asignan y utilizan contraseñas de usuarios, se deben seguir las siguientes reglas:

- Al firmar el acuerdo de confidencialidad los usuarios también aceptan la obligación de mantener sus claves en forma confidencial.
- Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la posibilidad de escoger su propia contraseña, en los casos corresponda.
- Las contraseñas utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo establecido precedentemente.
- Las contraseñas de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.
- El usuario debe confirmar la recepción de la contraseña vía correo electrónico.

- La contraseña no debe ser visible en la pantalla durante el inicio de sesión.

3.6.6 Controles para el proceso de Monitoreo del uso del sistema

Es importante contar con un monitoreo del uso del sistema realizada por el Propietario de la Información, con el apoyo de los involucrados de los procesos inmersos en el uso del sistema.

3.6.6.1 Registros y revisión de logs de administrador y operador

La siguiente política o norma deberá ser aplicada en las instituciones, es política de la institución:

Solicitantes de eventos a registrar

- El Oficial de Seguridad de la Información de la institución es responsable de la definición de los eventos de seguridad a ser registrados automáticamente en el sistema.
- Exclusivamente el Administrador Financiero podrá solicitar al Oficial de Seguridad de Información la registración de eventos adicionales en la medida que se correspondan con su información o personal a su cargo.
- Para situaciones de excepción, el Administrador Financiero y/o Talento Humano, puede solicitar la registración de eventos de algún usuario.

Tipos de eventos

- Se deben registrar todos los eventos relacionados con las configuraciones de seguridad en el sistema.

Acceso a los registros

Exclusivamente el Oficial de Seguridad, podrá acceder a los registros de eventos de seguridad en la medida que lo permita el sistema.

Eventos generales a registrar para todos los usuarios

- Accesos fallidos de ingreso de usuarios

- Alta, baja o modificación de usuarios y grupos
- Cambios en la configuración de la seguridad

Eventos especiales

- Todos los accesos no autorizados a información clasificada como de acceso autorizado.
- Todos los eventos de un usuario cuando sean específicamente solicitados.
- Todos los accesos para cualquier usuario que acceda a la información clasificada como sensible.
- Todos los accesos del Administrador Informático, de los usuarios de máximo riesgo y de los usuarios especiales.

Para el resto de los eventos, debe definir la opción de suspender la registración o escritura de los registros.

Acciones ante situaciones de anormalidad

El Responsable de Seguridad de TICs deberá:

- Analizar semanalmente las revisiones sobre los eventos y registros del sistema.
- Informar al Oficial de Seguridad de la Información ante incidentes observados.

El Oficial de Seguridad de la Información debe informar al Administrador Financiero, y de ser el caso convocar al Comité de Seguridad de cada institución a fin de tratar los casos de mayor importancia y dictaminar resoluciones pertinentes dentro de su ámbito de acción.

3.6.7 Otros controles adicionales

3.6.7.1 Control de capacitación y concientización de normas básicas de seguridad y normativa legal vigente

Como medida proactiva las entidades podrán solicitar al Ministerio de Finanzas e capacitaciones en temas de seguridad informática para los Administradores

Informáticos, Financieros y Responsable de Seguridad, específicamente en el cumplimiento y aplicación de los controles de seguridad a aplicarse.

El Ministerio de Finanzas podrá otorgar un certificado y licencia de autorización para el uso del sistema eSigef una vez que los usuarios de las instituciones hayan participado y aprobado dichos cursos.

3.6.7.2 Control de revisiones independientes

El Oficial de Seguridad de la Información de cada institución podrá ser contraparte ante el Ministerio de Finanzas para el control, seguimiento y mejoras para la implementación y aplicación de los controles propuestos.

El Ministerio de Finanzas podrá realizar las revisiones independientes que tuviere lugar de manera aleatoria a las entidades usuarias del sistema, del mismo modo tendrá la autorización de solicitar a los funcionarios administradores informáticos y financieros los reportes que considere pertinentes.

3.7 Cuadro general de controles de seguridad para las instituciones

En la tabla 10 se resumen los responsables, frecuencia de ejecución y archivos verificables para un control por parte de las autoridades de cada institución.

Tabla 10:
Resumen controles de seguridad

Código del Control	Control	Responsable	Frecuencia de Ejecución	Verificable
1.1	Registro de usuarios	Administrador Informático	Continuo	Escaneado del registro o bitácora de creación de usuarios
1.2	ABM de acceso de usuarios	Administrador Informático	Continuo	Escaneado del registro o bitácora de modificaciones de permisos de acceso
1.3	Bajas de usuarios	Administrador Informático	Continuo	Escaneado del registro o bitácora de bajas de usuarios

2.1	Revisiones periódicas de cuentas de usuarios desvinculados de la institución	Responsable de Seguridad Informática	Cada 15 días	Archivo NombreInstitución_ Revision_Periodica_ DiaMesAño.xlsx.

3.8 Nivel de madurez a implementar en las instituciones

En resumen, cada institución deberá adoptar las medidas necesarias para alcanzar al menos un nivel de madurez 3 (Definido) en los procesos de administración de usuarios en lo que respecta al manejo y uso del sistema eSigef.

De acuerdo a la información adicional identificada en las entrevistas se evidenció que existe en promedio un nivel de madurez 0 y 1 en la gestión de usuarios, por lo tanto es importante que las instituciones internamente incorporen procesos o procedimientos en la gestión de usuarios a un nivel 3 utilizando las mejores prácticas de seguridad de acuerdo a lo que indica la norma ISO 27002; el enfoque a procesos permitirá alcanzar un nivel de madurez adecuado en la gestión de usuarios, con lo cual podrán ser medidos y se conseguirá la mejora continua de los mismos.

CAPÍTULO IV
CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En el presente estudio y evaluación realizada se ha podido determinar que existen falencias en la gestión de usuarios en las instituciones y por tanto puntos de mejora en la gestión de los mismos en las instituciones en lo que respecta a: registro de usuarios, gestión de privilegios del sistema, con el fin de mejorar los procedimientos formales respectivos, para cumplir lo que dispone la normativa legal de los entes de control.

La teoría del fraude determinó que son involucrados los tres elementos según lo plantea el triángulo del fraude, motivo, oportunidad percibida, y racionalización, es importante entender los actos fraudulentos cometidos dentro de las organizaciones; un entendimiento profundo permitirá tener elementos que determinen las causas principales por las cuales se cometen estos actos. Al tener claro las causas que provocaron estos actos, permitirá establecer las acciones necesarias para contrarrestar estos hechos, como por ejemplo la aplicación de controles de seguridad informática y de la información, con el uso de políticas, normas y procedimientos que permitan minimizar el riesgo de posibles actos delictivos como lo constituye la malversación de fondos públicos, el enriquecimiento ilícito, entre otros.

La evaluación de riesgos efectuada, tomando como metodología la norma ISO 27005, determinó que existen riesgos en la gestión de usuarios en las instituciones, estos riesgos fueron determinados cualitativamente dando como resultado los de mayor riesgo el registro, modificación y cancelación de permisos, gestión de privilegios o permisos de usuarios y revisiones de la gestión.

Respecto a los controles de seguridad diseñados, al ser controles de gestión más que técnicos, resultan eficaces su aplicación por cuanto no se requiere de un mayor esfuerzo en determinar las brechas de seguridad y con esta el diseño de controles específicos, son prácticas de seguridad afinadas a la realidad del control considerando un nivel de madurez administrado o gestionado.

Las instituciones deben revisar íntegramente toda la documentación habilitante para el uso del sistema por parte de los usuarios operativos. Esta documentación de carácter obligatorio indicada en el Acuerdo N° 163 del Ministerio de Finanzas, acuerdos de confidencialidad y responsabilidad, formularios de creación, entre otras.

Es responsabilidad de las instituciones establecer procedimientos o procesos formales respecto a la desvinculación de usuarios, con el fin de desactivarlos en el sistema dentro del proceso normal de salida del usuario o en el caso de alguna notificación emergente que amerite la desactivación inmediata.

Las instituciones deben contar con una gestión de privilegios o permisos, con el fin de tener registros de la identificación del usuario con sus permisos asignados respectivamente, los cuales deben estar dados en función a criterios tanto de funciones como de tipo de solicitud, adicionalmente los mismos deberán ser registrados por el Administrador Informático con la finalidad de dar un sustento en casos de auditorías. Se deben establecer mecanismos de control y monitoreo de actividades del uso del sistema para lo cual se debe valer lo que indica la norma técnica ecuatoriana NTE ISO/IEC 27002.

Las mejores prácticas deberán acogerse en base a lo que en la norma ecuatoriana NTE ISO/IEC 27002 se indique y además hacer referencia a la normativa legal vigente en materia de seguridad de la información.

4.2 Recomendaciones

Se recomienda que se realicen actividades de control interno mediante la aplicación de controles preventivos: monitoreo del uso del sistema, revisión de registros de auditoría y logs de seguridad, estas actividades de control permitirán conocer de manera temprana alguna desviación o no conformidad con la normativa, las citadas pueden ser aplicadas en cualquier entidad pública o privada ya sean estas pequeñas o medianas.

Se recomienda implementar controles para la segregación de funciones y que estas sean reflejadas en la utilización del sistema, poniendo mayor énfasis los componentes o módulos transaccionales donde se manejan estados financieros, de contabilidad, tesorería y presupuesto. El control tiene como objetivo que exista una

segregación o separación de funciones entre actividades incompatibles como por ejemplo quien realiza un pago no debe ser quien lo autoriza.

Se recomienda estudiar a fondo los casos de fraudes financieros tanto a nivel nacional como internacional desde un punto de vista integral considerando el aspecto psicológico de las personas que lo cometen, por cuanto esto permitirá determinar que controles se podrían implementar, hay que tomar en cuenta que las circunstancias o condiciones con el pasar del tiempo cambian, puede ser posible que lo que por ahora no es una causa o motivo para cometer fraude interno, le día de mañana puede serlo.

Respecto a la evaluación de riesgos realizada en el presente trabajo se recomienda que sean referenciados como modelo para que en lo posterior la metodología pueda ser aplicada en las instituciones, a esto se recomienda se realice una evaluación propia en la gestión de usuarios a fin de que se identifiquen riesgos particulares. Se recomienda se realice un monitoreo de la matriz de riesgo realizada por cuanto con el tiempo los controles así como los procesos puede variar según los cambios externos y organizaciones.

En la aplicación de los controles diseñados se recomienda sean sometidos a revisiones periódicas constante por parte de alguna o todas las partes interesadas, siendo de esta manera su posible mejora continua protegiendo los recursos financieros que actualmente son escasos y por ende es necesaria su correcta y estratégica ejecución.

La aplicación de las mejores prácticas de seguridad norma NTE ISO/IEC 27002 objetivo del presente proyecto permitirá minimizar el riesgo de desvíos de fondos o fraudes financieros que podrían ser cometidos por personas inescrupulosas para su beneficio propio. Es importante indicar en este punto los controles diseñados en el presente son la base para el control interno dentro de las instituciones las cuales podrán ser reforzados con la utilización de otros controles indicados en dicha norma, es decir relacionados con procedimientos disciplinarios, mejoras en la seguridad técnica y funcional del sistema y otros.

Se recomienda la aplicación de estos controles en cualquier sistema transaccional o activo de información de soporte que represente ser crítico para la institución y que

pueda estar enmarcado dentro de un proceso de gestión de riesgos de seguridad de la información.

BIBLIOGRAFÍA

ACFE - "Association of Certified Fraud Examiners". (2010). *Reporte a las Naciones sobre el Fraude Ocupacional y el Abuso.* Mexico.

AICPA, American Institute of Certified Public Accountants. (1987). *Report of the National Commission on Fraudelent Financial Reporting Treadway Commission.* New York.

Alarcón, D. C. (Abril de 2009). EVALUACIÓN DE CONTROLES INFORMÁTICOS ADMINISTRATIVOS EN LA. Sangolquí, Pichincha, Ecuador.

Andagana, M. (Septiembre de 2009). Auditoría de riesgos informáticos en el Departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social. Quito, Pichincha, Ecuador.

Badillo, J. (2012). *7 Teorías Clave para Conocer, Comprender y Combatir el Fraude.* Paraguay.

Badillo, J. (2012). Auditoria Basada en Riesgos. Quito, Pichincha, Ecuador.

Clark, C. B. (14 de April de 2009). Fraud Prevention and Detection. Texas, EEUU.

Cobit4.1. (2007). Cobit4.1.

Contraloría General del Estado. (2009). Normas del Control Interno.

DNA. (1999). *La Consideración del fraude en los Estados Financieros.*

ElUniverso. (01 de 07 de 2012). Obtenido de http://www.eluniverso.com/2012/07/01/1/1355/mas-investigaciones-desvio-fondos-publicos.html

Kosutic, D. (2012). *Ciberseguridad en 9 pasos.* EPPS Services Ltd, Zagreb.

Krause, H. F. (2007). *Information Security Management Handbook.* Boca Raton, Florida: AUERBACH PUBLICATION.

LaHora. (01 de 07 de 2013). Obtenido de http://www.lahora.com.ec/index.php/noticias/show/1101528718#.Utbq6NLuKGM

Leon, J. (2012). El Cibercrime. Quito, Pichincha, Ecuador.

Ministerio de Finanzas. (22 de Octubre de 2010). Código Orgánico de Planificación y Finanzas Públicas. *Código Orgánico de Planificación y Finanzas Públicas*. Quito, Pichincha, Ecuador: Registro Oficial Suplemento #306.

Ministerio de Finanzas Acuerdo Ministerial N° 163. (24 de 1 de 2008). Acuerdo Ministerial N° 63. Quito, Pichincha, Ecuador.

Norma NTE INEN - ISO/IEC 27001. (s.f.).

Rodríguez Berzosa, L. (2012). Recuperado el 12 de 12 de 2013, de http://www.iec.csic.es/CRIPTONOMICON/articulos/expertos69.html

seguinfo. (24 de 07 de 2007). *seguinfo*. Obtenido de https://seguinfo.wordpress.com/2007/07/24/%C2%BFque-es-fraude-y-estafa-2/

Telegrafo. (12 de 01 de 2013). Obtenido de http://www.telegrafo.com.ec/justicia/item/suman-52-vinculados-en-proceso-por-desvio-de-fondos-publicos-en-el-ministerio-del-ambiente.html