ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

"REDUCCIÓN DE CONFLICTOS DE SEGREGACIÓN DE FUNCIONES EN SISTEMA ERP DE EMPRESA MULTINACIONAL COMERCIALIZADORA DE PRODUCTOS DE CONSUMO MASIVO"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

LETICIA ARACELI JARA JARA

GUAYAQUIL – ECUADOR

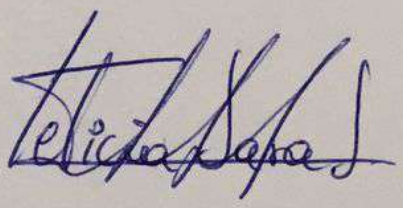
AÑO: 2017

AGRADECIMIENTO

Mis más sinceros agradecimientos a Dios por permitirme concluir este trabajo y a mi familia por apoyarme siempre y estar pendiente de mis logros profesionales.

DEDICATORIA

El presente proyecto lo dedico a mi familia y amigos y en especial a mi Madre que siempre me ha brindado su apoyo incondicional.



TRIBUNAL DE SUSTENTACIÓN

MGS. LENIN FREIRE

TUTOR

DIRECTOR DEL MSIG

MGS. JUAN CARLOS GARCÍA

TRIBUNAL

PROFESOR DELEGADO POR LA
UNIDAD ACADÉMICA

RESUMEN

Descripción del problema:

La empresa ejecutó un proyecto de migración de SAP R3 a SAP Netweaver. SAP R3 no tenía un módulo de Seguridades de tal forma que los roles técnicos de acceso a transacciones se asignaban directamente a los usuarios. SAP Netweaver ya incluye el módulo de Seguridades con las siguientes consideraciones:

- Los roles técnicos se agrupan en objetos denominados *roles de negocio*.
- Los usuarios se agrupan en objetos denominados *Jobs*.
- En lugar de asignar roles técnicos a usuarios se asignan *roles de negocio* a *Jobs*.

Debido a que un *rol de negocio* contiene más de un rol técnico, al asignarlo a los usuarios a través de los *Jobs* se otorgó accesos adicionales que causaron conflictos de segregación de funciones con los accesos previamente asignados.

Solución propuesta:

Debido a que los usuarios debían contar sólo con roles de acuerdo a sus funciones era necesario remover aquellos roles que generaban conflictos sin afectar la normal operación de la empresa. Para el efecto creamos un equipo especializado de profesionales con conocimientos de SAP en el módulo de Seguridades. Este equipo tenía la responsabilidad de identificar y analizar los riesgos, conflictos y códigos de transacción involucrados, así como los usuarios que hacían uso de estas transacciones y su frecuencia para finalmente proponer la remoción de aquellos accesos que ocasionaban los conflictos.

El equipo de especialistas reportó mensualmente al negocio las acciones de remoción efectuadas y los acuerdos a los que llegaba con el negocio para evitar estos riesgos evidenciando una disminución en el número de conflictos.

Los beneficios que ofrece esta solución son:

- La empresa registra un número bajo de conflictos de segregación de funciones contando con un sistema confiable y libre de riesgos financieros.
- La administración de accesos en SAP se centraliza en el equipo de especialistas en Seguridades quienes son los responsables de detectar nuevos conflictos bajo nuevas asignaciones o asignaciones no autorizadas y continuar con la limpieza de conflictos existentes.

ÍNDICE GENERAL

INTRODUCCIÓN

Mientras las empresas se apoyen con mayor frecuencia en aplicaciones informáticas para registrar sus operaciones y obtener así informes en línea acerca de sus ingresos y gastos, se ven obligadas a pre-cautelar sus finanzas sabiendo que el software que les sirve de soporte puede dar apertura a un sin número de riesgos si no se toman las acciones preventivas del caso. Adicionalmente la tecnología avanza a pasos agigantados dando lugar a nuevas iniciativas organizando de mejor manera las bases de datos, administración de usuarios de los sistemas y reduciendo los tiempos de respuesta ante los requerimientos de los ejecutivos de negocios. Es una realidad que si un software es implementado en una empresa, no pasan más de seis meses que nuevas versiones se encuentran disponibles que requieren sean actualizadas con el fin de estar al nivel de la competencia de otras aplicaciones o de otras empresas en cualquier parte del mundo. Esta necesidad de actualización surgió en la empresa que es objeto de nuestro análisis aumentando riesgos financieros cuyos conflictos técnicos relacionados debían ser eliminados y de no existir esa posibilidad debían ser implementados los controles adecuados de tal forma que el negocio logre minimizar los impactos financieros que podrían surgir sin una adecuada segregación de funciones.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

El Sistema SAP es un ERP (Enterprise Resource Planning) que apoya a la empresa en todas sus operaciones como Compras, Ventas, Registro y Movimiento de Inventarios, Contabilidad y Gestión del Recurso Humano. Como la empresa cuenta con procesos críticos y niveles de autorización, SAP otorga accesos al sistema a través de roles para asegurar que no todos los usuarios del sistema tengan acceso a todas las operaciones dentro de un proceso como por ejemplo Compras; sería crítico que un usuario tenga autorización para registrar pedidos de compras, aprobarlos y realizar su pago.

La empresa adquirió SAP en versión R/3 la cual no estaba integrada con el módulo de Gestión del Recurso Humano, en el año 2012 decide migrar a la versión SAP Netweaver con el fin de tener una mejor

organización en el modelo de Seguridad, un mayor control en la administración de usuarios al estar integrada con el módulo de Recursos Humanos y reducir el tiempo en la asignación de roles a los usuarios del sistema.

SAP Netweaver integra todas las aplicaciones SAP brindando al usuario la flexibilidad para ejecutar todas sus aplicaciones empresariales en una única plataforma integrada; entre las principales aplicaciones tenemos:

SAP NETWEAVER	
Aplicación SAP	**También conocido como...**
Enterprise Central Component	ECC, R/3, EP7
Supplier Relationship Management	SRM, GP2
Customer Relationship Management	CRM, LPN
Mobile Infrastructure	MI, EPM, GP2
Human Capital Management	HR, HCM, GP8
Business Intelligence	BI, BW, ER1
Master Data Management	MDM, GR7

Figura 1.1: Aplicaciones integradas en SAP Netweaver.

Los usuarios ingresan a SAP Netweaver haciendo click en este icono instalado en su equipo de trabajo.

1.2 ROLES EN SAP

Los roles técnicos son objetos a través de los cuales podemos otorgar permisos a los usuarios para que realicen sus operaciones en SAP.

Las operaciones son realizadas a través de la ejecución de códigos de transacción, por ejemplo la transacción ME21N permite crear órdenes de compra mientras que la transacción ME29N permite liberar o aprobar estas órdenes. Para evitar algún fraude en el sistema un usuario no debe tener acceso a las dos transacciones a la vez por lo tanto cada transacción está contenida en un rol distinto.

SEGURIDAD SAP		
Rol Técnico	**Transacción**	**Usuario SAP**
Rol Técnico A	ME21N – Crear órdenes de compra	Analista de Compras
Rol Técnico B	ME29N – Aprobar órdenes de compra	Gerente de Compras

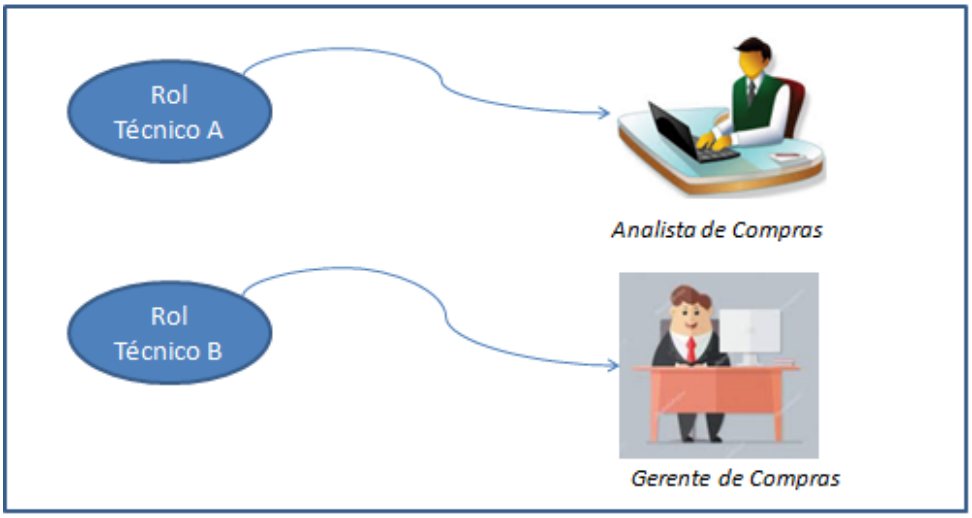


Figura 1.2: Ejemplo de roles que dan acceso a transacciones de Compras.

1.2.1 GLOSARIO DE TÉRMINOS.

ERP.- Son las siglas en inglés de Enterprise Resource Planning y se refiere a una aplicación informática que gestiona en forma integrada todos los procesos de negocio de una empresa.

SAP: Es un programa para aplicaciones de negocios. Sus siglas corresponden a "Systems, Applications, Products in Data Processing" de tal forma que SAP es Sistemas, Aplicaciones y Productos para el procesamiento de datos.

Transacción: Opción de SAP que permite a un usuario ejecutar una actividad en el sistema. Es un código de letras y números que al ser ejecutado en SAP el usuario tiene acceso a una pantalla de ingreso, consulta o modificación de datos del sistema.

Rol Técnico.- Grupo mínimo de transacciones SAP asignables a un usuario.

Función.- Actividad específica que puede, en algunos casos, ser ejecutada por una o más transacciones SAP. Estas pueden estar ubicadas en uno o más roles.

Segregación de funciones.- Es asegurar que un usuario no tenga los privilegios en el sistema para ejecutar dos o más

transacciones en conflicto que podrían poner en riesgo a la empresa.

Regla de segregación de funciones.- Combinación de dos o más funciones incompatibles. También conocida como riesgo de segregación de funciones.

Conflicto de segregación de funciones.- Es el incumplimiento de una regla o riesgo de segregación de funciones. Se genera un conflicto o problema cuando se combinan dos o más transacciones sensibles.

Los conflictos pueden ser analizados en dos niveles: Funcionales y Técnicos.

Conflicto Funcional.- Un usuario que ha quebrado una regla de segregación de funciones. También conocido como instancia de riesgo de segregación de funciones.

Conflicto Técnico.- Diferentes formas (diferentes transacciones) en las que un usuario ha quebrado una regla. Un solo conflicto funcional podría estar compuesto por varios conflictos técnicos.

Transacción sensible.- Una transacción que, al ser ejecutada en el sistema, afecta en forma negativa a los estados financieros de una empresa.

SAP Netweaver.- Es la base técnica de la familia de soluciones SAP.

Posición.- Asignación específica a los empleados de una empresa. Es un código de 8 caracteres e inicia con la secuencia 400 para Ecuador. Ejemplo: 40006442.

Directorio Activo.- Es un servicio establecido en un servidor en donde se crean usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red de una empresa, así como también la administración de políticas en toda la red.

SAP HCM (SAP Human Capital Management): Es una solución completa e integral de gestión de los recursos humanos. SAP HCM ofrece las herramientas necesarias para gestionar el personal de la empresa.

SAP IDM (SAP Identity Management): Es una aplicación de SAP Netweaver perteneciente a la Seguridad de SAP en donde

se administra en forma centralizada las identidades y accesos a usuarios SAP, para reducir riesgos y mejorar la seguridad.

Rol de Negocio.- Proporciona una perspectiva empresarial representando las tareas y actividades que un usuario está autorizado a realizar en el sistema SAP. Un Rol de Negocio está asociado a un Rol Técnico, a uno o más Roles Prescriptivos y a uno o más Roles de Valor Organizacional.

Country Job: Cargo de país que agrupa a los Roles de Negocio. Define las responsabilidades relacionadas a los procesos del negocio.

Mapeo de Roles: Consolidación de Country Jobs asignados a posiciones y empleados.

Job: Puesto de trabajo. Función que realiza el empleado en la empresa.

GRC (Gobierno, Riesgo y Cumplimiento): Herramienta de SAP diseñada para permitir a la organización tener una visión continua sobre sus actividades clave de cumplimiento en todos sus procesos de negocio, de esta forma asegurar un nivel elevado de cumplimiento de los controles internos.

Custodio de Accesos: Es el dueño de los roles inherentes a su proceso y por lo tanto de los accesos de los usuarios SAP, es quien aprueba o rechaza los requerimientos de asignación de roles a los usuarios del negocio.

MDA (Mesa de Ayuda): Es un conjunto de recursos tecnológicos y humanos destinado a prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las Tecnologías de la Información y la Comunicación.

Número de ticket: Número de caso asignado por la Mesa de Ayuda y con el cual se hace seguimiento al incidente o requerimiento solicitado por el usuario.

Requerimiento: Solicitud que genera la mejora del sistema, ya sea por funcionalidad o por ajuste. Además se consideran requerimientos aquellas solicitudes que permitan la utilización de alguna funcionalidad provista por el sistema, como lo son la creación de un usuario o la asignación de roles.

RH (Recursos Humanos): Es el área que administra (selecciona, contrata, forma, emplea y retiene) al personal de la empresa.

Gerente de Línea: Es el gestor al que los empleados o equipos individuales reportan directamente.

1.2.2 DISEÑO DE ROLES EN SAP R3 Y SAP NETWEAVER.

Los roles técnicos permiten la ejecución de una o más transacciones en SAP así como proveen autorización a uno o más Valores Empresariales como Sociedad o Centro y a una o más actividades como Consulta, Ingreso o Modificación. Por ejemplo el rol técnico PR0000.PUR_ORD_CRE permite ejecutar la transacción ME21N además de las listadas a continuación:

SEGURIDAD SAP	
Rol Técnico	**Transacción**
PR0000.PUR_ORD_CRE	ME21N – Crear órdenes de compra
	ME56 – Asignar solicitudes de pedido a proveedor
	ME57 – Grabar petición de oferta
	ME59N – Generación automática de órdenes de compra

Figura 1.3: Ejemplo de usuario asignado a un rol técnico con autorización a ejecutar cinco transacciones.

MODELO DE SEGURIDAD EN SAP R/3

ADMINISTRACIÓN DE USUARIOS

Los usuarios son creados en el sistema con la transacción SU01, esta operación se realiza dentro de cada aplicación SAP a la que requiere acceso el usuario registrando el código y nombre del usuario.

Debido a que los usuarios se crean en forma manual, se dan casos en los que se pueden crear usuarios genéricos para ser asignados a personas ajenas a la empresa como por ejemplo a los Auditores Externos y puedan consultar cierta información relacionada con sus funciones. Además, un empleado puede acceder a SAP con uno o más usuarios asignados a su persona. Esto genera un riesgo ya que podría darse el caso de que un Analista de Compras posea dos usuarios SAP, uno para generar órdenes de compra y otro para aprobar estas órdenes.

Los roles técnicos son asignados a los usuarios con la transacción PFCG.

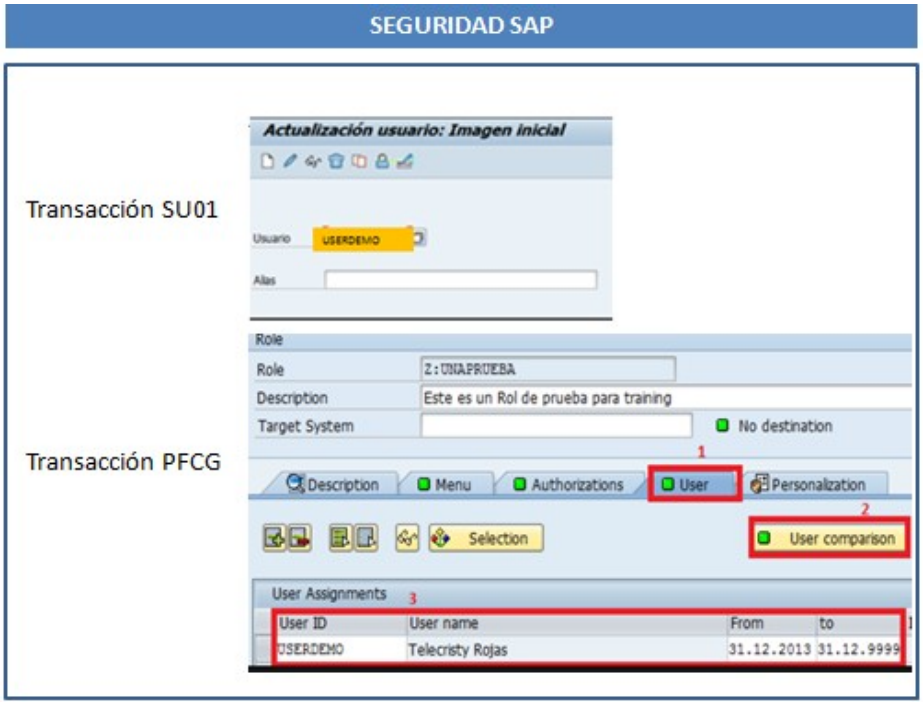


Figura 1.4: Transacciones en SAP que permiten administrar usuarios y roles.

ADMINISTRACIÓN DE ROLES

Cuando un usuario requiere acceso a una transacción determinada, el personal de soporte busca en el sistema los roles que contienen esta transacción, solicita la aprobación respectiva al negocio y asigna el o los roles aprobados al usuario. Como se observa, la asignación de roles se hace al usuario y no al cargo o posición que ocupa la persona que solicita el acceso, de esta forma, si por ejemplo el área de Compras tiene dos Analistas y sólo uno de ellos solicita la

nueva transacción, sólo el Analista que lo solicita contará con este acceso cuando los dos Analistas deberían tenerlo.

Figura 1.5: Menú SAP de los Analistas de Compras antes de levantar el requerimiento de accesos.

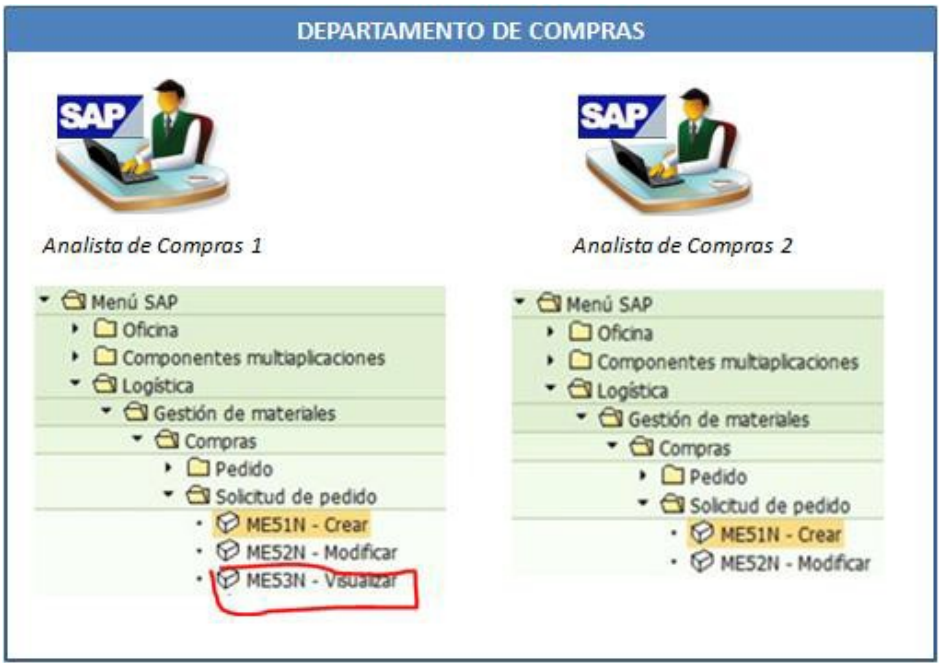


Figura 1.6: Menú SAP de los Analistas de Compras luego de ser atendido el requerimiento de accesos. Se observa que sólo el Analista de Compras 1 cuenta con la transacción solicitada (ME53N).

MODELO DE SEGURIDAD EN SAP NETWEAVER

En SAP Netweaver los roles técnicos son asignados a una Posición y un usuario vinculado a esa posición hereda los roles.

ADMINISTRACIÓN DE USUARIOS

Una Posición está vinculada a uno o más roles técnicos, esta posición fue creada previamente en SAP HCM cumpliendo la creación del cargo solicitado por el Gerente de Línea de la empresa.

Una vez que el empleado es contratado, el área de Recursos Humanos crea en SAP HCM el Número de Empleado y lo vincula a la Posición creada previamente, luego solicita al área de soporte la creación del Usuario de Red del empleado en el Directorio Activo de la empresa.

Finalmente un Job automático que se ejecuta diariamente en SAP toma el Número de Empleado y Usuario de Red del Directorio Activo, lee de SAP HCM la Posición en base al Número de Empleado, va a SAP IDM y toma los roles técnicos relacionados a la Posición para vincularlos al Usuario de Red. De esta forma el Usuario de Red queda asignado con los roles técnicos de la Posición asignada en HCM.

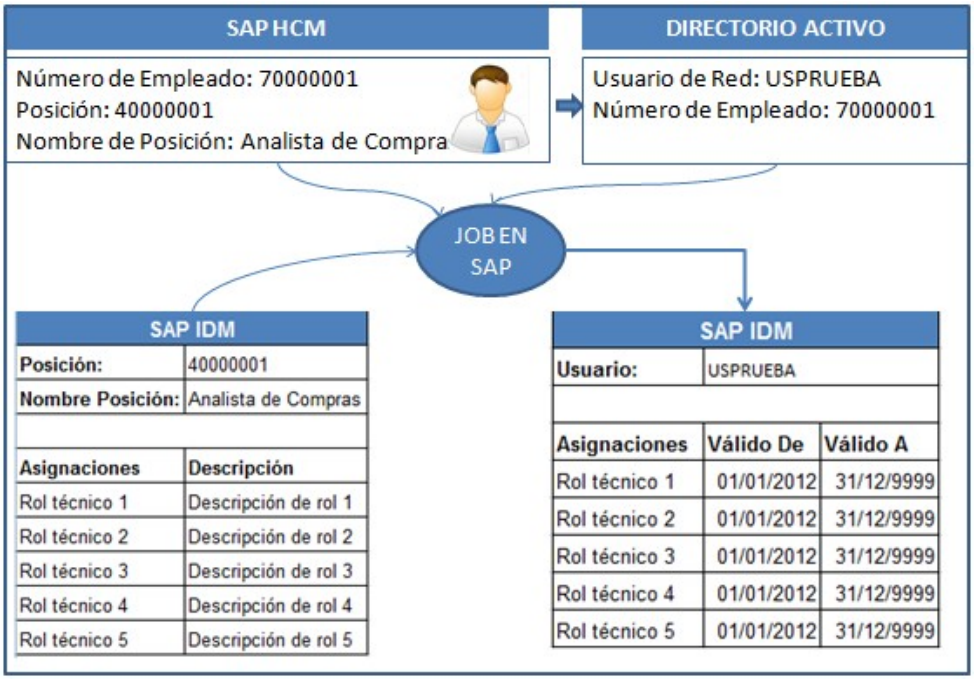


Figura 1.7: Proceso de creación de Usuario SAP a partir de la creación del Número de Empleado en SAP HCM.

ADMINISTRACIÓN DE ROLES

El equipo del proyecto de migración realizó un mapeo de roles apoyado con los expertos de los procesos del negocio. Esta actividad fue documentada en matrices elaboradas en Excel. Estas matrices contienen:

El Maestro de Empleados.- Listado de Empleados con nombres completos, su Función y Posición dentro de la Estructura Organizacional de la empresa.

El Catálogo de Roles de Negocio.- Listado de Roles de Negocio y sus correspondientes Roles Técnicos y Transacciones relacionadas.

La definición de Country Jobs.- Listado de códigos de Country Jobs con su descripción y correspondientes Roles de Negocio.

El listado de Roles de Valor Organizacional.

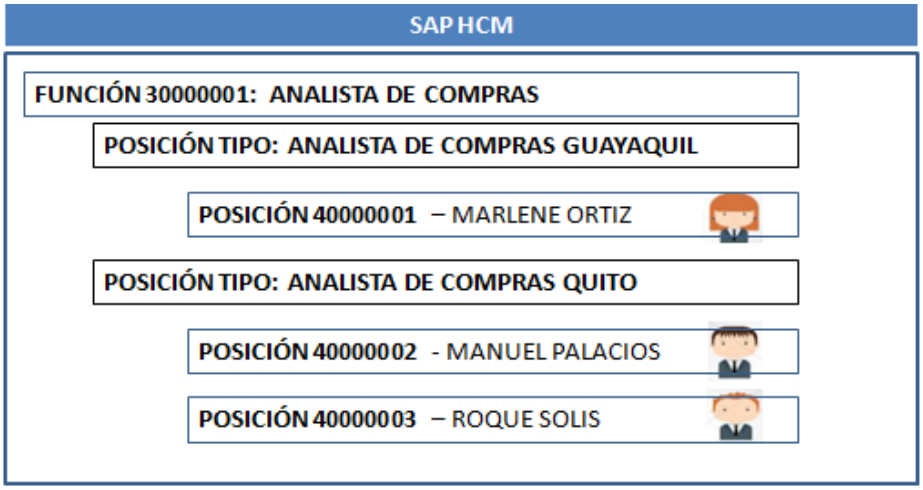


Figura 1.8 Ejemplo de posiciones configuradas dentro de una Función o Job.

La vinculación de Funciones a Country Jobs y Posiciones se registra en el archivo Maestro de Empleados y corresponde actualizarlo dos veces al mes debido a los movimientos de ingresos, salidas y cambios de Posición de los Empleados de la empresa.

MAESTRO DE EMPLEADOS				
Función	Country Job	Nombre de Country Job	Identificador de Posición	Nombre de Posición
30000001	ECCTJ_001	EC_COMPRAS_ANALISTA DE COMPRAS	40000001	ANALISTA DE COMPRAS GUAYAQUIL
30000001	ECCTJ_001	EC_COMPRAS_ANALISTA DE COMPRAS	40000002	ANALISTA DE COMPRAS QUITO
30000001	ECCTJ_001	EC_COMPRAS_ANALISTA DE COMPRAS	40000003	ANALISTA DE COMPRAS QUITO

Figura 1.9: Ejemplo de vinculación de la Función 30000001 de SAP HCM con el Country Job ECCTJ_001.

En el Catálogo de Roles cada Rol de Negocio contiene las autorizaciones necesarias para cumplir con una tarea específica, por ejemplo: Crear órdenes de compra. Esta tarea está definida en cinco roles de negocio porque va a depender de la clase de compra que realiza el negocio, esto es, de Materiales Directos, Indirectos, Documentos Confidenciales, Transporte de Existencias o Gastos de Envío. Por esta razón un Rol de Negocio está compuesto de un Rol Técnico, uno o más Roles Prescriptivos y uno o más Roles de Valor Organizacional.

El Rol Técnico es el objeto en SAP que provee autorización para ejecutar la transacción, Ejemplo: ME21N - Creación de órdenes de compra. Los roles prescriptivos son roles técnicos en SAP que autorizan la actividad a ser realizada dentro de la transacción y los roles de valor organizacional proveen acceso a los valores empresariales como Sociedad, Planta y Grupo de Compras.

Si un usuario solicita acceso a la transacción ME21N, el personal de soporte identifica en el Catálogo de Roles el Rol Técnico que contiene la transacción, luego obtiene el o los Roles de Negocio vinculados al Rol Técnico los cuales serán

puestos a consideración del Custodio de Accesos del negocio para su aprobación o rechazo.

CATÁLOGO DE ROLES (ROLES TÉCNICOS Y TRANSACCIONES)		
Rol Técnico	Código de Transacción	Descripción de Transacción
PR0000.PUR_ORD_CRE	ME21N	Crea órdenes de compra
PR0000.PUR_ORD_CHG	ME22N	Modifica órdenes de compra
PR0000.BUS_OBJ_DIS	ME23N	Visualiza órdenes de compra

Figura 1.10 Listado de Roles Técnicos que dan acceso a las transacciones en SAP.

CATÁLOGO DE ROLES (ROLES DE NEGOCIO Y ROLES TÉCNICOS)				
Identificación de Rol de Negocio	Nombre de Rol de Negocio	Rol Técnico	Rol Prescriptivo	Valores Organizacionales
BR00500	Creador de órdenes de compra - Documentos confidenciales	PR0000.PUR_ORD_CRE	PR0000&PDT_PO_CONF_ALL	Sociedad Planta Grupo de Compras Organización de Compras
BR00501	Creador de órdenes de compra – Materiales Directos	PR0000.PUR_ORD_CRE	PR0000&PDT_PO_DIR_MAT_ALL	Sociedad Planta Grupo de Compras Organización de Compras
BR00502	Creador de órdenes de compra – Materiales Indirectos	PR0000.PUR_ORD_CRE	PR0000&PDT_PO_IND_MAT_ALL	Sociedad Planta Grupo de Compras Organización de Compras
BR00503	Creador de órdenes de compra – Transporte de existencias	PR0000.PUR_ORD_CRE	PR0000&PDT_PO_STK_TRP_ALL	Sociedad Planta Grupo de Compras Organización de Compras

Figura 1.11 Listado de Roles de Negocio vinculados al Rol Técnico que da acceso a la transacción ME21N.

El Rol de Negocio aprobado es documentado en una plantilla para que sus Roles Técnicos sean asignados en SAP a la Posición del usuario solicitado y a su vez sea modificado el mapeo de roles del Country Job asociado a la Posición del usuario.

MAPEO DE ROLES			
Country Job	Nombre de Country Job	Identificación de Rol de Negocio	Nombre de Rol de Negocio
ECCTJ_001	EC_COMPRAS_ANALISTA DE COMPRAS	BR00445	Visualizados de órdenes de compra
ECCTJ_001	EC_COMPRAS_ANALISTA DE COMPRAS	BR00501	Creador de órdenes de compra – Materiales Directos
ECCTJ_001	EC_COMPRAS_ANALISTA DE COMPRAS	BR00502	Creador de órdenes de compra – Materiales Indirectos

Figura 1.12 Mapeo de roles actualizado del Country Job ECCTJ_001 luego de asignar a la Posición los Roles de Negocio BR00501 y BR00502.

1.3 DESCRIPCIÓN DEL PROBLEMA

Previo a la migración de SAP los usuarios del negocio ya contaban con roles técnicos que les autorizaba a realizar sus operaciones en el Sistema contando además con una gran cantidad de conflictos de segregación de funciones que no fueron mitigados, el proceso de migración no incluía en sus actividades la revisión y limpieza de conflictos existentes ni la remoción de roles técnicos ya asignados para luego ser asignados conforme al mapeo de roles. Adicional a esto, el

mapeo de roles fue definido sin una exhaustiva revisión de posibles conflictos resultando al final de la migración en 2.071 conflictos de segregación de funciones registrados en un universo de 1.203 usuarios del sistema.

Los conflictos se generaron por los siguientes motivos:

1. En SAP R/3 los usuarios con roles técnicos ya asignados cambiaban de posición o cargo y adquirían nuevos roles sin ser removidos los de la posición anterior provocando conflictos con los que ya tenían asignados.

2. En el mapeo de roles habían Country Jobs conteniendo roles de negocio que les permitía a los usuarios ejecutar las transacciones de todo un proceso del negocio como por ejemplo el ingreso de pedidos de compra y su correspondiente aprobación o liberación.

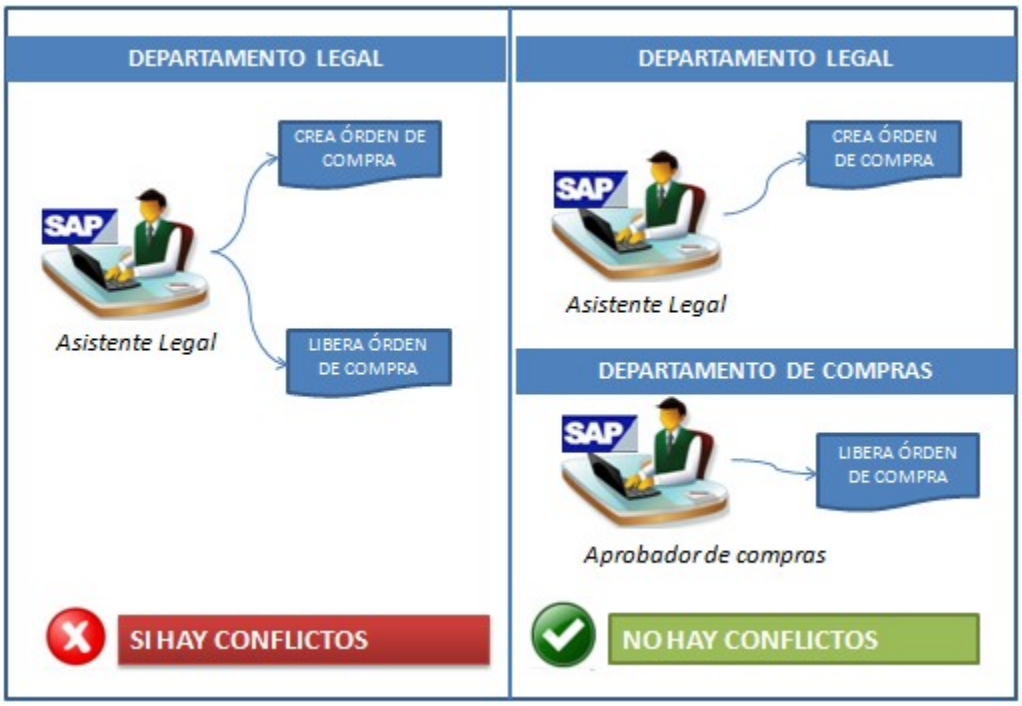


Figura 1.13 Ejemplo de una de las causas de conflictos: Un usuario tiene todas las autorizaciones para crear órdenes de compra y liberarlas, cuando esta última actividad la debe realizar el área de Compras bajo el respectivo análisis y control.

3. Algunas áreas contaban con empleados que tenían autorización para liberar documentos en caso de que el jefe inmediato se encuentre fuera de planta y sea necesaria una liberación urgente.

4. Cuando el equipo del proyecto entregó el sistema migrado al negocio la operación no podía detenerse por lo tanto el área de soporte atendía los requerimientos de asignación de roles a nuevos usuarios en base al mapeo de roles y como ya se mencionó ciertos cargos registraban

conflictos que al añadirse usuarios nuevos a estos cargos el número de conflictos aumentaba.

1.4 SOLUCIÓN PROPUESTA

Con el fin de evitar riesgos financieros en la empresa era necesario disminuir en gran medida el número de conflictos de segregación de funciones existentes en el sistema SAP, por lo tanto se propuso al negocio la remoción de accesos a los usuarios de aquellos cargos que contenían roles de negocio sensibles para la operación y, de no poder removerlos aplicar controles compensatorios que mitiguen los riesgos identificados. Adicional a estas actividades era necesario realizar análisis preventivos de conflictos en cada requerimiento de accesos que efectuaban diariamente los usuarios de la operación.

CAPÍTULO 2
METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS DE RIESGOS Y CONFLICTOS

Así como el equipo del proyecto entregó el sistema migrado también entregó una solución en SAP denominada GRC (Gobierno, Riesgo y Cumplimiento) que permite:

- Disponer de una matriz de riesgos en donde se registran las funciones que son incompatibles, por ejemplo crear compras y aprobarlas.
- Mantener y asegurar que se cumplan los controles internos de la empresa.
- Realizar análisis detectivos generando un reporte con una lista de usuarios SAP que registran riesgos y conflictos de segregación de funciones; esta información permite identificar los riesgos que pueden ser controlados ejecutando acciones coordinadas con el negocio.
- Realizar análisis preventivos de conflictos de segregación de funciones en los casos de nuevos requerimientos de accesos.

Para el cumplimiento de estas actividades la Gerencia de Auditoría, Riesgo y Control formó un equipo de especialistas en Seguridades de SAP quienes serían los encargados de disminuir en gran medida el número de conflictos de segregación de funciones, entregar al negocio una mapeo de roles depurado y controlar diariamente que los nuevos requerimientos no generen nuevos conflictos.

En adelante el equipo de especialistas será denominado AMS por sus siglas en inglés Access Management Specialist (Especialista de Administración de Accesos).

2.1.1 ANÁLISIS DETECTIVO.

SAP GRC es una aplicación que ayuda a realizar el análisis detectivo de los conflictos de segregación de funciones porque provee información de los usuarios con acceso a SAP que registran estos conflictos basado en la matriz de riesgos previamente definida por el equipo del proyecto y con la colaboración de los expertos en procesos de la empresa.

La forma de obtener esta información es haciendo click en uno de los enlaces disponibles en SAP GRC y en la pantalla resultante ingresar valores de filtro de datos como el conjunto de reglas de la empresa y la aplicación en donde requiero se haga el análisis, así se obtienen dos reportes, el primero

muestra a nivel general los usuarios que registran conflictos y el segundo muestra a nivel de detalle las transacciones asignadas y utilizadas por estos usuarios hasta la fecha en la que fue emitido el reporte.

SAP GRC			
USUARIO	ID DE RIESGO	NIVEL DE RIESGO	PROCESO
AALVAREV	ZM04	Medio	Materials Management
AARROBAO	ZS29	Bajo	Order to Cash
BAPOLOMA	ZM01	Bajo	Materials Management
CZAMBRAL	QM04	Bajo	Quality
CDIAZPAL	CO19	Alto	Commercial
ETARACES	PO60	Alto	Procure to Pay

Figura 2.1 Muestra del reporte de conflictos de segregación que registran los usuarios SAP.

A continuación una breve descripción de las columnas de este reporte:

Usuario: Es la identificación del usuario con acceso al Sistema SAP.

ID de Riesgo: Es el código del riesgo de segregación de funciones, identifica una amenaza para la empresa siempre que se combinen dos o más transacciones sensibles.

Nivel de Riesgo.- Es la categoría del riesgo: Alto, Medio y Bajo. La categoría es definida por el negocio basado en la criticidad de la operación ejecutada en el sistema.

Proceso: Comprende el conjunto de actividades a realizar para lograr un determinado objetivo en una área específica de la empresa. Los procesos afectados por los conflictos son:

Materiales Management (Gestión de Materiales).- Administración de materiales como por ejemplo la adquisición de materia prima de un proveedor.

Order to Cash (Gestión de la Orden).- Proceso de gestión de la orden de venta, desde que se recibe por parte del cliente hasta el cobro.

Procure to Pay (P2P) (Comprar para Pagar).- Proceso de compra desde el pedido hasta el pago al proveedor.

Quality.- Proceso de gestión de la calidad que se integra con los procesos de adquisición de materiales, producción y ventas. Verifica el cumplimiento de calidad de la materia prima.

Commercial.- Proceso de gestión de los pedidos del cliente incluyendo la expedición y facturación de las mercancías.

En la siguiente tabla se muestra cómo se encuentra definida la matriz de riesgos en SAP GRC y sobre la cual el sistema extrae aquellos usuarios que enfrentan una falta de segregación de funciones en las operaciones que realizan dentro de SAP.

Id Riesgo	Descripción del Riesgo	Funciones incompatibles	Transacciones SAP
ZM04	Crear y autorizar (liberar) el mismo documento de compra. Podría producirse la aprobación indebida de documentos de compra.	Función 1: Creación del pedido de compra	ME21N Crear pedido ME22N Modificar pedido
		Función 2: Aprobación pedidos / compras	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual
PO60	Crear facturas fraudulentas y procesar su pago automático.	Función 1: Contabilidad de Facturas	MIRO, Introducir factura FB60 Contabilizar factura FB65 Contabilizar abonos
		Función 2: Pagos	F-110 Pagos automáticos F-111 Pagos F-31 Pagos F-48 Anticipo F-53 Pagos
ZS29	Ningún usuario que realice ventas debe tener acceso a los registros contables	Función 1: Creación de orden de venta	VA01 Crea orden de venta
		Función 2: Genera factura de venta	VF01 Crea factura de venta

		y crea el documento contable	
ZM01	Registrar el conteo de inventario y contabilizar la diferencia de inventario. El jefe de Contabilidad es quien debe contabilizar los ajustes por diferencias.	Función 1: Documentación del conteo de inventario	MI01 Crear documento de inventario MI04 Registrar recuento real
		Función 2: Contabilización de diferencia de inventario	MI07 Contabiliza diferencia de inventario

Figura 2.2 Extracto de la matriz de riesgos registrada en SAP GRC.

Con el listado de usuarios con conflictos y la Matriz de Riesgos el equipo de AMS procede a realizar el análisis detectivo que consiste en:

a. Identificar los cargos de los usuarios con conflictos.

b. Identificar las transacciones sensibles asignadas a los usuarios que están causando conflictos.

c. Contrastar las transacciones con el mapeo de roles de los usuarios.

d. Acordar con el negocio la forma de remediar o mitigar los conflictos.

a. Identificar los cargos de los usuarios con conflictos.

Para identificar los cargos de los usuarios con conflictos es necesario la colaboración del área de Recursos Humanos en el sentido de que le entregue al equipo de AMS el maestro de empleados. Este archivo contiene el Usuario de acceso a SAP, el número de Posición y la Función o Job; cruzando los dos archivos se tiene el listado de usuarios con conflictos vinculados a su Country Job, tal como se muestra en la figura a continuación:

USUARIOS CON CONFLICTOS				
USUARIO	COUNTRY JOB	NOMBRE DE COUNTRY JOB	ID DE RIESGO	NIVEL DE RIESGO
AALVAREV	ECCTJ_0050	CONTROLADOR DE BODEGA	ZM04	Medio
AARROBAO	ECCTJ_0069	CAJERO LIQUIDADOR	ZS29	Bajo
BAPOLOMA	ECCTJ_0159	JEFE DE ALMACEN	ZM01	Bajo
CZAMBRAL	ECCTJ_0199	GERENTE DE CALIDAD	QM04	Bajo
CDIAZPAL	ECCTJ_0088	ANALISTA DE CRÉDITO	CO19	Alto
ETARACES	ECCTJ_0333	SUPERVISOR DE FACTURACIÓN	PO60	Alto

Figura 2.3 Usuarios con conflictos vinculados a sus Country Jobs.

b. Identificar las transacciones sensibles asignadas a los usuarios que están causando conflictos

Las transacciones sensibles que están causando conflicto se obtienen en base a la Matriz de Riesgos generada en SAP GRC. Por ejemplo el usuario AALVAREV registra el riesgo ZM04, este código es filtrado en la Matriz de Riesgos y se

obtiene el detalle de transacciones tal como se observa en la siguiente figura:

Id Riesgo	Descripción del Riesgo	Funciones incompatibles	Transacciones SAP
ZM04	Crear y autorizar (liberar) el mismo documento de compra. Podría producirse la aprobación indebida de documentos de compra.	Función 1: Creación del pedido de compra	ME21N Crear pedido ME22N Modificar pedido
		Función 2: Aprobación pedidos / compras	ME28 Liberar pedido de forma colectiva ME29N Liberar pedido individual

Figura 2.4 Transacciones sensibles vinculadas al riesgo ZM04.

De las transacciones listadas obtengo los roles de negocio con la ayuda del Catálogo de Roles, luego se verifica si los Roles de Negocio forman parte del Mapeo de Roles del usuario con conflictos.

A continuación se describe cómo emplear el Catálogo de Roles para obtener el Rol de Negocio en base a un código de transacción:

El código de transacción ME21N se filtra en la matriz de diseño de Roles Técnicos del Catálogo:

CATÁLOGO DE ROLES		
Transaction Code	Transaction Code Description	Task Role Name
ME21N	Create Purchase Order	PR0000.PUR_ORD_CRE

Figura 2.5 Rol Técnico asociado a la transacción ME21N.

Se obtiene el rol técnico PR0000.PUR_ORD_CRE relacionado al código de transacción y se filtra en la matriz de Roles de Negocio del Catálogo:

CATÁLOGO DE ROLES		
Business Role ID	Business Role Name	Task Role Name
BR00501	Procurement - Purchase Order Creator - Direct Materials	PR0000.PUR_ORD_CRE

Figura 2.6 Rol de Negocio BR00501 asociado al Rol Técnico PR0000.PUR_ORD_CRE.

c. Contrastar las transacciones con el Mapeo de Roles de los usuarios.

A continuación se describe cómo emplear el Mapeo de Roles para identificar si una transacción vinculada a un Rol de Negocio está definida o incluida en el Country Job del usuario:

En el literal b identificamos que la transacción ME21N está vinculada al Rol de Negocio BR00501, este código es filtrado en el mapeo de roles confirmando que el Rol de Negocio en cuestión si está definido en el Country Job ECCTJ_0050 del usuario con conflicto AALVAREV:

MAPEO DE ROLES			
COUNTRY JOB	NOMBRE DE COUNTRY JOB	IDENTIFICACIÓN DE ROL DE NEGOCIO	NOMBRE DE ROL DE NEGOCIO
ECCTJ_0128	ESPECIALISTA DE EMBARQUE	BR00501	Procurement - Purchase Order Creator - Direct Materials
ECCTJ_0130	ANALISTA DE COMPRAS	BR00501	Procurement - Purchase Order Creator - Direct Materials
ECCTJ_0050	CONTROLADOR DE BODEGA	BR00501	Procurement - Purchase Order Creator - Direct Materials
ECCTJ_0107	ESPECIALISTA DE ADJUNTOS	BR00501	Procurement - Purchase Order Creator - Direct Materials
ECCTJ_0129	ESPECIALISTA EN CULTIVOS	BR00501	Procurement - Purchase Order Creator - Direct Materials

Figura 2.7 Mapeo de roles del Country Job ECCTJ_0050.

d. Acordar con el negocio la forma de remediar o mitigar los conflictos.

En forma general, si las transacciones están mapeadas pero no han sido ejecutadas por los usuarios se procede a la remoción de los roles que dan acceso a estas transacciones y a la actualización del Mapeo de Roles (Roles de Negocio asignados a Country Jobs), esto último implica la aprobación de los Custodios de Accesos del negocio. La remoción se debe realizar siempre y cuando ningún otro usuario del mismo cargo tenga la necesidad de utilizar estas transacciones.

Si las transacciones están mapeadas y si han sido ejecutadas por los usuarios se coordina una reunión con el Jefe o Gerente de línea del área en donde labora el usuario para revisar la forma de remediar el conflicto.

Si las transacciones no están mapeadas y no han sido ejecutadas por los usuarios se procede a la remoción de sus Roles de Negocio del Country Job de los usuarios.

Si las transacciones no están mapeadas y si han sido ejecutadas por los usuarios se coordina una reunión con el Jefe o Gerente de línea del área en donde labora el usuario para revisar la forma de remediar el conflicto y actualizar el Mapeo de Roles en caso de que aplique un cambio.

En el caso de que ciertos conflictos no puedan ser eliminados con la remoción de roles es necesario revisar si sus riesgos registran controles que mitiguen estos conflictos y confirmar con el negocio si los controles son aplicados.

2.1.2 REMEDIACIÓN Y MITIGACIÓN DE CONFLICTOS.

REMEDIACIÓN DE CONFLICTOS

La remediación consiste en remover de los usuarios los roles de acceso a las transacciones sensibles en SAP eliminando de esta forma los conflictos de segregación de funciones. Esta actividad conlleva a actualizar el Mapeo de Roles removiendo los Roles de Negocio de los Country Jobs de los usuarios que registran los conflictos.

La remediación también ocurre cuando se re-diseñan los Roles de Negocio o Roles Técnicos. Si en el análisis se observa que un Rol de Negocio incluye un Rol Prescriptivo o de Valor Organizacional que no corresponde y causa conflictos, se procede con el re-diseño removiendo estos últimos roles del Rol de Negocio; esto implica también la remoción en SAP.

MITIGACIÓN DE CONFLICTOS

La mitigación se da cuando no es factible la remoción de roles ya sea porque el negocio no cuenta con recursos de personal que les permita segregar las funciones o porque no está en los planes de la empresa contratar más personal en el área que cuenta con estos conflictos.

La mitigación no elimina el conflicto, permite que el riesgo se mantenga en el sistema aplicando controles que ayuden a evitar o detectar si se ha generado en el sistema alguna actividad no autorizada o fraudulenta.

La empresa ya contaba con controles ejecutados por el negocio para ciertos riesgos y uno de los objetivos del equipo de AMS era eliminar en lo posible los conflictos para estos riesgos de tal forma que los controles tiendan también a disminuir.

2.2 PROCESOS DEL EQUIPO DE SEGURIDADES

Con el objetivo de reducir el número de conflictos de segregación de funciones y evitar que se generen nuevos ante los requerimientos diarios de accesos a SAP el equipo de AMS ejecuta los siguientes procesos:

a. Generar en el sistema el listado de usuarios con conflictos.

b. Remediar o mitigar conflictos en base al análisis de riesgos y conflictos.

c. Informar mensualmente al negocio de las remediaciones realizadas, controles pendientes y planes a seguir.

d. Atender nuevos requerimientos de accesos de los usuarios realizando un análisis preventivo simulando la asignación del rol requerido.

e. Actualizar el Mapeo de Roles.

PROCESO DE REDUCCIÓN DE CONFLICTOS

La reducción de conflictos existentes se hizo en base al análisis del informe generado en SAP GRC de donde se obtiene el listado de los usuarios con acceso a transacciones sensibles y el número de veces ejecutadas, así como también los riesgos que registran.

Si las transacciones sensibles no fueron ejecutadas por los usuarios se incluyeron en la propuesta de remoción de sus roles.

Si las transacciones si fueron ejecutadas entonces se efectuó entrevistas con los usuarios clave de los procesos para conocer las transacciones que utilizan y revisar la factibilidad de remover aquellas sensibles. Si no es posible la remoción, el negocio debía ejecutar un control.

La semana siguiente a las entrevistas, se daba a conocer a los Gerentes de Línea y Auditoria la propuesta de remoción y los controles que deben ser implementados en los casos en donde el conflicto no iba a ser eliminado. A su vez se comunicaba al negocio las transacciones que iban a ser removidas de los usuarios.

Se tomó una muestra de los usuarios de la propuesta y se levantó el requerimiento de remoción a Mesa de Ayuda, una semana después se solicitó la remoción para los usuarios restantes de la propuesta. Esto se hizo con el fin de que el impacto sea menor en caso de haber realizado remociones de accesos importantes para el negocio; primero se removía a un número reducido de usuarios y estábamos atentos ante algún

reclamo por falta de accesos. Si no había ninguna novedad en una semana, se procedía con la remoción completa.

Luego de cada remoción el equipo de AMS realiza una actualización al Mapeo de Roles eliminando de los Country Jobs los Roles de Negocio relacionados a las transacciones que fueron removidas de los usuarios.

PROCESO DE ADMINISTRACIÓN DE ACCESOS

El proceso de administración de accesos gestiona los requerimientos de accesos a los usuarios en SAP en diversos escenarios como:

1. Definir un nuevo Country Job
2. Cambiar un Country Job existente
3. Definir una nueva Posición
4. Cambiar una Posición Tipo existente
5. Asignar un nuevo Empleado a una Posición existente
6. Cambiar de Posición al Empleado

De estos escenarios, los cuatro primeros requieren un análisis preventivo de conflictos de segregación de funciones. Para los dos últimos no hay riesgo de conflictos a menos que las posiciones a donde van a ser ubicados los empleados ya cuenten con conflictos.

Definir un nuevo Country Job

Cuando el negocio crea un cargo y este no se encuentra en el Mapeo de Roles, es necesario que el Gerente de Línea planifique una reunión con el equipo de AMS y RH para identificar los Roles de Negocio a los que debe tener acceso este cargo o Country Job.

Pasos	Actividad	Responsable
1	Planificar una reunión con el equipo de AMS y RH	Gerente de Línea
2	Listar los Roles de Negocio y de Valor Organizacional que definen el Country Job	Gerente de Línea, RH y AMS
3	Generar un requerimiento con MDA solicitando la creación del Country Job	Gerente de Línea
4	Generar un ticket de atención y asignarlo al grupo de AMS	MDA
5	En SAP GRC realizar el análisis preventivo de segregación de funciones ingresando cada uno de los roles técnicos y prescriptivos relacionados a los Roles de Negocio definidos en el paso 2	AMS
6	Notificar al Gerente de Línea de aquellos roles que no van a ser considerados por generar conflictos	AMS
7	Solicitar vía correo electrónico la aprobación de los Custodios de Accesos de los Roles de Negocio que no generan conflictos	AMS
8	Si los Custodios de Accesos aprueban, se actualiza el Mapeo	AMS

	de Roles incluyendo el nuevo Country Job con los Roles de Negocio aprobados	
9	Registrar el ticket como resuelto y notificar al Gerente de Línea	AMS

Figura 2.8 Lista de actividades del proceso de definición de un nuevo Country Job.

Cambiar un Country Job existente

Este caso ocurre cuando un usuario requiere acceso a transacciones, reportes o links que no fueron incluidos o definidos previamente en su Country Job.

Pasos	Actividad	Responsable
1	Levantar el requerimiento con MDA	Gerente de Línea
2	Generar un ticket de atención y asignarlo al equipo de AMS	MDA
3	Identificar el o los Roles de Negocio relacionados a la transacción	AMS
4	En SAP GRC realizar el análisis preventivo de segregación de funciones	AMS
5	Notificar al Gerente de Línea de aquellos roles que no van a ser considerados por generar conflictos	AMS
6	Solicitar vía correo electrónico la aprobación de los Custodios de Accesos de los Roles de Negocio que no generan	AMS

	conflictos	
7	Si los Custodios de Accesos aprueban el o los Roles de Negocio, éstos son documentados en una plantilla para que sus roles técnicos sean asignados en SAP a una o más Posiciones relacionadas al Country Job. Escalar ticket a MDA.	AMS
8	Asignar Roles Técnicos en SAP en base a la plantilla entregada por el equipo de AMS. Devolver ticket a AMS.	MDA
9	Actualizar el Mapeo de Roles, registrar el ticket como resuelto y notificar al Gerente de Línea que el requerimiento ha sido atendido.	AMS

Figura 2.9 Lista de actividades del proceso de cambios a un Country Job existente.

Definir una nueva posición

Una nueva posición puede ser requerida por dos motivos, el primero se relaciona con una nueva Posición Tipo y el segundo con una Posición adicional a las ya existentes en una Función y Posición Tipo definidos.

Pasos	Actividad	Responsable
1	En SAP HCM crear una Posición dentro de la Estructura Organizacional de RH vinculándola	RH

	a una Función nueva o existente	
2	Levantar el requerimiento con MDA	Gerente de Línea
3	Escalar el ticket al AMS para el aprovisionamiento de roles de acuerdo al cambio de Posición	MDA
4	Revisar el requerimiento con el solicitante y partes interesadas para definir los roles a ser asignados a la Posición. Si la Función y Posición Tipo no existen, primero deben crearse estos objetos para luego crear la Posición	AMS
5	Si la posición se relaciona con una nueva Posición Tipo, en SAP GRC realizar el análisis preventivo de segregación de funciones	AMS
6	Notificar al Gerente de Línea de aquellos roles que no van a ser considerados por generar conflictos	AMS
7	Si la posición se relaciona con una nueva Posición Tipo, solicitar vía correo electrónico la aprobación de los Custodios de Accesos de los Roles de Negocio que no generan conflictos	
8	Generar la plantilla de roles aprobados y escalar el ticket a MDA	AMS
9	Realizar la asignación de Roles Técnicos a la Posición en SAP	MDA
10	Registrar el ticket como resuelto y notificar al solicitante	MDA

Figura 2.10 Lista de actividades del proceso de definición de una nueva Posición.

Cambiar una Posición Tipo existente

Si una Posición Tipo ya se encuentra mapeada y requiere un acceso adicional a un rol de Valor Organizacional, se trata de un requerimiento de accesos solicitando cambios a una Posición Tipo.

Pasos	Actividad	Responsable
1	Levantar el requerimiento con MDA	Gerente de Línea
2	Escalar el ticket al AMS	MDA
3	En SAP GRC realizar el análisis preventivo de segregación de funciones	AMS
4	Notificar al Gerente de Línea de aquellos roles que no van a ser considerados por generar conflictos	AMS
5	Solicitar vía correo electrónico la aprobación de los Custodios de Accesos de los Roles de Valor Organizacional que no generan conflictos	AMS
6	Generar la plantilla de roles aprobados y escalar el ticket a MDA	AMS
7	Realizar la asignación de Roles Técnicos a la Posición en SAP	MDA
8	Registrar el ticket como resuelto y notificar al solicitante	MDA

Figura 2.11 Lista de actividades del proceso de cambios a una Posición Tipo.

Como se indicó previamente, los dos escenarios restantes: Asignar posición a un nuevo Empleado y cambiar de Posición al Empleado, no requieren que el AMS haga un análisis de segregación de funciones puesto que no se van a añadir roles a una Función o Posición, sólo se va a asignar una Posición al Empleado y así éste último se proveerá en SAP de los roles previamente definidos en esta posición.

2.2.1 ANÁLISIS PREVENTIVO.

El análisis preventivo de segregación de funciones consiste en simular la asignación de Roles Técnicos al usuario de SAP para identificar si se generan conflictos con los roles ya asignados a este usuario. La aplicación que ayuda a realizar esta simulación es SAP GRC quien se basa en las reglas de riesgos registradas en el sistema y definidas previamente por el negocio.

Para poner un ejemplo vamos a suponer que el usuario USVENDE1 es un vendedor y está autorizado a registrar y modificar Pedidos u Órdenes de Venta en el sistema, por lo tanto en SAP tiene asignados los roles técnicos SL0000.SLS_ORD_CRE Y SL0000.SLS_ORD_CHG que dan acceso a las transacciones VA01 y VA02, respectivamente.

CATÁLOGO DE ROLES		
Transaction Code	Transaction Code Description	Task Role Name
VA02	Change Sales Order	SL0000.SLS_ORD_CHG
VA01	Create Sales Order	SL0000.SLS_ORD_CRE

Figura 2.12 Roles Técnicos asociados a las transacciones VA01 y VA02.

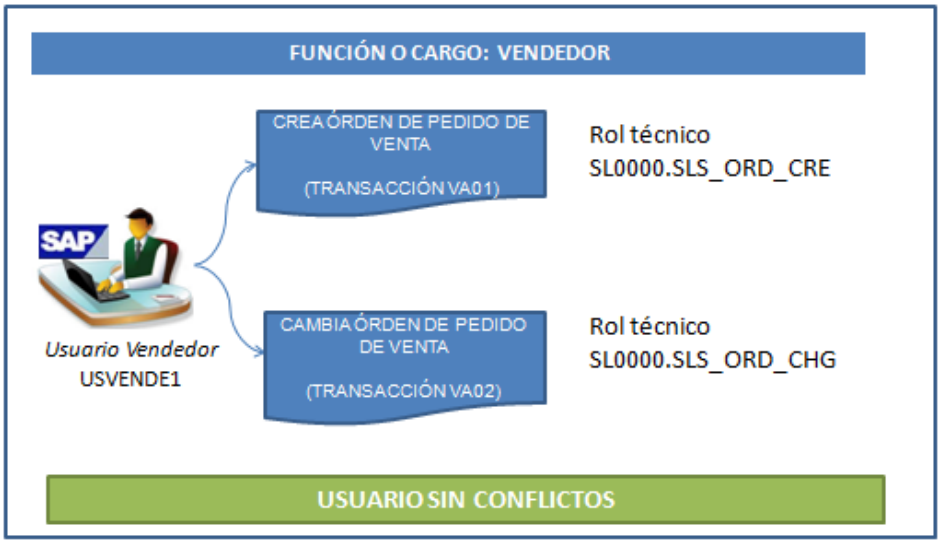


Figura 2.13 Transacciones autorizadas a ser ejecutadas por el usuario Vendedor.

Por algún acuerdo con su Gerente de Línea solicita autorización para crear y contabilizar facturas con la transacción VF01.

Cuando el ticket de atención llega al equipo de AMS, el análisis preventivo empieza con la identificación del Rol Técnico que da acceso a la transacción VF01; para el efecto se toma el Catálogo de Roles y se filtra por código de transacción encontrando que el rol técnico es SL0000.SLS_BIL.

CATÁLOGO DE ROLES		
Transaction Code	Transaction Code Description	Task Role Name
VF01	Create Billing Document	SL0000.SLS_BIL

Figura 2.14 Rol Técnico asociado a la transacción VF01.

Filtrando por el Rol Técnico se busca en el Catálogo de Roles el Rol de Negocio asociado:

CATÁLOGO DE ROLES (ROLES DE NEGOCIO Y ROLES TÉCNICOS)				
Identificación de Rol de Negocio	Nombre de Rol de Negocio	Rol Técnico	Rol Prescriptivo	Valores Organizacionales
BR00608	Facturación de Ventas	SL0000.SLS_BIL	Mapeado vía OV roles	Sociedad
BR00608	Facturación de Ventas	SL0000.SLS_BIL	Mapeado vía OV roles	Planta
BR00608	Facturación de Ventas	SL0000.SLS_BIL	Mapeado vía OV roles	Organización de Ventas
BR00608	Facturación de Ventas	SL0000.SLS_BIL	COLAEC&PC_EC-ALL_ALL	Centro de Beneficio

Figura 2.15 Rol de Negocio asociado a un Rol Técnico.

Se observa que el rol de negocio BR00608 se compone además del rol prescriptivo COLAEC&PC_EC-ALL_ALL y de tres roles de valor organizacional que, si no están asignados al usuario, deben ser considerados en la simulación de asignación de roles. Vamos a suponer que los tres roles de valor organizacional ya están asignados al usuario SAP.

Una vez identificados los roles, el AMS ingresa a SAP GRC, selecciona la opción "Simulación a nivel de usuario" y en la pantalla resultante ingresa el usuario, ambiente de SAP y Roles Técnicos que podrían ser asignados al usuario:

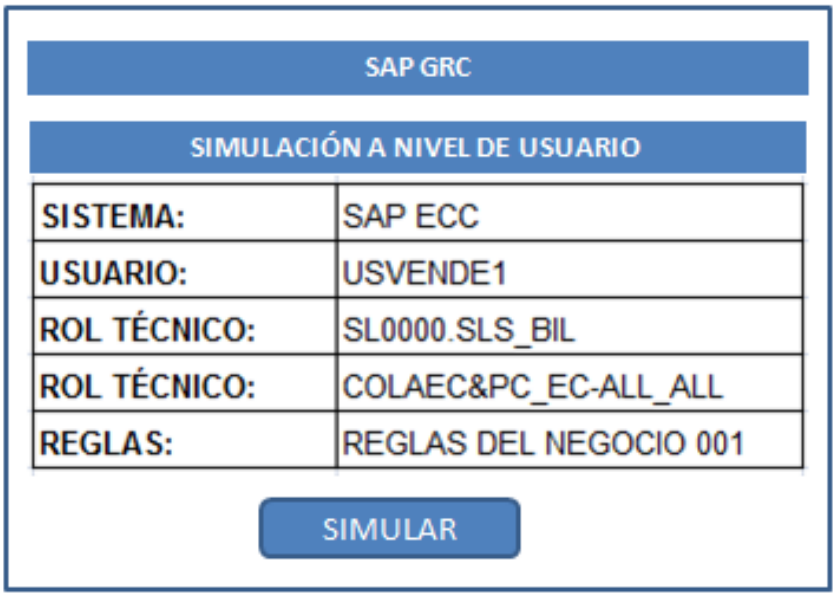


Figura 2.16 Filtro de datos a ser ingresados en la opción "Simulación de Nivel de Usuario" dentro de SAP GRC.

Al seleccionar REGLAS DEL NEGOCIO 001 estamos indicando al sistema que el análisis preventivo lo haga en base al conjunto de reglas previamente definidas por el negocio y clasificadas como REGLAS DEL NEGOCIO 001, de las cuales he mostrado un extracto en la figura 2.2 de este documento.

El sistema encuentra que el usuario USVENDE1 podría incurrir en el riesgo ZS29 ya que ningún usuario que realice ventas debe tener acceso a los registros contables, esto es, si ya cuenta con la función de Crear Órdenes de Venta, no debe tener la función de Generar Facturas de Venta y Crear los Documentos Contables respectivos.

Finalmente el sistema emite un informe por pantalla mostrando en forma general y detallada el rol que estaría causando un conflicto de segregación de funciones para el usuario USVENDE1. Con esta información el AMS notifica al Gerente de Línea que no es posible asignarle la transacción VF01 por el conflicto identificado; si el Gerente de Línea insiste con el acceso, el AMS se reúne con Él para llegar a un acuerdo el cual podría ser mover al empleado a una Posición y cargo que contenga la autorización para generar Facturas de Venta, esta decisión debe ser tomada en conjunto con el área de Recursos Humanos.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 EVOLUCIÓN DEL PROCESO DE ELIMINACIÓN DE CONFLICTOS

Cuando la empresa concluyó con la migración del sistema SAP, registraba 2.071 conflictos funcionales y 15.792 conflictos técnicos. Fue entonces que inició la formación del equipo de Especialistas en Seguridades SAP AMS con el objetivo de lograr una reducción en el número de conflictos funcionales. El equipo de AMS inició sus actividades en el año 2012.

En Julio del 2012 se dio por terminado el lanzamiento de la segunda versión de SAP Netweaver y el equipo de AMS tenía cinco meses para trabajar en la reducción de conflictos llegando a tener en Diciembre de ese año 1.004 conflictos funcionales y 4.242 conflictos técnicos.

En Febrero del 2013 el equipo del proyecto de migración lanzó la tercera versión de SAP Netweaver registrando un ligero aumento en el

número de conflictos siendo 1.030 funcionales y 4.409 técnicos. Este aumento se debía a que se instalaban nuevas iniciativas en el sistema acompañadas de nuevas autorizaciones a roles técnicos dando lugar al ligero incremento de conflictos. Sin embargo en Septiembre de ese año se logró una reducción importante, esto es, 408 conflictos funcionales y 791 conflictos técnicos. En Octubre del mismo año el equipo del proyecto lanza una cuarta versión del sistema registrando 473 conflictos funcionales y 1.407 conflictos técnicos.

El equipo de AMS continúa trabajando sobre la última versión del sistema hasta que en Enero del 2014 logra la máxima reducción, esto es 375 conflictos funcionales y 1.108 conflictos técnicos. Sin embargo, a finales de Enero de este año se realiza la creación de un Job en el área de Distribución un tanto similar en sus funciones y roles de SAP a un Job que ya registraba conflictos y que se mantenían con la condición de que el negocio ejecute los controles de mitigación, al ser replicados los roles indicados en otro Job los conflictos aumentaron reflejándose en Febrero del mismo año 453 conflictos funcionales y 1.135 conflictos técnicos.

A continuación se muestra un gráfico de barras que ilustra la evolución del proceso de eliminación de conflictos descrita en los párrafos anteriores:

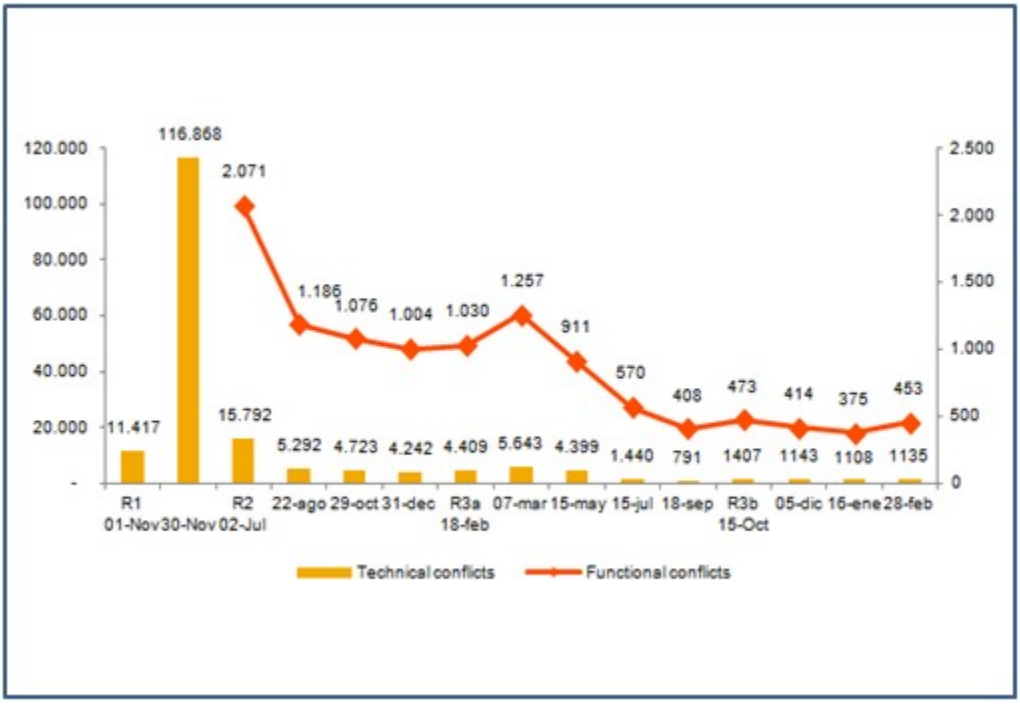


Figura 3.1 Evolución de la reducción de conflictos desde el año 2012 hasta el 2014.

3.1.1 DISMINUCIÓN DE CONFLICTOS POR NIVEL Y PROCESO

Es importante mencionar que las actividades de reducción de conflictos se enfocaban primero en aquellos conflictos de nivel "Alto" porque eran los que tenían mayor impacto negativo financiero en la empresa, es así que para Febrero del 2014 la empresa mantuvo al final 23 conflictos funcionales Altos, siendo este número producto del incumplimiento de dos reglas de segregación de funciones por dos Jobs del área de Crédito y un Job del área de Facturación. Siendo así el negocio implementó dos controles para vigilar que no se cometan fraudes por estos

usuarios que mantenían autorizaciones a transacciones sensibles para el negocio.

Número de Conflictos Funcionales	#
Alto	23
Medio	281
Bajo	149
Total	**453**

Figura 3.2 Número de Conflictos funcionales por nivel de conflicto, a Febrero del 2014.

En cuanto a los procesos de negocio el mayor número de conflictos (402) recae en el proceso de Gestión de Materiales incumpliendo seis reglas de segregación de funciones. Los jobs o cargos relacionados con este proceso corresponden a tres áreas del negocio: Distribución, Manufactura y Ventas incluyendo cargos como Controlador de Bodega, Líder de Turno, Coordinador de Subproducto, Cajero Liquidador, Líder de Operación, Analista y Coordinador de Equipos de Frío. Le siguen en número de conflictos los usuarios con autorizaciones a los procesos de Order To Cash, Commercial, Procure To Pay y Quality.

Conflictos funcionales por proceso	Alto	Medio	Bajo	Total
Materials Management		279	123	402
Order to Cash			23	23
Commercial	21			21
Procure to Pay	2	2		4
Quality			3	3
Total general	**23**	**281**	**149**	**453**

Figura 3.3 Número de Conflictos funcionales por proceso de negocio, a Febrero del 2014.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. Cuando las empresas deciden apoyarse en aplicaciones empresariales deben tener en cuenta que pueden exponerse a fraudes debido a una incorrecta administración de permisos en su Sistema.
2. Es necesario que las empresas dispongan de los servicios de personas y procesos especializados en la administración de Seguridades.
3. Las empresas deben contar con una Matriz de Riesgos y Controles y velar porque esos controles se cumplan con el fin de prevenir fraudes financieros.

RECOMENDACIONES:

1. Se recomienda que las empresas se provean de los servicios de administración de Riesgos y Control con personas o empresas que no

2. estén vinculadas con aquellas que brinden la solución empresarial, de esta forma se logrará una administración transparente y libre de riesgos.
3. La administración de Seguridades y de Riesgos y Control debe ser permanente en el tiempo porque los negocios son dinámicos y las funciones de los empleados de una empresa varían conforme a las necesidades del mercado y los objetivos planteados en la empresa.

BIBLIOGRAFÍA

[1] Sergio Ríos Huércano, Fundamentos de ITIL,
http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf ,
fecha de consulta Octubre 2017

[2] Rodrigo Baldecchi Q., Implementación efectiva de SGSI ISO 27001,
https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf ,
fecha de publicación Septiembre 2014

[3] Ernst & Young - México, Un enfoque basado en riesgos para la segregación de funciones,
http://www.ey.com/Publication/vwLUAssets/Perspectivas_relacionadas_con_el_riesgo_de_TI/$FILE/Enfoque_basado_en_riesgos_para_la_segregacion_de_funciones.pdf,
fecha de consulta Octubre 2017

[4] José Díaz Morales Socio de Ernst & Young, La Ley Sarbanes-Oxley y la Auditoría,
http://pdfs.wke.es/5/3/4/4/pd0000015344.pdf,
fecha de publicación Septiembre 2005