UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

FACULTAD DE ESTUDIOS SUPERIORES
A R A G Ó N

DISEÑO DE SEGURIDAD EN SAP

INFORME DEL EJERCICIO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE

INGIENIERO EN COMPUTACIÓN

P R E S E N T A:

JUAN ARREOLA VÁSQUEZ

A S E S O R:

MTRO. JUAN GASTALDI PÉREZ

México, Marzo 2013

Agradecimeintos

Con profundo agradecimiento a mis padres por su incondicional apoyo en aquellos días de escuela y de siempre.

Para mis hermanos, que han sido mis entrañables compañeros de mesa, de sueños, de tiempo y espacio.

Con singular afecto a Cristina por los buenos tiempos en esas aulas y en la vida misma.

Para Erick y para Kevin que me enseñaron a madurar y a valorar las cosas más importantes de la vida, y me enseñaron a vivirla en el aquí y en el ahora.

Para esos amigos que han compartido la vida conmigo, los de entonces, los de siempre y los de ahora.

Para aquellos mentores que transmitieron en mi esos conocimientos y actitudes para enfrentar con éxito el momento del mundo que nos tocó vivir.

Para la Universidad Nacional Autónoma de México, por la que guardo una deuda eterna de honor, valor y orgullo.

A todos ellos dedico este trabajo y dedico también mi compromiso por el reto constante de seguir creando, produciendo e innovando. Y con entusiasmo pago también esa deuda en el gusto de seguir transmitiendo la experiencia, los conocimientos y las mejores prácticas profesionales a los más jóvenes.

INDICE

Capitulo I – La Seguridad en SAP 3
Breve historia del SAP y quiénes lo usan 3
Productos de SAP 4
Descripción de la Seguridad en SAP 5
Términos en Seguridad SAP 5
Segregación de Funciones (SOD) / Sarbanes-Oxley Act - (SOX) 7
Capitulo II - Mis funciones diseñando Seguridad SAP 7
Desarrollo profesional en el área de Seguridad SAP 7
Mi colaboración en Seguridad SAP. Proyectos relevantes 7
Neoris SC 7
Rediseño de Seguridad SAP de Cemex Europa 7
Rediseño de Seguridad SAP de BAFAR 8
Soporte al Go Live de Seguridad SAP de MAQSA 9
Rediseño de Seguridad SAP de Cemex México 10
Soporte a la operación de Seguridad SAP de Peñafiel 10
Rediseño de Seguridad SAP de Sultana 10
Rediseño de Seguridad SAP de Cemex Colombia, Puerto Rico y República Dominicana 11
Capitulo III – La Implementación de la Seguridad en SAP ECC 12
Administración de Usuarios 13
Pruebas Unitarias: 14
Pruebas Integrales: 14
Aprobación de pruebas unitarias e integrales: el equipo funcional entregará un documento de aceptación de que las pruebas fueron satisfactorias. 15
Administración de Roles 15
El nombre de los roles debe seguir el siguiente formato: 15
Diseño de Roles 17
Mantenimiento de Roles 19
Administración de Usuarios 21
Revisión de objetos obsoletos 22
Aplicación de la Segregación de Funciones (SOD) 23
Diagrama SOD 25
Conclusiones 26
Bibliografía 28

Introducción

Haber elegido la carrera de Ingeniería en Computación en la Universidad Nacional Autónoma de México fue sin duda de las decisiones mas trascendentes de mi vida. Elegir esta noble profesión en un momento en que el mundo de la informática iniciaba un proceso de progreso exponencial ha sido un verdadero reto al que he enfrentado con entusiasmo y pasión. Y esa evolución nunca se detendrá, de aquellos procesadores Z80 de entonces solo queda el recuerdo. Cada consultor, programador y en general cada profesional relacionado con el mundo de la informática sabe que tiene que ir reinventandose cada año, cada mes, cada día. Sabe que debe tomar decisiones para seguir tal o cual tendencia, o método para seguir ofreciendo las mejores soluciones y mantenerse actualizado y ser competitivo en un mundo cambiante que cada vez exige mas y mejores sistemas acorde a las nuevas necesidades tecnológicas, legales, sociales, empresariales, etc.

Entre todo este universo de sistemas y soluciones, SAP ejemplifica la nobleza de un sistema fuerte, complejo, flexible y con amplias áreas de oportunidad y desarrollo.

Es en este sistema SAP donde he tenido la oportunidad de desarrollarme los últimos años después de haber iniciado mi carrera profesional en las teconologías de Mainframe. Y he valorado las diferencias de laborar en ambientes financieros como bancos y aseguradores donde predomina el Mainframe y una amplia variedad de empresas medianas y grandes donde predomina SAP, como mineras, de la industria alimentaria, cemento, etc.

El área de Seguridad en SAP se ha venido convirtiendo en un tema muy relevante desde que en el año 2002 se creó la Ley Sarbanes Oxley en Estados Unidos como resultado de los sonados quiebres de las empresas WorldCom y Enron. Sobre todo para aquellas empresas que cotizan en bolsa y que están obligadas a ser auditadas periódicamente en su integridad de la información, autorización, segregación de funciones y todos los aspectos de seguridad que reduzcan los riesgos de fraude y quiebre en la operación.

Capitulo I – La Seguridad en SAP

Breve historia del SAP y quiénes lo usan

SAP fue fundada en 1972 en la Ciudad de Mannheim, Alemania, por antiguos empleados de IBM (Claus Wellenreuther, Hans-Werner Hector, Klaus Tschira, Dietmar Hopp y Hasso Plattner) bajo el nombre de "SAP Systemanalyse, Anwendungen und Programmentwicklung". El nombre fue tomado de la división en la que trabajaban en IBM.

La corporación SAP fue fundada en 1972 y se ha desarrollado hasta convertirse en la quinta más grande compañía mundial de software[1]. SAP R/3 es un nombre usado que hace referencia a una empresa y a su vez el de un sistema informático. Este sistema comprende muchos módulos completamente integrados, que abarca prácticamente todos los aspectos de la administración empresarial. Ha sido desarrollado para cumplir con las necesidades crecientes de las organizaciones mundiales y su importancia esta más allá de toda duda. SAP ha puesto su mirada en el negocio como un todo, así ofrece un sistema único que soporta prácticamente todas las áreas en una escala global. Proporciona la oportunidad de sustituir un gran número de sistemas independientes, que se han desarrollado e instalado en organizaciones ya establecidas, con un solo sistema modular. Cada módulo realiza una función diferente, y trabaja de manera integral con otros y ofrece compatibilidad a lo largo de las funciones de una empresa.

Después de haber dominado el mercado, la empresa afronta una mayor competencia de Microsoft e IBM. En marzo de 2004 cambió su enfoque de negocio en favor de crear la "plataforma" que desarrolla y utiliza, la nueva versión de su software NetWeaver.

Es en este punto donde SAP se encuentra enfrentado con Microsoft e IBM, en lo que se conoce como "la guerra de las plataformas". Microsoft ha desarrollado una plataforma basada en la Web llamada .NET, mientras IBM ha desarrollado otra llamada WebSphere.

[1] http://www.sap.com/corporate-en/our-company/history/

A comienzos de 2004 sostuvo conversaciones con Microsoft sobre una posible fusión. Las empresas dijeron que las conversaciones finalizaron sin un acuerdo. Sin embargo, a comienzos del 2006 fue anunciada una alianza muy importante entre SAP y Microsoft para integrar las aplicaciones ERP de SAP con las de Office de Microsoft bajo el nombre de proyecto "Duet".

La compra de SAP por parte de Microsoft habría sido uno de los acuerdos más grandes en la historia de la industria del software, dado el valor de mercado de la alemana, de más de 55.000 millones de euros (junio 2004).

SAP ha conquistado clientes de forma consistente para aumentar la cuota del mercado global entre sus cuatro principales competidores a un 55% a fines de 2004, desde un 48% dos años antes. La participación combinada de Oracle y PeopleSoft declinó de un 29% a un 23%.

SAP es una compañía alemana que opera con 28 sucursales afiliadas y 6 compañías asociadas, manteniendo oficinas en 40 países.

Productos de SAP

SAP trabaja en el sector de software de planificación de recursos empresariales (o ERP por las siglas en inglés de Enterprise Resource Planning). El principal producto de la compañía es R/3, en el que la R significa procesamiento en tiempo real y el número 3 se refiere a las tres capas de la arquitectura de proceso: bases de datos, servidor de aplicaciones y cliente. El predecesor de R/3 fue R/2.

Otros productos de SAP son APO (Advanced Planner and Optimizer), BW (Business Information Warehouse), BI (Business Intelligence), Customer Relationship Management (CRM), SRM (Supplier Relationship Management), Human Resource Management Systems (EHRMS), Product Lifecycle Management (PLM), KW (Knowledge Warehouse) RE (Real Estate), FI/CO (Financial Accounting/Controlling).

SAP también ofrece una nueva plataforma tecnológica denominada SAP NetWeaver. Esta plataforma tecnológica convierte a SAP en un programa Web-enabled, lo que significa que estaría totalmente preparado para trabajar con él mediante la web, se puede trabajar con SAP mediante cualquier navegador de internet si se tienen los componentes apropiados de SAP NetWeaver (SAP Portals).

Aunque sus principales aplicaciones están destinadas a grandes empresas, SAP también se dirige a la pequeña y mediana empresa con productos como SAP Business One y mySAP All-in-one.

SAP cuenta también con verticales y microverticales. Las verticales son conocidas también como IS o Industry Solution y son SAP orientados a diversas industrias, como por ejemplo periódicos, mineras, compañías de telecomunicaciones. Las microverticales son SAP que atienden a industrias específicas, como por ejemplo:

empresas agroexportadoras, piscifactorías, etc. Las Verticales son desarrolladas por SAP y las microverticales por los socios de SAP.

En muchos casos la adopción de SAP por las empresas se hace mediante la contratación de consultoras especializadas.

Descripción de la Seguridad en SAP

La Seguridad en SAP trabaja con la creación de usuarios y asignación de roles. Cuando el usuario intenta entrar al sistema, éste valida que exista en la base de datos de usuarios. Que la contraseña sea correcta, que no esté bloqueado y que la fecha de validez no esté vencida.

Al ejecutar las transacciones en SAP, el sistema valida que el usuario tenga todas las autorizaciones necesarias para ejecutar su tarea mediante los roles que tiene asignado.

Debido a que los roles se asignan a muchos usuarios, cualquier modificación que realice en el role afectará a los usuarios que tengan asignado dicho role. Las transacciones no se pueden asignar directamente a los usuarios.

La construcción de un role comienza con la asignación de transacciones, esto se realiza a través de la transacción PFCG “profile generator tool”. Luego se debe agregar los valores en los objetos de autorización, se debe evitar colocar “*” en los campos de los objetos de autorización.

La construcción y mantenimiento de los roles en SAP requiere de la interacción del equipo de Seguridad y los expertos funcionales del negocio. Adicionalmente se requiere la validación de dueños de proceso que conozcan las responsabilidades y trabajo de los usuarios finales.

Términos en Seguridad SAP

Autorización: Son permisos que obtiene el usuario cuando ejecutan una transacción.

Usuario final: Es un usuario que no es responsable de la administración, configuración, soporte y desarrollo del sistema SAP. Es decir, solo ejecuta transacciones pertenecientes al negocio.

Acceso por herencia: Son usuarios que tienen acceso a través de un role donde las transacciones y funcionalidades provienen de un role padre.

AS400: Es un equipo de IBM de gama media y alta, para todo tipo de empresas y grandes departamentos.

Role Compuesto: Es un role que tiene asignado mas de un role simple (master/derivados roles) esto simplifica la asignación de roles a usuarios. Esto puede complicar la administración del acceso de seguridad.

Role Derivado: Es un role que tiene referencia a un role Maestro, donde las transacciones , objetos y valores son heredados, por lo tanto lo único que se puede modificar son los valores organizativos.

Role de Visualización: Es un role que tiene toda la información de visualización necesaria para un proceso a través de transacciones SAP. Los datos sensibles tienen que ser separados de la visualización solo debe de permitir el acceso a un conjunto de usuarios.

Role General: Es un role que tiene transacciones que son utilizadas por todos los usuarios de la organización. Este role se le deberá asignar a todos los usuarios.

Role de Trabajo: Es un role que contiene todas las transacciones que un usuario necesita para realizar su trabajo (no contiene transacciones generales ni de visualización).

Role Padre o Maestro: Es un role que no hace referencia a otros roles, en el se asigna las transacciones y valores de los campos de los objetos que no sean Niveles Organizativos.

Sarbanes Oxley (SOX): Ley de Revisión periódica de Controles de los sistemas.

Security Controllers: Persona que tiene la responsabilidad de regular los procedimientos y políticas para la administración de roles y usuarios. Ejemplo: Dueño de Procesos, Control interno.

Segregation of Duties (SOD): Combinación de transacciones y objetos de autorizaciones que incrementa el riesgo de que los usuarios realicen fraudes y acciones indebidas en el sistema SAP.

Objetos Sensibles: Estos son objetos que tienen una cantidad inusual de riesgo y por lo tanto deben estar rigurosamente controlados, con reglas específicas alrededor de su utilización en roles.

Estrategia Tres Niveles: Estrategia para decidir que tipo de transacciones se deben de agrupar en un role Maestro. Los tres niveles se clasifican en: Role general, Roles de Visualización y Roles de trabajo.

Usuario: Persona(s) con acceso a SAP.

UserID: Identificación que se utiliza para nombrar los empleados en SAP.

Segregación de Funciones (SOD) / Sarbanes-Oxley Act - (SOX)

La segregación de funciones (SOD) es un control interno para prevenir o disminuir la ocurrencia de errores al ejecución de transacciones inadecuadas. Esto asegura que diversas funciones de un área de proceso, se separen de modo que no hay individuo en una posición que pueda cometer errores e irregularidades fraudulentas.

El objetivo de SOX es proteger a inversionistas mejorando la exactitud y la confiabilidad de los accesos corporativos hechos conforme leyes de seguridades.

Capitulo II - Mis funciones diseñando Seguridad SAP

Desarrollo profesional en el área de Seguridad SAP

Como en todo tiempo y en toda área, la mayor parte de las compañías requieren personal con experiencia. Pero hay quienes atinadamente confían en el hambre de triunfo y que como recién egresados tenemos las ganas de aprender y demostrar nuestra valía con un pequeño o gran empujón que nos proporcionen.

Aunque mi desarrollo previo había sido trabajando con Mainframe, con el cual había participado en proyectos en España, Holanda, Estados Unidos y México; Neoris SC me dió la oportunidad de dar un giro profesionalmente al entrar a la tecnología SAP**.**

Mi colaboración en Seguridad SAP. Proyectos relevantes.

Neoris SC

Rediseño de Seguridad SAP de Cemex Europa

Mi primera asignación trabajando para Neoris fue participando en el rediseño de la seguridad para Cemex a implementarse en países como Reino Unido, Francia, Polonia, Hungría y Croacia. La necesidad de un rediseño en la Seguridad provino de un cambio gradual de los sistemas de Cemex a nivel mundial, donde no había un sistema homogéneo debido a que las adquisiciones de diversas compañías había dado como resultado que los países de Europa tuvieran como base de operación el sistema SAP mientras que en la mayoría de los países de América se trabajaba con JD Edwards.

Este proyecto implicaba rediseñar la Seguridad SAP con la que Europa ya operaba y que estaba basada en un modelo de roles compuestos y que dificultaba el mantenimiento y el cumplimiento de las Leyes SOX de segregación de funciones. Se elaboró un diseño basado en una estrategia de tres niveles basada en solo Roles Maestros y Roles Derivados.

En este proyecto estuve a cargo de un equipo de construcción que tenía la responsabilidad del desarrollo de los roles de seguridad. Trabajamos en contacto directo con los usuarios de los diferentes países para efecto de pruebas y puesta en producción. Aplicamos los procesos de SoD tanto a nivel role como nivel usuario para dejar el sistema a punto para las auditorías y certificaciones apropiadas para que Cemex cumpliera con la normatividad requerida para cotizar en Bolsa.

Siendo mi primer proyecto en el área de seguridad SAP esta experiencia resultó ser especialmente enriquecedora para mi en el sentido laboral y profesional. Además del aprendizaje técnico y funcional que obtuve, también tuve tiempo de conocer a Neoris como empresa y personalmente decidí que continuaría consolidandome como consultor de SAP dentro de Neoris, la mejor empresa en la que he trabajado hasta ahora.

Rediseño de Seguridad SAP de BAFAR

Mi siguiente asignación fue hacerme cargo del proyecto de Rediseño de Seguridad en BAFAR de la ciudad de Chihuahua.

El rediseño de Seguridad de BAFAR consistió en la implementación de los escenarios necesarios para tener una administración adecuada de usuarios y roles minimizando el esfuerzo en la etapa de soporte.

El objetivo fue el rediseño y construcción de roles de acceso que contemplaran las actividades de la empresa dentro de las aplicación SAP ECC y BI asegurando un funcionamiento libre de problemas de segregación de funciones y que cubriera la operación requerida.

Debido a que BAFAR tenía una operación tradicional de seguridad, sin organización clara en la separación por funciones o posiciones de trabajo. Con un uso exclusivo de Roles Maestros; manipulación manual de objetos de autorización, una nomenclatura de roles poco definida y una ausencia de segregación de funciones que provocaba la existencia de conflictos por transacciones incompatibles. Se presentó la propuesta con los siguientes puntos:

- Una seguridad por posiciones de trabajo y basada en estrategia de tres capas: (Roles de Accesos General, Roles de Visualización y Roles de Trabajo).

- Una Seguridad por Roles Maestros y Derivados.
- Manejo de objetos de autorización a través de la Transacción SU24.
- Nomenclatura con longitud fija y de acuerdo a un formato de función, módulo y ubicación.
- Análisis de VIRSA en 3 etapas del proyecto, remediación de los conflictos con la separación de transacciones.

El objetivo general del proyecto fue logrado, con el rediseño y construcción de roles de acceso que contemplan las actividades de la empresa dentro de la aplicación SAP se aseguró un funcionamiento libre de problemas de segregación de funciones y se cubrió la operación requerida. Quedaron algunas situaciones en valores y objetos que tendrían que irse definiendo con la operación diaria. El apego en lo posible a las políticas y procedimientos en el futuro mantendría el sistema organizado para facilitar el mantenimiento y evitar la creación de nuevos conflictos por segregación de funciones.

Soporte al Go Live de Seguridad SAP de MAQSA

El proyecto de implementación de SAP en la empresa MAQSA en Chihuahua vino después de algunas situaciones tensas entre la empresa y otra consultoría que inicialmente había comenzado con esta implementación.

Esta empresa tenía sus sistemas bajo una base de AS400 y fue difícil el cambio para ellos en todos los sentidos.

Finalmente participé para dar soporte a la seguridad resolviendo los problemas de permisos que se iban presentando durante las implementación del sistema, y también capacitando al personal interno que se quedaría a cargo de esta función para que en la medida de lo posible cuidara las reglas mínimas para mantener una seguridad SAP estable y alerta ante los posibles riesgos.

Puesto que MAQSA no quiso implementar el modelo de Seguridad basado en los tres niveles y solo se crearon roles muy generales mi función consistió primordialmente en asegurar el buen inicio de la operación durante las primeras semanas en que entró en función. Esto con el objetivo de que los permisos de Seguridad no fueran un obstáculo en los procesos funcionales de la actividad diaria.

Al final dí una capacitación en seguridad SAP para que el personal interno de la empresa pudiera seguir administrando adecuadamente el sistema ya implementado y dejé un manual que yo mismo elaboré para las mejores prácticas de seguridad.

Rediseño de Seguridad SAP de Cemex México

Le llegó el turno a México en la estrategia de Cemex de implementar el rediseño en sus sistemas. Y siendo México el país con la operación mas grande constituía el reto mas importante en cuanto al tiempo, riesgo y recursos.

En el cambio de JD Edwards a SAP se incluyó el mismo modelo de Seguridad implementado en Europa.

Estuve a cargo del equipo de Construcción de la parte de Backoffice para el proyecto de Rediseño de la Seguridad. La ejecucion del diseño e implementacion de la seguridad para los modulos de FI, SD, PM, PP, PS. Y la aplicación de los procesos de SoD tanto a nivel Role como a nivel Usuario..

La liberación de este sistema fue particularmente compleja ya que fue una gran cantidad de roles y de usuarios. Pero con todo se logró una operación limpia y sin problemas. La producción dentro de los negocios de Cemex no tuvo ningún contratiempo por problemas derivados de la seguridad y los requerimientos que surgieron en el momento de la puesta en marcha del proyecto fueron atendidos con rapidez.

Soporte a la operación de Seguridad SAP de Peñafiel

Temporalmente estuve apoyando la operación de la Seguridad SAP en Peñafiel la cual tenía algunas cosas interesantes como la operación del nuevo sistema GRC que sustituye a VIRSA en la función de la Segregación de Funciones.

Pocas son las empresas que manejan actualmente esta versión y fue una buena oportunidad para conocerlo un poco y apreciar las diferencias con respecto a la versión anterior.

Laboré en el soporte de la operación diaria atendiendo problemas de Seguridad y atendí requerimientos de creación de nuevos roles y usuarios.

Rediseño de Seguridad SAP de Sultana

Mi siguiente asignación fue la implementación de la Seguridad SAP para la empresa Sultana.

Una empresa relativamente pequeña y sin que los empleados tuvieran mucha experiencia y conocimiento en SAP. Tuve responsabilidades mas amplias a la hora de diseñar el modelo de Seguridad.

Además de diseñar los roles me dí a la tarea también de decidir los valores organizacionales que debían llevar para cumplir las diferentes actividades de los puestos. Esto normalmente lo define un funcional de cada módulo dentro de un proyecto pero al no haberlo o al no tener la suficiente experiencia para hacerlo, se me brindó la oportunidad de hacer estas actividades propias de un funcional de Finanzas y de Logística.

Fue una agradable satisfacción lograr implementar este modelo el cual diseñé no solo como consultor de Seguridad SAP sino también con consultor funcional de FI.

Rediseño de Seguridad SAP de Cemex Colombia, Puerto Rico y República Dominicana.

Esta vez le llegó el turno a Colombia, Puerto Rico y República Dominicana.

Ya con la misma inercia y experiencia de haber implementado la Seguridad SAP para Europa y México se procedió a repetir los mismos pasos para estos países.

Mi labor al igual que en los anteriores países consistió en participar en el rediseño, pruebas y liberación con el mismo resultado exitoso que en los anteriores.

A pesar de que Cemex había entrado desde hace tiempo en situaciones de crisis por la deuda y falta de liquidez que era de dominio público, los proyectos nunca se detuvieron y por el contrario se trabajó en hacer las cosas de una mejor manera y eficacia en estos proyectos que están dándole valor competitivo a la empresa.

Esta última experiencia en Cemex constituyó el colofón a un largo proyecto que implicó la instalación de SAP en toda la operación global de la empresa. Después de participar en diferentes etapas durante este proceso llegué a conocer perfectamente los procesos y protocolos de seguridad. Y profesionalmente llegué a la conclusión de que después de administrar la seguridad de un sistema SAP en una empresa tan grande y compleja como Cemex, cualquier otra me parecería sencilla.

Capitulo III – La Implementación de la Seguridad en SAP ECC

El diseño en la seguridad SAP

El diseño de seguridad SAP consiste en la implementación de los escenarios necesarios para tener una administración adecuada de usuarios y roles minimizando el esfuerzo en la etapa de soporte, proporcionando un conjunto de procesos para asegurar los controles apropiados para el mantenimiento de seguridad SAP.

El objetivo es el diseño y construcción de roles de acceso que contemplen las actividades de la empresa dentro de las aplicación SAP asegurando el buen funcionamiento que cubra todos los procesos del negocio.

Estrategia de seguridad en tres niveles

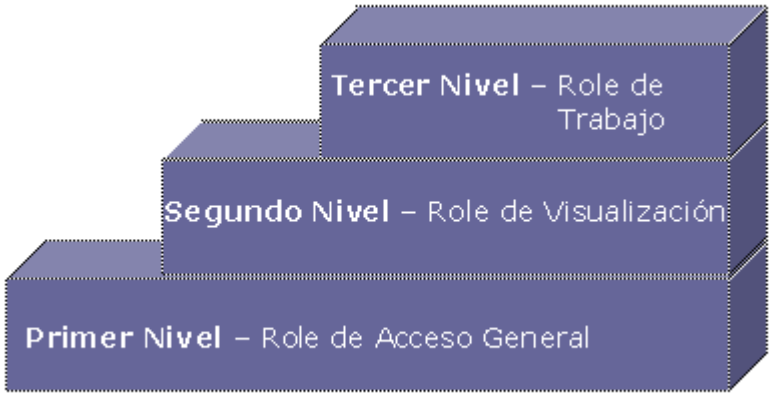
Los roles deben crearse con la estructura de tres niveles donde:

Primer Nivel, creación de un role de acceso general. Este role incluye autorizaciones que todos los usuarios requieran, por ejemplo la impresión, visualización de Job, acceso a SAP Office.

Transaction	Description
SBWP	SAP Business Workplace
SESS	Session Manager Menu Tree Display
SM37	Overview of job selection
SMX	Display Own Jobs
SO00	SAPoffice: Short Message
SO01	SAPoffice: Inbox
SOBN01	1 Personal data
SP01	Output Controller
SP02	Display Spool Requests
SSC0	SAP Appointment Calendar (Employee)
SSC1	SAP (own) Appointment Calendar
SU3	Maintain Users Own Data
SU53	Evaluate Authorization Check

Segundo Nivel, corresponde a roles de visualización de la información para datos no sensibles. Éstos roles contienen el volumen más grande de transacciones. Los roles de visualización se deben de crear para todos los usuarios que trabajan en el área funcional. Además deben existir roles de visualización de datos sensibles, éste debe ser asignado a usuarios limitados. Por lo tanto deben de crearse roles de Visualización para cada área funcional (PM, FI, QM, SD, entre otros). Las transacciones incluidas en estos roles no deberán estar en los roles de trabajo.

Tercer Nivel, se basa en roles de trabajo y es la más crítica a controlar. Estos roles deben ser construidos con base en la posición de trabajo que lleva a cabo el usuario en la empresa. Cada diseño limita al usuario a uno o varios roles de trabajo. Las anomalías ocurrirán en las unidades pequeñas donde los usuarios realizan funciones múltiples. Este role de trabajo debe incluir todas las transacciones y objetos de autorización que un usuario necesita para hacer sus actividades.



Los propietarios de roles (Funcionales, dueños de procesos) son los responsables de indicar las transacciones y determinar en que role deben de estar agregadas y que valores deben de ser incluidos en los campos de los objetos de autorización, para así garantizar el acceso correcto a los usuarios.

Administración de Usuarios

Acceso a Usuarios: El acceso a los usuarios a los sistemas de SAP tiene que ser aprobado, antes de crearle el UserID.

En los sistemas de producción se requiere por lo menos dos niveles aprobación para crear el usuario al empleado.

Cada role debe tener un propietario y este propietario es responsable de las aprobaciones.

Con la implementación de la estrategia de los tres Niveles los usuarios deben de tener generalmente tres roles (general, visualización, trabajo).

Accesos temporales: Son accesos que se otorgan al usuario de manera temporal delimitando la fecha de validez del role, mayormente son transacciones de

mantenimiento los cuales les autoriza realizar funciones que no corresponden a su posición de trabajo

Estrategia para pruebas: El objetivo de la estrategia de las prueba es verificar que todos los roles estén construidos correctamente con poca redundancia.

Pruebas Unitarias:

- ✓ Se construye un ID de usuario por cada role.
- ✓ Toda la prueba será realizada con datos de una compañía piloto donde los niveles organizacionales dependerán de estos, el equipo funcional debe de indicar con que compañía requieren realizar sus pruebas.
- ✓ Se probará cada una de las transacciones que se encuentren en los roles de manera unitaria, desde la ejecución de la transacción hasta la comprobación del resultado.
- ✓ Cuando suceda error de autorización, se debe enviar el log a través de la SU53.
- ✓ El equipo de seguridad modificará el role y se asegurará de actualizar la SU24 para que el role no tenga objetos de autorización tipo cambio ni manuales, se asegurará de colocar valores reales no (*) en los campos.
- ✓ Se debe realizar pruebas positivas y negativas de las funciones de la transacción.

Pruebas Integrales:

- ✓ Se construye un ID de usuario por cada posición de trabajo, los usuarios deben de tener las funcionalidades de los usuarios finales.
- ✓ Toda la prueba será realizada con datos de una o mas compañías pilotos donde los niveles organizacionales dependerán de estos, el equipo funcional debe de indicar con que compañía requieren realizar sus pruebas.
- ✓ Realizar las pruebas positivas y negativas de las funciones y de acceso a la organización.
- ✓ El escenario de prueba debe ser suministrado por el equipo funcional.
- ✓ Las pruebas deben de realizarse para completar el ciclo de un proceso. Ejemplo: Desde la creación de una Solicitud de Compras hasta la creación de la factura para el pago al proveedor.
- ✓ Cuando suceda error de autorización, se debe enviar el lóg. a través de la SU53.
- ✓ El equipo de seguridad modificará el role y se asegurará de actualizar la SU24 para que el role no tenga objetos de autorización tipo cambio ni manuales, se asegurará de colocar valores reales no (*) en los campos.

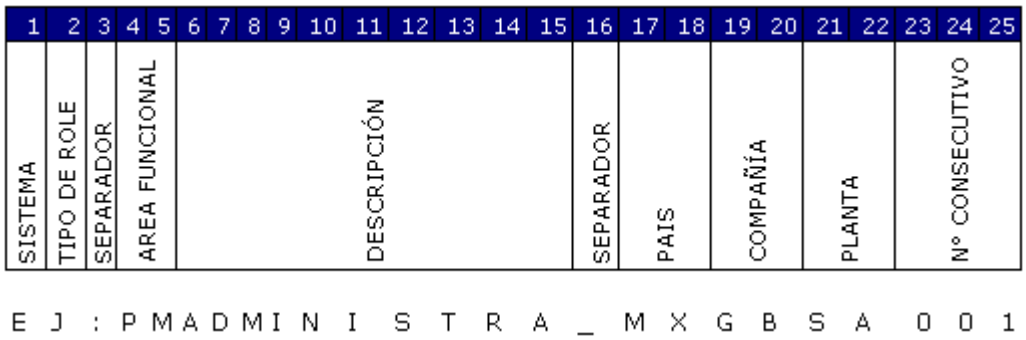
Aprobación de pruebas unitarias e integrales: el equipo funcional entregará un documento de aceptación de que las pruebas fueron satisfactorias.

Administración de Roles

Role Naming Convention: El propósito de una buena nomenclatura es facilitar el análisis y los controles de identificación:

Sistema.
Dueño del proceso (Esto es necesario para realizar las segregación de funciones respectivamente)
Tipo de role como de trabajo, derivados, display. (Es necesario para así identificar los tipos de roles)
Acceso a datos de la organización.

El nombre de los roles debe seguir el siguiente formato:



Roles Maestros:
Posición 1-> Sistema (se debe identificar debido a que existen varios componentes SAP)
E - ECC6 (ERP)
B - BI
Posición 2 -> Tipo de Role (Necesario para identificar los tipos de roles)
B - Communication and Interface Roles
D –Display roles
F - Fire fight roles
G - General Access
J - Job roles
W -Work Flow roles
Posición 3 □ Separador
: - Roles simples
+ - Roles Compuestos
Posición 4-5□ Área Funcional (Esto es necesario para realizar las segregación de funciones respectivamente)
Dos caracteres que representan el área funcional.

Ejemplo:

Modulo	Area Funcional	Descripción
Finanzas	GL	General Ledger
Finanzas	AP	Accounts Payable
Finanzas	AR	Accounts Receivable
Finanzas	TV	Travel Expense
Finanzas	PS	Project System
Finanzas	CO	Product Costing
Finanzas	TR	Treasury
Producción	PP	Production Planning
Logistica	SD	Sales and Distribution
Logistica	LE	Logistics Execution Transportation
Gestión de Materiales	MM	Materiales
Calidad	QM	Quality
Mantenimiento de Planta	PM	Mantenimiento de Planta

Posición 6-15 Descripción, texto descriptivo de 10 caracteres.
Roles Derivados:
Posición 16 Separador de roles maestros

_
Posición 17-18 País
2 caracteres correspondientes al código ISO
MX - México
Posición 19-20 Compañía

Cod	Descripción	Posición 19-20
1000	Grupo Bafar SAB de CV	GB
1001	Carnes Selectas Baeza	CB
1002	Cibalis SA de CV	CI
1003	Lectus Corporativo SA	LC
1004	Lectus Industrial SA	LI
1005	Lectus SA de CV	LE
1006	Serv Corporativos Lerma	SC
1007	Lectus Comercial SA de CV	LO
1008	Hendler S de RL de CV	HE
1009	Promotora Tres Hermanos	TH
1010	Proyectos Inmob Carnemart	PI
1011	Inmuebles Forza SA de CV	IF
1012	Inmobiliaria Carnetec SA	IC
1013	Demarius SA de CV	DE
1014	Aiax SA de CV	AI
1015	Destinia Agencia de Viaje	DA
1018	Vextor Activo SA de CV	VA
2000	Inst y Maquinaria INMAQ	IM
3000	Onus Comercial SA de CV	OC
4000	Intercarnes SA de CV	IC
5000	Intercarnes Texas Co.	IT
9000	LongHorn Warehouses Inc	LH

Posición 21-22 Planta ,
Ver archivo Name role_Position 21-22.xls (tabla con valores)

Posición 23-25 Secuencia de tres números.
Todas las abreviaturas (país, negocio, organización, etc.) se deben definir y mantener en forma global.

Diseño de Roles

Todos los diseños de los role en SAP deben comenzar con un listado de transacciones, mediante un archivo donde se reflejen los proceso del negocio.

Los archivos están separados por sub módulos, los propietarios de los roles deben de determinar que transacciones deben tener cada posición de trabajo.

Para la estrategia de tres niveles el propietario del role debe simplificar la acción del role de trabajo agrupando las transacciones de visualización las columnas del role de display.

Luego deben asociar solamente las transacciones de modificación en columnas del role de trabajo correspondiente.

Ejemplo:

Transacción	Descripción	Area Funcional	Role de trabajo 1	Role de trabajo 2	Role de trabajo 3	Role de Visualización
MIGO	Goods Movement	MM	X			
ME21N	Create Purchase Order	MM	X	X		
IW31	Create Order	PM			X	
MD04	Display Stock/Requirements Situation	MM				X
MIRO	Enter Incoming Invoice	FI	X			
ME22N	Change Purchase Order	MM		X		
CV03N	Display document	SD				X
FS10N	Balance Display	FI				X

Después de que se construyan los roles, los cambios se deben indicar a la de la siguiente manera.

- Letra X – Transacciones asignadas durante la etapa de Diseño.
- Letra A (ADD) – Indica que se requiere asignar una transacción al role.
- Letra D (Delete) – Indica que se requiere eliminar una transacción al role.

Niveles organizacionales:
Se agregará una nueva columna en la hoja “Levels Org”

- (ADD) – Indica que se requiere asignar un nuevo un valor de un Nivel Organizacional de una o varias compañías.
- (Delete) – Indica que se requiere eliminar un valor de un Nivel Organizacional de una o varias compañías.

Change	Cod. Levels Org	Description Level Org	Company 1	Company 2	Company 3
ADD	WERKS	Plant	C401	R314	R103
	BUKRS	Company code	1003	1006	1005
ADD	KOART	Account type	S	S	S
DELETE	KOART	Account type	K	K	K

Mantenimiento de Roles

El propietario del role selecciona una copia de la matriz actualizada publicada en (Por definir).

Los cambios son aplicados según las instrucciones del diseño del role.

Si la transacción que se desea asignar al role no es propiedad del solicitante se debe de solicitar la aprobación al propietario de dicha transacción.

El equipo seguridad controlará la versión de la matriz contra la última versión publicada. Si la versión es diferente se regresa el requerimiento al propietario del role para que actualice la ultima versión de la matriz.

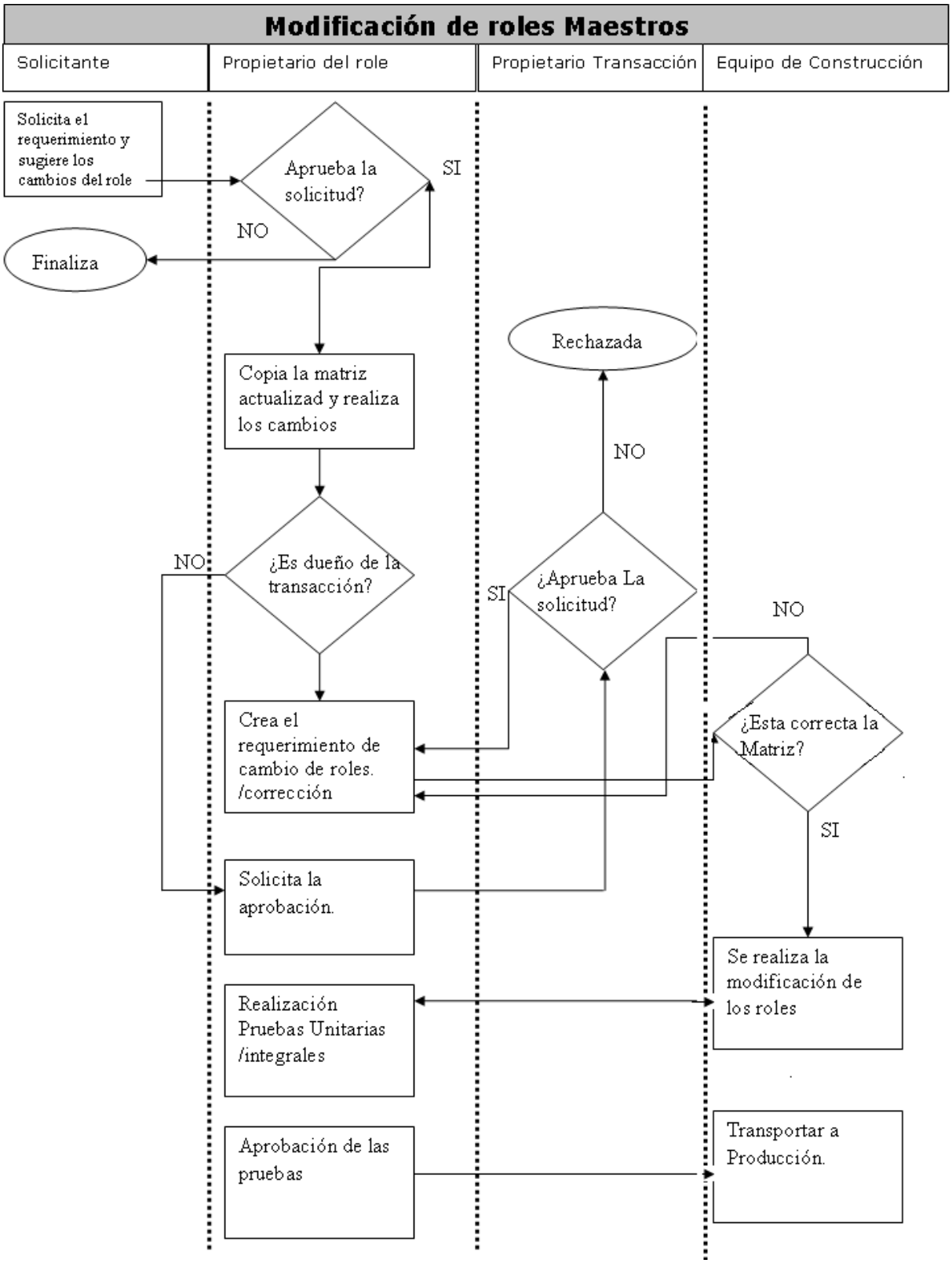
La nueva matriz se publica, con la nueva versión, antes de que se realicen los cambios.

Se realiza la programación para el cambio del role.

Se realizan las pruebas unitarias del role.

Luego se realiza las pruebas integrales en el ambiente de calidad.

Una vez que la prueba es completada y se tienen todas las aprobaciones del buen funcionamiento del role, este deberá transportarse a producción.


Modificación de roles Maestros
Solicitante
Propietario del role
Propietario Transacción
Equipo de Construcción
Solicita el requerimiento y sugiere los cambios del role
Aprueba la solicitud?
SI
NO
Finaliza
Copia la matriz actualizad y realiza los cambios
¿Es dueño de la transacción?
NO
Crea el requerimiento de cambio de roles. /corrección
Solicita la aprobación.
Realización Pruebas Unitarias /integrales
Aprobación de las pruebas
Rechazada
NO
¿Aprueba La solicitud?
SI
NO
¿Esta correcta la Matriz?
SI
Se realiza la modificación de los roles
Transportar a Producción.

Administración de Usuarios

Proceso para la solicitud de Acceso:

- Los accesos a los usuarios finales se debe realizar mediante la política establecida en la empresa.
- La solicitud de acceso a los roles Fire-Fighter, se realizará mediante cortos periodos para que el funcional o usuario final pueda resolver la falla o problema en el sistema de producción.
- Este procedimiento deberá ser documentado y validado por Control Interno.
- El perfil de SAP_ALL no debe ser usado.
- El acceso de roles FIRE Fighter debe ser otorgado por área funcional.
- El periodo máximo de asignación debe ser de dos días para resolver la falla o problema en producción. Luego de ese tiempo se debe de solicitar de nuevo la aprobación.
- Se debe de monitorear el usuario mientras tenga el role de Fire-Fighter.

La solicitud de acceso OSS se establecerá otorgando un usuario. El equipo de seguridad enviará una solicitud al equipo basis para que abran la conexión, la cual debe de tener lo siguiente:

- Número de Nota OSS.
- Cliente donde va a accesar.
- Duración de acceso (Máximo 7 dias).
- Area funcional que necesita validar. Las peticiones con SAP_ALL se deberán de rechazar.

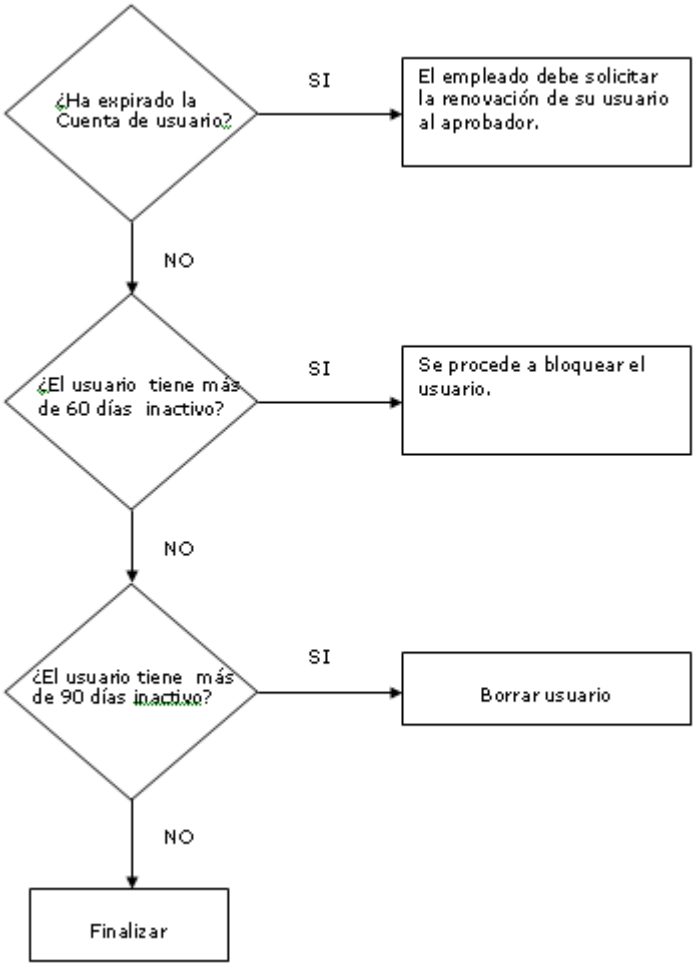
Todas las cuentas de usuarios SAP deben crearse con fecha de vencimiento. Esto se debe utilizar para todas las cuentas del diálogo del empleado.
Las cuentas que no necesitan expiración:

- Usuarios de Sistemas
- Usuarios de Jobs.

Las cuentas que necesitan fecha de expiración:

- Usuarios consultores, máximo seis meses.
- Usuarios OSS, máximo 7 días.
- SAP early watch (monitoreo del sistema), máximo 14 días.
- Roles de acceso a FIRE Fighter, máximo 2 días.
- Roles On demand, máximo 7 días.

Diagrama de Validación de Acceso.



Revisión de objetos obsoletos

Es importante revisar los sistemas de SAP periódicamente para identificar objetos de seguridad obsoletos o los que no se utilizan. Éstos incluyen:
Los roles no asignados a los usuarios, considerando que los roles Maestros nunca deben asignarse directamente a los usuarios.
SAP users de usuarios que ya no trabajen en la empresa.
Usuarios que no han utilizado el sistema SAP por determinado tiempo.
Transacciones asignadas a roles que no han sido usados.

Aplicación de la Segregación de Funciones (SOD)

Los requerimientos de Acceso para la Ley SARBANES-OXLEY son los siguientes:

- Acceso abierto y segregación de funciones son los principales controles para la Ley Sarbanes-Oxley (SARBOX).

- Los problemas de acceso representan los riesgos más significativos para la mala opinión de los Auditores Internos relacionada a los controles internos.

- La revisión de los responsables de los Procesos de Negocio (BPO's, Business Process Owners) es clave para los controles relacionados a los accesos.

La Ley SARBANES OXLEY se basa en las siguientes acciones:

- Sección 302: Es requerida una certificación anual (Compañías fuera de USA) o cuatrimestral (Compañías Americanas) por el CEO / CFO para la SEC relacionada al adecuado cumplimiento de los reportes financieros.

- Sección 404: Es requerido un reporte anual de la Administración General relacionado al Control Interno. Este reporte deberá expresar la responsabilidad de los gerentes en relación al establecimiento y mantenimiento apropiado de la estructura y procedimientos de CI para los reportes financieros.

En este paso se procede a aplicar un análisis de los conflictos en los que se pudo haber incurrido al momento de agrupar las transacciones en un role o bien al momento de asignar los roles a los usuarios.
Existen herramientas especiales como la nueva versión de GRC con la que se puede obtener un análisis por role o un análisis por usuario. A estos conflictos se les puede combatir de dos maneras: Por medio de una remediación o por medio de una mitigación.

En el caso de una remediación se procede a separar las transacciones en conflicto en diferentes roles.

En el caso de una mitigación se procede a conservar el acceso bajo un constante monitoreo de las actividades efectuadas.

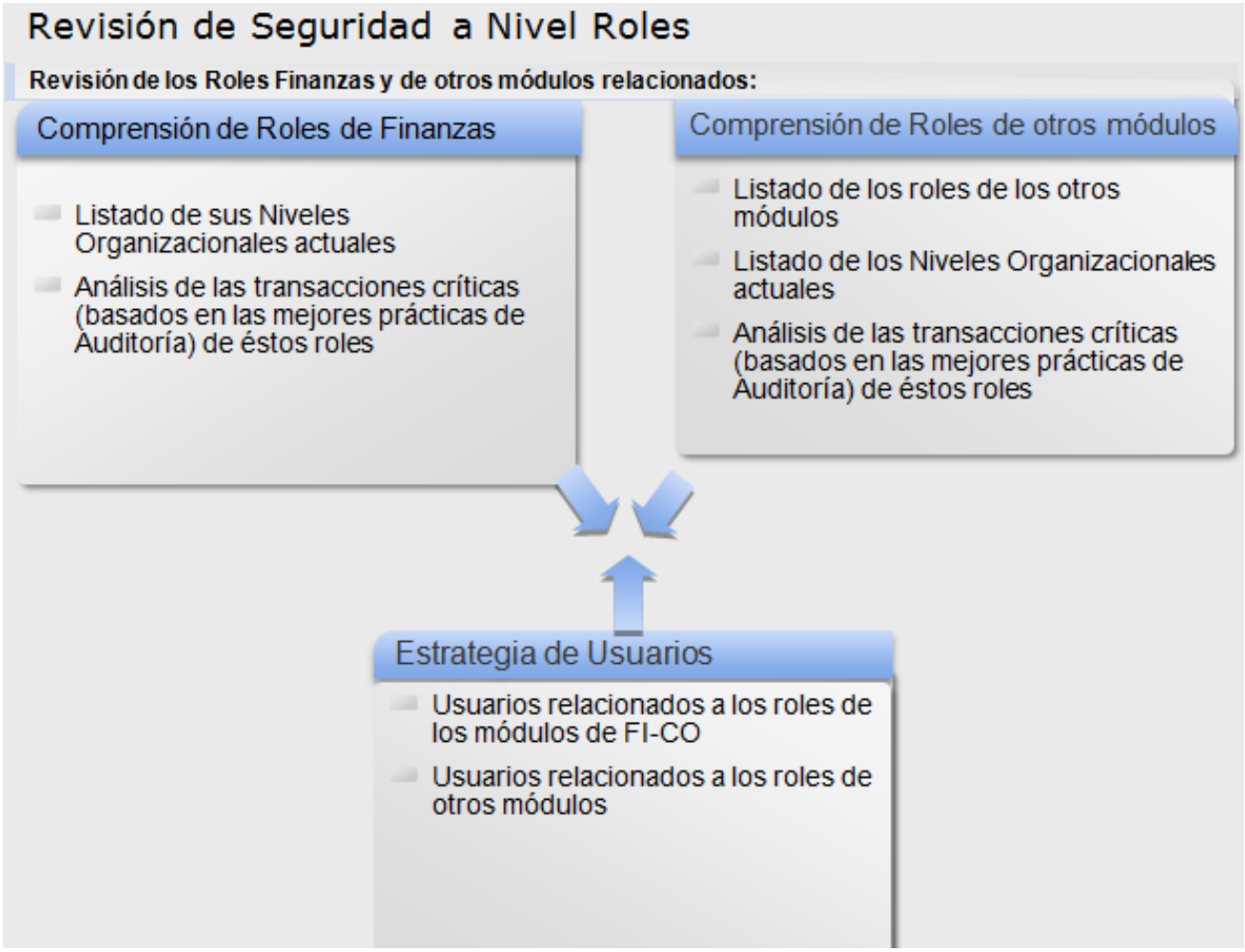
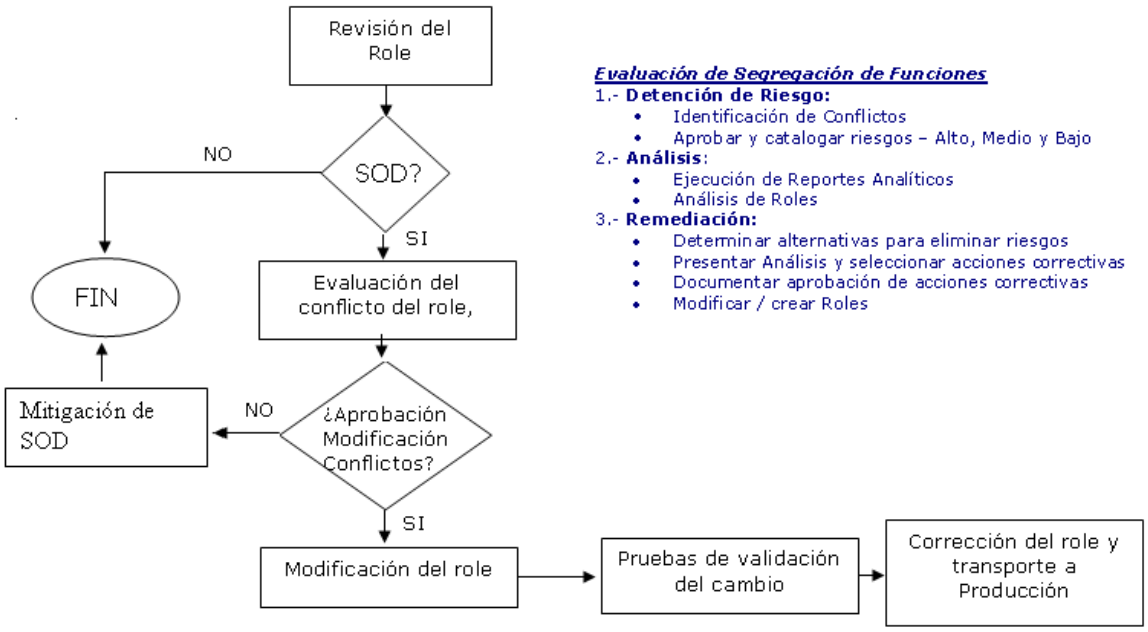

Revisión de Seguridad a Nivel Roles
Revisión de los Roles Finanzas y de otros módulos relacionados:
Comprensión de Roles de Finanzas
Listado de sus Niveles Organizacionales actuales
Análisis de las transacciones críticas (basados en las mejores prácticas de Auditoría) de éstos roles
Comprensión de Roles de otros módulos
Listado de los roles de los otros módulos
Listado de los Niveles Organizacionales actuales
Análisis de las transacciones críticas (basados en las mejores prácticas de Auditoría) de éstos roles
Estrategia de Usuarios
Usuarios relacionados a los roles de los módulos de FI-CO
Usuarios relacionados a los roles de otros módulos

Diagrama SOD



Conclusiones

SAP es un sistema en constante evolución que cada día aborda nuevos negocios y mercados. Cada vez agrupa mas tecnologías No SAP que añaden mayor complejidad a la operación.

En esta misma dinámica el tema de la Seguridad en SAP se vuelve un tema relevante ante la necesidad de seguir manteniendo una misma fiabilidad e integridad en los procesos. A través de nuevas plataformas como el Identity Management y el Single Sign On se continúa dando una respuesta sólida y flexible que van de la mano con el crecimiento del sistema.

Hasta ahora mi experiencia diseñando la seguridad en sistemas SAP me ha permitido desarrollar procesos sólidos que se apegan a los estándares de control y auditoría que dan como resultado un alto nivel de confiabidad en los accesos a los sistemas de las diferentes empresas en donde he laborado como consultor de seguridad SAP.

De todas ellas Cemex ha sido definitivamente la empresa donde he tenido la oportunidad de lograr un desarrollo mas amplio debido a las características propias de esta compañía: una multinacional con una gran variedad de aplicaciones, una gran cantidad de usuarios y con la obligación de mantener un sistema sólido por las regulaciones propias de la Ley SOX para poder cotizar en bolsa. Una empresa en constante transformación que para mantenerse al frente del mercado busca también mantenerse al tope de la tecnología.

Debido a la Ley SOX, SAP tuvo que cambiar el enfoque de su seguridad de roles compuestos a roles maestros con derivación. Puesto que un enfoque con roles compuestos impide la adecuada segregación de funciones y tiende a anidar las autorizaciones en complicadas tramas de autorizaciones. Asi con la utilización de roles maestros y roles derivados SAP permitió a las empresas diseñar su seguridad de una manera mas sencilla de implementar y de mantener; y lo mas importante, les permitió aplicar adecuadamente la segregación de funciones para cumplir cabalmente con la Ley SOX. Este enfoque lo tuvimos que cambiar en Cemex y lo mismo en otras empresas como Bafar, MAQSA y Sultana.

Hoy en día todas las empresas aún las mas modestas que utilizan un sistema SAP, buscan maneras de mantener el control ante posibles fraudes internos que menoscaben su patrimonio, y son cada vez más las empresas que aún sin cotizar en bolsa buscan mantener en sus accesos esta segregación de funciones para minimizar estos riesgos y buscan tener un diseño de seguridad sólido y fácil de mantener como lo es el diseño de tres capas.

Existen muchas posibles maneras de implementar una solución en SAP, y por lo tanto también existen muchas maneras de abordar el tema de seguridad en SAP. Algunas empresas prefieren accesos mas abiertos de tal modo que la seguridad interfiera la menos posible con la operación. Pero hay otras empresas que exigen un alto nivel restrictivo en los accesos y autorizaciones.

He aprendido a valorar las necesidades de cada implementación y a ejercer mis propuestas como consultor de Seguridad para que cada compañía obtenga un verdadero valor al implementar su estrategia de Seguridad.

Al implementar cualquier medida de seguridad debe valorarse también el costo de una amenaza al sistema contra el costo de la medida de seguridad.

Un sistema de seguridad SAP bien organizado, bien diseñado y bien administrado proporciona a la empresa una base sólida y confiable contra cualquier amenaza de quiebre o de fraude.

Bibliografía

http://help.sap.com

ADM940 - SAP Authorization Concept. 2006 SAP AG.

ADM950 - Secure SAP System Management. 2006 SAP AG.

ADM960 - Security in SAP system Environments. 2006 SAP AG.

TZNWIM – SAP NetWeaver Identity Management. 2007 SAP AG.

Denise Vu Broady, Holly A. Roland. SAP GRC for Dummies. Indianapolis. Wiley Publishing, Inc. 2008.