ANÁLISIS DEL NIVEL DE SEGURIDAD DE LOS ROLES Y PRIVILEGIOS, EN EL SISTEMA SAP ERP DE COLPENSIONES, TOMANDO COMO REFERENCIA LA NORMA ISO 27001 Y LAS GUÍAS DE SEGURIDAD DE SAP

CESAR OCTAVIO FARFAN CORREA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION SEGURIDAD INFORMATICA
CEAD JOSE ACEVEDO Y GOMEZ
2017

ANÁLISIS DEL NIVEL DE SEGURIDAD DE LOS ROLES Y PRIVILEGIOS, EN EL SISTEMA SAP ERP DE COLPENSIONES, TOMANDO COMO REFERENCIA LA NORMA ISO 27001 Y LAS GUÍAS DE SEGURIDAD DE SAP

CESAR OCTAVIO FARFAN CORREA

PROYECTO DE SEGURIDAD INFORMÁTICA

Asesor:
JOSE HERNANDO PENA HIDALGO
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION SEGURIDAD INFORMATICA
CEAD JOSE ACEVEDO Y GOMEZ
2017

Nota de Aceptación

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá 18 julio de 2017

AGRADECIMIENTOS

El presente trabajo está dedicado a toda mi familia y amigos que me han apoyado y motivado para cumplir con este reto y poder continuar así con mi crecimiento profesional.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

El modelo de roles y privilegios que se tiene implementado actualmente en Colpensiones carece de un adecuado análisis en los procesos que se manejan en esta organización, lo que genera riesgos en la seguridad de la información, conflicto de segregación de funciones y dificultad en la administración de los mismos, por tal motivo es importante realizar un levantamiento de información por cada área de la organización que permita identificar los procesos del negocio ejecutados, los actores que intervienen en este proceso y reestructurar el esquema de roles y privilegios, logrando así garantizar la integridad, confiabilidad y disponibilidad del sistema de información ERP SAP apoyados en la norma internacional ISO 27001.

1. PLANTEAMIENTO DEL PROBLEMA

El modelo de seguridad que se encuentra actualmente implementado no cuenta con la correcta asignación de roles y privilegios en el sistema ERP SAP, lo cual genera conflicto de segregación de funciones y se materializa como un riesgo, que puede generar traumatismos en la operación, por tal motivo es importante tomar como referencia la norma internacional ISO 27001 y realizar el análisis de la seguridad de los roles y privilegios en el sistema ERP de Colpensiones partiendo del principio del menor privilegio que garantice acceso a funcionarios de acuerdo a su cargo o función en el interior de la organización.

1.1 DESCRIPCIÓN DEL PROBLEMA

Esquema de roles y privilegios en Colpensiones que carece de un adecuado análisis de seguridad en cuanto a sus roles, privilegios, flujo de autorización para la asignación de los permisos y control sobre el ciclo de vida de los usuarios que ponen en riesgo la integridad, confidencialidad y disponibilidad de la información.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede garantizar una correcta configuración de permisos y asignación adecuada de los mismos a través de roles en el sistema ERP SAP implementado en Colpensiones, tomando como referencia la norma ISO 27001?

2. JUSTIFICACION

El análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones se realizó con el fin de garantizar la adecuada configuración del sistema de información a través de roles que garanticen la correcta segregación de funciones, mitigando así los riesgos que puedan afectar la integridad, disponibilidad y confidencialidad de la información.

Lo anterior beneficio no solo al grupo de gestión de accesos y roles en su proceso diario de administración, si no al resto de las áreas de la organización quienes podrán estar seguros de que los accesos solicitados cuentan con un respectivo ciclo de certificación en el cual los funcionarios designados por cada área ejecutaran sus procesos de negocio en el ambiente de pruebas del sistema de información SAP, realizaron la documentación de las mismas y la entregaran al gestor de roles para que procediera a realizar el transporte de roles al sistema productivo este proceso se realizó partiendo del principio del menor privilegio, adicionalmente el proceso para solicitud de acceso a los módulos de SAP contara con un respectivo flujo de autorización que brindara a los solicitantes acceso oportuno al sistema de información y trazabilidad en las solicitudes realizadas ya que estás serán centralizadas en la mesa de servicios de la organización mediante requerimientos internos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones que se tienen actualmente implementados en Colpensiones.

3.2. OBJETIVOS ESPECÍFICOS

- Realizar un informe con el análisis de riesgo que permita identificar la situación actual del modelo de roles y autorizaciones del sistema SAP.
- Realizar un estudio de metodologías y herramientas que puedan ser utilizadas para el desarrollo del proyecto.
- Generar política que contemple los lineamientos que deben ser tenidos en cuenta para los roles que por necesidad del negocio presenten conflicto de segregación de funciones.
- Definir e implementar controles que permitan garantizar el ciclo de vida de los usuarios en la organización.

4. MARCO REFERENCIAL

4.1. ANTECEDENTES

El proyecto denominado “Reingeniería de perfiles de seguridad informática para SAP unificado para la empresa Ternium”, presentado por Juan Fuentes en la Universidad de los Andes Mérida de Venezuela. En el proyecto se explica el proceso de reingeniería de perfiles para el activo de información SAP. Este proyecto servirá como referencia para el iniciar con el análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones de la reestructuración de roles y privilegios que se tiene actualmente implementado en Colpensiones.

El proyecto implantación de un sistema ERP SAP en una empresa presentado por Enrich Cardona, Roger de la universidad politécnica de Catalunya. De este proyecto se pretende extraer información que permita fortalecer el esquema de roles que se tiene actualmente en Colpensiones, al revisar el detalle de este proyecto de evidencia que cuenta con la metodología especifica que involucra desde su fase de preparación del proyecto todos los aspectos que se deben tener encuentra para lograr una implementación de calidad que brinde a las áreas funcionales de la organización la integración necesaria para que su ERP sea eficiente y administrable en su línea de tiempo.

4.2 MARCO CONTEXTUAL

El proyecto se implementará en la Administradora Colombiana de Pensiones Colpensiones, la cual es una empresa industrial y comercial del estado, organizada como entidad financiera de carácter especial, vinculada al ministerio de trabajo.

Decreto número 2011 DE 2012 del 28 de septiembre de 2012 por el cual se determina y reglamenta la entrada en operación de la Administradora Colombiana de Pensiones- COLPENSIONES y se dictan otras disposiciones:

La Administradora Colombiana de Pensiones - COLPENSIONES, hace parte del Sistema General de Pensiones y tiene por objeto la administración estatal del Régimen de Prima Media con Prestación Definida, las prestaciones especiales que las normas legales le asignen y la administración del Sistema

de Ahorro de Beneficios Económicos Periódicos de que trata el Acto Legislativo 01 de 2005, en los términos que determine la Constitución y la Ley, en su calidad de entidad financiera de carácter especial.

Organigrama y equipo Humano

Figura 1 Organigrama Colpensiones

Fuente: https://www.colpensiones.gov.co/publicaciones/es-O/116/Nuestro_Equipo

4.3 MARCO TEÓRICO

Para el proyecto análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones que se tiene actualmente implementado en Colpensiones se definen los siguientes temas: ISO/IEC 27001-.2013, ISO 31000:2009 administración de riesgos, normas, ISO/IEC 27002, SAP ADM 900 fundamentos de seguridad, SAP ADM 940 conceptos de autorización y SAP ADM 950 administración de la auditoria de SAP, los cuales fundamentan las buenas prácticas que se deben tener en cuenta para lograr el ciclo de vida de los usuarios en cuanto a manejo de ausentismos, vacaciones, incapacidades, retiros garantizando así el buen manejo de novedades reportados por la

organización y mitigando así los riesgos que se puedan presentar en la organización en cuanto a la fuga de información y manejo del ciclo de vida del usuario.

Dentro de la terminología de SAP se relaciona a continuación varios aspectos que se deben tener en cuenta a la hora de iniciar con el proceso de análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones, dado que son esenciales para el fortalecimiento del proceso que brinde a la organización la confianza necesaria para apoyar el proceso y articular las áreas de negocio que están involucradas en el mismo.

Tabla 1 Variables De Seguridad

Variable	Características	Controles
Roles	Brindan al usuario acceso a los recursos del sistema de acuerdo con las transacciones que lo componen.	Validar que las transacciones que componen los roles no presenten conflicto de segregación de funciones.
Parámetros de contraseñas	Hacen referencia a los lineamientos que se deben aplicar para que las contraseñas cumplan con un nivel de seguridad óptimo.	Validar que se cumplan los siguientes requisitos: Longitud mínima de la contraseña 8 caracteres. Que estas caduquen cada cierto tiempo, bloqueo por intentos fallidos, diccionario de contraseñas conocidas y la correcta asignación de contraseñas a cuentas administradoras.
Privilegios	Los privilegios en los sistemas de información brindan la oportunidad de acceso o no acceso a esta, se debe partir siempre del principio del menor privilegio.	Validar que los privilegios asignados son los que el funcionario requiere para cumplir su función.
Súper usuarios	Los usuarios administradores o súper usuarios son los que cuentan con acceso total al servidor a nivel de privilegios del sistema, generalmente es recomendable segregar este usuario y proceder con el bloqueo del mismo.	Validar que el uso de estos usuarios se encuentre restringido, en caso de que sean usados se debe documentar el motivo por el cual es usado soportado por la autorización de la alta gerencia.

Tabla 1. (Continuación)

Variable	Características	Controles
Actualizaciones del sistema	Brindan a los servidores soluciones a fallas de seguridad, fallas en sus elementos de configuración la aplicación responsable de estas actualizaciones mitiga riesgos en la operación diaria.	Validar que los servidores de la organización cuenten con una política centralizada de actualizaciones periódicas de sus sistemas y su respectivo control de cambios. Recomendado por el fabricante o por el repositorio central.
Objetos de autorización	Compilan los tipos de permisos que internamente pueden tener dichos roles	Validar que los objetos de autorización críticos del sistema cuenten con solo actividad de visualizar.

Fuente: El autor

4.4 MARCO CONCEPTUAL

4.4.1. ISO 27001

Modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

4.4.2. ISO 31000:2009

Brinda los principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.

4.4.3. Vulnerabilidad

Debilidad de los sistemas de información que pueden ser utilizada de forma maliciosa con fines destructivos, lucrativos y en algunos casos solo por obtener reconocimiento y que puede afectar de forma considerable los pilares centrales de la seguridad informática como lo son la integridad, confidencialidad y disponibilidad de la información.

4.4.4. Amenaza

Posibles problemas que pueden afectar la disponibilidad, integridad, confidencialidad y seguridad de la información en las organizaciones.

4.4.5. Riesgo

La materialización de una amenaza que aprovecha una vulnerabilidad expone a las organizaciones y sus activos de información.

4.4.6. Principio del menor Privilegio

En seguridad de la información, el principio de mínimo privilegio se fundamenta básicamente en brindar la autorización necesaria para que los usuarios realicen las operaciones requeridas sin exceder sus funciones dentro de los sistemas de información a los cuales se les otorgo el acceso.

4.4.7 Confidencialidad

La información debe ser accesible sólo a aquellas personas autorizadas.

4.4.8. Integridad

La información y sus métodos de procesamiento deben ser completos y exactos.

4.4.9. Disponibilidad

La información y los servicios deben estar disponibles cuando se le requiera.

4.4.10. Segregación de funciones

La segregación de funciones es el método que usa para separar las responsabilidades a la hora de la ejecución de los procesos garantizando un correcto flujo de aprobación por distintos actores.

4.2. MARCO LEGAL

4.2.1. LEY 1273 DE 2009

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen:

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

4.2.3. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El proyecto análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones se realizó para las siguientes dependencias: Gerencia Nacional Económica, Vicepresidencia de Financiamiento e Inversiones debido a la importancia y criticidad de los procesos que en estas se manejan y que están fuertemente ligados a los pilares fundamentales de la seguridad de la información como lo son la confidencialidad, integridad y disponibilidad de la misma, el proyecto tiene como finalidad asegurar los módulos de SAP CO/HCM/FI (CO: contable y FI, financiero) de esta organización.

5. MARCO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

En el presente proyecto se realizará una investigación cuantitativa, de una población de 200 roles del sistema implementados en la organización y que están dispersos en 162 cuentas de usuario activos del sistema SAP, de los cuales en el proceso de análisis del nivel de seguridad de los roles y privilegios quedaron 51 roles del sistema debidamente segregados y ajustados de acuerdo a los objetos de autorización y actividades del sistema debidamente configurados.

Aplicada, ya que se dará solución a los conflictos identificados de segregación de funciones, riesgos en los procesos ejecutados por las áreas funcionales y facilitará la administración del modelo de creación y asignación de roles y privilegios del sistema SAP.

5.1.2. METODOLOGIA DE DESARROLLO

Para el desarrollo del proyecto se realizaron las siguientes actividades que conllevaron al cumplimiento de cada uno de los objetivos específicos:

5.1.3. Objetivo 1

Realizar análisis de riesgo que permita identificar la situación actual del modelo de roles y autorizaciones del sistema SAP.

Actividades

Elaborar documento donde se identifiquen los riesgos a los que se encuentra expuesto el actual esquema de roles de Colpensiones.

5.1.4. Objetivo 2.

Definir la metodología y las herramientas que se utilizaran para el desarrollo del proyecto.

Actividades

Implementar metodología que permita tener control sobre cada una de las fases necesarias para llevar a cabo el proyecto.

5.1.5. Objetivo 3

Definir los lineamientos y flujos de autorización que se deben tener en cuenta para los roles que por necesidad del negocio presenten conflicto de segregación de funciones.

Actividades

Documentar el listado de roles que presenten conflicto de segregación de funciones con su respectiva justificación y listado de autorizadores.

5.2.6. Objetivo 4

Implementar controles que permitan garantizar el ciclo de vida de los usuarios en la organización.

Actividades

Tomar como referencia la norma ISO 27001 y 27002 para aplicar controles relacionados con los siguientes Ítems: manejo de ausentismos, incapacidades, vacaciones, retiros de la organización esto con el fin de que se pueda dar el manejo adecuado a este tipo de situaciones administrativas con oportunidad y así garantizar la confidencialidad, integridad y disponibilidad de la información.

6. PRODUCTO A ENTREGAR

Al finalizar el proyecto se contará con los siguientes entregables:

- Roles ajustados en el sistema ERP de SAP de acuerdo a la certificación realizada por los funcionarios de cada dependencia que participaron en el proyecto.
- Matriz actualizada de roles y transacciones debidamente certificadas por cada dependencia avaladas por los gerentes de área.
- Formato de gestión de usuarios y privilegios con la relación de los roles ajustados por cada dependencia.
- Documento con el estándar para nombramiento de roles.
- Lineamiento para el manejo que se debe dar a los usuarios con privilegios de administración.
- Documentos con los controles que se deben realizar en el sistema que garanticen el ciclo de vida del usuario.
- Instructivo para el proceso de creación de usuarios y asignación de roles.
- Instructivo para el bloqueo de usuarios e inactivación de los roles.

6.1 RECURSOS NECESARIOS PARA EL DESARROLLO

Los recursos que necesarios para el análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones, se relacionan en la siguiente tabla.

Tabla 2 Recursos para el desarrollo del proyecto

TIPO DE RECURSO	RECURSO	COSTOS
Humano	Profesional SAP Netweaver	$ 4000.000
Tecnológico	Portátil para trabajo en campo.	$ 1600.000
Tecnológico	Internet Móvil	$100.000

Fuente: El autor

7. CRONOGRAMA DE ACTIVIDADES

Tabla 3: Cronograma de Actividades

		Nombre	Duración	% Completado	Inicio	Fin
5	✓	⊟**PLANEACION**	10d	100%	**07/04/2016**	**07/15/2016**
6		Entregar listado de cargos, funciones y transacciones requeridas por área.	10d	100%	07/04/2016	07/15/2016
7		⊟**EJECUCION**	131d?	44%	**07/15/2016**	**12/27/2016**
8	✓	Verificar conflictos de segregación de funciones de la matriz entregada	30d	100%	07/15/2016	08/23/2016
9		Análisis de las transacciones por módulos y agrupación por Roles de acuerdo con	30d	90%	08/23/2016	09/29/2016
10		Entregar matriz depurada notificando conflicto de segregación de funciones.	15d	0%	09/29/2016	10/18/2016
11		Establecer y documentar los lineamientos para soportar los roles que presentan c	10d?	0%	10/18/2016	10/31/2016
12		Construir rol en ambiente de pruebas y asociar los objetos de autorización y ámbit	25d	0%	10/31/2016	11/30/2016
13		Pruebas de los roles generados y certificación de los mismos	15d	0%	11/30/2016	12/19/2016
14		Realizar actualización del formato de gestión de usuarios con los roles certificados	3d	0%	12/19/2016	12/22/2016
15		Configuración del rol en producción.	1d	0%	12/22/2016	12/23/2016
16		Solicitud asignación del roles a los funcionarios de área.	1d	0%	12/23/2016	12/26/2016
17		Asignación de roles a los usuarios autorizados por cada área.	1d	0%	12/26/2016	12/27/2016
18		⊟**CIERRE**	1d	0%	**12/27/2016**	**12/28/2016**
19		Presentación de Cierre del Proyecto (Acta de Cierre)	1d	0%	12/27/2016	12/28/2016

Fuente: El autor

8. DESARROLLO DEL PROYECTO

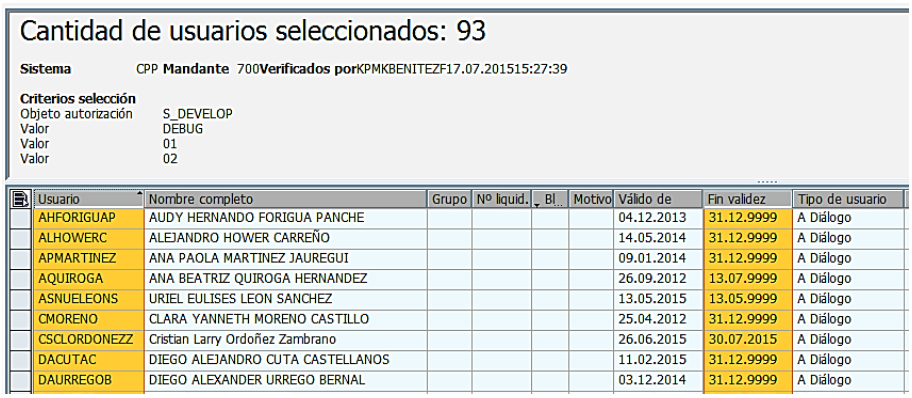
ANALISIS DE RIESGOS

Con el fin de dar viabilidad al proyecto de análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones para la Administradora colombiana de Pensiones Colpensiones se detallan las actividades que se realizaron con el fin de identificar el estado actual de los roles del sistema.

1. Accesos y autorización a la Actividad DEBUG

Se observó en ambiente productivo 73 usuarios con acceso a la ejecución del DEBUG, 67 de ellos son usuarios finales. El total de usuarios en PRD es de 235, más del 28% cuenta con este acceso crítico.

Figura 2 Usuarios Acceso Debug.



Cantidad de usuarios seleccionados: 93

Sistema CPP **Mandante** 700**Verificados por**KPMKBENITEZF17.07.201515:27:39

Criterios selección
Objeto autorización S_DEVELOP
Valor DEBUG
Valor 01
Valor 02

Usuario	Nombre completo	Grupo	Nº liquid.	Bl...	Motivo	Válido de	Fin validez	Tipo de usuario
AHFORIGUAP	AUDY HERNANDO FORIGUA PANCHE					04.12.2013	31.12.9999	A Diálogo
ALHOWERC	ALEJANDRO HOWER CARREÑO					14.05.2014	31.12.9999	A Diálogo
APMARTINEZ	ANA PAOLA MARTINEZ JAUREGUI					09.01.2014	31.12.9999	A Diálogo
AQUIROGA	ANA BEATRIZ QUIROGA HERNANDEZ					26.09.2012	13.07.9999	A Diálogo
ASNUELEONS	URIEL EULISES LEON SANCHEZ					13.05.2015	13.05.9999	A Diálogo
CMORENO	CLARA YANNETH MORENO CASTILLO					25.04.2012	31.12.9999	A Diálogo
CSCLORDONEZZ	Cristian Larry Ordoñez Zambrano					26.06.2015	30.07.2015	A Diálogo
DACUTAC	DIEGO ALEJANDRO CUTA CASTELLANOS					11.02.2015	31.12.9999	A Diálogo
DAURREGOB	DIEGO ALEXANDER URREGO BERNAL					03.12.2014	31.12.9999	A Diálogo

Fuente: El autor

Riesgo inherente asociado

- Omisión del esquema de seguridad
- Accesos ilimitados al sistema

RECOMENDACIÓN

Es recomendable que el acceso a las funciones de desarrollos, incluida la capacidad para modificar programas ABAP esté totalmente restringida en producción. Si se requiere acceso a realizar DEBUG, debe ser asignado a usuarios altamente capacitados, con las autorizaciones correspondientes.
Monitorear los usuarios con acceso a inspeccionar el código fuente de SAP (DEBUG) incluso en ambiente de desarrollo ya que se podría llegar a vulnerar la seguridad del ambiente productivo por un cambio y transporte no deseado. Este modo de ejecución se habilita cuando el usuario cuenta accesos al objeto de autorización S_DEVELOP, campo ACTVT 02 (modificar) y campo OBJTYPE con valor DEBUG.

Implementar controles para salvaguardar el acceso al objeto de autorización S_DEVELOP para asegurar que los cambios en el ambiente productivo son implementados de manera controlada por usuarios autorizados.
Desactivar el acceso a usuarios no autorizados a la opción de DEBUG en producción.

Esta actividad debe estar controlada y asignada únicamente a usuarios de soporte y/o especialistas en el sistema SAP.

2. Accesos a tablas críticas del sistema: S_TABU_DIS

Se observó en ambiente productivo 90 usuarios con acceso a modificar todas las tablas del sistema SAP. Más del 38% del total de usuarios en ambiente PRD, cuenta con la posibilidad de alterar y manipular datos sensibles del sistema.

Figura 3 Acceso Tablas Críticas

Cantidad de usuarios seleccionados: 128

Sistema CPP **Mandante** 700**Verificados por**KPMKBENITEZF28.07.201513:21:02

Criterios selección
Objeto autorización S_TABU_DIS
Valor 02
Valor 01

Usuario	Nombre completo	Grupo	Nº liquid.	Bloq.	Motivo	Válido de	Fin validez	Tipo usuario	U
AALGARRA	ALEXANDRA ALGARRA CALLEJAS			🔒	ADM	01.01.2012	31.12.9999	A Diálogo	
ABELTRAN	ANDREA BELTRAN ESCOBAR					25.04.2012	31.12.9999	A Diálogo	
AHFORIGUAP	AUDY HERNANDO FORIGUA PANCHE					04.12.2013	31.12.9999	A Diálogo	
AIBANEZ	ARELIX DEL PILAR IBAÑEZ QUEVEDO			🔒	ADM	25.04.2012	04.01.2015	A Diálogo	
ALHOWERC	ALEJANDRO HOWER CARREÑO					14.05.2014	31.12.9999	A Diálogo	
AMROMEROC	ANGELA MARIA ROMERO CUPAJITA					06.10.2014	31.12.9999	A Diálogo	
APEREZ	PEREZ REYES ALEJANDRO			🔒	ADM	22.07.2013	18.01.2015	A Diálogo	
APMARTINEZ	ANA PAOLA MARTINEZ JAUREGUI					09.01.2014	31.12.9999	A Diálogo	
AQUIROGA	ANA BEATRIZ QUIROGA HERNANDEZ					26.09.2012	13.07.9999	A Diálogo	
ARAMIREZ	Ana Maria Ramirez					25.04.2012	31.12.9999	A Diálogo	

Fuente: El autor

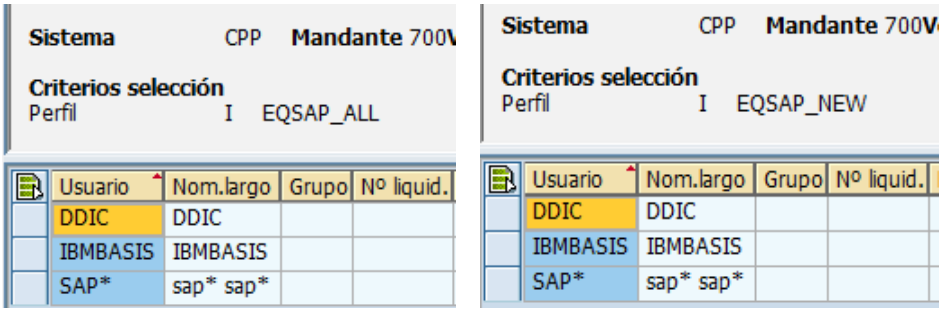
Riesgo inherente asociado

Posibles problemas de integración de la información, redundancia de datos, indisponibilidad del sistema, errores en la consistencia de datos, posible pérdida de información de las operaciones ejecutadas en el sistema.

3. Aseguramiento de Perfiles Críticos

Se identificó en ambiente SAP productivo la asignación de los perfiles SAP_ALL y SAP_NEW a los siguientes usuarios, evidenciando que no se realiza ningún tipo de monitoreo sobre las actividades ejecutadas a través de estos perfiles:

Figura 4 Súper Usuarios SAP



Fuente: El autor

Adicionalmente se observó que no se cuenta con un estándar formalizado para el aseguramiento de los perfiles críticos del sistema SAP (SAP_ALL, SAP_NEW, S_USER_SAP, S_A.SYSTEM, S_SYST_ALL, S_A.SYSTEM, S_A.CUSTOMIZ, S_A.DEVELOP, S_USER_ALL, S_ABAP_ALL). Estos son perfiles estándar de SAP y otorgan accesos absolutos a los usuarios que los posean.

Riesgo inherente asociado

Posibilidad de realizar todas las actividades disponibles en el sistema SAP sin restricción de accesos.

Incapacidad para identificar de manera completa y oportuna las actividades críticas ejecutadas por usuarios.

RECOMENDACIÓN

Documentar los lineamientos para la administración de perfiles críticos en ambientes de DEV, QAS y PRD en SAP, con el fin de restringir el acceso y la asignación de este tipo de permisos.

Realizar una revisión respecto a las actividades realizadas con este perfil por usuarios terceros (IBM), detectando posibles acciones erróneas o fraudulentas. Se sugiere considerar dentro del estándar los perfiles:

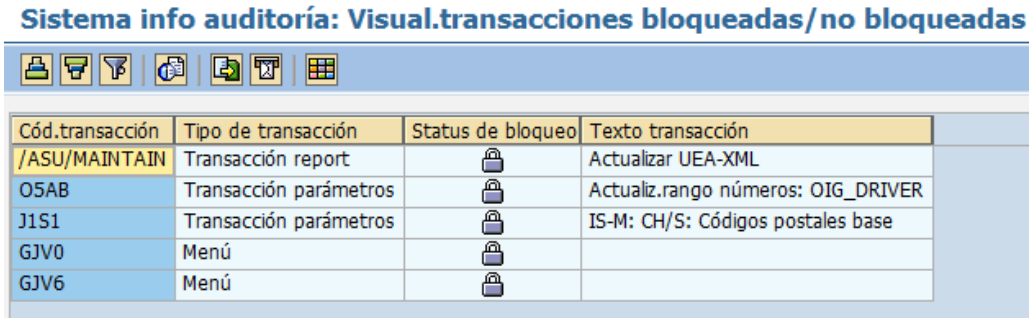
SAP_ALL: Permite acceso ilimitado a todo el Sistema.
SAP_NEW: Proporciona acceso ilimitado a todas las autorizaciones adicionales con nuevas versiones de SAP.
S_A.SYSTEM: Acceso ilimitado a todos los usuarios, perfiles y autorizaciones
S_SYST_ALL: Permite acceder a todas las autorizaciones del sistema.
S_A.CUSTOMIZ: Permite acceder a todas las autorizaciones necesarias para actividades de la configuración del Sistema
S_A.ADMIN: Otorga acceso a autorizaciones para la administración del sistema SAP.
S_A.DEVELOP: Acceso al entorno de desarrollo.
S_USER_ALL: Permite acceder a todas las autorizaciones para el mantenimiento de usuarios.

4. Bloqueo de transacciones críticas en ambiente productivo

Las transacciones críticas SM01 / SM19 / SCC5 / SCCL / SCC9 / SM12 / SM49 / SM69 / SLG2 / ST36 / E42F/ MASS no se encuentran bloqueadas en ambiente PRD.

Durante la revisión no fue posible identificar la responsabilidad acerca del bloqueo y/o desbloqueo de transacciones en los ambientes productivos; la responsabilidad del bloqueo de transacciones críticas no está claramente documentada.

Figura 5 Transacciones Críticas



Cód.transacción	Tipo de transacción	Status de bloqueo	Texto transacción
/ASU/MAINTAIN	Transacción report		Actualizar UEA-XML
O5AB	Transacción parámetros		Actualiz.rango números: OIG_DRIVER
J1S1	Transacción parámetros		IS-M: CH/S: Códigos postales base
GJV0	Menú		
GJV6	Menú		

Fuente: El autor

Riesgo inherente asociado

La inadecuada administración de transacciones críticas en el sistema podría permitir y autorizar a los usuarios a la ejecución de actividades críticas, no asignadas a sus funciones, a través del esquema de autorizaciones configurado actualmente en el sistema SAP.

RECOMENDACIÓN

Definir y formalizar la asignación de la responsabilidad del bloqueo y desbloqueo de transacciones en ambientes productivos. Esta definición puede incluir:

- Responsables del bloqueo y desbloqueo
- Procedimiento de desbloqueo y bloqueo
- Autorizados para solicitar el bloqueo y/o desbloqueo de transacciones
- Realizar el bloqueo de las siguientes transacciones en el ambiente productivo:
  SM01 / SM19 / SCC5 / SCCL / SCC9 / SM12 / SM49 / SM69 / SLG2 / ST36 / E42F/ MASS

Crear roles específicos para dichas transacciones, que permanezcan sin asignación. Estos roles deberán asignarse únicamente en casos de emergencia, debidamente justificados, autorizados y documentados

5. Roles no asignados en ambiente PRD

Se identificaron un total de 257 roles Z creados en ambiente productivo; 87 de ellos no se encuentran asignados a usuarios en el sistema SAP, deteriorando la calidad de datos e información y generando dificultad para gestionar la administración de accesos a usuarios finales.

Figura 6 Roles Sin Asignación

Mdte.	Rol	Idioma	ID
700	Z_ADM_SAP_GRUPO_BASIS	S	1
700	Z_BASIC_SERVICE_V1	E	1
700	Z_BCM_AGRUPADOR_PAGOS	S	1
700	Z_BCM_ANULADOR_LOTES	S	1
700	Z_BCM_AUTORIZADOR_PAGOS	S	1
700	Z_BCM_VISUALIZADOR_BCM	S	1
700	Z_CONSUL_CONTINT_HCM	S	1
700	Z_DEVOLUCIONES_APORTES	S	1
700	Z_FI_DM_ACTFIJOS	E	1
700	Z_FI_DM_ACTFIJOS	S	1
700	Z_MM_COM_BENEF	E	1
700	Z_MM_COM_BEPS	E	1
700	Z_MM_COM_CCIAL	E	1
700	Z_MM_COM_CONTINT	E	1
700	Z_MM_COM_FININVER	S	1
700	Z_MM_COM_INGPROC	E	1
700	Z_MM_COM_JURID	S	1
700	Z_MM_COM_PLANRIES	E	1
700	Z_MM_COM_REDES_CANALES	S	1
700	Z_MM_COM_SERVCIUD	S	1

Fuente: El autor

Riesgo inherente asociado

Dificultad en la gestión de administración de roles y usuarios en el sistema SAP.
Aumento en la probabilidad de asignación incorrecta de accesos a usuarios.
Posibilidad alta de violar reglas de segregación de funciones.

RECOMENDACIÓN

Estudiar la necesidad de mantener en ambiente productivo los roles sin usuarios asignados y definir su eliminación del mandante o transportarlos al mandante de QA sí serán utilizados en el futuro.
Efectuar la depuración correspondiente de los roles identificados, realizando la asignación y/o eliminación de estos. Evaluar la posibilidad de realizar el download de los roles no asignados a usuarios en ambiente PRD al mandante de QAS.

METODOLOGIA PARA EL ANÁLISIS DEL NIVEL DE SEGURIDAD DE LOS ROLES Y PRIVILEGIOS, EN EL SISTEMA SAP ERP DE COLPENSIONES.

Con el fin de realizar el análisis del nivel de seguridad de los roles y privilegios del sistema de información SAP en Colpensiones se propone la siguiente metodología basada en las buenas prácticas de SAP compuesta por las siguientes fases que garantizaron la correcta definición de los roles y privilegios del sistema.

- Preparación
- Análisis y Conceptualización
- Implementación.
- Control de Calidad y pruebas.
- Paso a Producción.
- Estabilización.

En cada fase se proponen actividades, responsables y entregables.

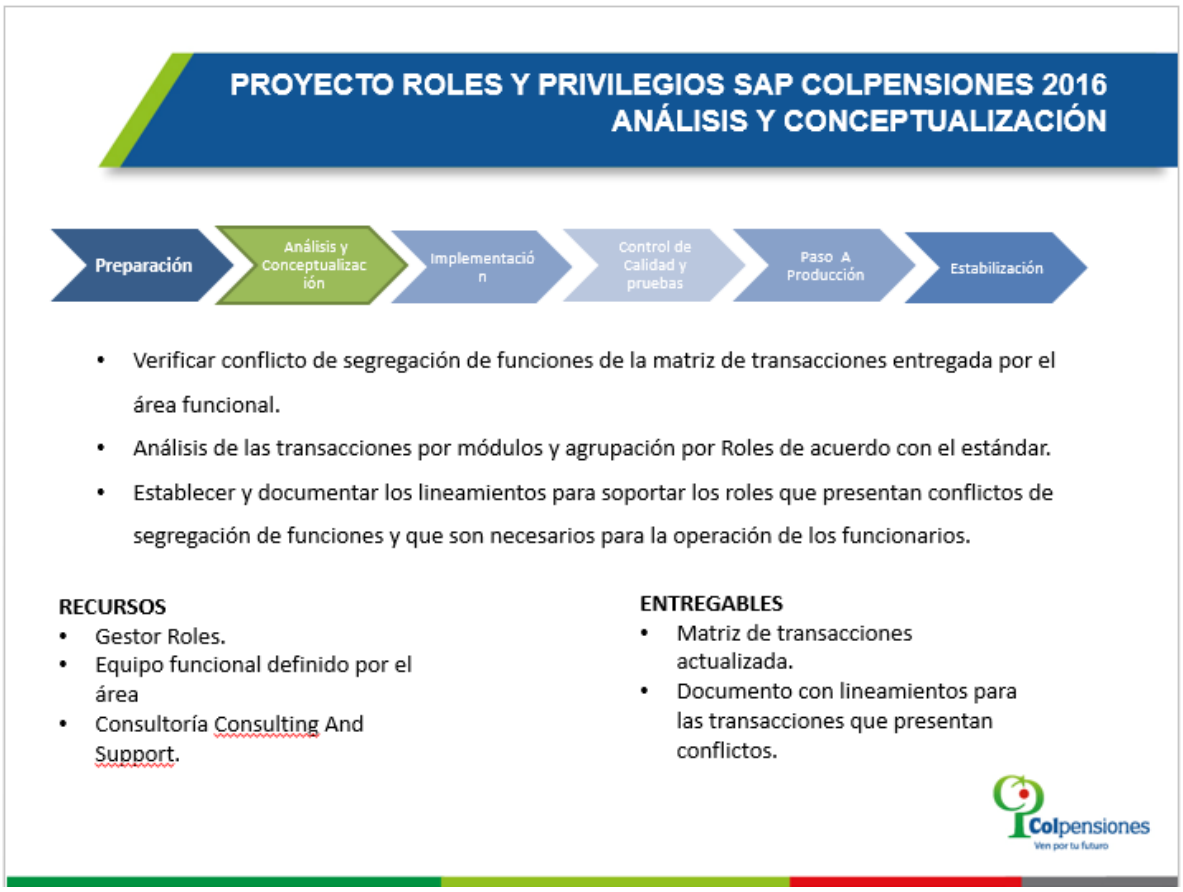
Para la fase de preparación se realizó reunión donde se definieron responsables, actividades a realizar en el proceso de análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones, se definieron cuáles serán los entregables y se ajustó el cronograma de trabajo de acuerdo a las observaciones de los miembros que participaron en el proyecto.

Figura 7 Fase Preparación

Fuente: El autor

Figura 8 Análisis y conceptualización

Para la fase de análisis y conceptualización se realizó proceso a través de herramientas ofimáticas de cruce de información referente a las transacciones solicitadas por cada una de las áreas involucradas en el proyecto identificando posibles conflictos de segregación de funciones y para el caso en que se evidencien realizar el correspondiente reporte y trabajar conjuntamente con las áreas con la finalidad de mitigar estos conflictos y continuar con el proceso, posteriormente se procede a realizar la agrupación de transacciones por roles en matriz Excel que contendrá nombre de rol, login de usuario, transacción asociada al rol y descripción de la transacción.



Fuente: El autor

Para la fase de implementación se procedió a realizar la creación de los roles de SAP en el mandante de calidad de acuerdo con el levantamiento de información realizado en la fase de conceptualización, se asociaron usuarios a los roles

construidos y se dispuso la activación de usuarios en este ambiente con el fin de garantizar la realización del proceso de documentación y certificación de los mismos.

Figura 9 Implementación

Fuente: El autor

Figura 10 Control de calidad y pruebas

En esta fase se describen las actividades que se realizaran en la fase de control de calidad y pruebas la cual consiste en que cada funcionario de la organización realice la validación de las transacciones asignadas y documente su correcto funcionamiento, esto con el fin de que se pueda dar el paso a producción mitigando los errores que se puedan generar y garantizar la disponibilidad de los procesos de negocio, una vez se tengan los roles ajustados se actualizara el formato de gestión de usuarios para relacionar los nombres de los nuevos roles

del sistema SAP y los autorizadores para cada uno de estos, adicionalmente se entregaran las matrices de roles a cada una de las áreas funcionales las cuales tendrán como responsabilidad la administración de la misma respecto a la asignación de roles a nuevos funcionarios o asignación de transacciones a un rol.

Fuente: El autor

Figura 11 Paso a Producción.

En la fase de implementación se realizó el paso a producción de los roles que fueron certificados en el mandante de calidad, para este caso el gestor de roles procedió con la ejecución de las siguientes actividades:

Proceso de descarga masiva de los roles certificados, solicitud de transporte de los mismos del ambiente de calidad al ambiente productivo SAP, una vez los roles se transportaron a producción se realizó el proceso de generación de los perfiles de cada uno de estos roles con el fin de garantizar su funcionamiento. El gestor de roles también solicito a los autorizadores de cada proceso de negocio formalizar la

solicitud de asignación de los nuevos roles a los funcionarios que lo requieran y posteriormente realizo la asociación de rol por usuario en el sistema SAP de acuerdo con lo solicitado.

Fuente: El autor

En esta fase detallan las actividades que se realizarán en la fase de estabilización la cual consiste en brindar un soporte oportuno a cada uno de las áreas que se encuentran trabajando con la nueva estructura de roles esto con el fin de garantizar los procesos misionales de la organización, en caso de que se requiera acceso a una nueva transacción se debe validar la viabilidad de asignación y documentar las matrices a que haya lugar.

Figura 12 Fase de estabilización.

Fuente: El autor

LINEAMIENTOS Y CONTROLES

Definir los lineamientos y flujos de autorización que se deben tener en cuenta para los roles que por necesidad del negocio presenten conflicto de segregación de funciones.

OBJETIVO

Establecer lineamientos para determinar los controles que se deben aplicar a los roles que presenten conflicto de segregación de funciones.

ALCANCE

Los lineamientos descritos en el presente documento aplican para la construcción de roles del sistema ERP de SAP de Colpensiones

Responsables:

El gestor de Roles debe validar que en la construcción de los roles no se presenten este tipo de conflictos, en caso dado que se presenten debe notificar al área para que determine las acciones que se tomaran para mitigar este riesgo.

Lineamientos:

Lineamiento 1. Para los roles del sistema SAP que presenten conflictos de segregación de funciones se debe solicitar al key user el tipo de control que se debe implementar para garantizar que este tipo de incompatibilidad sea monitoreada en el sistema.

Lineamiento 2. Activar en el sistema ERP de SAP log de auditoria transaccional con el fin de notificar a las áreas mensualmente las actividades realizadas por este tipo de usuarios y mitigar los riesgos relacionados con este tipo de conflicto.

Implementar controles que permitan garantizar el ciclo de vida de los usuarios en la organización.

Con el fin de garantizar el ciclo de vida de los usuarios de Colpensiones en el sistema de información SAP se procedió a realizar la implementación de los siguientes controles basados en las recomendaciones de la norma ISO 27002 domino 11 control de acceso. Estos controles fueron definidos teniendo en cuenta que las organizaciones hoy en día no llevan el control necesario sobre los usuarios que se van de la entidad los cuales en algunos casos cuentan con privilegios elevados y quedan disponibles para que sean usados de manera fraudulenta y poner en riesgo la confidencialidad, integridad y disponibilidad de la información e infraestructura tecnológica. Adicionalmente se recomienda contemplar la implementación de controles sobre las cuentas de usuarios administradoras, cuentas de usuarios de proveedores y generar reportes mensuales que se crucen con la planta de personal vigente de la organización con el fin de garantizar que solo los usuarios que tienen contrato actual en la organización sean los que están activos en los sistemas.

Entre los controles que se implementaron se relacionan los siguientes:

Nombre del Control:

No LogOn 30 días SAP.

Objetivo del Control:

Garantizar la disponibilidad de los accesos a los usuarios que hagan uso frecuente de las aplicaciones corporativas y evitar el préstamo y/o secuestro de credenciales.

Descripción del Control:

Generar un reporte de los usuarios activos que no presenten LogOn durante un periodo de 30 días calendario, estos usuarios serán bloqueados cambiando su estado en la aplicación y se modificará la fecha de vigencia al día de la ejecución del control.

Responsable:

Gestor de Revisión Periódica - Grupo de Gestión de Accesos VOT.

Categoría:
Preventivo.

Frecuencia:
Semanal.

Nombre del Control:
Revisión de accesos a los sistemas de información por ausentismos y retiro en Aplicación SAP.

Objetivo del Control:
Garantizar que no se realicen conexiones indebidas en el sistema de información SAP.

Descripción del Control:
Aplicar los bloqueos e inactivaciones necesarias notificadas por Talento Humano en el sistema de información SAP según corresponda con los accesos que tenga asignados el usuario que se desvincula o presenta ausentismo, se debe solicitar a

Servicios TI la generación de un caso para que sirva como trazabilidad de la gestión realizada.

Responsable:
Gestor de Revisión Periódica, Talento Humano.

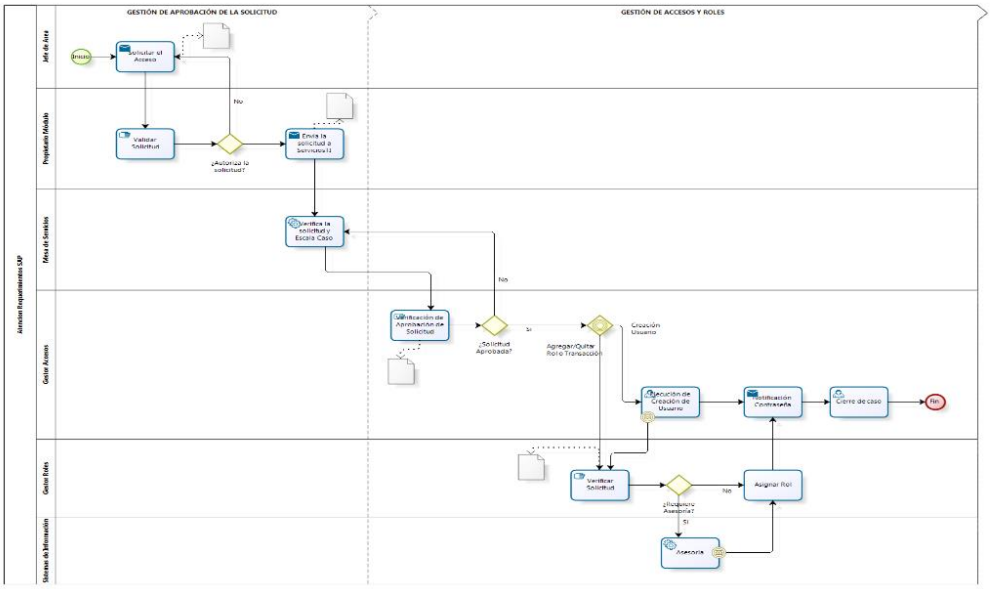
Categoría:
Preventivo.

Frecuencia:
Cada vez que se requiera.

A continuación, se relacionan imágenes del detalle del flujo de atención de requerimientos e incidentes en SAP los cuales hacen parte del ciclo de vida del usuario.

Para este flujo se evidencia que las personas que intervienen en el proceso de creación de usuarios o asignación de permisos son los siguientes: jefe de área, propietario del módulo de SAP, mesa de servicios Colpensiones, gestor de accesos, gestor de roles y sistemas de información se detallan la responsabilidad que cada uno tiene dentro del proceso de atención de requerimientos y los aspectos que se deben tener en cuenta para cumplir con su parte de proceso.

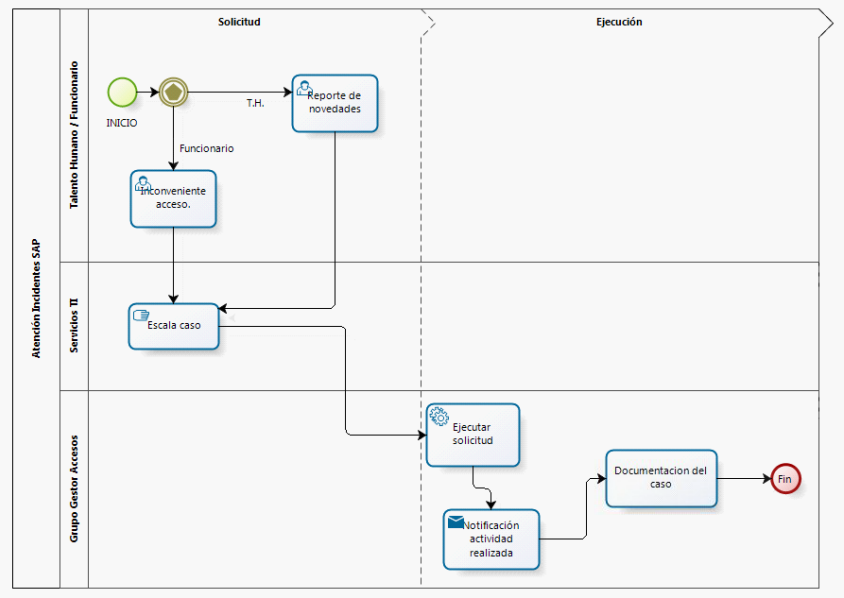
Figura 13 Atención Requerimientos SAP



Fuente: El autor

En el flujo de atención de incidentes de la figura 15 se detallan los pasos que debe realizar el funcionario o talento humano para el proceso de activación o inactivación de usuarios en el sistema de información SAP, los responsables de cada actividad como lo son el funcionario, talento humano, y el gestor de acceso.

Figura 14 Atención Incidentes SAP



Fuente: El autor

ANEXOS

Como evidencia del proyecto análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones s se relacionan los siguientes anexos en los cuales se pueden constatar el cumplimiento de los objetivos propuestos y la entrega del insumo (Matrices de Roles Y Privilegios) a las áreas de negocio de la organización.

Anexo A. Matriz Roles Y transacciones

En la siguiente tabla se evidencia la creación y agrupamiento de transacciones por rol y su denominación.

Tabla 4 Resumen Matriz Roles y transacciones

Rol	Nombre Transacción	Descripción Transacción
Z_AA_ACIVOS	AFAB	Contabilizar amortización
	AFBP	Crear log de contabilización Amo
	AW01N	Asset Explorer
Z_AA_VISUALIZAR_ACTIVOS	AS03	Visual.registro maestro AF
Z_BLOQUEO_TRANSACCIONES	SM01	Bloquear transacciones
Z_FI_ACTUALIZACION_SET	GS02	Modificar set
Z_FI_ANULACIONES	AB08	Anular partidas indiv.de act.fijos
	F.80	Anular documentos en masa
	FB02	Modificar documento
	FB08	Anular documento
	FB18	Actualizar textos mail estándar
	FBRA	Anular compensación
	MR8M	Anulación doc.factura
Z_FI_CAJAS_MENORES	FBCJ	Libro de caja
	FBCJC6	Actualiz.rango números: CAJO_DOC3
	S_ALR_87012309	Libro de caja
	Z_ALR_87012309	Libro de caja
Z_FI_CIERRE	AJAB	Cierre ejercicio
	AJRW	Cambio de ejercicio
	F.07	Libro mayor: Arrastre saldos
	FAGL3KEH	Libro mayor: CeBe estándar
	FAGLGVTR	Libro mayor: Arrastre saldos
	MMPV	Desplazar periodos
	MMRV	Contab. en periodo ant. autorizado
	OB52	C FI Actual. tabla T001B
	OKP1	Actualizar bloqueo de períodos
	ZCIERRE_ANUAL	ABAP - Cierre mensual
	ZCIERREM	Cierre mensual por Ledger
	ZCIERREM_FON	ABAP - Cierre mensual

Anexo B. Documento con el estándar para nombramiento de roles.

OBJETIVO

Establecer reglas claras en la construcción de identificadores de roles en el sistema de información SAP.

ALCANCE

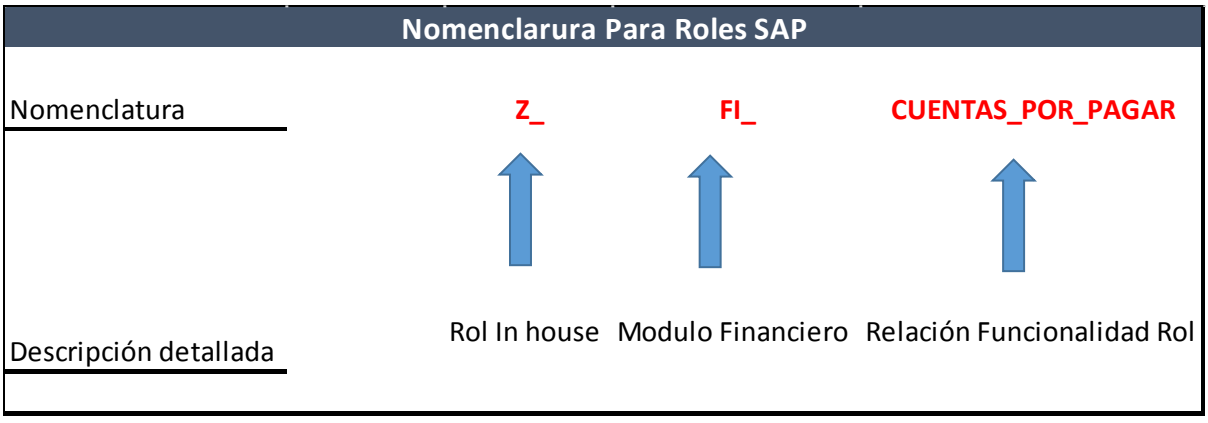
Los lineamientos descritos en el presente documento aplican para la construcción de roles del sistema ERP de SAP de Colpensiones

RESPONSABLES

El gestor de Roles debe configurar los identificadores de nomenclatura de roles.

En la siguiente tabla se aclara como deben ser construidos los roles donde Z_ hace referencia a que es un rol echo en casa, FI_ modulo del sap al cual corresponden las transacciones y la parte 3 del rol es la descripción del mismo en este ejemplo se evidencia que el rol es para la funcionalidad de cuentas por pagar en el sistema de información SAP.

Figura 15 Nomenclatura Roles ERP SAP Colpensiones



Anexo C. Lineamiento para el manejo que se debe dar a los usuarios con privilegios de administración.

Objetivo del lineamiento:

Establecer la política de lineamientos de configuración generales y específicos en SAP con el fin de realizar el adecuado aseguramiento del sistema.

- Implementar seguridad en la creación y configuración accesos de usuarios de Colpensiones por medio de técnicas que incluyan estándares de buenas prácticas de configuración.
- Aseguramiento de Usuarios Estándar estableciendo un lineamiento estándar formalizado para el aseguramiento de las cuentas de usuario estándar de SAP, en los diferentes mandantes, para la ejecución de tareas administrativas SAP (SAP*, DDIC, y Early Watch).

CONFIGURACIÓN

Tabla 5.Línea Base SAP

Configuración General		
Política	**Nombre**	**Observaciones.**
G1	Crear una cuenta de usuario estándar que permita realizar operaciones administrativas, reemplazando SAP*. Este usuario debe ser asignado al grupo SUPER.	Ninguna
G2	El parámetro login/no_automatic_user_sapstar debe tener asignado el valor 1 (uno).	Esto evitará que en caso de eliminar el usuario SAP*, el mecanismo de seguridad de SAP creará nuevamente este usuario con la contraseña inicial (PASS). Con esto, se mitiga el riesgo que una persona que tenga conocimiento de la contraseña por defecto podría ingresar a SAP utilizando esta cuenta. Este parámetro deshabilita las características especiales de SAP* en un evento de recreación del usuario.

Tabla 4. (Continuación)

G3	**No elimine DDIC o sus perfiles. DDIC es necesario para determinadas tareas de instalación y actualización, la logística de software, y para el Diccionario ABAP.**	**Si se borra este se traduce en pérdida de funciones en estas áreas.**

Medidas de seguridad - Información general (RFC)		
Medidas generales		
MG1	La restricción de Mantenimiento, las autorizaciones para destinos RFC (transacción SM59).	
MG2	Restringir el acceso a la tabla RFCDES (información sobre los destinos RFC).	
MG3	Utilice los controles de autorización en los módulos de función (aplicación) si desea llamar a estos módulos utilizando RFC.	
MG4	Utilizar Secure Comunicaciones de la red.	
MG5	Desconectar la vigilancia remota de puertas de enlace de SAP.	
MG6	Permitir las autorizaciones para Trazas RFC y Depuración De manera restrictiva.	
MG7	Garantizar que el uso del trace sea permitido solo a usuarios especializados en el manejo y configuración del mismo.	
Medidas especiales para servidores externos RFC		
ME1	Evitar el mal uso del kit de desarrollo de software RFC.	
ME2	Permitir solo conexiones RFC de los sistemas conocidos.	
ME3	Restringir el uso de programas de servidor RFC externos.	
ME4	Restringir el acceso a la RFC Programa RFCEXEC a programas propios del sistema operativo donde se encuentre implementado SAP.	
SAP* - DDIC - Early Watch		
P1	Cambiar todas las contraseñas por defecto para estos usuarios.	
P2	Hacer una copia del usuario SAP* de acuerdo al estándar de nombramiento de usuarios de servicio definido por la organización con un nombre determinado para cada Mandante del sistema y asegurar la contraseña. Este usuario tendrá los perfiles SAP_ALL y SAP_NEW.	Ninguna

Tabla 4. (Continuación)

P3	Eliminar el perfil SAP_ALL del usuario SAP*	Esta configuración no permitirá acceso a todas las transacciones del sistema.
P4	Bloquear el usuario SAP* permanentemente y permitir su uso únicamente en los eventos críticos que lo requieran, bajo autorización de un nivel superior y plena supervisión de las actividades.	Ninguna
P5	Permitir el uso del usuario copia del SAP* únicamente en los eventos críticos que lo requieran, bajo autorización del gerente de infraestructura garantizando la supervisión de las actividades ejecutadas.	Ninguna
P6	Aplicar las políticas 1, 2, 3,4 y 5 en los ambientes no productivos destinados para SAP.	Ninguna
P7	Cambiar la contraseña que viene por defecto para el usuario DDIC en el mandante 066, por una que cumpla con los estándares definidos por la organización.	Ninguna
P8	Inactivar las características especiales de SAP*, modificando el parámetro login/no_automatic_user_sapstar con un valor de (1).	Ninguna
P9	Cambiar la contraseña cada vez que se utilice el usuario SAP*.	Ninguna
P10	Para el usuario SAP* en el mandante 001 se debe únicamente cambiar la contraseña que trae por defecto y establecer una periodicidad para el cambio de contraseñas de los usuarios del sistema, por una que cumpla con las mejores prácticas y políticas de la organización.	Ninguna
Recomendación	Monitorear las actividades de usuario SAP* y el usuario que lo reemplaza a través del log de auditoría del sistema SAP.	

Tabla 4. (Continuación)

Los usuarios de Soporte Remoto Garantizar que los usuarios de soporte remoto cuenten con las siguientes características: **1.** Que sea un usuario con estándar de nombramiento de la organización (Nemotecnia de Nombre). **2.** Activar vigencia de la cuenta de usuario. **3.** Asignar roles específicos para la actividad de soporte requerida. **4.** Activar vigencia de los roles.			
UR1	Definir un usuario especial para el acceso remoto. No utilice cualquiera de los usuarios estándar.		Ninguna
UR2	Definir un procedimiento para activar y desactivar el usuario. Activarla sólo cuando sea necesario y desactivarlo una vez terminada la sesión remota.		Ninguna
UR3	No revele la contraseña de este usuario a través de la sesión remota. Enviarlo a través de un canal separado, como un correo electrónico o una llamada telefónica de retorno. Cambiar la contraseña una vez haya finalizado la sesión.		Ninguna
UR4	Bloquear el usuario SAP *, DDIC, EarlyWatch y su apoyo a los usuarios remotos. Desbloquearlos sólo cuando sea necesario.		Tenga en cuenta que nunca debe ser necesario el uso de SAP *.
Parámetros de seguridad SAP			
Sesión del usuario			
SU1	login/disable_multi_gui_login	Deshabilitar login de múltiples sesiones	Valor=1
SU2	login/fails_to_user_lock	Cantidad de intentos de ingreso fallidos antes de que el sistema bloquee el usuario.	Valor=2
SU3	login/fails_to_session_end	Después de x errores al entrar la clave de acceso en el sistema SAP R/3 el sistema se bloquea.	Valor=3
SU4	rdisp/gui_auto_logout	Segundo sin actividad para que se cierre la sesión.	Valor=1800
SU5	login/failed_user_auto_unlock	Define si los bloqueos de usuario debido a los intentos fallidos de inicio de sesión se eliminan automáticamente a la medianoche.	Valor=0

Tabla 4. (Continuación)

Robustez de la clave			
RC1	login/min_password_diff	Mínimos caracteres diferentes entre la nueva clave y la anterior	Valor=4
RC2	login/min_password_digits	Cantidad mínima de dígitos	Valor=2
RC3	login/min_password_letters	Cantidad mínima de letras	Valor=2
RC4	login/min_password_lng	Cantidad de caracteres mínimos de clave	Valor=(8 -12)
RC5	login/min_password_lowercase	Cantidad mínima de minúscula en la clave utilizada.	Valor=5
RC6	login/min_password_specials	Cantidad mínima de caracteres especiales.	Valor=3
RC7	login/min_password_uppercase	Cantidad mínima de mayúscula en la clave utilizada.	Valor=4
RC8	login/password_expiration_time	Validez máxima (en días) de la clave.	Valor=30
RC9	login/password_history_size	Tamaño del historial de claves utilizadas.	Valor=10
RC10	login/password_charset	Este parámetro define los caracteres de los cuales una contraseña puede constituirse.	Valor=1
Password Logon			

Tabla 4. (Continuación)

PL1	login/password_compliance_to_current_policy	Los valores permitidos: 0 - sin verificación; 1 - el sistema comprueba durante la contraseña de la conexión si la contraseña actual cumple con las normas de la contraseña actual y la fuerza un cambio de contraseña si este no es el caso. Valor por defecto: 0 Disponible después de SAP NetWeaver 6.40	Valor=1
PL3	login/password_change_for_SSO	Comprueba si el usuario debe cambiar su contraseña.	Valor=1
PL4	login/password_history_size	Especifica el número de contraseñas (elegido por el usuario, y no el administrador) que el sistema almacena y que el usuario no puede utilizar de nuevo.	Valor=10
PL5	login/password_change_waittime	Especifica el número de días que un usuario debe esperar antes de cambiar la contraseña de nuevo.	Valor=1
Other Password Profile Parameters			
PP1	login/password_downwards_compatibility	Especifica el grado de compatibilidad con versiones anteriores.	Valor=1
Multiple Logon			

Tabla 4. (Continuación)

MP1	login/disable_multi_gui_login	Controla la desactivación de múltiples inicios de sesión de diálogo	Valor=1
Registros de auditoría			
RA1	Rec/client	Log de modificaciones a tablas.	All o el código de mandante productivo.
RA2	Rsau/enable	Auditoria de Seguridad	Valor=1
RA3	rsau/local/file	Especifica la ubicación del registro de auditoría del servidor de aplicaciones.	/usr/sap/<SID>/<instno>/log/ audit_<SAP_instance_number>
RA4	rsau/max_diskspace_local	Especifica la longitud máxima del registro de auditoría.	1.000.000 bytes
RA5	rsau/selection_slots	Especifica el número de ranuras de selección para la auditoría.	Valor=2
Inicio de sesión con SSO Ticket			
IS1	login/accept_sso2_ticket	Permite o bloquea el inicio de sesión mediante el ticket SSO.	Valor=1
IS2	login/create_sso2_ticket	Permite la creación de tickets SSO.	Valor=2
IS3	login/ticket_expiration_time	Define el período de validez de un ticket de SSO.	Valor=8:00
IS4	login/ticket_only_by_https	Especifica cómo el sistema establece el ticket de inicio de sesión, generado al iniciar sesión mediante HTTP (S), en el explorador.	Valor=0

Tabla 4. (Continuación)

IS5	login/ticket_only_to_host	Especifica cómo el sistema establece el ticket de inicio de sesión, generado al iniciar sesión mediante HTTP (S), en el explorador.	Valor=0
Otros parámetros de inicio de sesión			
OP1	login/disable_cpic	Rechazar las conexiones entrantes del tipo CPIC	
OP2	login/no_automatic_user_sapstar	Controlar la emergencia de usuario SAP * (más información: notas de SAP2383 y 68048)	Valor=1
OP3	login/update_logon_timestamp	Especifica la exactitud de la marca de tiempo de inicio de sesión.	Valor=m

Fuente: el autor

RIESGO DE NO APLICAR LA CONFIGURACION

- No contar con un estándar formalizado para el aseguramiento de usuarios estándar, podría materializarse en que se realicen actividades erróneas o fraudulentas que comprometan la integridad, confidencialidad y disponibilidad de la información.

- Uso no autorizado del súper usuario SAP*, el cual cuenta con acceso a los perfiles SAP_ALL.

- Lo anterior, tiene la posibilidad de generar ataques externos con súper usuarios conocidos y con acceso total al sistema SAP, así como, la no detección de actividades indebidas durante actividades de soporte y/o mantenimiento del sistema.

Anexo D. Documentos con los controles que se deben realizar en el sistema que garanticen el ciclo de vida del usuario

Nombre del Control:
No LogOn 30 días SAP.

Objetivo del Control:
Garantizar la disponibilidad de los accesos a los usuarios que hagan uso frecuente de las aplicaciones corporativas y evitar el préstamo y/o secuestro de credenciales.

Descripción del Control:
Generar un reporte de los usuarios activos que no presenten LogOn durante un periodo de 30 días calendario, estos usuarios serán bloqueados cambiando su estado en la aplicación y se modificará la fecha de vigencia al día de la ejecución del control.

Responsable:
Gestor de Revisión Periódica - Grupo de Gestión de Accesos VOT.

Categoría:
Preventivo.

Frecuencia:
Semanal.
Nombre del Control:
Revisión de accesos a los sistemas de información por ausentismos y retiro en Aplicación SAP.

Objetivo del Control:
Garantizar que no se realicen conexiones indebidas al aplicativo SAP.

Descripción del Control:
Aplicar los bloqueos e inactivaciones necesarias notificadas por Talento Humano en la aplicación SAP según corresponda con los accesos que tenga asignados el usuario que se desvincula o presenta ausentismo, se debe solicitar a Servicios TI la generación de un caso para que sirva como trazabilidad de la gestión realizada.

Responsable:
Gestor de Revisión Periódica, Talento Humano.

Categoría:
Preventivo.

Frecuencia:

Cada vez que se requiera.

Anexo E. Instructivo para el proceso de creación de usuarios y asignación de roles.

OBJETIVO

Presentar el instructivo para realizar la creación de usuarios y asignación de roles en la aplicación SAP.

ALCANCE

El presente instructivo brinda el paso a paso para la validación de licencias disponibles y creación de usuarios en la aplicación SAP en los diferentes mandantes de acuerdo a la solicitud registrada en el Formato No 1 Gestión de Usuarios y Privilegios con las respectivas autorizaciones.

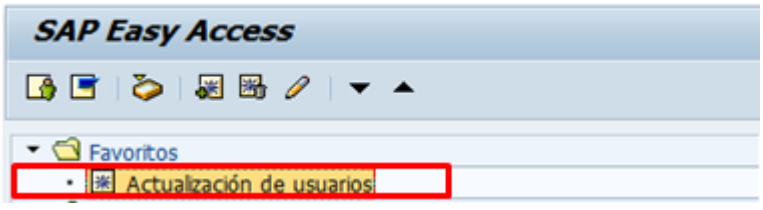
RESPONSABLE

La aplicación del instructivo, así como el acatamiento de sus principios y directrices es responsabilidad del gestor de accesos y el Gestor de Roles.

ACTIVIDADES DEL GESTOR DE ACCESOS.

a) Doble clic en la transaccion **Actualizacion de usuarios.**

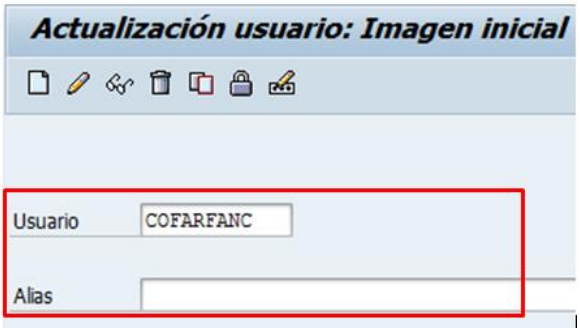
Figura 16. Ejecutar transacción SU01.



Fuente: El Autor

b) En el campo **Usuario** conformamos el login de acuerdo al Estandar Creación Usuarios y Contraseñas, el campo **Alias** se deja vacio este se insertara mas adelante.

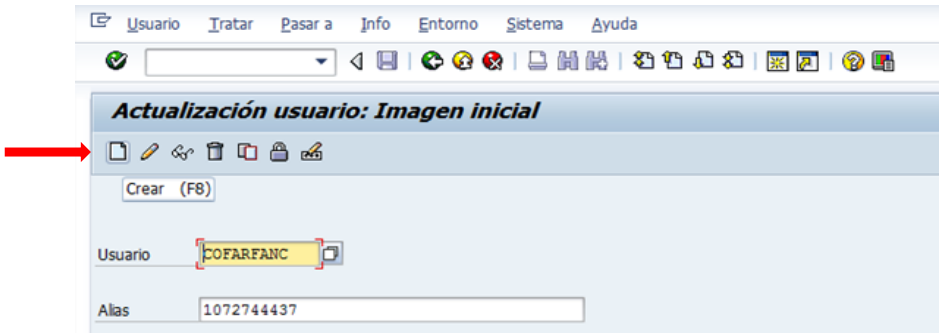
Figura 17 ingreso datos usuario



Fuente: El Autor

c) Dar clic el icono (Crear) o simplemente la funcion F8.

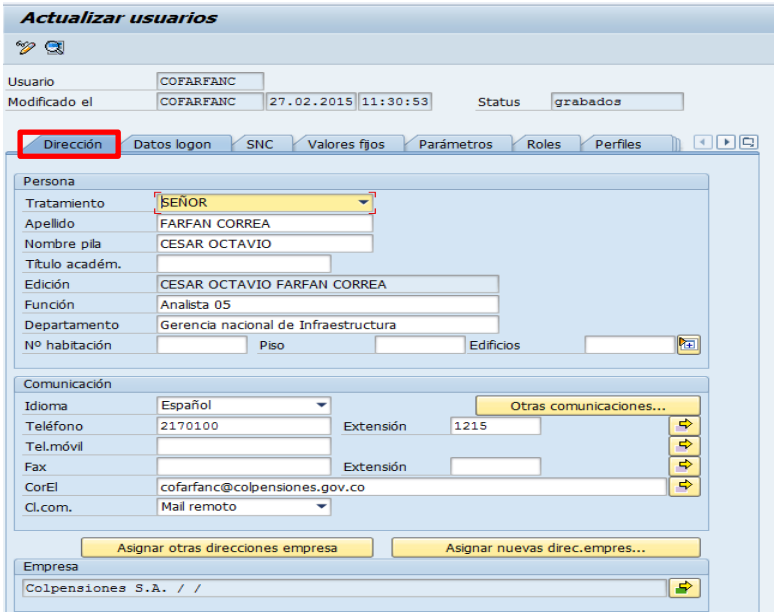
Figura 18 Ingreso Modulo Crear usuario



Fuente: El Autor

d) En la pestaña Dirección ingresamos los siguientes datos del funcionario: Tratamiento, Apellido, Nombre pila, edición, función (esta campo hace referencia al cargo del funcionario), departamento (Gerencia a la cual pertenece el funcionario), teléfono, extensión, correo electrónico, cl.com (se deja por defecto mail remoto)

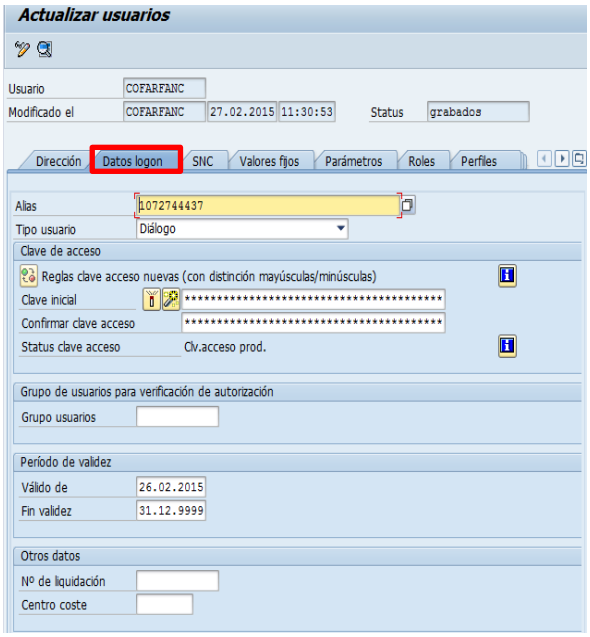
Figura 19 Ingreso Modulo Crear usuario



Fuente: El Autor

e) Ingresar a la pestaña **Datos logon** donde se indica el tipo de usuario que se va a crear, para el caso de los usuarios asignados a funcionarios de Colpensiones que usan la aplicación permanentemente el acceso que se otorga es usuario de dialogo, se asigna una contraseña inicial la cual debe cumplir con el siguiente estándar 4 Mayúsculas, 5 minúsculas, 3 números y dos caracteres especiales. En el campo periodo de validez se ingresa como fecha inicial el día en que se crea el usuario, para el caso en los que se especifica la vigencia a un usuario se ajusta la fecha para que se acople a lo solicitado, para los casos de los empleados con contrato a término indefinido se ajusta para que la fecha quede sin caducidad.

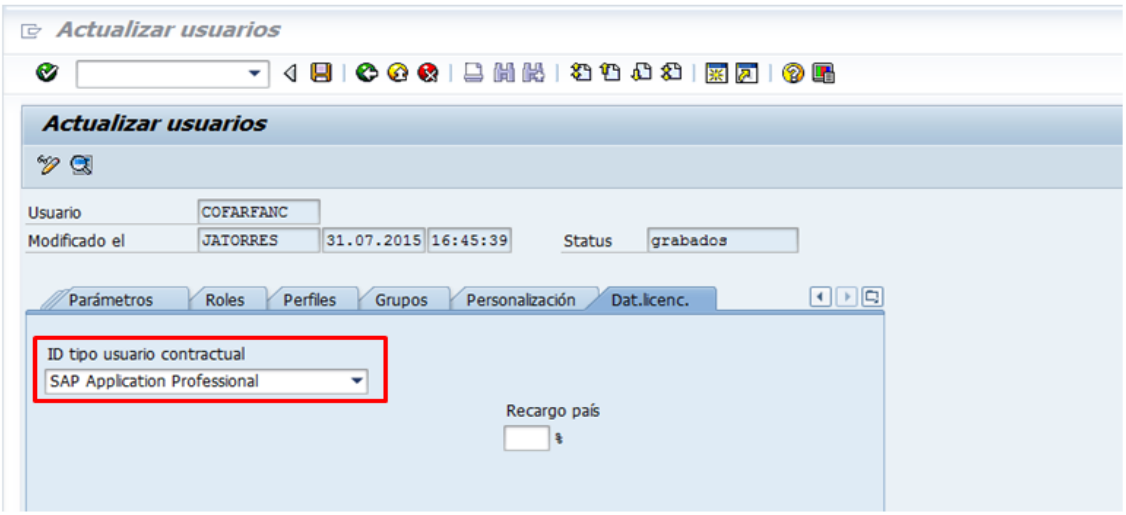
Figura 20 ingreso cedula y contraseña



Fuente: El Autor

f) Ingresar a la pestaña dat.licenc y para el caso de las personas que tienen cargo de profesionales o administradores y debe tener la licencia **SAP application Profesional** como se muestra en la siguiente imagen.

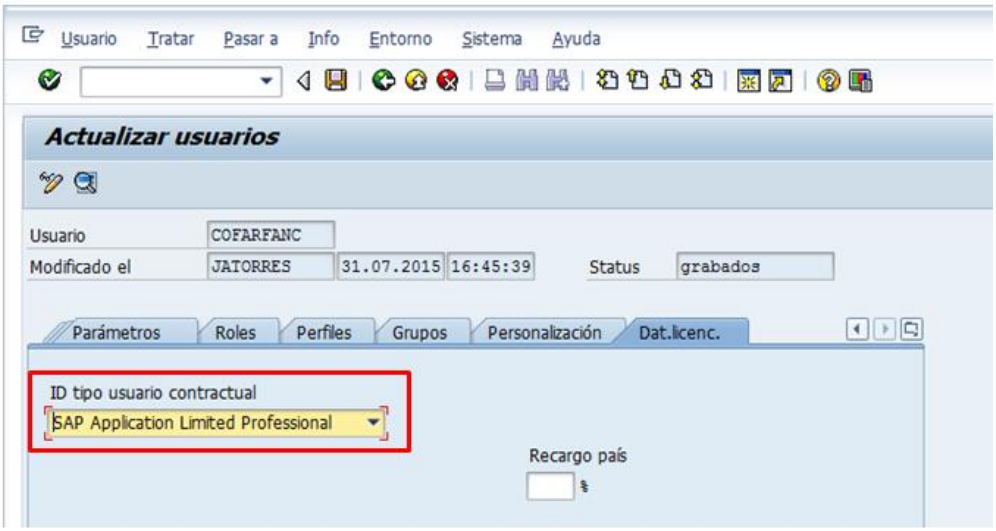
Figura 21. Asignación licencia a usuarios.



Fuente: El Autor

g) Para el caso de las licencias para los cargos asistenciales, analistas y aprendices se debe asignar la licencia **SAP Application Limited Professional** como se evidencia en la siguiente imagen.

Figura 22 Lineamiento para asignación de licencias.



Fuente: El Autor

h) Proceder a guardar los cambios dando clic en el icono (guardar)

Figura 23 Guardar gestión realizada.

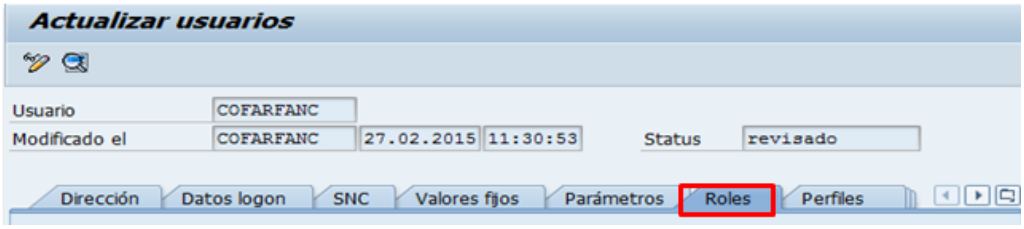
Fuente: El Autor

ACTIVIDADES DEL GESTOR DE ROLES.

Asignación de roles.

a) Ingresar a la pestaña Roles.

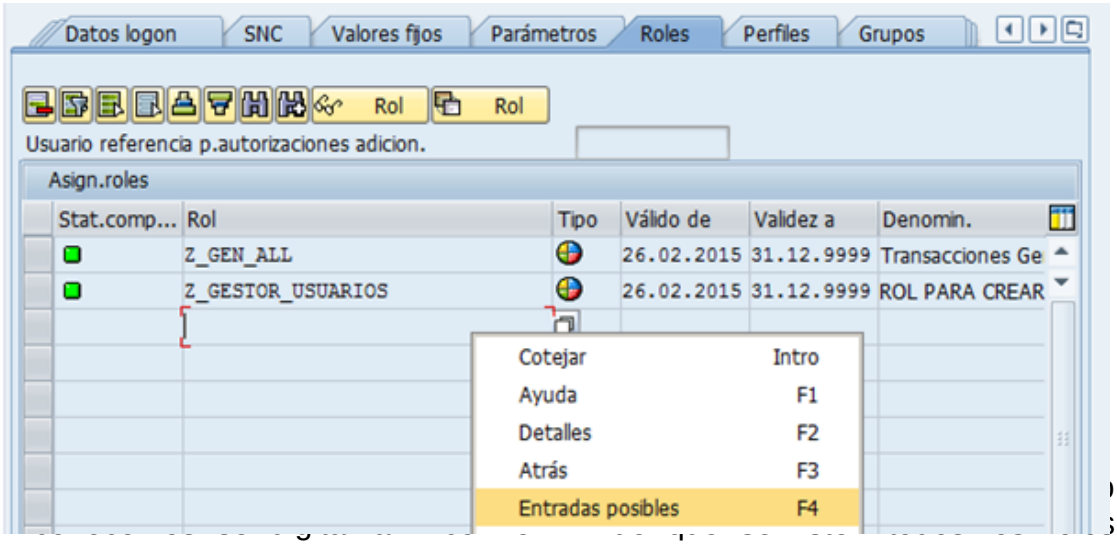
Figura 24 Ingreso modulo Roles.



Fuente: El Autor

b) Nos ubicamos en la siguiente fila vacía y procedemos a buscar el rol dando clic derecho sobre la casilla y seleccionar la opción entradas posibles o simplemente presionando la función f4.

Figura 25. Asignación de roles en el sistema.

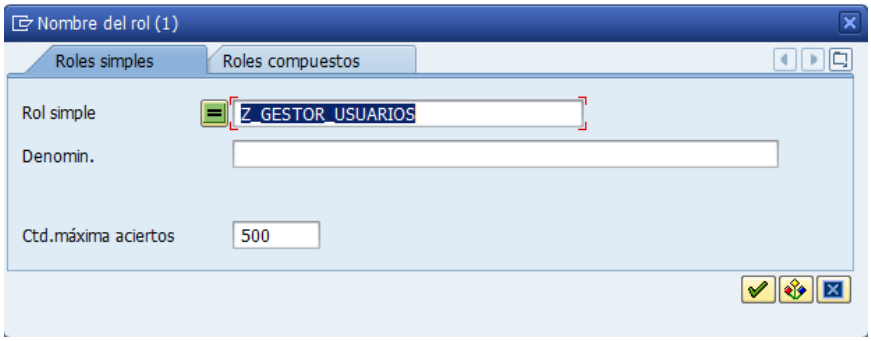


Fue

existentes.

Búsqueda del rol por nombre del Rol:

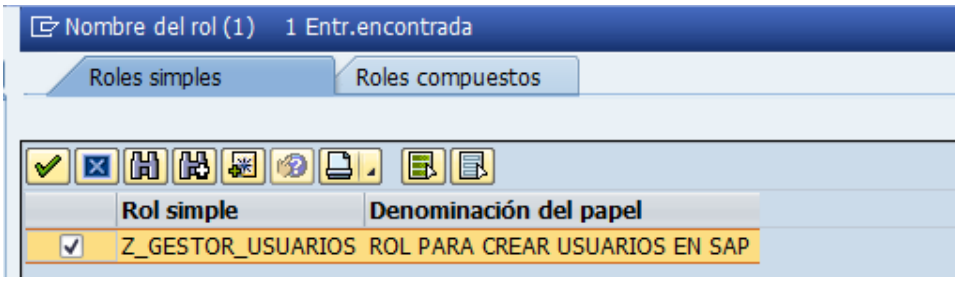
Figura 26. Modulo búsqueda de roles.



Fuente: El Autor

d) Seleccionar el rol que se desea asignar y clic en el botón (tomar).

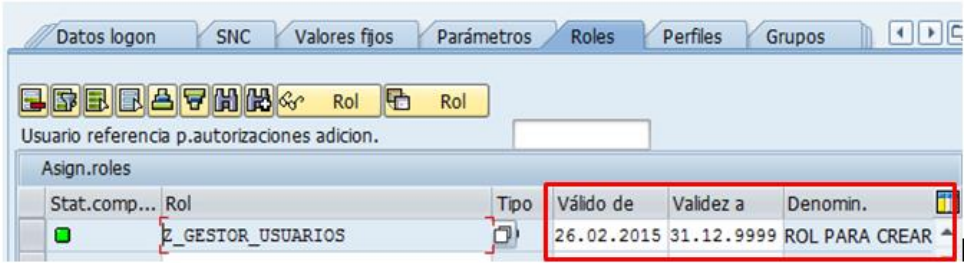
Figura 27. Seleccionar roles a asignar.



Fuente: El Autor

e) Posterior a seleccionar el rol se procede a definir la valides del rol, en el campo valido de (se ingresa la misma fecha de ingreso del funcionario y la validez se determinará según la solicitud que radiquen en la mesa de servicios.

Figura 28. Ajuste vigencia Roles.



Fuente: El Autor

f) Proceder a guardar los cambios dando clic en el icono (guardar)

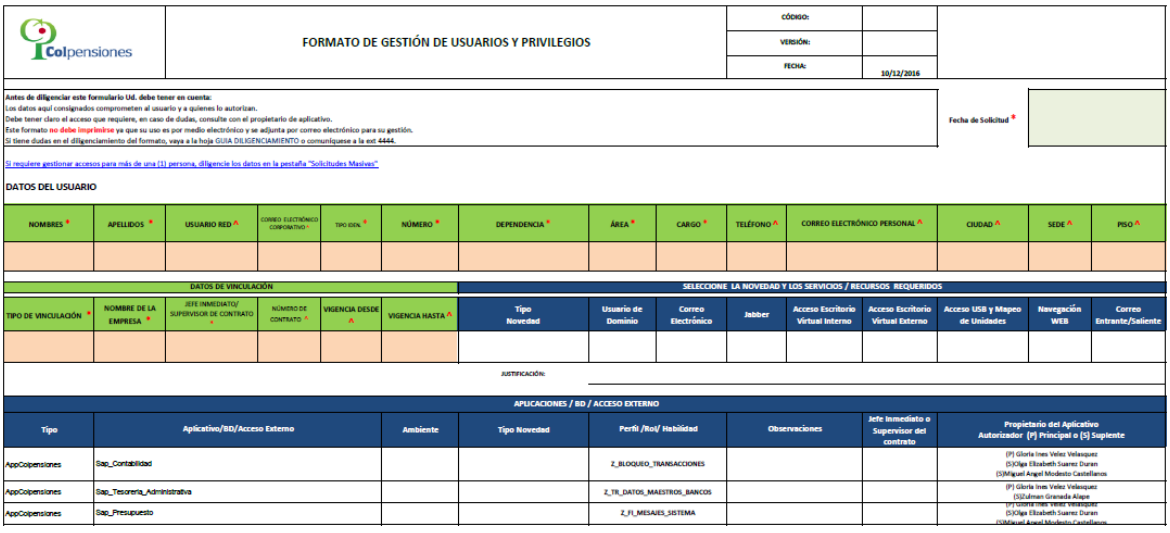
Figura 29. Guardar cambios en asignación de roles.

Fuente: El Autor

Anexo F. Formato de gestión de usuarios y privilegios.

Los nuevos roles fueron relacionados en el formato de gestión de usuarios y privilegios de la organización y divulgado entre las áreas para que hagan uso del mismo de acuerdo al flujo de autorización expuesto anteriormente.

Figura 30. Ejemplo formato Gestión de usuarios y privilegios.



Colpensiones

FORMATO DE GESTIÓN DE USUARIOS Y PRIVILEGIOS

CÓDIGO:
VERSIÓN:
FECHA: 10/12/2016

Antes de diligenciar este formulario Ud. debe tener en cuenta:
Los datos aquí consignados comprometen al usuario y a quienes lo autorizan.
Debe tener claro el acceso que requiere, en caso de dudas, consulte con el propietario de aplicativo.
Este formato no debe imprimirse ya que su uso es por medio electrónico y se adjunta por correo electrónico para su gestión.
Si tiene dudas en el diligenciamiento del formato, vaya a la hoja GUIA DILIGENCIAMIENTO o comuníquese a la ext 4444.

Fecha de Solicitud *

Si requiere gestionar accesos para más de una (1) persona, diligencie los datos en la pestaña "Solicitudes Masivas"

DATOS DEL USUARIO

NOMBRES *	APELLIDOS *	USUARIO RED ^	CORREO ELECTRÓNICO CORPORATIVO *	TIPO IDEN. *	NÚMERO *	DEPENDENCIA *	ÁREA *	CARGO *	TELÉFONO ^	CORREO ELECTRÓNICO PERSONAL ^	CIUDAD ^	SEDE ^	PISO ^

DATOS DE VINCULACIÓN						SELECCIONE LA NOVEDAD Y LOS SERVICIOS / RECURSOS REQUERIDOS								
TIPO DE VINCULACIÓN *	NOMBRE DE LA EMPRESA *	JEFE INMEDIATO/ SUPERVISOR DE CONTRATO *	NÚMERO DE CONTRATO ^	VIGENCIA DESDE ^	VIGENCIA HASTA ^	Tipo Novedad	Usuario de Dominio	Correo Electrónico	Jabber	Acceso Escritorio Virtual Interno	Acceso Escritorio Virtual Externo	Acceso USB y Mapeo de Unidades	Navegación WEB	Correo Entrante/Saliente

JUSTIFICACIÓN:

APLICACIONES / BD / ACCESO EXTERNO

Tipo	Aplicativo/BD/Acceso Externo	Ambiente	Tipo Novedad	Perfil /Rol/ Habilidad	Observaciones	Jefe Inmediato o Supervisor del contrato	Propietario del Aplicativo Autorizador (P) Principal o (S) Suplente
AppColpensiones	Sap_Contabilidad			Z_BLOQUEO_TRANSACCIONES			(P) Gloria Ines Velez Velasquez (S)Olga Elizabeth Suarez Duran (S)Miguel Angel Modesto Castellanos
AppColpensiones	Sap_Tesoreria_Administrativa			Z_TR_DATOS_MAESTROS_BANCOS			(P) Gloria Ines Velez Velasquez (S)Zulman Granada Alape
AppColpensiones	Sap_Presupuesto			Z_FI_MESAJES_SISTEMA			(P) Gloria Ines Velez Velasquez (S)Olga Elizabeth Suarez Duran (S)Miguel Angel Modesto Castellanos

Fuente: El Autor

Anexo G. Instructivo para el bloqueo de usuarios e inactivación de los roles

OBJETIVO

Presentar el instructivo para realizar masivamente bloqueos de cuentas y desbloqueos de las mismas en SAP.

ALCANCE

El presente instructivo brinda el paso a paso para el bloqueo y desbloqueo masivo de usuarios con el fin de minimizar los tiempos en la ejecución de actividades diarias.

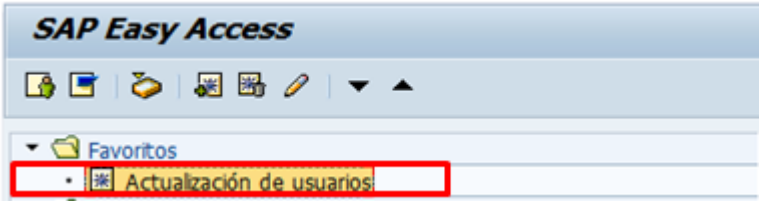
RESPONSABLE

La aplicación del instructivo, así como el acatamiento de sus principios y directrices es responsabilidad del gestor de accesos del aplicativo SAP.

Instructivo

a) Doble clic en la transaccion **Actualizacion de usuarios.**

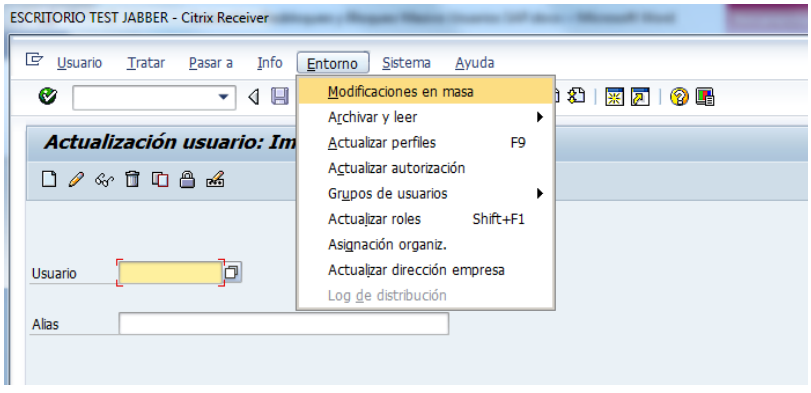
Figura 31. Ingreso modulo usuarios.



Fuente: El Autor

b) En el menu **Entorno** ingresamos seleccionamos a la opcion **Modificaciones en masa** y damos clic.

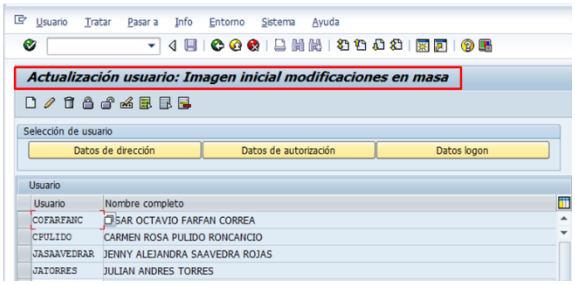
Figura 32 Modificación en masa usuarios.



Fuente: El Autor

c) Nos aparece pantalla de Modificaciones en masa, en esta pegaremos **(ctrl+v)** o **(clic derecho pegar)** en las filas los usuarios que deseamos modificar como aparece en la siguiente imagen.

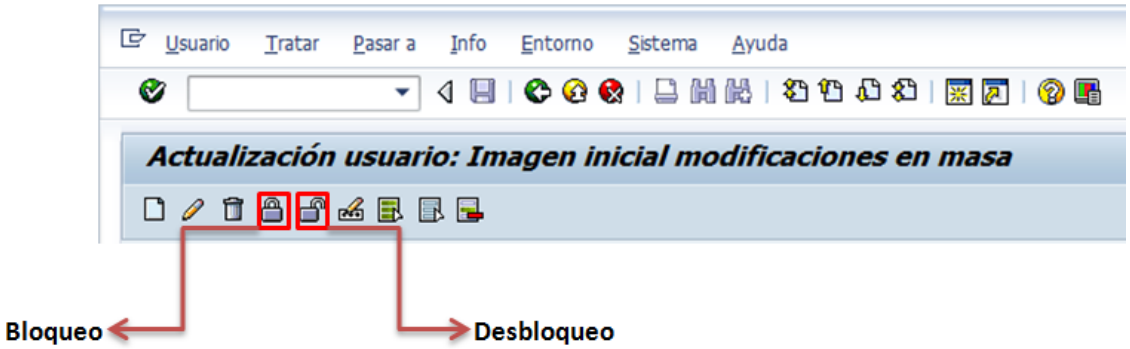
Figura 33. Actualización estado Usuario



Fuente: El autor

d) Posterior se realizara la actividad que sea necesaria como: bloqueo masivo o desbloqueo masivo dando clic en los iconos según sea el caso.

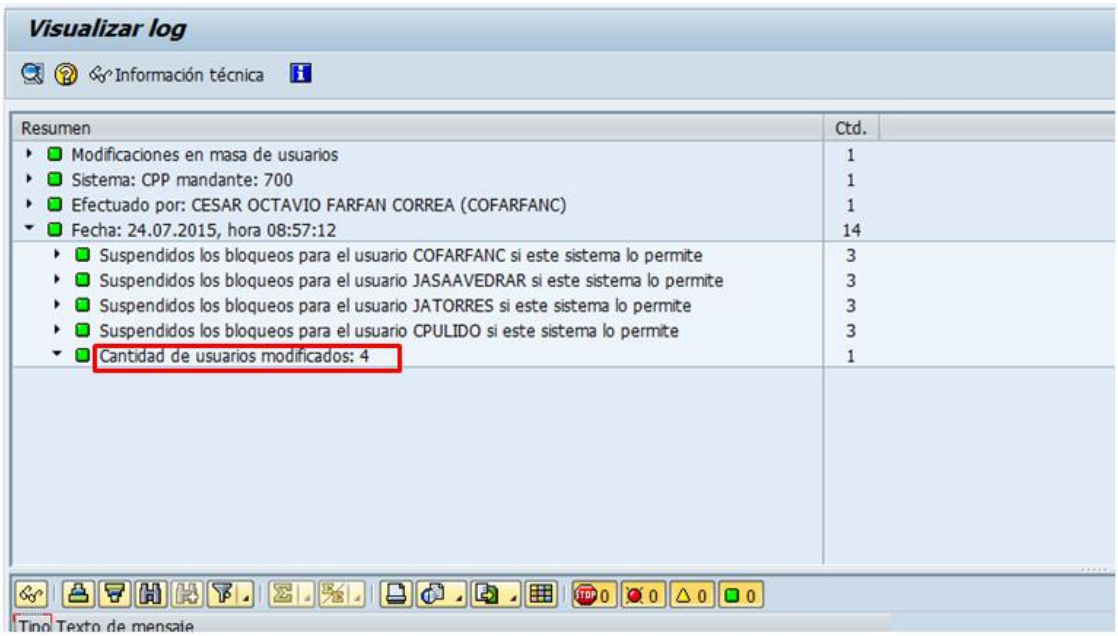
Figura 34. Selección acción que se aplicara sobre el usuario.



Fuente: El autor

e) Al dar clic en las opciones de bloqueo o desbloqueo el sistema despliega mensaje indicando el estado de la ejecución y como se evidencia en la gráfica la cantidad de usuarios modificados.

Figura 35. Visualizar log de evento.



Fuente: El autor

Anexo H.Informe De Cierre De Proyecto Análisis Del Nivel De Seguridad De Los Roles y Privilegios, En el Sistema SAP ERP de Colpensiones.

ANTECEDENTES

De acuerdo al diagnóstico de segregación de funciones en el sistema de información SAP se evidencio:

- Ausencia de matriz de roles por cargo, falta de lineamientos formalizados que especifiquen los roles por cargos para cada proceso de negocio, que deben tenerse en cuenta como base para realizar la asignación de permisos.
- No se observa un procedimiento formalizado para la asignación de autorizaciones a usuarios en el sistema SAP, que incluya el aval y control de los dueños de proceso previo a otorgar el acceso al sistema.

- La administración del sistema SAP carece de un plan de trabajo detallado y formalizado para la administración, control y monitoreo de actividades críticas, en la cual se defina, objetivo, alcance, esfuerzo, roles, responsabilidades, estrategias, lineamientos técnicos, actividades transversales y prioritarias en temas tales como:

  - ✓ Administración, control y monitoreo de segregación de funciones.
  - ✓ Asignación, modificación y eliminación de roles y transacciones.
  - ✓ Estándar para la creación de roles en ambiente productivo.
  - ✓ Estándar para la creación de usuarios en ambientes SAP.

PLAN DE ACCION

De acuerdo a los hallazgos valorados en el informe de la Oficina de control Interno la Vicepresidencia de Operaciones Y Tecnología estableció un plan de mejoramiento con el fin dar solución al hallazgo garantizando lo siguiente:

- ✓ Roles libres de conflictos de segregación de funciones.
- ✓ Roles con autorizaciones a funciones de negocio para reflejar una función de trabajo específica.
- ✓ Transacciones u opciones de menú asignadas a un único rol.
- ✓ Los roles de visualización no deben contener actividades de modificación.
- ✓ Las transacciones de consulta deben estar separadas de creación, modificación, borrado, anulación.

Perfilamiento Roles SAP: Se efectuó la reestructuración de permisos, a nivel de roles y transacción en el ERP de SAP, con el fin de garantizar la correcta segregación de funciones, de acuerdo a lo anterior se realizaron las siguientes actividades con el apoyo de los funcionarios asignados por la Gerencia Nacional Económica:

- ✓ Conformación del grupo de trabajo, con los funcionarios de la Gerencia Nacional Económica (GNE) y del grupo de seguridad y gestión de accesos de la Vicepresidencia de Operaciones y Tecnología.
- ✓ Se diseñó la matriz de asignación de roles, usuarios y transacción de la Gerencia Nacional Económica.
- ✓ Se revisaron los roles y transacciones descritas en la matriz.
- ✓ Se agruparon las transacciones SAP por funcionalidad.
- ✓ Se crearon los roles en el mandante de calidad en el sistema de información SAP.

- ✓ Se realizaron las pruebas y se certificaron por parte de los usuarios funcionales de la GNE, distribuidos en las coordinaciones de presupuesto, contabilidad y tesorería.
- ✓ De acuerdo a los resultados de las pruebas se ajustaron los perfiles y objetos de autorización asociados a las transacciones.
- ✓ Se efectuó la documentación de las pruebas por parte de los usuarios funcionales.
- ✓ Se formalizó la matriz de roles, diseñada por usuarios, cargo, transacciones y procesos.
- ✓ Se efectuó el paso a productivo de los roles y permisos a los usuarios funcionales.
- ✓ Se realizó la formalización por parte de la VOT del formato de gestión de usuarios y privilegios actualizado con los responsables del proceso de la Gerencia Nacional Económica

La información y los soportes se encuentran en la siguiente ruta del drive a la cual se les otorgo permisos de consulta a los siguientes funcionarios:

givelezv@colpensiones.gov.co
zugranadaa@colpensiones.gov.co
oesuarezd@colpensiones.gov.co
mmodesto@colpensiones.gov.co
lanietor@colpensiones.gov.co

En la siguiente ruta del drive

https://drive.google.com/open?id=0B2_9N0dHsowXMFZ0QUIwNk9TM00

RESULTADOS OBTENIDOS

A continuación, se relacionan los roles, transacciones y descripciones, presentadas el día 06 de octubre de 2016 a la Vicepresidencia de Operaciones y Tecnología, Vicepresidencia Administrativa, el grupo de seguridad y gestión de accesos y a la Gerencia Nacional Económica:

Tabla 6. Información de los roles, transacciones que lo componen y descripción de las misma se crearon 35 roles y el total de transacciones asociadas es de 443.

Rol	Nombre Transacción	Descripción Transacción
Z_AA_ACIVOS	AFAB	Contabilizar amortización
	AFBP	Crear log de contabilización Amo
	AW01N	Asset Explorer
Z_AA_VISUALIZAR_ACTIVOS	AS03	Visual.registro maestro AF
Z_BLOQUEO_TRANSACCIONES	SM01	Bloquear transacciones
Z_FI_ACTUALIZACION_SET	GS02	Modificar set
Z_FI_ANULACIONES	AB08	Anular partidas indiv.de act.fijos
	F.80	Anular documentos en masa
	FB02	Modificar documento
	FB08	Anular documento
	FB18	Actualizar textos mail estándar
	FBRA	Anular compensación
	MR8M	Anulación doc.factura
Z_FI_CAJAS_MENORES	FBCJ	Libro de caja
	FBCJC6	Actualiz.rango números: CAJO_DOC3
	S_ALR_87012309	Libro de caja
	Z_ALR_87012309	Libro de caja
	ZTR010	**ABAP - Conciliación Bancaria**
	FS00	**Actual.dat.mtros.cta.mayor**
	FS03	**Visualizar maestro**
	FSP0	**Reg.ctas.mayor en plan ctas.**
	KE51	**Crear centro de beneficio**
	LSMW	**Legacy System Migration Workbench**
	S_ALR_87002480	**Actividad IMG: CFORFBTHKON**

Tabla 5. (Continuación)

Rol	Nombre Transacción	Descripción Transacción
Z_FM_CIERRE	FMBOSTAT	Obj.presupuesto - Actualizar status
	FMCI_COPY_NEXT_YEAR	Copiar pos.presup.en año siguiente
	FMCYRESET	Anular datos presupuesto (prepar.)
	FMIR	Actual.detallada reglas per.abiertos
	FMJ0	Saldo cero manual
	FMJ2	Cierre ejerc.: Arrastrar comprom.
	FMJ3	Anular arrastre de comprometido
	FMMC	Cierre de comprometido CP
	FMMI	Actualiz.en masa interv.abiertos
	FMOD	Sustituya fecha de actualización CP
	FMOPER	Períodos presupuestación abiertos
	FMRE_SERLK	Cierre de documentos presupuestarios
	FMYC	Control del control presupuestario
	FMYCR	Asignación de objeto CP: Actualiz.
Z_FM_CONSULTA_PRESUPUESTO	FM3N	Pos.presupuestarias p.ctas.de mayor
	FMCIE	Visualizar pos.presup.: Jerarquía
	FMRP_RFFMEP1OX	Comprometido y traslados de recursos
	FMX3	Visualizar reserva de recursos
	FMZ3	Visual.compromiso gastos
	ZBC05A	Ejecución Presupuestal de Gastos
	ZBC111	Ingresos por CeGe
	ZBC112	Ingresos por PosPre
	ZBC12A	Ejecución Pptal acumulada por PosPre
Z_FM_EJECUCION_PRESUPUESTAL	FMBB	Workbench presupuestación
	FMN0	Prog.postcontabilización docs.FI
	FMN4N	Reestructuración de pedidos
	FMN5N	Reestructuración documentos presup.
	FMW1	Crear bloqueo de recursos
	FMW2	Modificar bloqueo recursos
	FMWA	Crear traslado de recursos
	FMX1	Crear reserva de recursos
	FMX2	Modificar reserva de recursos
	FMX6	Reducción manual reserva recursos
	FMZ1	Crear compromiso gastos
	FMZ2	Modif compromiso gastos
	FMZ6	Reducción manual compromiso gastos
	ME28	Liberar pedido
	ME29N	Liberar pedido
	ZHCM_CONTRIBUCIONES	Cuadro de Contribuciones
	ZHCM_REPORT_INTPRESU	Reporte Integración Presupuestal

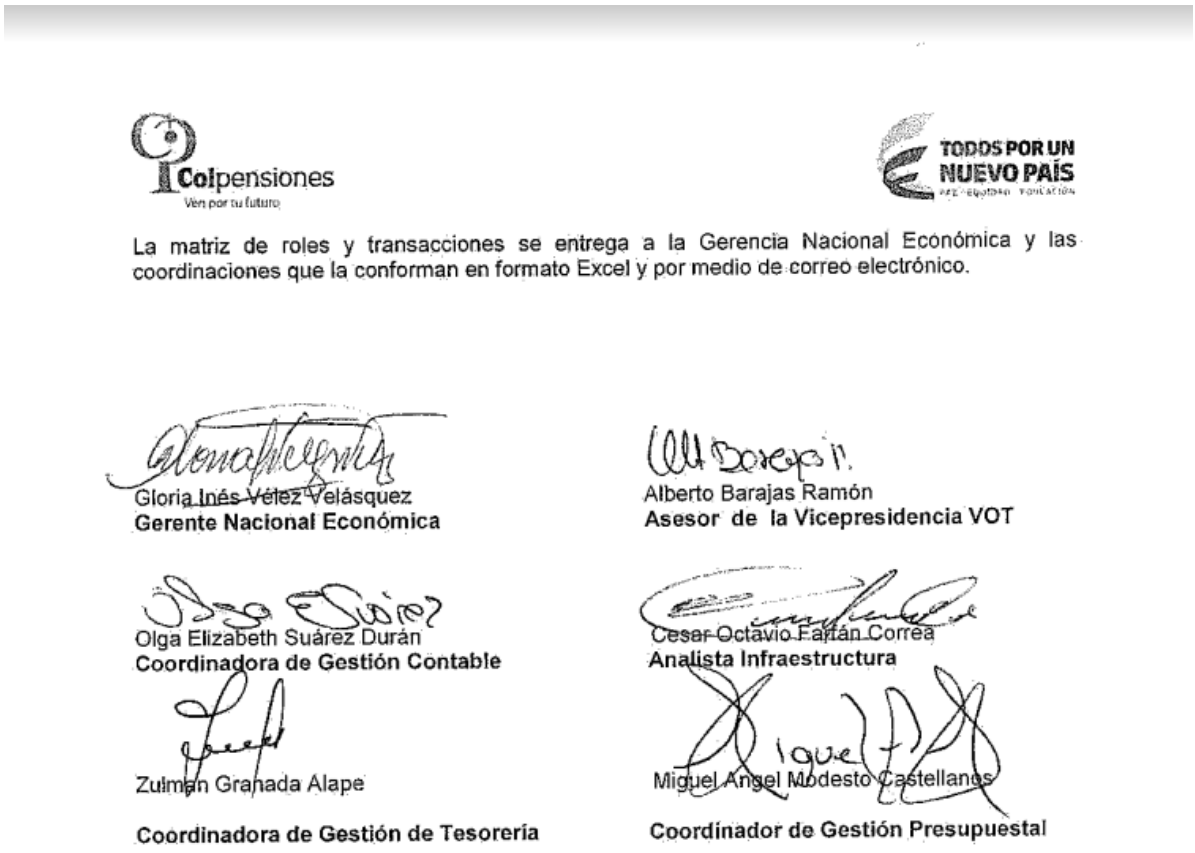
Tabla 5. (Continuación)

Rol	Nombre Transacción	Descripción Transacción
Z_FI_VISUALIZAR_CONTABILIDAD	F.01	Report ABAP: Balance
	F.10	Libro mayor: Planes cuentas
	FAGLB03	Visualización de saldos
	FAGLL03	PIs, cuentas de mayor (nuevo)
	FB03	Visualizar documento
	FBL1N	Partida individual acreedor
	FBL3N	Partida individual cuentas mayor
	FBL5N	Partida individual deudores
	FBV3	Visualizar documento preliminar
	FD10N	Visualización de saldos: Deudores
	FK10N	Visualización de saldos: Acreedores
	FS03	Visualizar maestro
	FS10N	Visualización de saldos
	KS03	Visualizar un centro de coste
	MK03	Visualizar acreedor (compras)
	OBYC	C FI Tabla T030 rmk+espacio
	S_ALR_87012284	Balance/PyG
	S_ALR_87012326	Plan de cuentas
	S_ALR_87012332	Extractos ctas.deud./acreed./mayor
	S_ALR_87013611	Centros coste: Real/Plan/Desviación

Fuente: El autor.

La matriz de roles y transacciones se entrega a la Gerencia Nacional Económica y las coordinaciones que la conforman en formato Excel y por medio de correo electrónico.

Figura 36 Evidencia Firma Matriz Roles Y transacciones Construida.



Fuente: El autor.

Anexo I Resumen analítico RAE.

Título del texto	Análisis del nivel de seguridad de los roles y privilegios, en el sistema sap erp de colpensiones, tomando como referencia la norma iso 27001 y las guías de seguridad de sap
Nombres y Apellidos del Autor	Cesar Octavio Farfán Correa
Año de la publicación	2017
Resumen del texto: El análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones se realizó con el fin de garantizar la adecuada configuración del sistema de información a través de roles que garanticen la correcta segregación de funciones, mitigando así los riesgos que puedan afectar la integridad, disponibilidad y confidencialidad de la información.	
Palabras Claves	Objeto autorización roles – Riesgo Amenaza Vulnerabilidad Control Procesos Segregación Principio Menor Privilegio QA Transporte.
Problema que aborda el texto: Esquema de roles y privilegios en Colpensiones que carece de un adecuado análisis de seguridad en cuanto a sus roles, privilegios, flujo de autorización para la asignación de los permisos y control sobre el ciclo de vida de los usuarios, poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información.	
Objetivos del texto: Realizar análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones que se tienen actualmente implementados.	
Hipótesis planteada por el autor: Al haberse realizado en análisis del nivel de seguridad del esquema de roles y privilegios de SAP, es importante contemplar la hipótesis de que por falta de	

previsión de las áreas que participaron en dicho proceso no hayan realizado e adecuado nivel de riesgos en cuanto a los conflictos de segregación de funciones.

Tesis principal del autor:

El análisis del nivel de seguridad de los roles y privilegios, en el sistema SAP ERP de Colpensiones se realizó con el fin de garantizar la adecuada configuración del sistema de información a través de roles que garanticen la correcta segregación de funciones, mitigando así los riesgos que puedan afectar la integridad, disponibilidad y confidencialidad de la información.

Argumentos expuestos por el autor:

El análisis del nivel de seguridad de los roles y privilegios se llevó a cabo utilizando la metodología acelerada de SAP la cual consta de 6 fases en la que cada fase corresponde a una serie de actividades a desarrollar, entregables y responsables de cada proceso, seguimiento a nivel de Project debidamente concertado con los involucrados en el proceso, reporte de avances e identificación de barreras que afectaran los cronogramas establecidos y validación de alternativas que brinden oportunidad de mejora continua del proyecto.

Conclusiones del texto:

El desarrollo del proyecto brindo a las áreas funcionales de Colpensiones la seguridad de contar con la asignación de roles específicos acordes a la necesidad de los procesos misionales, garantizando que no se presente conflictos de segregación de funciones, flujos de autorización debidamente establecidos y el aseguramiento de los parámetros críticos del sistema garantizando la confidencialidad, integridad y disponibilidad del activo de información SAP.

Bibliografía citada por el autor:

Mejores Prácticas en la Implementación de SAP {En línea}. {Consultado el 25 abril de 2016}. Disponible en: http://www.auditool.org/blog/control-interno/298-mejores-practicas-en-la implementación-de-sap.

10 razones de por qué elegir SAP como ERP para tu empresa {En línea}. {Consultado el 25 abril de 2016}. Disponible en: http://orekait.com/blog/por-que-elegir-sap-erp/

Segregación de funciones. Sistema de Información SAP 27001 {En línea}. {Consultado el 11 mayo de 2016}. Disponible en: http://www.kpmg.com/pe/es/servicios/advisory/consultoriaenriesgos/paginas/sod.aspx

Por qué SAP {En línea}. {Consultado el 16 mayo de 2016}. Disponible en: http://www.informatica-hoy.com.ar/sap/Que-es-SAP.php

[Vulnerabilidad {En línea}. {Consultado el 14 mayo de 2016}. Disponible en: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

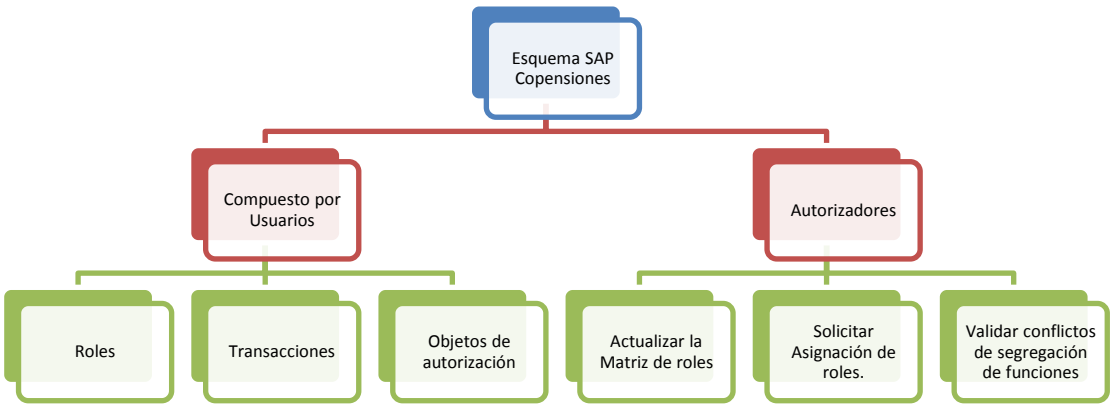
Juan Fuentes. Reingeniería de perfiles de seguridad informática para SAP Unificado para la empresa Venezuela. {En línea}. {01 de septiembre de 2008}. {Consultado el 15 de mayo 2016}. Disponible en: http://tesis.ula.ve/pregrado/tde_arquivos/8/TDE-2009-10-05T09:34:37Z-644/Publico/Fuentes%20Juan.pdf

Ley 1273 de 2009 {Consultado el 20 mayo de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

Enrich Cardona, Roger.Implantación de un sistema ERP SAP en una empresa {En línea}. {23 de febrero de 2013}. {Consultado el 10 de marzo 2016}. Disponible en: http://upcommons.upc.edu/bitstream/handle/2099.1/18382/PFC_Implantaci%C3%B3n%20de%20un%20sistema%20ERP%20SAP%20en%20una%20empresa.pdf?sequence=1

Nombre y apellidos de quien elaboró este RAE	Cesar Octavio Farfán Correa
Fecha en que se elaboró este RAE	29 de Julio de 2017

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:



Comentarios finales:

El proyecto brindo a la organización mecanismos y controles que garanticen la correcta agrupación de permisos a roles y la aplicación de las recomendaciones de SAP en cuanto a los parámetros de seguridad que debe tener el sistema ERP en el cual la organización tiene alojada su información de negocio.

9. CONCLUCIONES

El análisis realizado al modelo de seguridad de los roles y privilegios del sistema SAP ERP de Colpensiones permitió a la organización identificar los riesgos asociados al esquema implementado y las recomendaciones a seguir para mitigarlos garantizando el cumplimiento del principio del menor privilegio y la segregación de funciones entre sus áreas de trabajo.

Este proceso permitió concientizar a los grupos de trabajo la importancia de la seguridad en los sistemas de información y los beneficios que se obtienen al realizar el perfilamiento de los roles del sistema por procesos de negocio, documentados, con flujos de autorización establecidos y los respectivos controles de acceso definidos.

9.1. CONCLUCIONES

La búsqueda de metodologías para abordar este tipo de proyectos permitió ampliar los conocimientos sobre el sistema de información SAP, aterrizar los objetivos propuestos y poder presentar a las áreas de negocio un plan de trabajo que ofreciera la confianza de realizar cambios de alto impacto en sus procesos sin afectar significativamente la operación del servicio, brindar un soporte oportuno a las novedades que se presentaran y articular a las áreas de negocio con las áreas de tecnología, actividad que nunca se había realizado debido a que no se contaba con una metodología divulgada que permitiera realizar este tipo de integración y la cual fue fundamental para el logro de lo propuesto a la organización.

9.1.2. CONCLUCIONES

La política con los lineamientos para los roles del sistema que presentaron conflicto de segregación de funciones, permitió a las áreas de negocio en donde no fue posible segregar al menor privilegio implementar controles internos para reducir al máximo la materialización de los riesgos que conlleva convivir con este tipo de conflictos y contar con la documentación que soporte el motivo por el cual no fue posible separar ciertos procesos e identificar fácilmente los funcionarios que están expuestos a este tipo de riesgo, garantizando el cumplimiento de las recomendaciones realizadas por los entes de control de la organización.

Adicionalmente al dejar en evidencia la existencia de los conflictos de segregación de funciones las áreas de negocio expuestas iniciaron con procesos de capacitación y transferencia de conocimiento que permitan romper con la dependencia de ciertos funcionarios en procesos que deben ser ejecutados por 1 o varias personas en un flujo de trabajo establecido.

9.1.3. CONCLUCIONES

Al definir controles que garantizaran el ciclo de vida de los usuarios en el sistema de información SAP tales como control de vigencias a las cuentas de acceso, control de conexiones , control de expiración de cuentas de usuario , control de novedades de nómina, se evidencio que algunos sistemas de información no contaban con este tipo de mecanismos y fueron replicados con el fin de estandarizar la gestión de accesos en la organización y fortalecer las recomendaciones de las normas internacionales ISO como lo son los dominios de la 27002.

Las aplicaciones de controles en el ciclo de vida de los usuarios brindan a las organizaciones una capa más en su esquema de seguridad y mitigan los riesgos que se pueden derivar de no contar con los mismos.

10. REFERENCIAS BIBLIOGRÁFICAS

Mejores Prácticas en la Implementación de SAP {En línea}. {Consultado el 25 abril de 2016}. Disponible en: http://www.auditool.org/blog/control-interno/298-mejores-practicas-en-la implementacion-de-sap.

10 Razones de por qué elegir SAP como ERP para tu empresa {En línea}. {Consultado el 25 abril de 2016}. Disponible en: http://orekait.com/blog/por-que-elegir-sap-erp/

Segregación de funciones. Sistema de Información SAP 27001 {En línea}. {Consultado el 11 mayo de 2016}. Disponible en: http://www.kpmg.com/pe/es/servicios/advisory/consultoriaenriesgos/paginas/sod.aspx

Por qué SAP {En línea}. {Consultado el 16 mayo de 2016}. Disponible en: http://www.informatica-hoy.com.ar/sap/Que-es-SAP.php

[Vulnerabilidad {En línea}. {Consultado el 14 mayo de 2016}. Disponible en: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

Juan Fuentes. Reingeniería de perfiles de seguridad informática para SAP Unificado para la empresa Venezuela. {En línea}. {01 de septiembre de 2008}. {Consultado el 15 de Mayo 2016}. Disponible en: http://tesis.ula.ve/pregrado/tde_arquivos/8/TDE-2009-10-05T09:34:37Z-644/Publico/Fuentes%20Juan.pdf

Ley 1273 de 2009 {Consultado el 20 mayo de 2016}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

Enrich Cardona, Roger.Implantación de un sistema ERP SAP en una empresa {En línea}. {23 de febrero de 2013}. {Consultado el 10 de Marzo 2016}. Disponible en: http://upcommons.upc.edu/bitstream/handle/2099.1/18382/PFC_Implantaci%C3%B3n%20de%20un%20sistema%20ERP%20SAP%20en%20una%20empresa.pdf?sequence=1