Universidad Autónoma de Querétaro
Facultad de Informática
Maestría en Sistemas de Información: Gestión y Tecnología

Control y manejo de seguridad para el sistema ERP (SAP), por medio de la definición de roles transaccionales.

TESIS

Que como parte de los requisitos para obtener el grado de la
Maestría en Sistemas de Información: Gestión y Tecnología

Presenta:
ISC. Juan Francisco Quiñones Sánchez

Dirigido por:
Dr. Ubaldo Chávez Morales

SINODALES

Dr. Ubaldo Chávez Morales
Presidente

Dra. Rosa María Romero González
Secretario

MISD. Juan Salvador Hernández Valerio
Vocal

Dr. Alberto Lara Guevara
Suplente

MSI. Ernesto Ruvalcaba Durán
Suplente

M.C. Ruth Angélica Rico Hernández
Directora de la Facultad

Dr. Irineo Torres Pacheco
Director de Investigación y Posgrado

Centro Universitario
Querétaro, Qro.
Agosto de 2013
México

RESUMEN

El objetivo de este trabajo de tesis es implementar un sistema de información que permita auditar de manera periódica las operaciones que se ejecutan en el sistema SAP, por medio de los empleados de la compañía, y tener la posibilidad de establecer medidas preventivas y de mejoramiento que contribuyan a reducir el número de conflictos a nivel planta. Actualmente SAP es un sistema de tipo ERP que se encuentra presente en la mayoría de las empresas controlando procesos de finanzas, manufactura, ventas, operación, recursos humanos, etc. El éxito de una compañía depende principalmente de la calidad de la información y de la velocidad con que pueda ser compartida, es por esto que administrar la seguridad informática es de vital importancia para el crecimiento empresarial. Como primer punto, se establecieron los procedimientos para identificar claramente los tipos de conflictos que generan los empleados al ejecutar transacciones en el sistema SAP, así como los algoritmos de programación para vincular la información con la solución del problema. Posteriormente, se elaboró la documentación necesaria sobre la problemática que actualmente vive la compañía y que se desea resolver mediante este sistema de información. Finalmente se implementó el sistema Sap Security vía intranet, con módulos de actualización de base de datos como captura, consultas e informes. De esta forma los conflictos generados por los usuarios, son controlados mediante el desarrollo de técnicas de análisis y seguimiento para los diferentes perfiles de usuario, permitiendo generar documentación y reduciendo costos de operación para la compañía.

SUMMARY

The objective of this thesis is to implement an information system that allows to audit periodically the operations that were executed in the SAP system, by employees of the company, and to be able to establish preventive measures and improvement that help to reduce the number of conflicts at the plant. Actually SAP is a type of system ERP, which is used in most of the companies for controlling processes in finance, manufacturing, sales, operations, human resources, etc. The success of a company mainly depends on the information quality and its speed to be shared, this is why computer security is critical management to business growth. As the first point, the procedures were established to identify clearly the types of conflicts that were generated by employees to execute transactions in the SAP system and programming algorithms to link the information with the problem solution. Subsequently, the necessary documentation of the company problems was developed to be solved by this system. Finally, the Sap Security system was implemented via intranet, with upgrade modules of database like capture, queries and reports. Thus, the generated conflicts by users, are controlled by the development of analysis and monitoring techniques for different user profiles, allowing to generate documentation and reducing operating costs of the company.

C O N T E N I D O

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

1.1 Definición del Proyecto

La evolución y crecimiento de las compañías así como sus necesidades para resolver sus problemas administrativos y de operación han propiciado el desarrollo de software dedicado. Administrar la seguridad informática de las empresas es una tarea compleja, ya que existen varios factores que pueden dificultar el funcionamiento de las compañías.

Actualmente la compañía Procter & Gamble planta Mariscala, México, utiliza el sistema de transacciones SAP de tipo ERP, el sistema lleva el control de múltiples actividades, como el control de las líneas de producción, creación de órdenes de compra dirigidas a los proveedores, manipulación y reportes de información, etc.

Los conflictos que generan los usuarios por medio de la ejecución de transacciones críticas en el sistema SAP, representan una gran preocupación en la seguridad de los procesos de la compañía.

El contar con un software de apoyo al sistema SAP, permitirá efectuar el seguimiento y control de los conflictos generados, facilitando la supervisión y auditoría de la ejecución de transacciones dentro de los procesos de la organización. Con ello, se contará con elementos que faciliten la toma de decisiones.

El control y manejo de conflictos transaccionales vía Internet se convierte en una herramienta muy útil cuando se muestran al mismo tiempo las causas y operaciones que los causaron. La definición de procedimientos, algoritmos de programación y el uso de bases de datos contribuyen para que un sistema de apoyo al sistema de Información (SAP) proporcione los resultados esperados.

Particularmente, el caso de estudio de la tesis se realiza en base al tema de la seguridad informática que se enfoca a la protección de toda la infraestructura computacional y todo lo relacionado con ésta, ya que la seguridad informática abarca todo lo que la organización valore y que signifique un riesgo si llega a manos de otras personas.

En cuanto a la infraestructura, para implantar las medidas preventivas y de mejoramiento que contribuyan a reducir el número de conflictos generados por los usuarios al ejecutar transacciones en el sistema SAP, es importante también contar con información estadística como reportes mensuales, trimestrales y por año con la finalidad de poder conocer el nivel de control de la problemática existente. Con estos aspectos, se pretende contar con una herramienta de conocimiento y con características de los conflictos, planes de acción, reportes, etc., con el objetivo de tener mayor control sobre las operaciones realizadas en SAP y contar así con mayor accesibilidad, confiabilidad e interactividad con la información vía intranet.

Además, es importante actualizar y vincular la información de la base de datos, cuyo contenido, estará cambiando constantemente. Por tanto, se investigan y aplican procedimientos de filtrado de información mediante algoritmos de programación, con la finalidad de poder proporcionar información verídica y sobre todo lo que el usuario desea ver como reporte. Realizando investigaciones sobre las tecnologías disponibles para el desarrollo de aplicaciones, a fin de contar con las mejores herramientas para poder obtener los mejores resultados en el desarrollo del proyecto, utilizando formatos que faciliten el intercambio de información y que impliquen un menor costo para el usuario. [Charte, 2002]

Finalmente, es importante implementar los módulos de administración que permitan integrarse a la aplicación web con el objetivo de capturar información, realizar consultas y actualizar de las Bases de Datos con información de accidentes.

1.2 Objetivos

- Revisar y controlar de manera periódica accesos al sistema SAP.
- Identificar accesos no permitidos de acuerdo a la función de cada usuario.
- Controlar y manipular las transacciones ejecutadas por los usuarios y que no están permitidas para cada perfil de usuario.
- Generar documentación cuando exista un conflicto perteneciente al permiso y razón de negocio de los diferentes procesos en planta.

1.3 Alcance

El sistema debe comprender la siguiente funcionalidad:

- Los accesos al sistema deberán ser por medio de usuarios registrados en intranet.
- El sistema debe contener menús visibles para cada perfil de usuario: administrador del sistema, usuarios y key users (usuarios líderes en cada área de producción).
- El menú de administrador contendrá las formas de altas, bajas ó modificaciones de los siguientes catálogos de información:
    - Key Users
    - GBU (agrupación a la que pertenece un conjunto de transacciones en SAP)
    - Modelos de Usuarios (grupo de perfiles que puede utilizar un usuario)
    - End user (usuarios que utilizan SAP).
- El menú de Key users contendrá las formas de alta, bajas ó modificaciones de:
    - Modelos de Usuarios
    - End Users
    - Documentación de conflictos (Si los usuarios ya realizaron la documentación correspondiente a cada conflicto).
- El sistema validara por cada usuario el proceso al que pertenece como al modelo al que se encuentra asignado

- Validará por cada usuario, los roles que están en un modelo definido contra los roles asignados en SAP.

- En caso de que los roles documentados y los roles en SAP no concuerden, se generará un reporte mostrando el usuario, el modelo afectado y los roles que no se encuentren alineados; en caso de que el modelo contenga conflictos

- El Key users podrá realizar los cambios después de la validación y crear si es necesario un nuevo modelo o hacer modificaciones en la asignación del modelo al usuario.

- En caso que la nueva asignación de roles ocasione un conflicto, será necesario realizar la documentación de la razón de negocio.

- La documentación de la razones de negocio para los conflictos se llevara a cabo en el momento de una alta de roles en un modelo de usuario.

- Los conflictos deberán ser documentados por área y modelo de usuario al que está siendo afectado.

2. MARCO TEÓRICO

2.1 Conceptos fundamentales de los Sistemas de Información

En este capítulo se aborda el tema de los Sistemas de Información, incluyendo sus conceptos y actividades básicas así como su evolución. Lo anterior para visualizar el tema desde sus componentes básicos hasta la forma en que se organiza la información para dar cumplimiento con las expectativas del campo al cual da servicio.

2.1.1 Entrada de Información

Los sistemas de información cuentan con procesos mediante los cuales toman los datos que necesitan con la finalidad de procesar información, ya sea de forma manual o de forma automática.

La introducción de datos de forma manual se refiere al hecho de que el usuario mete la información de manera directa, mientras que la automática lo hace a través de módulos programados que meten la información de forma inmediata tomando en cuenta parámetros o reglas y generalmente son bloques de información.

2.1.2 Almacenamiento de Información

Los Sistemas de información tienen la capacidad de guardar las actividades que realizan, por medio de esta propiedad ellos pueden recordar procesos anteriores y mostrar los resultados deseados a los usuarios. La información es almacenada en unidades de almacenamiento como pueden ser discos duros, unidades de cinta magnética, diskettes, unidades de cd-rom, etc.

2.1.3 Procesamiento de Información

El procesamiento de la información es muy importante para la obtención resultados ya que se pueden realizar cálculos siguiendo una estructura preestablecida, con la finalidad de transformar datos en información que pueda ser tomada para la toma de decisiones.

2.1.4 Salida de Información

La salida es la capacidad para obtener información procesada de un sistema de información, es importante mencionar que la salida de un sistema podría ser la entrada de otro sistema o módulo.

2.2 Sistemas Inteligentes de tipo ERP

En los últimos años ha existido gran avance en las diferentes tecnologías de información, esto ha permitido crear sistemas de información más sofisticados e integrados. Los sistemas de tipo ERP (Enterprise Resource Planning) son ejemplo de ello, estos sistemas son aplicaciones de gestión empresarial las cuales fueron diseñadas para cubrir todas las áreas funcionales de la organización, generando un flujo de trabajo entre los usuarios mejorando considerablemente el trabajo cotidiano.

Con la necesidad de automatizar funciones de producción comenzaron a nacer diversos sistemas para el control de materiales, productos y servicios, pero el verdadero control de la producción surgió con la planeación en función de la capacidad de los materiales.

La automatización de las funciones productivas fue evolucionando pero ahora también consideraba la capacidad de las líneas de producción, Tomando en cuenta la necesidad de reducir costos, después siguió la evolución pero ahora la planeación de la producción estaba en función de las demandas de los clientes, mejorando la atención y el servicio a los clientes.

La evolución del software empresarial ha sido de gran importancia para la integración de procesos, dando lugar a los primeros proveedores de software empresarial, que incluían todas las funciones de una empresa de manufactura, tanto administrativas como de producción.

Fue toda esta evolución y las empresas involucradas los que inventaron el término ERP (Enterprise Resource Planning), lo que significa planeación de la empresa a partir de sus recursos.

Los sistemas ERP, los cuales constituyen un paquete de negocios para las empresas permiten automatizar e integrar la mayoría de los procesos, tener información y poder consultar dicha información en tiempo real.

El objetivo principal de los sistemas ERP es coordinar los negocios de las empresas desde el manejo de proveedores hasta la facturación de los clientes, ayudando a que la información fluya a las diferentes áreas de la compañía como son: producción, finanzas, recursos humanos, etc.

2.3 Propósito de los Sistemas de Inteligencia de Negocios

En un inicio puede parecer que el análisis de datos es un proceso sencillo y fácil de conseguir sin embargo la información suele presentarse de manera estática y no permite profundizar en los datos, navegar entre ellos y manejarlos desde diferentes perspectivas.

Los Sistemas Expertos cuentan con las siguientes características proporcionando ventajas competitivas sobre sus competidores:

- **Generación de informes dinámicos, flexibles e interactivos:** El usuario podrá ver la información con diferentes puntos de vista y diferentes perspectivas aclarando todas sus dudas en tiempo real.

- **No requiere conocimientos técnicos:** El usuario con poco conocimiento podrá crear gráficos, informes y navegar entre ellos, con la finalidad de examinar toda la información disponible.

- **Rapidez en el tiempo de respuesta:** Generalmente se utiliza un modelo de bases de datos bien estructurados en donde la tecnología de manejo de cubos y datawarehouse están presentes haciendo que las consultas por los usuarios sean casi de manera inmediata.

- **Integración entre todos los departamentos de la compañía:** Es necesario garantizar la calidad y la integración de los datos por medio y métricas entre las diferentes unidades de la empresa con la finalidad de realizar una integridad referencial absoluta.

- **Cada usuario dispone de información adecuada:** Cada usuario solo podrá tener acceso a la información que necesita, correspondiente a su área de trabajo, evitando que tenga acceso a toda la información y que sea lo que realmente necesita.

- **Disponibilidad de información histórica:** En este tipo de sistemas expertos podemos encontrar diariamente la comparación de datos actuales con información de otros períodos históricos de la compañía con la finalidad de realizar análisis de tendencias, evolución de parámetros, mediciones, etc.

El objetivo principal de los sistemas inteligentes es explotar al máximo la información residente en una base de datos corporativa (datawarehouse) mostrando informes muy dinámicos con gran potencial de navegación y utilizando siempre una interfaz gráfica muy amigable, vistosa y sencilla. [Herrera, 2004]

2.4 Seguridad Informática

La seguridad en los procesos informáticos es de vital importancia para las compañías, ya que la información y los datos que ahí se manejan son muy valiosos y deberán estar protegidos adecuadamente para garantizar la ejecución correcta de transacciones. [Aguirre, 2006]

El principal objetivo de este proyecto es dar seguimiento y control a los conflictos generados en la ejecución de transacciones críticas por los usuarios por medio del sistema SAP, proporcionando técnicas de análisis y solución de problemas.

El desarrollo de técnicas de seguridad en los procesos informáticos ha sido objeto de estudio durante muchos años, y con el crecimiento exponencial de la tecnología, se pueden implementar algunos algoritmos que no podrían ser puestos en marcha anteriormente debido a limitaciones tecnológicas. [Hallikainen, 2000]

La industria cada día demanda más sistemas de información debido a su necesidad de mejorar la calidad de producción. Se busca que estos sistemas provean de información exacta y completa acerca de fallas o errores en los diferentes procesos que faciliten la toma de decisiones.

Toda organización debe estar a la vanguardia de los procesos de cambio, en donde disponer de información continua, confiable y en tiempo constituye una gran ventaja fundamental donde tener información es tener el poder.

La seguridad informática debe garantizar la disponibilidad, la recuperación (en caso de errores), la integridad y la confidencialidad de los sistemas de información.

Con la finalidad de identificar problemas en los sistemas de información antes de cualquier pérdida de información se recomienda:

- Implementar Políticas de Seguridad Informática
- Identificación de Problemas
- Desarrollo de un Plan de Seguridad Informática
- Análisis de la seguridad en los equipos de computación
- Realizar auditorías y revisión de sistemas

Los sistemas de información están cada día más expuestos a sufrir diversos ataques informáticos que puedan robar información y la prevención es la mejor arma para combatir estos problemas. [Saltzer, 1974]

2.5 SAP en México

SAP es una compañía multinacional del software especializada en sistemas de tipo ERP, fue creada en 1972, en Alemania, actualmente cuenta con miles de empleados, es el líder mundial en ERP y sus aplicaciones se encuentran instaladas en la mitad de las empresas a nivel mundial.

SAP permite llevar la gestión de varias compañías simultáneamente y utilizan una filosofía en donde sus aplicaciones se pueden adaptar a todo tipo de negocio, sin embargo SAP consciente de que cada negocio tiene sus particularidades desde 1995 también ha desarrollado soluciones más hechas a la medida.

El sistema SAP en México ha tenido una gran aceptación por las empresas debido a que sus productos y servicios son de gran calidad ayudando a los empleados a tener autonomía para tomar decisiones y tomar riesgos. Es una cultura de independencia y madurez asumiendo la responsabilidad total en la toma de decisiones, pues no existen controles de tiempos, horarios, jornadas de trabajo, restricciones ó reglas.

SAP cuenta con las siguientes características de liderazgo, razones por las cuales ha sido de gran aceptación en México:

- Los managers de cada área son responsables de cada área, donde cada persona es responsable de cumplir sus objetivos.

- Cuenta con un programa de evaluación de desempeño el cual es establecido de tal manera que no existe ningún empleado que no cuente con objetivos claros desde el inicio del año.

- El liderazgo se ha transformado en parte por la gran influencia del sistema SAP, haciendo un liderazgo más institucional por medio de la aportación de muchos elementos culturales.

- Se utilizan programas de capacitación para todos los empleados, además de programas que ayudan a identificar a los lideres a quienes se les capacita de manera especial.

- Generación de Transacciones y operaciones de control de producción de manera eficiente y sencilla.

- Manejo de Proveedores y cartera de clientes utilizando una comunicación más real y transparente.

El sistema SAP en México ha venido a revolucionar la tecnología que trabaja en una aplicación para que los empleados tengan mejor acceso a la información empresarial.

2.6 SAP en Procter & Gamble

La evolución y crecimiento de las compañías así como sus necesidades para resolver sus problemas administrativos y de compra de equipos ha propiciado el desarrollo de software dedicado.

El éxito de una compañía depende de la calidad de la información y de la velocidad con que pueda ser compartida, estos puntos son básicos para que sistemas como SAP (Compañía multinacional del software especializada en sistemas de tipo ERP) alcanzaran gran popularidad y ventas en tan poco tiempo. [Fajardo, 2002]

El sistema SAP integra sus procesos de negocios ayudando a toda la empresa a funcionar más ordenadamente, controlando procesos de finanzas, manufactura, ventas, operación, recursos humanos, etc.

Administrar la seguridad de las empresas es una tarea compleja, ya que existen varios factores que pueden dificultar el accionar de una empresa. El sistema SAP facilita el manejo de datos, procesos, responsabilidades y funciones de usuarios, como consecuencia las empresas cuentan con mayor control de análisis de riesgos, accesos, autorizaciones, etc. Algunos de los módulos de aplicación en los que interviene son: [Haberkorn, 2003]

- Gestión financiera: Contabilidad financiera, estructuras organizativas.
- Control de operaciones: Gastos generales, costos de producto.
- Tesorería: Control de fondos, flujo de caja.
- Sistema de proyectos: Costos de proyecto.

- Gestión de recursos humanos:
    a) Gestión de personal
    b) Gestión de la organización
    c) Reclutamiento
    d) Capacitación
    e) Evaluación de desempeño
    f) Desarrollo de personal
    g) Cálculo de la nómina
    h) Gestión de tiempo

- Ventas y distribución: Pedidos de ventas, solicitudes, pedidos abiertos al público.
- Ejecución de logística: Gestión de entregas y necesidades.
- Gestión de materiales
- Gestión de almacenes:
    a) Plan de mantenimiento
    b) Planificación de Producción

Básicamente SAP ofrece soluciones a la medida de cada empresa, con gran flexibilidad integrando los procesos internos de cada compañía, además intercomunicar a las empresas con otras empresas de proveedores ó clientes a través de Internet, logrando incrementar sus ventas y utilidades. [Biao, 2002]

La integración de herramientas de oficina como Microsoft Word, Microsoft Excel, etc., es una gran ventaja para las empresas, ya que permiten estabilizar sus procesos creando un ambiente de trabajo de gran seguridad y confiabilidad en todos los movimientos de la compañía. El flujo de trabajo general del ERP se muestra en la Figura 2.1.

Figura 2.1. Modelo de Trabajo SAP.

Actualmente la compañía Procter & Gamble planta Mariscala México, utiliza el sistema de transacciones ERP (SAP). El sistema lleva el control de múltiples actividades, como el control de las líneas de producción donde se programan los productos y los materiales a producir. El sistema también controla el manejo de proveedores quienes abastecen el material requerido para construcción, limpieza, cableado, producción, etc.

El sistema SAP proporciona a los gerentes de planta la facilidad de poder realizar múltiples transacciones que afectarán las diferentes áreas de las plantas como son: crear órdenes de compra a los proveedores, autorizar órdenes de compra, programar el proceso de producción, control de embarques, etc. [Höhn, 2001]

Los procesos son controlados y monitoreados continuamente dándoles la facilidad a los empleados de producción, de poder conocer los materiales que van a utilizar en la fabricación de productos terminados en la planta.

3. METODOLOGÍA

3.1 Metodología de Investigación

El método de investigación que se utilizará es el método científico, en base a la investigación que se realizó en el marco teórico. A continuación se describen las etapas requeridas para cumplir con el objetivo de este trabajo. [De los Santos, 2009]

- Llevar a cabo un estudio del estado del arte de los procesos que ejecutan los usuarios en la compañía.
- Analizar las necesidades y requerimientos de los procesos actuales de la compañía.
- Obtener reportes de transacciones ejecutadas en el sistema SAP para poder aplicarles algoritmos de programación y métodos estructurados, con la finalidad de identificar claramente los conflictos generados por los usuarios.
- Llevar a cabo diferentes experimentos análisis de resultados realizando comparaciones para verificar que la información obtenida sea realmente válida.
- Generar Planes de Acción para evitar los conflictos generados en un futuro.
- Implementar un programa de mantenimiento y control para el sistema SAP Security.

3.2 Definición de requerimientos y necesidades de la compañía

3.2.1. Generación de conflictos

Se generan conflictos cuando se realizan dos o más transacciones en SAP, las cuales por políticas de la empresa no pueden ser ejecutadas al mismo tiempo. Por ejemplo: realizar una orden de compra de un equipo y autorizar esa misma orden de compra por el mismo usuario, en ese momento se genera un conflicto, el cual debe ser documentado, justificando el porqué se llevaron a cabo esas operaciones, además se pondrán en marcha planes de acción sobre el conflicto dándoles un seguimiento para su solución. Como se muestra en la Figura 3.1.

Una transacción es cualquier tipo de operación que realizan los usuarios en el sistema ERP (SAP), con la finalidad de satisfacer las necesidades de la compañía.

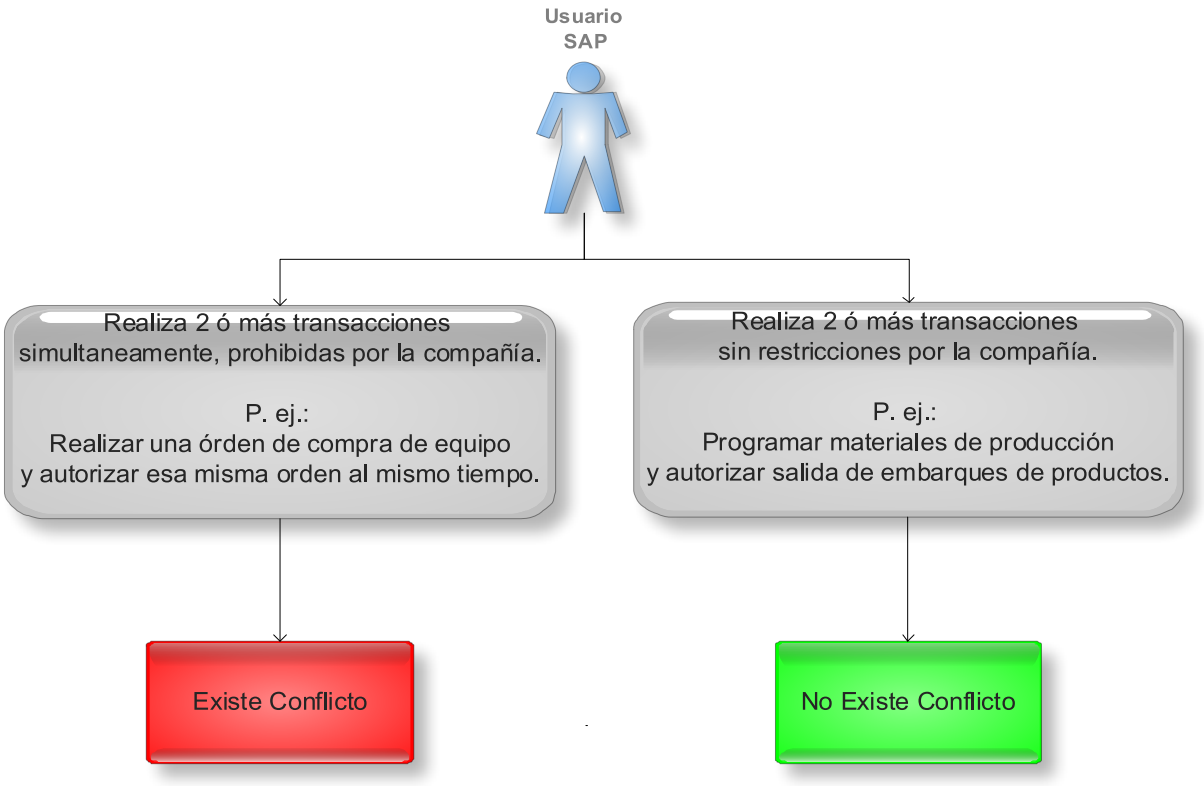


Figura 3.1. Modelo de Conflicto.

El problema en la compañía surgió al no controlar gran cantidad de transacciones que se realizan por una gran cantidad de usuarios. Las transacciones son clasificadas tomando en cuenta el perfil que tenga el usuario. Al conjunto de transacciones que se le asigna a cada usuario, se le llama Modelo de Usuario.

Los Modelos de Usuario pueden contener transacciones que si se llegan a ejecutar pueden generar un conflicto.

El problema de los modelos de usuario no es tener transacciones que puedan originar un conflicto, sino ejecutar esas transacciones prohibidas por la compañía al mismo tiempo. El Esquema de Modelo de Usuario se muestra en la Figura 3.2:

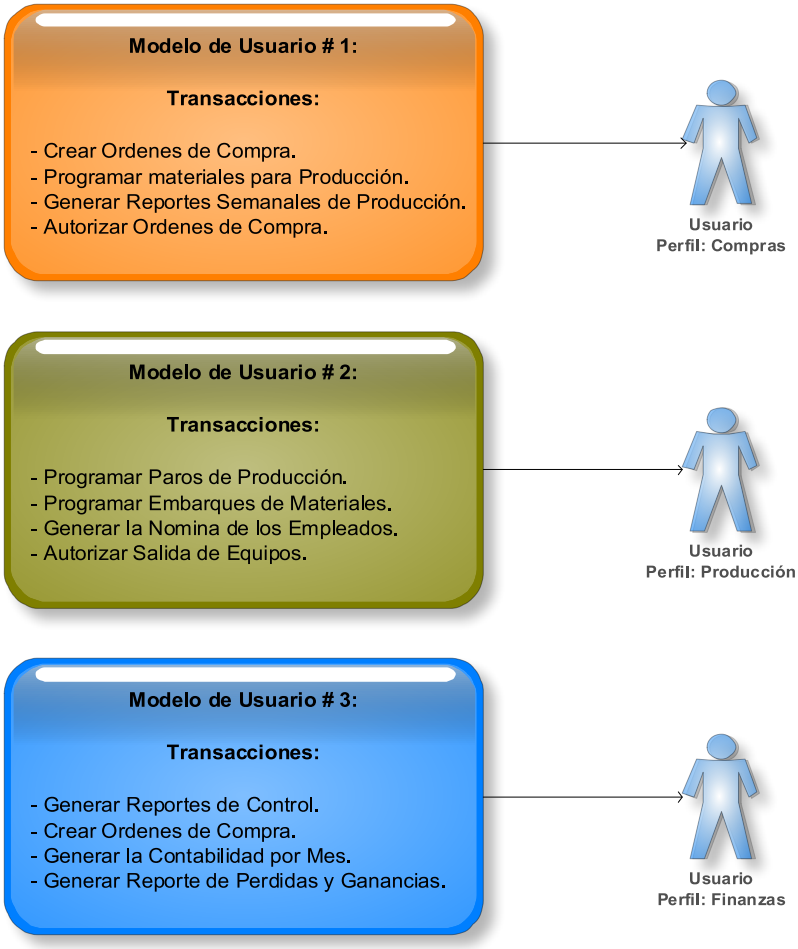


Figura 3.2. Modelo de Usuario.

Los conflictos generados deberán ser documentados con las razones de negocio que la compañía admite, justificando el porqué se ejecutaron esas transacciones, utilizando el documento de incidente y compensatorio. En caso de no justificar el conflicto, la compañía tomará las acciones necesarias para solucionar el problema. El proceso de generación de conflictos por los usuarios se muestra en la Figura 3.3.

El documento de Incidente es un formato el cual debe ser documentado con la información del incidente que se genera con el conflicto y la ejecución de transacciones criticas no permitidas por un solo perfil de usuario.

El documento Compensatorio es un documento en el cuál se debe llevar un control de todos los conflictos generados mensualmente especificando que usuarios realizaron cada incidente, con la finalidad de contar con esta información para las auditorías en la planta.

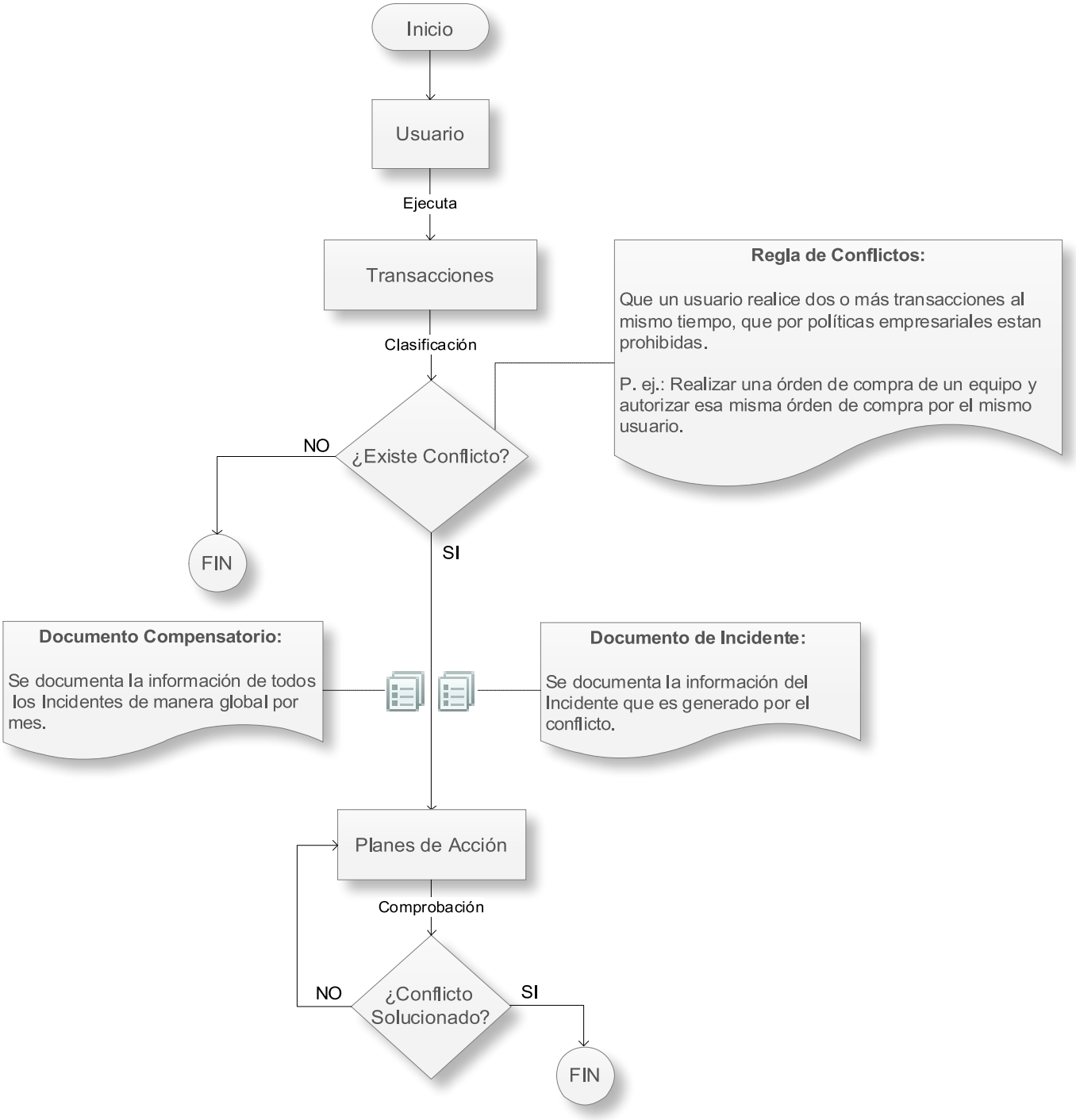


Figura 3.3. Modelo de Generación de Conflictos en SAP.

3.2.2 Generación de password sharing

Mantener las contraseñas confidenciales son una regla que se debe cumplir para cualquier sistema de Procter & Gamble, y el sistema SAP no es la excepción.

Por este motivo, el reporte de Password Sharing fue creado para monitorear las transacciones ejecutadas por los usuarios que puedan estar compartiendo sus ID y/o contraseñas incurriendo en un conflicto de confidencialidad.

La compañía Procter & Gamble planta Mariscala México, labora con tres turnos de trabajo en el día:

- Primer Turno: 6:00 a.m. a 2:00 pm.
- Segundo Turno: 2:00 p.m. a 10:00 p.m.
- Tercer Turno: 10:00 p.m. a 6:00 a.m.

Por políticas de la empresa ningún usuario podrá hacer transacciones en SAP utilizando la contraseña de acceso de otro usuario, cuando esta situación llega a ocurrir se genera un Password Sharing, el cual es un conflicto para la compañía. Los Passwod Sharing deberán documentarse justificando el incidente y aplicando la asignación de planes de acción para resolver este problema.

El proceso de monitoreo de Password Sharing se hace a través de los movimientos que se registran en el sistema ERP (SAP), obteniendo la hora, el día y el Id del usuario que los generó, con la finalidad analizar la información y poder determinar la existencia de Password Sharings.

Los turnos tienen un rango de 45 minutos entre cada uno, para dar tiempo al traslape de usuarios en la operación; por lo tanto, los horarios programados de los turnos, para el sistema de Password Sharing quedan de la siguiente manera:

- Primer Turno: 6:45 a.m a 2:44 p.m.
- Segundo Turno: 2:45 p.m a 10:44 p.m.
- Tercer Turno: 10:45 p.m a 6:44 a.m.

Para que pueda ser identificado un caso de Password Sharing, es necesario el cumplimiento de las siguientes condiciones:

1. Si hay movimientos en 3 turnos consecutivos, en cualquiera de las combinaciones, será considerado un caso de Password Sharing con status en rojo.

2. Si hay movimientos en 2 turnos consecutivos, en cualquiera de las combinaciones, será considerado un caso de Password Sharing con status en amarillo, el cual es solo una advertencia de conflicto.

Un incidente de Password Sharing con status en amarillo tiene un nivel de gravedad baja, ya que pueden existir turnos mixtos donde los usuarios ejecutan transacciones en dos turnos, por lo que deben también justificarse, documentarse y aplicarles planes de acción para su solución.

Un incidente de Password Sharing con status en rojo tiene un nivel de gravedad alta, ya que indica que el usuario ejecutó transacciones en tres turnos consecutivos sin descanso, este es un caso que debe ser investigado, ya que es imposible que alguien trabaje tres turnos consecutivos sin parar. El esquema de generación de Password Sharing se muestra en la Figura 3.4.

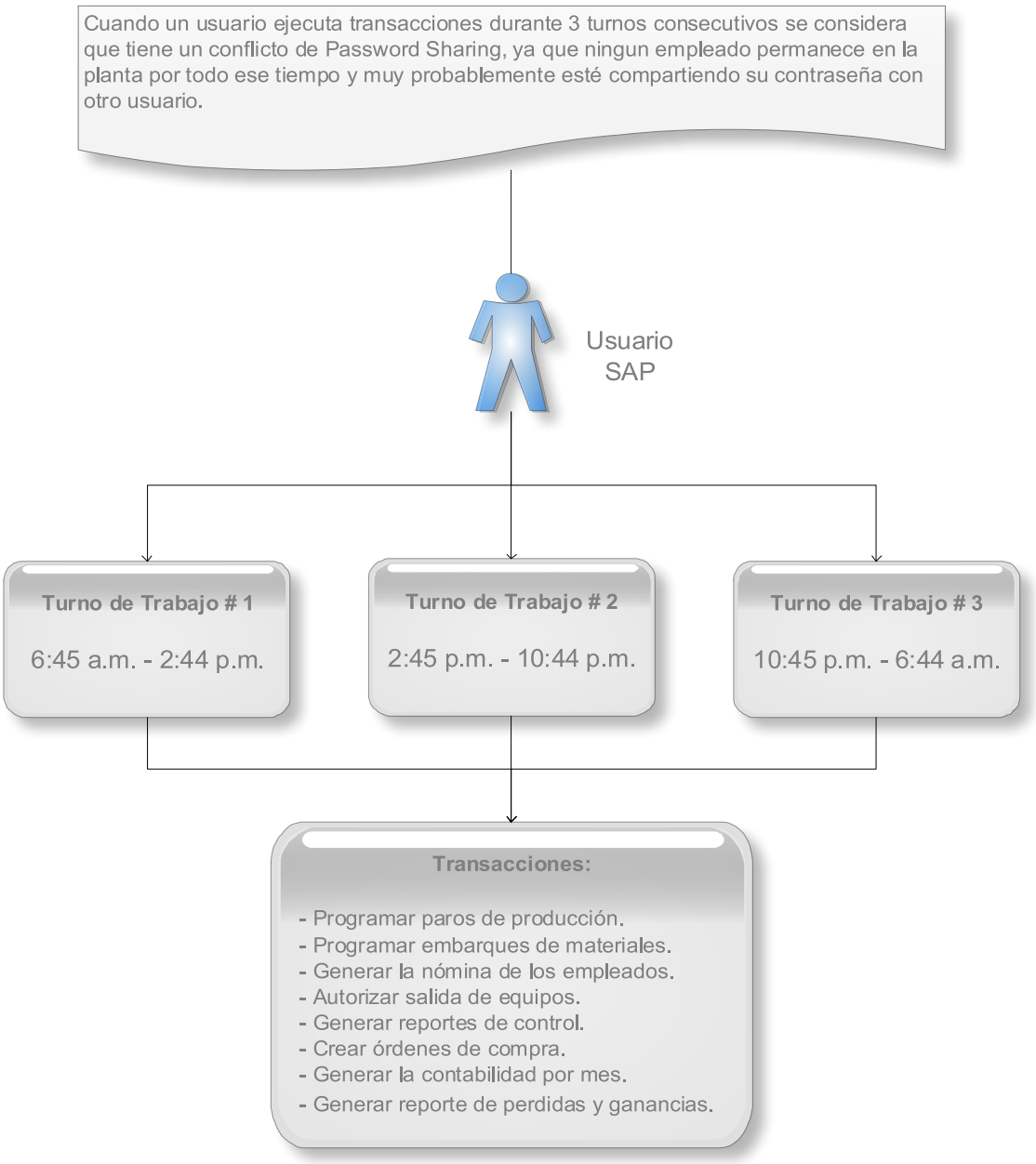


Figura 3.4. Modelo de Password Sharing.

Si el resultado de la investigación confirma la existencia del Password Sharing, se aplicará al usuario la sanción correspondiente a una falta grave de confidencialidad de la compañía.

En la Tabla 3.1 se muestra el método de validación que se implementará en el proyecto para determinar el nivel de riesgo de los casos de password sharing detectados. También se muestran todas las combinaciones posibles de ejecución de transacciones en diferentes turnos, identificando posibles conflictos.

Usuario Ejecuta Transacciones en 3 Turnos Consecutivos.	**Password Sharing Status Rojo**
Usuario Ejecuta Transacciones en el 2do, 3er y 1er Turno Consecutivos.	**Password Sharing Status Rojo**
Usuario Ejecuta Transacciones en el 3er, 1er y 2do Turno Consecutivos.	**Password Sharing Status Rojo**
Usuario Ejecuta Transacciones en el 1er y 2do Turno.	**Password Sharing Status Amarillo**
Usuario Ejecuta Transacciones en el 2do y 3er Turno.	**Password Sharing Status Amarillo**
Usuario Ejecuta Transacciones en el 1er y 3er Turno.	**Password Sharing Status Amarillo**
Usuario Ejecuta Transacciones en 1 solo Turno.	**No Existe Password Sharing**

Tabla 3.1. Modelo de Generación de Password Sharings en SAP.

3.2.2.1 Ejemplo de password sharing

Existen dos tipos de Password Sharing:

- ***Password Sharing Diario:*** Se manifiesta cuando un usuario tiene movimientos en tres turnos consecutivos sin importar el orden como en el siguiente caso y se considera el password sharing en el día que tenga más movimientos registrados, como se muestra en la Tabla 3.2.

days	shift1	shift2	shift3
01/03/2011	0	2	5
02/03/2011	2	3	6
03/03/2011	0	2	1

days	shift1	shift2	shift3
01/03/2011	0	0	5
02/03/2011	2	3	6
03/03/2011	0	2	1

Tabla 3.2. Password Sharing Diario.

- ***Password Sharing Final de Mes:*** Se manifiesta cuando un usuario tiene movimientos en tres turnos consecutivos al final de cada mes, considerando también el mes siguiente, y se registra el password sharing que tenga más movimientos registrados en el día, como se muestra en la Tabla 3.3.

days	shift1	shift2	shift3
31/02/2011	0	2	5
01/03/2011	2	3	6
02/03/2011	0	2	1

days	shift1	shift2	shift3
31/02/2011	0	2	5
01/03/2011	2	3	6
02/03/2011	1	2	1

Tabla 3.3. Password Sharing Final de Mes.

3.3 Integración de Bases de Datos

En esta etapa, la Base de Datos de SAP Security es vinculada para realizar el análisis de reportes que provienen del sistema SAP, así mismo, la información es distribuida a las diferentes fuentes de datos de la base de datos integrando los procesos de manera unificada. Lo anterior fue realizado mediante algoritmos de programación en el software Microsoft Visual Studio .NET, así como el modelado de la base de datos utilizando el software SQL Server 2000, respetando el software estándar para la compañía.

Los algoritmos realizan análisis y reportes vinculando la información con las necesidades del usuario. A continuación, los módulos que se utilizan para llevan el control de conflictos y password sharings realizados, los cuales son descritos brevemente.

3.3.1 Usuarios

Con la finalidad de llevar el control del personal que ejecuta operaciones en el sistema SAP, se crea este modulo de usuarios, ya que es de vital importancia mantener comunicación con los usuarios vía correo electrónico, ofreciéndoles la disponibilidad de los datos que se requieren.

3.3.2 Usuarios Clave

Cada área de Producción tiene un líder de cuadrilla que es denominado Key User, el cual es el encargado de llevar el control y seguimientos de planes de acción a los conflictos generados por los usuarios en el sistema SAP.

3.3.3 Transacciones

Las Transacciones es el conjunto de operaciones las cuales un usuario puede ejecutar en el sistema SAP, este módulo es creado para que el administrador de bases de datos (DBA Data Base Administrator), pueda guardar, editar y modificar estas operaciones.

3.3.4 Cajas de Operación

Las cajas de operación son grupos de transacciones, que se agrupan con la finalidad de ser destinadas a las diferentes áreas de la compañía y cada caja de operación solo puede ser utilizada por usuarios que tengan los suficientes privilegios de accesos.

3.3.5 Habilidades Críticas

Las Transacciones son clasificadas por el administrador de bases de datos con el objetivo de identificar las operaciones que si se llegan a ejecutar dos o más veces simultáneamente en el sistema SAP, podrían ocasionar un conflicto para la compañía.

3.3.6 Conflictos

Este módulo almacena los conflictos generados en el sistema SAP por los usuarios, teniendo un mejor control y análisis de los mismos.

3.3.7 Tipos de Conflictos

Los conflictos con clasificados de la siguiente manera:

- **Conflictos:** Se generan cuando el usuario ejecuta 2 o más transacciones las cuales si se ejecutan simultáneamente ocasionan un problema según políticas de la compañía.
- **Password Sharing:** Se genera cuando un usuario realiza movimientos (Transacciones) en el sistema SAP durante 3 turnos consecutivos, ya que se considera que el usuario no debe permanecer en planta durante todos esos periodos y por políticas de la empresa se determina que está compartiendo su contraseña de acceso a SAP con otro Usuario, incurriendo en un conflicto empresarial.
- **Conflictos de Calidad:** Este problema se presenta cuando el usuario ejecuta 2 o más transacciones críticas para la empresa pero que se presentan específicamente para el área de calidad ya que su manejo es por separado debido a que es un área de vital importancia.

3.3.8 Modelos de Usuario

Para cada área donde se encuentran los usuarios es permitido ejecutar ciertas Transacciones, las cuales son agrupadas formando modelos con las finalidad poder restringir a los usuarios en la ejecución de operaciones para determinada área y tomando en cuenta sus privilegios de usuario.

3.3.9 Roles de Usuario

Los usuarios son clasificados por rol de usuario, determinando el nivel de privilegios en la ejecución de operaciones en el sistema SAP.

3.3.10 Roles de Usuario

Los usuarios son clasificados por rol de usuario, determinando el nivel de privilegios en la ejecución de operaciones en el sistema SAP.

3.3.11 Áreas

Las Áreas son utilizadas para realizar la clasificación de la información y poder determinar los niveles de acceso para usuarios y administradores en el sistema.

3.3.12 Centros de Costos

Los Centros de Costos son cuentas que se manejan para hacer cargos económicos sobre gastos de equipos, servicios, etc., en donde los usuarios y áreas pertenecen a determinados centros de costos, por medio de los cuales se puede tener un mayor control sobre los gastos y operaciones de la empresa.

3.3.13 Dueños de Centros de Costos

Son aquellos usuarios que son los responsables de las cuentas de los centros de costos, quienes administran los gastos de los equipos y servicios.

3.3.14 Documentación de Incidentes

Se realiza la documentación de los conflictos generados por los usuarios, teniendo físicamente la información para poder cubrir las auditorias que se realicen en un futuro, comprobando la ejecución de los conflictos por medio de la documentación.

3.3.15 Planes de Acción

Para poder dar solución a los conflictos generados por los usuarios se implementan planes de acción para dar seguimiento y solución a dichos conflictos, los cuales serán clasificados en baja, media y alta prioridad.

3.3.16 Estatus de Planes de Acción

Con la finalidad de estar monitoreando el avance de los planes de acción sobre los conflictos se colocan los siguientes estatus sobre los mismos abierto, cerrado y en curso.

3.3.17 Cartas Responsivas

Cuando un Conflicto es generado por un usuario automáticamente se le genera una carta responsiva responsabilizándolo por sus actos, quedando así la evidencia necesaria para comprobar dichos conflictos y para que el usuario pueda controlarlos y resolverlos.

3.3.18 Excepciones de Conflictos para Usuarios

Este modulo almacena las excepciones en las que un usuario en pocas ocasiones podría trabajar en la compañía durante 3 turnos simultáneamente, y que por medio de justificaciones previamente aprobadas no causará conflicto en la ejecución de transacciones.

Todos los módulos están interrelacionados con la finalidad de mantener la integridad de la base de datos estructurando mecanismos para controlar los accesos y proteger la privacidad de la información.

3.4 Proceso de SAP Security

El procedimiento que se llevará a cabo el sistema SAP Security para controlar y mantener la seguridad del sistema SAP se realizará a través de una depuración de roles, la cual se hace cada 2 meses en todos las áreas de producción (PE, WM, SIP, Finanzas, etc.) de toda la Planta Procter & Gamble Mariscala, las cajas de SAP donde se encuentran las transacciones y a las que se les hace esta depuración son: L6P430 y L7P410.

La depuración se realiza a través de reportes extraídos de sistema de SAP y en formatos de Excel donde se llevan las listas de accesos y modelos de usuario que el Key User define.

Responsables:

- **Key Users:** es un usuario de un área en especifico y es el responsable de administrar y actualizar la información para la depuración de roles y revisión de perfiles de usuario.

- **SAP Security:** es el responsable de verificar, evaluar e informar que la información se actualice en tiempo y conforme a lo preestablecido.

Conceptos:

- **Transacciones:** Código que ejecuta una función dentro del sistema de SAP.

- **Rol de SAP:** Un rol es un conjunto de transacciones con funcionalidades específicas para un perfil definido.

- **Modelo de usuario:** Es un grupo de roles de SAP que son conjuntadas para un puesto en especifico.

3.4.1 Proceso de Definición de Accesos

Los accesos al sistema de SAP son definidos por los Key User de cada área. Por lo que en cada uno de los procesos se tienen accesos diferentes según el perfil del puesto de trabajo.

Los KU son los responsables de mantener la documentación y actualización de un archivo (Excel) con la lista de los usuarios pertenecientes a su área, de esta manera se tiene identificados a los usuarios finales por área, grupo de trabajo y modelo de usuario. La documentación de la lista como los modelos de usuarios se encuentra centralizada en una unidad de almacenamiento en red, donde cada KU tiene su propia carpeta con su información.

La asignación de roles a los usuarios se da en dos siguientes casos:

1. Usuario Nuevo
2. Cambio de Puesto del usuario, ya sea en la misma área ó en un área diferente.

En ambos casos el Key User tendrá que analizar las transacciones a utilizar en ese puesto, es decir, el usuario debe tener solo acceso a las transacciones necesarias para su perfil de trabajo.

Después de analizar las transacciones hay que revisar los roles de SAP que existen para un área determinada y que están disponible para su asignación al usuario, si el rol que se haya encontrado esta dentro del área, se asignara el rol, en caso de que no se encuentre en su área, será criterio del Key User agregar el rol que crea conveniente.

3.4.2 Proceso de Modelo o Perfil de Usuario

El modelo de usuario como se mencionó anteriormente es un grupo de transacciones de SAP, las cuales son agrupadas para ser asignadas como modelo o perfil de usuario a un determinado puesto o perfil de trabajo.

Cada uno de los usuarios está ligado a un solo modelo de usuario, y un modelo de usuario puede tener uno o más usuarios asignados. Cuando un usuario es dado de alta en SAP, se debe de asignar a un modelo de usuario, por lo que este usuario heredará todas las transacciones que puede ejecutar y que están almacenadas en un modelo de usuario.

Los Key Users serán también los responsables de definir y mantener actualizado todos los modelos de usuario pertenecientes a su proceso.

Los modelos de usuario deben clasificarse dependiendo de sus funciones, como en el proceso de planeación existe el modelo denominado MPS, donde los usuarios asignados tendrán el permiso de ejecutar instrucciones para el proceso de producción.

Los casos en los que un modelo de usuario debe crearse o modificarse, teniendo en cuenta que el Key Users aplicará uno u otro caso según su criterio:

1. Cuando se encuentre un usuario con transacciones que no existan en ningún modelo de usuario ya definido.

2. Cuando hay conflicto dentro de un modelo de usuario y no haya razón de negocio para que exista ese conflicto.

3.4.3 Proceso de Conflictos

Los conflictos se crean en el momento que dos habilidades o actividades críticas se ejecutan en el sistema SAP por una misma persona.

Los conflictos deben tener la documentación necesaria donde describa la necesidad del negocio en ejecutar esas habilidades críticas. La documentación de los conflictos se hará en el sistema, para tener control sobre las razones de negocio en cada una de las áreas.

Para cada modelo de usuario debe de realizarse una documentación acerca del conflicto que se está generando, independientemente de si se ejecuta o no. Los Key Users también serán los responsables de actualizar y documentar las razones de negocio para los conflictos.

3.5 Representación Técnica del Sistema Sap Security

A continuación se describe la estructura actual del sistema SAP security para la importación de datos, control de conflictos, manejo de usuarios, transacciones, centros de costos, etc., posteriormente se desarrolla el modelo propuesto, y finalmente, se incluye una descripción funcional del sistema.

3.5.1 Obtención de Reportes en el Sistema SAP

La manera en que el sistema SAP Security Web trabaja, se basa principalmente en la carga de información que es obtenida a través de reportes. Estos reportes se extraen del sistema SAP R/3 v.6.4 y una página Global de SAP Security llamada SAP Security Tracking, que solo está disponible para la intranet local de la compañía.

Estos dos sistemas son parte fundamental para alimentar el sistema de SAP Security Web, ya que los documentos de controles compensatorios hacen referencia a ellos para generar los reportes de control y la realización de la compensación de conflictos.

De esta manera el sistema SAP Security Web puede mostrar los usuarios que además de tener conflictos en sus perfiles, realizan o ejecutan el conflicto. Tanto la ejecución como la carga de los reportes solo la debe realizar el administrador del sistema, como lo muestra la Figura 3.5.

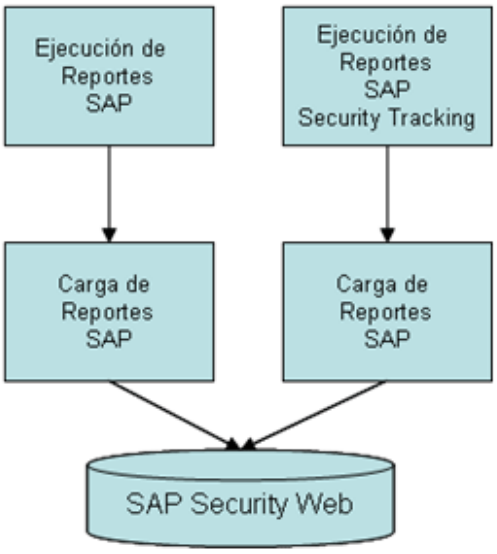


Figura 3.5. Modelo de Reportes SAP.

Para la carga de los conflictos, es necesario entrar a la página de SAP Security Tracking disponible solo para la intranet de la compañía (Link: http://bdc-intra564.internal.pg.com//GLOBAL/GBS/sap-access-V2.nsf).

Obtener el reporte de transacciones ejecutadas en SAP por los usuarios durante la semana anterior obteniendo el reporte cada lunes de la semana actual, como se ilustra en las Figura 3.6 y 3.7. Este reporte está disponible en el apartado General Documentation >> 3ª. Conflicts >> Region LA CEEMEA,GC,AAI,NEA Site and BU (Fecha).

Figura 3.6. Obtención del Reporte de Transacciones SAP.

Al dar clic sobre el link vendrá la fecha del último documento de conflictos, generalmente, es la fecha del primer día de la semana actual, confirmando que es el nuevo documento de conflictos más reciente.

Dar clic para entrar a la siguiente pagina, y mostrara un archivo .Zip el cual debemos guardarlo localmente para posteriormente manipularlo al formato que se desea.

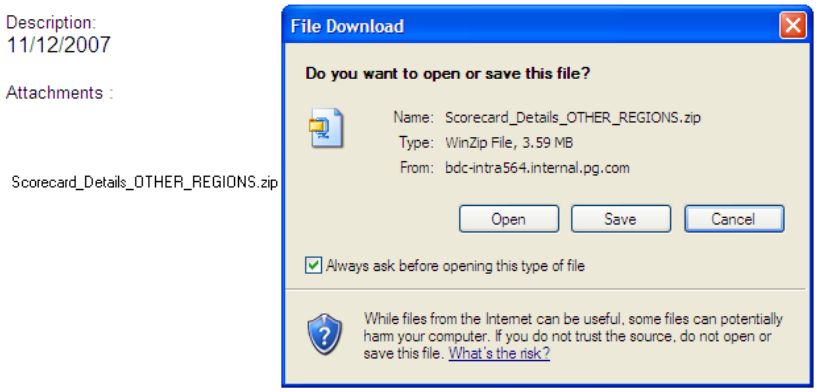


Figura 3.7. Reporte de Transacciones SAP.

Después de guardar el documento, seguir los siguientes pasos:

1. Abrir el documento
2. En Hoja Sheet1, Filtrar:
    a. Región: LA (Latinoamérica excluye otras plantas del mundo)
    b. Country: México
    c. Site: Planta Mariscala (Ubicada en Guanajuato).
3. Dar doble clic sobre el número total, y de esta manera se genera otra hoja automáticamente con el número total de conflictos en la planta Mariscala México.
4. Copiar la hoja nueva con todos los registros de los conflictos en otro libro nuevo de Excel, el nombre de la hoja como: hoja1, dejando solo una hoja en todo el libro de Excel.
5. Remover las filas Date_Eliminated y BU_Action_Required
6. Grabar el libro de Excel con el nombre: masterdata.xls (resultado total de transacciones ejecutadas en SAP semanalmente.)

3.5.2 Carga y Análisis de Conflictos

Para subir el reporte de Transacciones en el sistema SAP (Master Data) es necesario ir a la página de SAP Security WEB >> Herramientas >> Subir Conflictos (Figura 3.8).

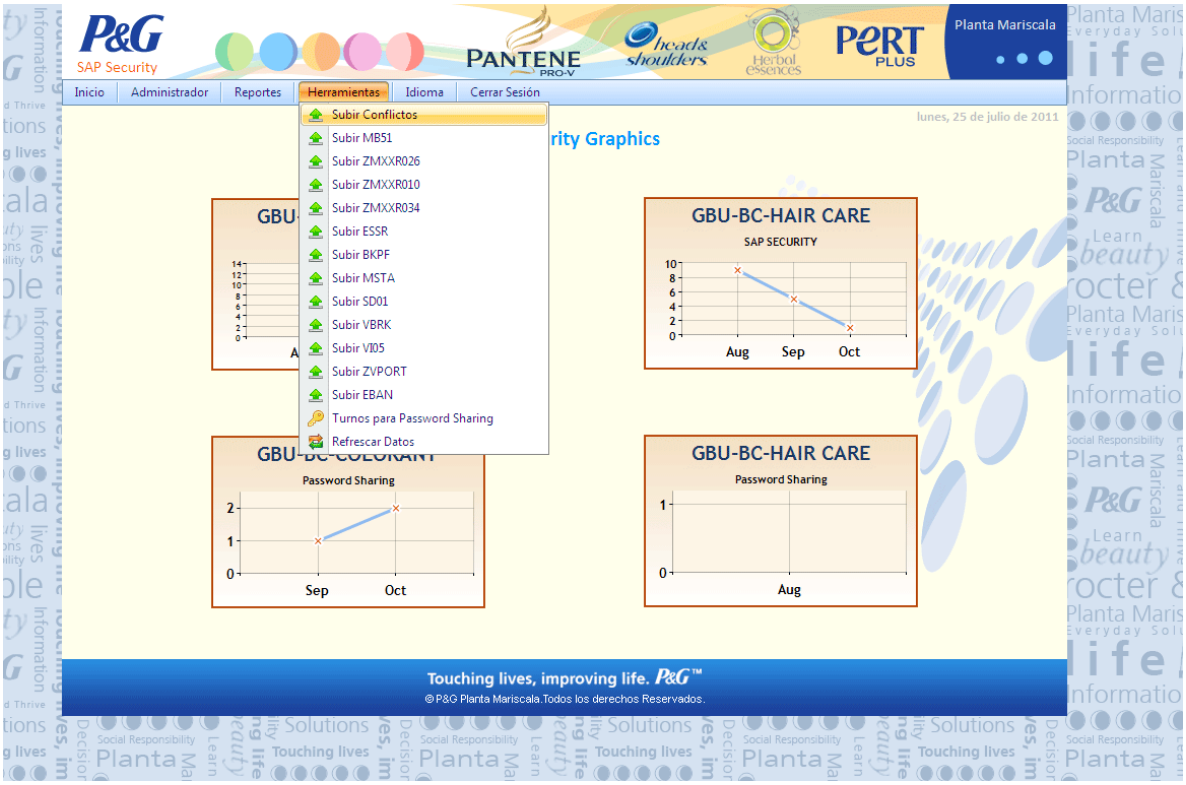


Figura 3.8. Interface del Sistema SAP Security.

Aparecerá una ventana pidiendo la ruta del archivo para realizar la carga. Dar clic en el botón Browse..., buscar el archivo masterdata.xls en la carpeta donde se haya guardado el documento. Dar clic en Send Files para empezar con la carga de datos.

Al término de la carga, enviara un mensaje de éxito, el sistema deberá ser capaz de analizar todos los movimientos y operaciones de los usuarios con la finalidad de guardar esa información en la base de datos determinando cuales perfiles de usuario están en riesgo de tener conflictos ya que tienen asignado en su role operaciones que si se ejecutan al mismo tiempo ocasionan un problema para la compañía.

El archivo master data funciona como un tipo de advertencia para los usuarios ya que al terminar el proceso de análisis de manera correcta, les manda un correo electrónico para notificarles que su role de usuario tiene cierto número de transacciones y que algunas de ellas si se llegan a ejecutar simultáneamente con otras transacciones de carácter crítico llegarán a realizar un conflicto el cual se deberá justificar y resolver.

Existen otros tipos de reportes los cuales se extraen del sistema SAP, y que a diferencia del reporte master data que solo funciona como advertencia para los usuarios para que no ejecuten ciertas transacciones, estos reportes que se muestran a continuación ya nos ayudan a determinar la existencia de conflictos por parte de los usuarios:

- El siguiente reporte ayuda a determinar los Conflictos de tipo Password Sharing:

    a) Reporte MB51

- Los siguientes reportes ayudan a determinar los Conflictos de Ejecución de Transacciones:

    a) Reporte ZMXXR026
    b) Reporte ZMXXR010
    c) Reporte ZMXXR034
    d) Reporte ESSR
    e) Reporte BKPF
    f) Reporte MSTA
    g) Reporte SD01
    h) Reporte VBRK
    i) Reporte VI05
    j) Reporte ZVPORT
    k) Reporte EBAN

3.5.3 Documentos Compensatorios

Es necesario realizar un documento compensatorio para todos los usuarios que en su perfil tienen el riesgo de ejecutar conflictos que se van reportando en la página global del Tracking con la finalidad de justificar porque los usuarios cuentan con ese modelo de usuario. En la página de SAP Security Web se tiene una herramienta especial para llevar a cabo esta operación.

- Entrar a la página de SAP Security Web (http://mariscala2.internal.pg.com/sapsecurity/)
- Ir al menú de Reportes >> Reporte de Conflictos

Se mostrará una pantalla con una lista de categorías de todos los conflictos que existen (no únicamente los generados), esta lista se actualiza cada semana, por lo que siempre se visualizará la información cargada del mes actual.

Los campos que se visualizan son:

- **Conflict ID:** Identificador de conflicto.
- **Description:** Descripción o nombre del conflicto.
- **Compensated, Open, Removed:** Se refieren a la cantidad de usuarios que tiene este conflicto en los diferentes status, el cual pueden ser: Compensado, Abierto y Removido.
- **Total:** Total de usuarios con ese tipo de conflicto.
- **%Conflict:** Es el porcentaje del total de conflictos documentados, el cual debe estar siempre al 100%, en caso contrario nos indica que alguno de los conflictos que se encuentran con status Abierto no se ha compensado.
- **Users:** Este campo nos indica el número de usuarios que además de tener el conflicto en su rol, el usuario está ejecutando transacciones críticas las cuales están generando conflicto para la compañía.
- **%Documentado:** Nos indica el porcentaje de los usuarios que han realizado la documentación del reporte de incidente.
- **%Autorizado:** Nos indica el porcentaje de incidentes documentados, que han sido autorizados.
- **Ability:** Es el identificador de las transacciones críticas que originaron el conflicto, para que exista un conflicto debe tener por lo menos dos transacciones críticas.
- **Description:** Es la descripción de las Transacciones críticas a la cual hace referencia en el campo anterior.

- **Reports:** Muestra los reportes de excel de los cuales se obtuvieron los conflictos.

3.5.4 Reporte de Incidente

El Reporte de Incidente es un formato el cual debe ser documentado con la información del incidente que es generado por el conflicto y la ejecución de transacciones criticas no permitidas en un solo perfil de usuario.

Cada usuario que tenga el incidente debe realizar el reporte, el cual contiene los siguientes campos:

- **Incident:** Es el número consecutivo de incidente dado por el sistema automáticamente al momento de documentar.
- **Date:** Fecha de documentación que da el sistema.
- **Key User:** Nombre del Key User (líder del área) del usuario que generó el conflicto.
- **Process Involved:** Proceso o departamento involucrado en el incidente si existe.
- **End User:** Nombre del usuario final que genera el conflicto.
- **Conflict:** Descripción de conflicto que se está documentando.

Para que un Reporte de Incidente este totalmente documentado necesita cumplir con las Autorizaciones de los líderes de las áreas para avalar que el conflicto se ha justificado o resuelto de manera correcta.

El área de autorizaciones son las firmas electrónicas de tres líderes:

1. **Key User:** Líder del Área.
2. **SAP Council:** Líder general SAP Council.
3. **Boss of Area:** Jefe de Áreas en Total Planta.

Las tres partes del reporte de incidente, Encabezado, Cuerpo del Reporte y Autorizaciones, son esenciales y fundamentales para dar seguimiento al incidente, si algún campo del formato no es llenado correctamente o dejado en vacío, el documento no podrá ser guardado y quedará como pendiente de documentar.

Al guardar el documento, se envía un mail de notificación a todos los autorizadores, con un link hacia el reporte para la revisión y autorización del reporte de incidente.

Después de ser revisado y aprobado por los Autorizadores la imagen de no aprobado cambiará a imagen de ya aprobado para cada uno de los autorizadores, en donde los incidentes deberán estar documentados a más tardar el viernes de la misma semana.

3.5.5 Reporte de Calidad

Este Reporte nos ayudará a monitorear las transacciones ejecutadas específicamente para el área de calidad en el proceso de producción. Estos movimientos solo los usuarios del proceso de calidad pueden generarlos y ejecutarlos.

En el reporte se puede seleccionar también el sistema o caja de SAP que se desea ejecutar (L6P, L7P), desplegando el reporte con la información de acuerdo a lo solicitado. Finalmente se mostrara la lista de los usuarios que están ejecutando movimientos de Calidad, y que no están autorizados para hacerlo, dado que no pertenecen a esa área.

Para cada usuario debe documentarse el incidente mostrándose dos iconos de estado:

 .- El Icono indica que el reporte de incidente no se ha documentado.

 .- El icono indica que el reporte de incidente fue documentado.

3.5.6 Reporte de Planes de Acción

Como se mencionó anteriormente, durante la documentación de los conflictos, se pueden agregar uno o varios Planes de Acción para dar solución o justificar los conflictos con el objetivo de monitorear el seguimiento a estos conflictos.

Este reporte podrá ser visualizado mensualmente la información que se desea monitorear, Mostrando una pantalla con una lista de todos los Planes de Acción documentados durante el periodo seleccionado previamente. Esta lista se actualiza cada semana, por lo que siempre se visualizará la información cargada del mes actual.

3.5.7 Reporte de Incidentes No Aprobados

Cada uno de los incidentes documentados, requiere de la revisión y autorización de los líderes responsables:

1. **Key User:** Líder del Área.
2. **SAP Council:** Líder general SAP Council.
3. **Boss of Area:** Jefe de Áreas en Total Planta.

Para poder monitorear los documentos que aún no han sido firmados por alguno de estos líderes, se deberá especificar el año fiscal de trabajo ya que para la compañía Procter & Gamble un año fiscal abarca desde 01 de Julio del presente año hasta el 30 de Junio del siguiente año, una vez que se especifica el año fiscal de trabajo aparecerá la información de los incidentes que están pendientes de autorizar por lo menos por alguno de los responsables.

3.5.8 Reporte de Tipo Scorecard

Para mantener la información que se genera de manera centralizada y resumida, existe una tabla de resultados o scorecard de todos los incidentes generados por los usuarios, sean Conflictos ó casos de Password Sharing a lo largo del Año Fiscal.

El scorecard es una pantalla con la Tabla 3.4 resumida y unas gráficas en la parte inferior, esta información corresponde al mes y el año fiscal que se requiere visualizar en la tabla y en las gráficas.

La tabla de resultados muestra el número de incidentes generados por mes, a lo largo del año fiscal seleccionado, seccionado por Área de producción. Este número de incidentes incluye tanto a los Conflictos generados, como a los casos de Password Sharing presentados; sin embargo, su administración se realiza por separado.

Es importante comentar que los conflictos que se manejan en la tabla, son los generados por los usuarios, más no los conflictos que existen en su perfil; pues un usuario puede tener un conflicto de roles, pero no hacer uso de ellos para generar el conflicto como tal.

Se manejan 3 colores con los que se rellena cada casilla de la tabla; estos son indicadores del porcentaje de avance para el seguimiento de los incidentes, tales que:

Color	% de avance
	95 – 100 %
	90 – 95 %
	0 – 90 %

Tabla 3.4. Estado de Avance para Incidentes.

Ahora bien; cuando los incidentes generados aún no han sido documentados, los porcentajes de sus columnas pueden estar todas en 0, y sus casillas aparecer en color rojo, o bien, aparecer un porcentaje incompleto en la casilla Doc, indicando existencia de incidentes por documentar.

3.5.9 Gráficas

La otra parte del Scorecard son las gráficas, las cuales representan los datos de la tabla de una manera más visual. Existen varios niveles de visualización en las graficas:

1. Visualización general total áreas: En la primera gráfica que se muestra por default en el scorecard, ahí se visualiza el número de conflictos generados por mes durante el año fiscal seleccionado. Para visualizar el detalle de un mes en específico, se podrá tener acceso dando clic en el nombre del mes y se mostrará un siguiente nivel de detalle.

2. Visualización por mes específico y área: Esta gráfica muestra el número de conflictos generados por área durante el mes. Para pasar al siguiente nivel de visualización, dar clic sobre la barra de la gráfica del área deseada

3. Visualización de usuarios: muestra una tabla de los usuarios del área seleccionada, que generaron el conflicto. En esta tabla se indica el tipo de conflicto generado, así el nombre del usuario que lo generó.

3.6 Funcionalidad del Sistema

El sistema comprenderá la siguiente funcionalidad:

1. Los accesos al sistema deberán ser por medio del usuario de intranet.

2. El sistema debe contener menús para un administrador del sistema y uno de Usuarios o Key Users.

3. El menú de Key Users contendrá las formas de alta, bajas o cambios de:
   - Modelos de usuarios
   - Lista de usuarios finales
   - Documentación de conflictos

4. El sistema validará por cada usuario el proceso al que pertenece como al modelo de usuario al que se encuentra asignado.

5. Validará por cada usuario, las transacciones que están en un modelo de usuario definido contra las transacciones que se encuentran en SAP con el objetivo de tener actualizado el sistema.

6. En caso de que las transacciones de los modelos de usuario y las transacciones en SAP no concuerden, se generará un reporte mostrando el usuario, el modelo afectado y las transacciones que no se encuentren alineadas; en caso de que el modelo contenga conflictos.

7. El Key User podrá realizar los cambios después de la validación de transacciones contra el sistema SAP y crear si es necesario un nuevo modelo de usuario ó hacer modificaciones en la asignación de dicho modelo.

8. En caso que la nueva asignación de transacciones ocasione un conflicto, será necesario realizar la documentación de la razón de negocio por la cual se ejecutará el conflicto.

9. La documentación de la razones de negocio para los conflictos se llevará a cabo en el momento de una alta de transacciones para un modelo de usuario.

10. Los conflictos deberán ser documentados por área y modelo de usuario al que está siendo afectado.

3.7 Caracterización de la interfaz gráfica de usuario

Mediante el uso de un navegador Web, y con programación en Visual Studio .NET y base de datos Microsoft SQL Server v.2005 a continuación se muestran las pantallas vinculadas al sistema propuesto y desarrollado en este trabajo.

La página de inicio (Figura 3.9) representa la primera impresión para el usuario final, mostrando gráficas de control y monitoreo para cada una de las áreas de producción de la compañía así como los menús de Inicio, Administrador, Reportes, Herramientas, Idioma y Cerrar Sesión, los cuales ayudarán al usuario a realizar sus operaciones de manera fácil y sencilla.

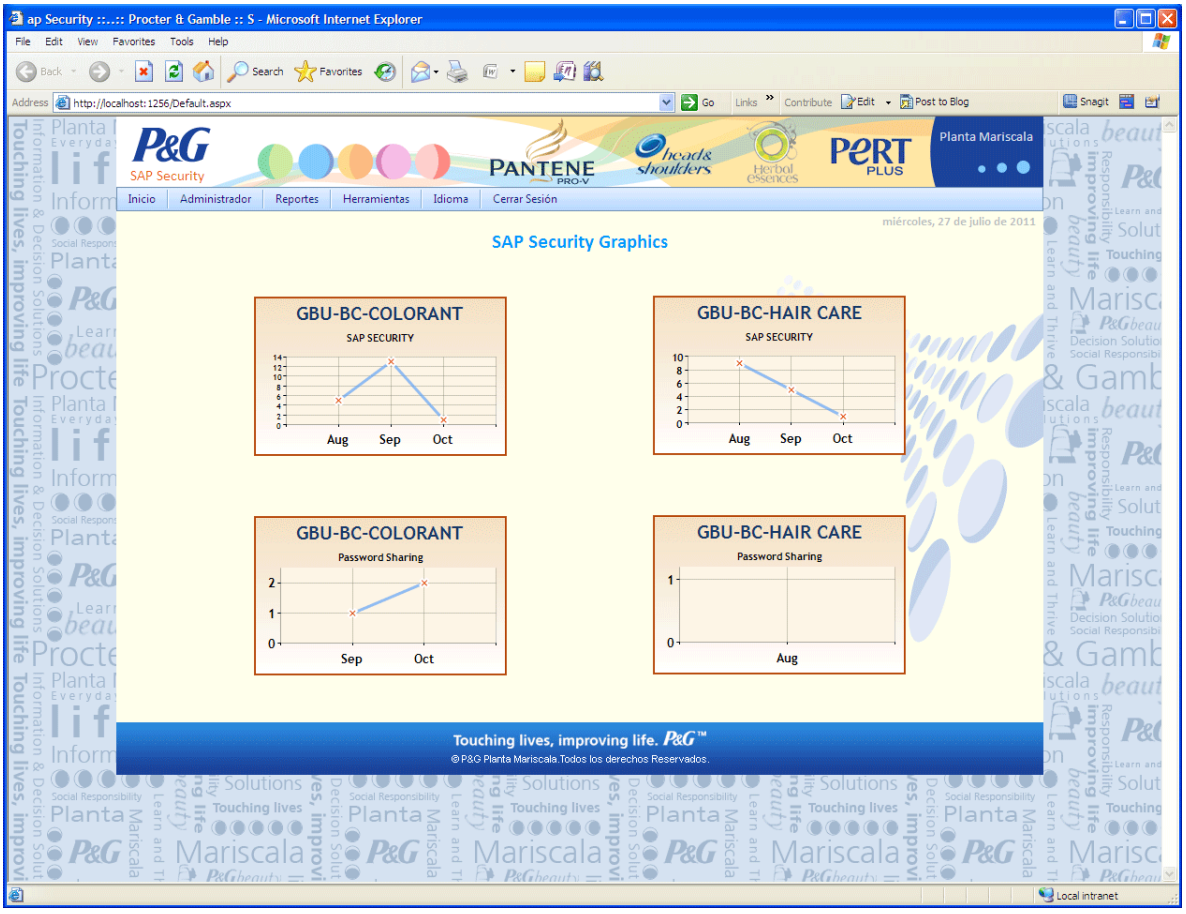


Figura 3.9. Página de Inicio Sap Security.

3.8.1 Menú Inicio

El menú Inicio ayudará al Usuario para regresarse o navegar hacia la página de inicio para visualizar las gráficas de control ó entrar a otra opción de los menús de acceso.

3.8.2 Menú Administrador

El menú Administrador (Figura 3.10) contiene las siguientes funciones:

- Modelos de Usuario: En esta sección se podrá asignar al usuario los modelos de usuario los cuales son un conjunto de transacciones que se pueden ejecutar en el sistema SAP y que el líder de su área (Key User) del usuario determinará correcto para su perfil de usuario.

- Catálogo de Usuarios: En esta sección maneja las altas, bajas y modificaciones de todos los usuarios que cuenten con acceso al sistema SAP, y que puedan ejecutar transacciones dependiendo de su perfil de usuario.

- Razones de Negocio: Como se ha explica anteriormente existen modelos de usuario que contienen transacciones que si se ejecutan simultáneamente ocasionan un conflicto, en ocasiones especiales es necesario para la empresa ejecutar esas transacciones aunque se origine un conflicto y el catalogo de razones de negocio será indispensable para justificar dichos procedimientos.

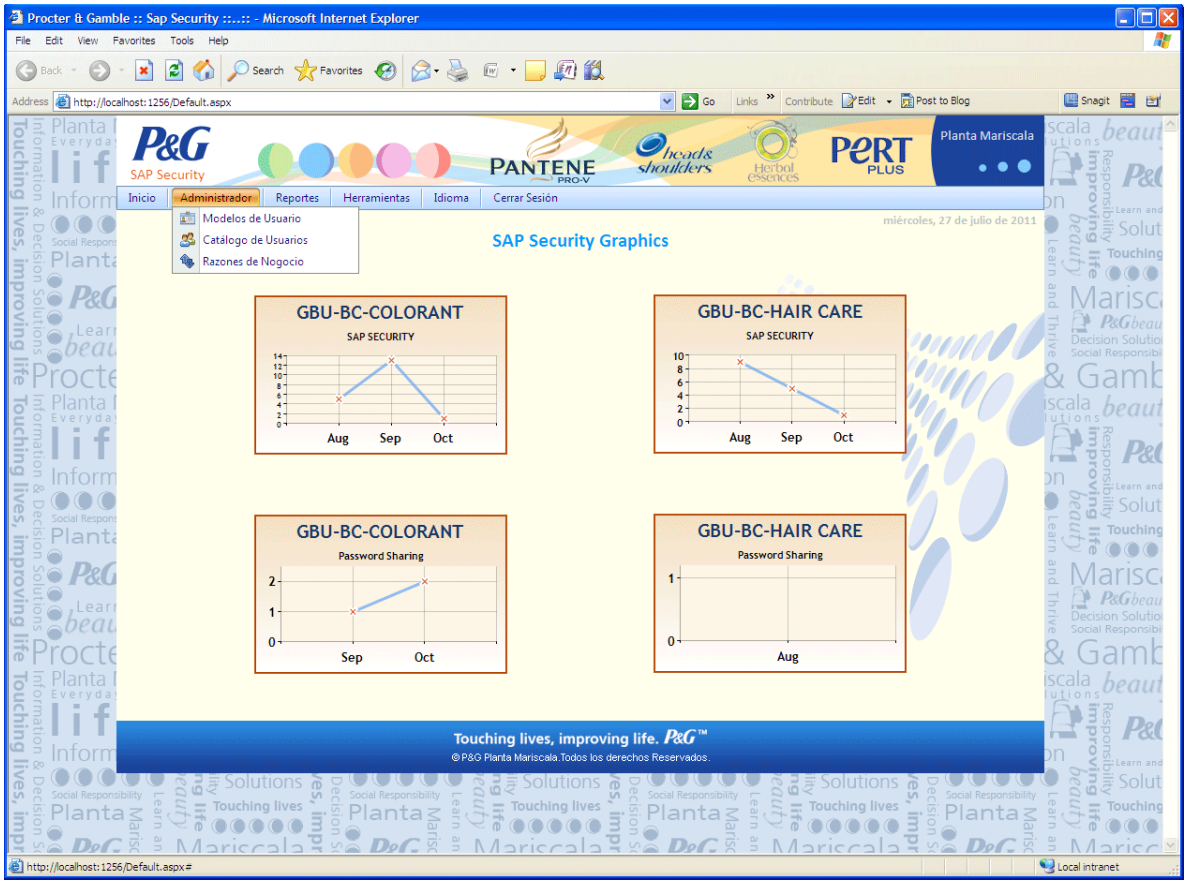


Figura 3.10. Menú Administrador Sap Security.

3.8.3 Menú Reportes

El menú Reportes (Figura 3.11) contiene las siguientes funciones:

- Reporte de Conflictos: Maneja un Reporte de control y manejo de Conflictos, donde el usuario podrá tener una visión panorámica de todos los conflictos generados mensualmente y por año fiscal.

- Reporte de Calidad: Maneja un Reporte de control y manejo de Conflictos específicamente para el área de calidad.

- Reporte de Password Sharing: Este Reporte monitorea a los usuarios que son considerados por la empresa como prestamistas de sus claves y contraseñas de acceso al sistema SAP.

- Reporte de Planes de Acción: Reporte para dar seguimiento al avance de solución de los planes de acción sobre los conflictos generados por los usuarios.

- Reporte de Documentos No Aprobados: Reporte para los administradores del sistema y los líderes de las áreas (Key Users), con la finalidad de poder identificar los conflictos que aun no se documentan y las razones por lo cual no se ha hecho.

- Reporte de Scorecard: Reporte General seccionado por mes, año y área de producción, el cual proporciona una visión general de los conflictos y procedimientos que se están realizando para resolver estos conflictos.

- Reporte de Cambios de Área: Reporte para dar seguimiento a los usuarios que por alguna razón cambiaron de área y que por lo tanto deben de cambiar su modelo de usuario, pero su historial de usuario debe ser guardado para futuras consultas de la información anterior.

- Reporte de Número de Días de Password Sharing: Reporte que monitorea el número de días que se consideran como excepciones de password sharing, cuando los usuarios que por algún motivo tuvieron que trabajar durante 3 turnos seguidos durante cierto número de días en la planta, pero que esta situación fue justificada por el líder del áreas previamente sin la generación de conflictos.

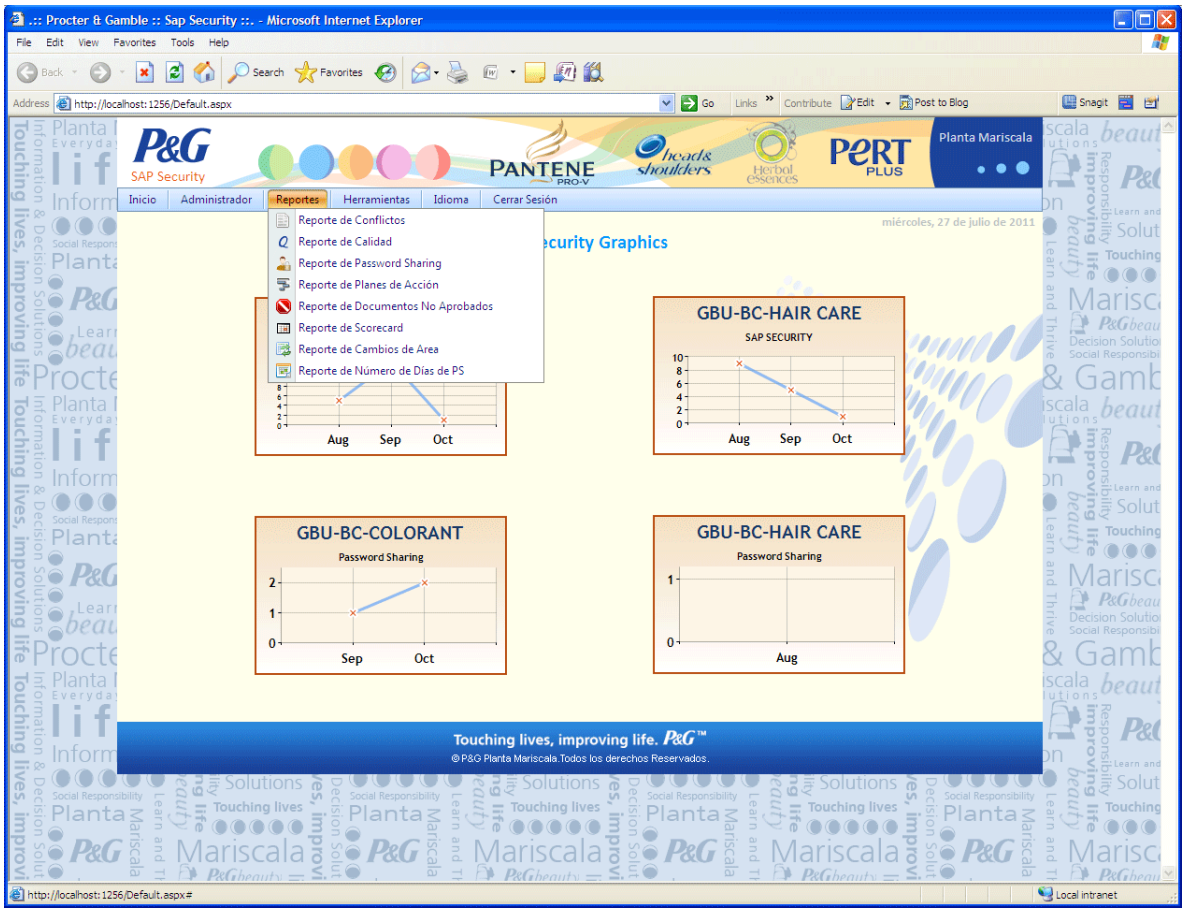


Figura 3.11. Menú Reportes Sap Security.

3.8.4 Menú Herramientas

El menú Herramientas (Figura 3.12) contiene los submenús que ayudarán al usuario a subir y actualizar semana a semana la generación de conflictos y password sharing por parte de los usuarios, también contiene la opción Turnos para Password Sharing, la cual nos ayudará a que un usuario el cual trabajará durante 3 turnos consecutivos en planta y que esté justificado y aprobado previamente no se tomará en cuenta como password sharing.

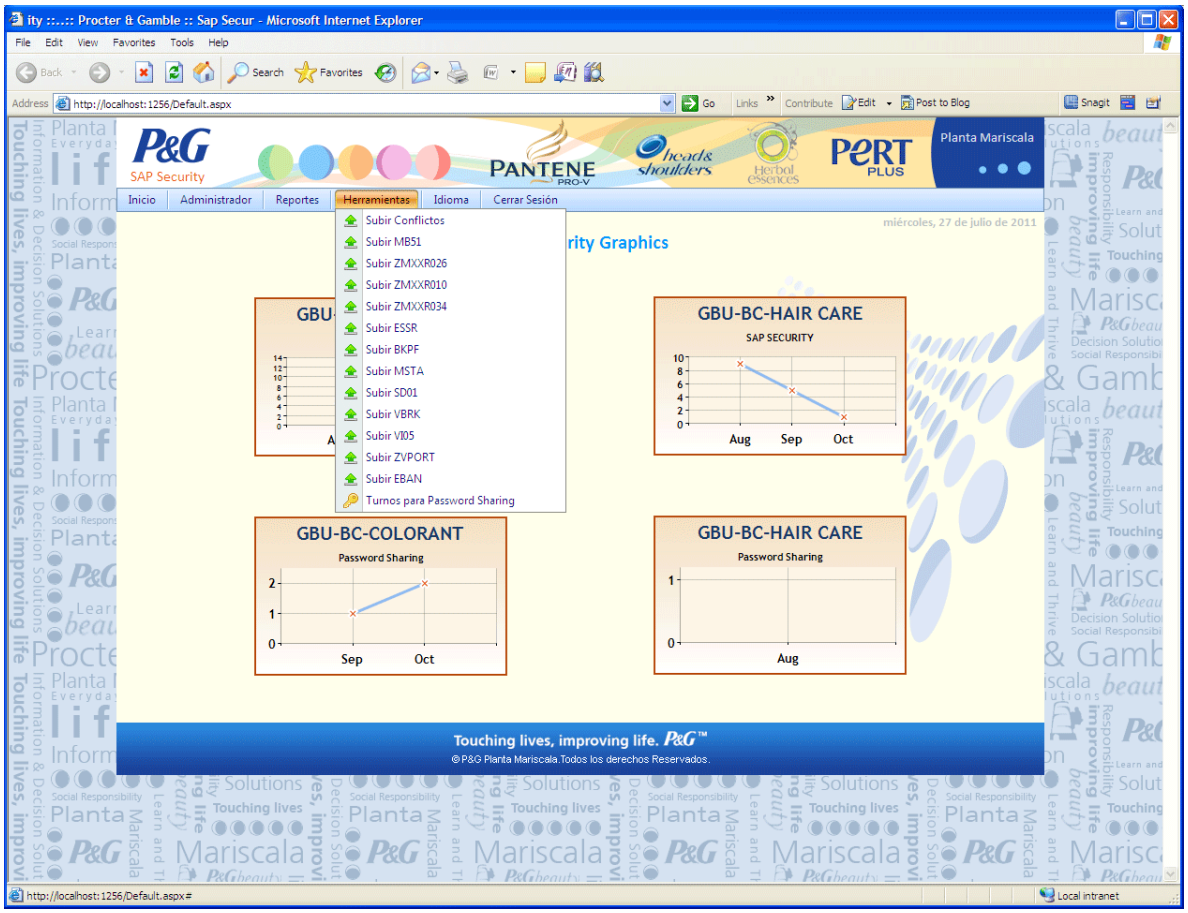


Figura 3.12. Menú Herramientas Sap Security.

3.8.5 Especificación del software

La programación del sistema se realizó con las características de hardware y software que a continuación se describen:

Ambiente operativo

- Servidor: Windows XP Professional
- Cliente: Internet Explorer ó Mozilla FireFox

Programación

- Servidor:
  ASP NET.
  Editor de ASP NET, Microsoft Visual Studio 2008.
  Microsoft SQL Server, ver 2005.
  Ambiente grafico para Bases de Datos, SQL Server 2005.
  Analizador de Consultas para SQL Server.
- Del cliente: HTML, JavaScript

Servidor de aplicaciones:

- IIS (Internet Information Server) versión 6.0.

4. RESULTADOS

Mediante este trabajo de tesis se difunde la cultura de prevención y control sobre los conflictos que generan por medio de la utilización del sistema SAP, a una mayor cantidad de usuarios, que únicamente requieren la conexión a la Intranet de la planta Internet y el uso de sus credenciales de acceso, para conocer y monitorear los conflictos, password sharing, planes de acción y la documentación que se genera y con ello tomar las medidas preventivas y de mejoramiento que contribuyan a reducir el índice de conflictos mediante el sistema propuesto. Y al mismo tiempo se cubre la necesidad de difusión en formatos de datos que facilitan el intercambio de información a un menor costo para el usuario.

La definición de los procedimientos en el sistema, así como su vinculación con las bases de datos, son estructuradas mediante algoritmos de programación, proporcionando la actualización de datos diariamente.

La propuesta del sistema SAP Security como apoyo al sistema de tipo ERP SAP, para la administración de la información de conflictos generados hacia una aplicación cliente/servidor en ambiente Web, incluye beneficios tanto en la forma de capturar la información así como en la de visualizar de manera rápida y general el estado en que se encuentra el uso correcto del sistema SAP. Aspectos como la disponibilidad de resultados en un menor tiempo, respaldo y control de la información de conflictos, etc. son algunas de las ventajas de un sistema con arquitectura cliente/servidor, además de que las herramientas empleadas en su elaboración, mediante el software la tecnología ASP NET, facilita la optimización de la infraestructura del sistema.

5. CONCLUSIONES, IMPLICACIONES Y TRABAJO A FUTURO

En este trabajo de tesis se definieron procedimientos para el manejo y control de conflictos generados por los usuarios en el sistema SAP. Se elaboraron los algoritmos de programación para vincular la información con la base de datos implementada. La representación gráfica de la información vía Intranet se elaboró con base en herramientas de software comercial. Lo anterior facilitó la diseminación de información vía web, y representa la base para contar con información descriptiva que contribuya a solucionar y dar seguimiento a los conflictos generados por los usuarios en SAP.

Como trabajo futuro, en el ámbito de los reportes, documentación y seguimientos de control para los conflictos, será importante el desarrollar recomendaciones para visualizar grandes cantidades de datos sin restricciones métodos de actualización y mantenimiento de la información con la finalidad de tener mayor consistencia e integridad en la base de datos.

También será importante desarrollar métodos para que el sistema sea inteligente para resolver cualquier tipo de problema técnico que se presente y en consecuencia lentitud para visualizar los datos en un explorador. También, la construcción del mejoramiento de la seguridad informática en el sistema por medio de mayor confidencialidad y privacidad de la información.

Finalmente, es importante el trabajo que pueda desarrollarse en el tema de funcionalidad más simple y rápida que por medio de la realización de análisis de usabilidad por parte de los usuarios se podrían hacer mejoras al sistema para que se pueda obtener el máximo provecho.

En virtud de lo anterior, este trabajo representa un esfuerzo inicial por contar con un sistema de seguridad en SAP, el cual pueda ser distribuido en todas las plantas de Procter & Gamble a nivel Latinoamérica, puntualizando la manipulación de información por medio de su intranet empresarial.

GLOSARIO

Transacción SAP: Operaciones que se realizan en el sistema SAP, para llevar control y mantenimiento de la producción en la empresa.

ERP (Enterprise Resource Planning): Son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con muchas operaciones de producción.

Interfaz Gráfica de Usuario: El conjunto de herramientas visuales (tales como iconos, pantalla, barras de herramientas etc.) a través de las cuales el usuario se comunica con la computadora.

Algoritmo: Es un conjunto de instrucciones bien definidas, las cuales describen el proceso que se debe seguir para dar solución a un problema específico.

Software: Es una colección de programas informáticos y datos relacionados que proporcionan instrucciones para decirle a la computadora lo que debe hacer y cómo hacerlo.

Key User: Es el administrador asignado por área de producción que se encarga de asignar y regular los roles de usuario, con la finalidad de tener controlado las acciones y movimientos de los usuarios.

Servidor Web: Es una aplicación de software que suministra archivos en respuesta a las peticiones de los navegadores Web. En ocasiones, también se hace referencia a un servidor Web como servidor HTTP.

Scorecard: También se le conoce como cuadro de mando integral, es un método para medir las actividades de la compañía, proporcionando a los gerentes una mirada global y poder así tomas decisiones.

Password Sharing: Se refiere al hecho de que un usuario comparta su contraseña para ser utilizada en el sistema SAP, por 3 ó más turnos consecutivos.

SAP Council: Es el líder del sistema SAP, quien debe mantener el control y seguimiento a los conflictos generados por los usuarios en SAP.

Conflicto en SAP: Se genera cuando un usuario ejecuta transacciones que se encuentran dentro de su rol de usuario, pero que por políticas de la empresa no debe de ejecutarlas.

Rol de Usuario: Es un conjunto de transacciones que se encuentran clasificadas para cada área de producción y que son asignadas a cada usuario por parte del key user.

SAP Security Tracking: Es una página web global que se encuentra disponible en la intranet de la compañía y donde pueden tener acceso todas las plantas de Procter & Gamble en el mundo, con la finalidad de obtener todas las transacciones que han ejecutado los usuarios durante un rango de tiempo.

Data Warehouse: Es un repositorio de datos, el cual es alimentado por diferentes fuentes de información, en donde la información es manipulada y transformada para generar nuevas consultas, análisis, reportes con el objetivo de llegar a la toma de decisiones.

REFERENCIAS

Aguirre, J. 2006. Seguridad Informática. Madrid España: Ed. EUI – UPM Company. ISBN: 84-86451-69-8.

Biao, F. 2002. SAP® BW: A Step-by-Step Guide. U.S.A: Ed. Addison Wesley Company. ISBN: 0-201-70366-1.

Charte, F. 2002. Bases de datos con Microsoft Visual Basic .NET. Madrid, España: Ed. Artes Gráficas Guemo, S.L. ISBN: 84-415-1375-9.

De los Santos, S. 2009. Una al día - Once años de seguridad informática. Mexico: Ed. Hispasec. ISBN: 978-1-4092-4380-9.

Fajardo, J. 2002. Lessons Learned from Testing SAP R/3. Consultado el: 15/02/2011, Disponible en: http://www.stickyminds.com/getfile.asp?ot=XML&id=6489&fn=XUS3009597file1.doc.

Haberkorn, E. 2003. Gestión Empresarial con ERP. São Paulo, Brasil: Ed. Microsiga SA. Company. ISBN: 85.346.1230-7.

Hallikainen, A. 2000. Reasons for ERP Acquisition., Consultado el: 28/01/2011, Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.367&rep=rep1&type=pdf.

Herrera, J. 2004. Seguridad en Redes. Barcelona España: Ed. Eureca Media, S.L.ISBN: 84-9788-212-1.

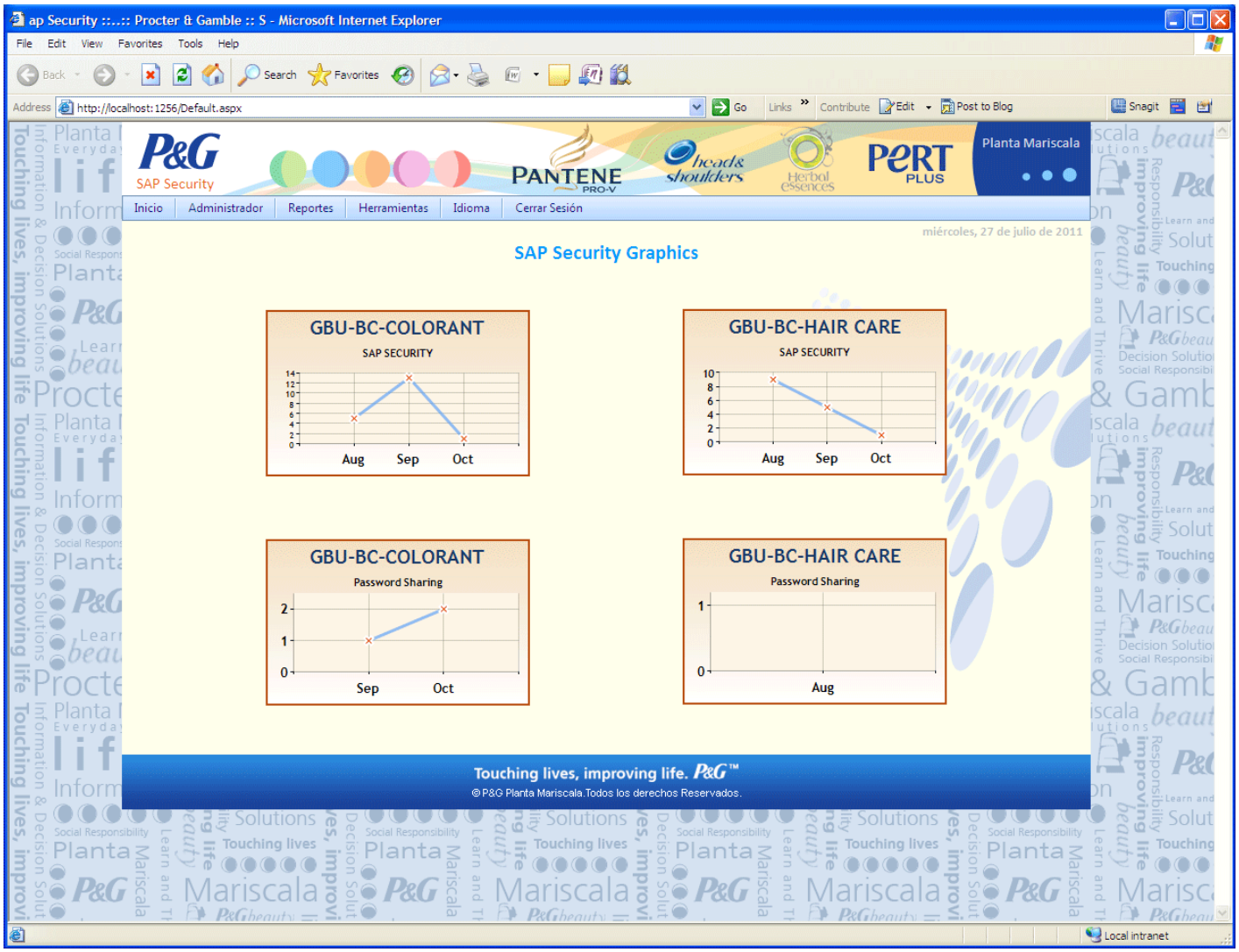
Höhn, S. 2001. Automated Checking of SAP Security Permissions., Consultado el: 10/02/2011, Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.9570&rep=rep1&type=pdf.

McConnell, S. 2006. Software Estimation. U.S.A: Ed. Microsoft Press A Division of Microsoft Corporation. ISBN: 0735605351.

Saltzer, J.H. 1974. The Protection of Information in Computer Systems, Consultado el: 05/03/2011, Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.9257&rep=rep1&type=pdf.

ANEXO A

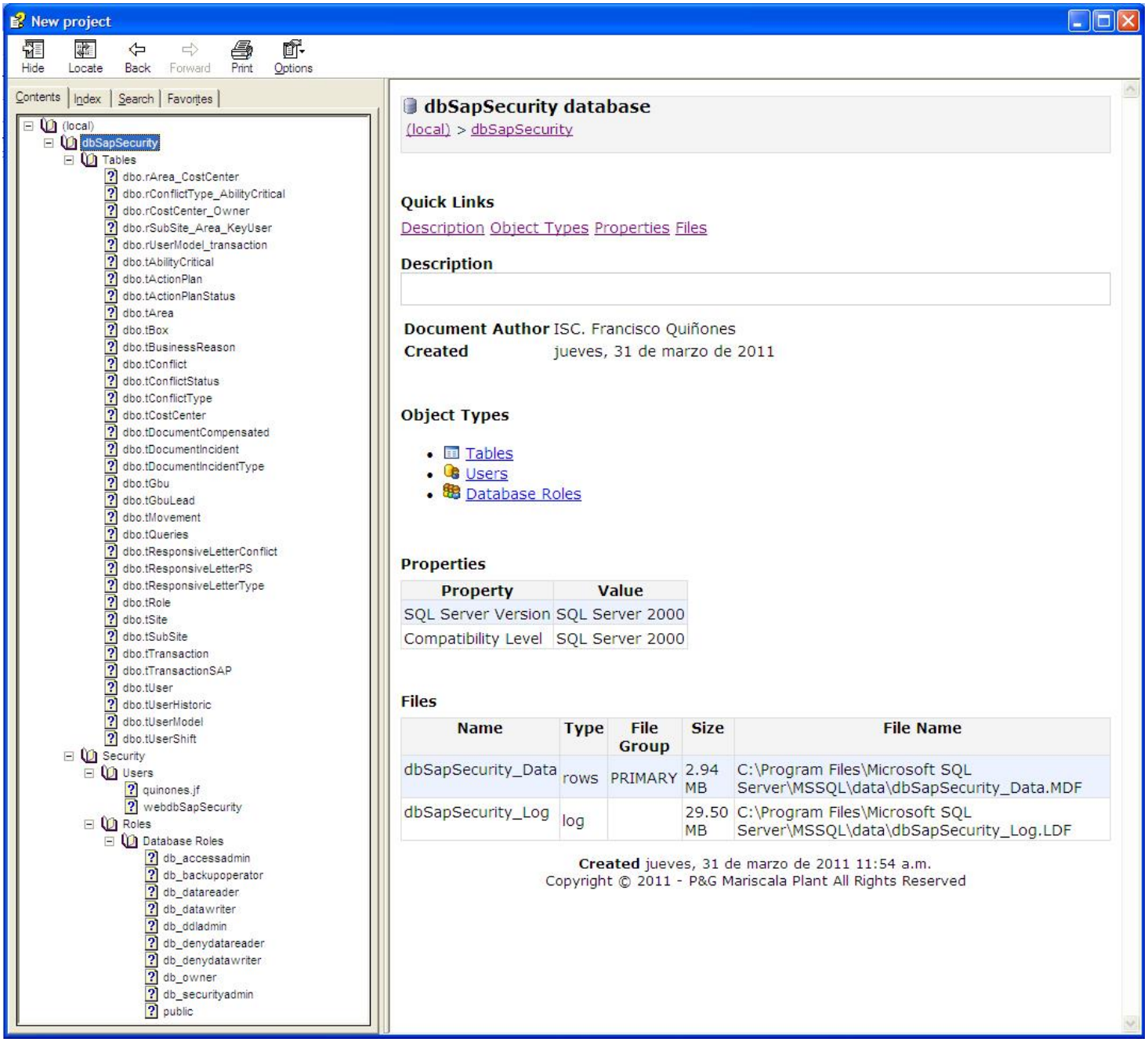
Interfaz Gráfica de Usuario Propuesta
y Desarrollada en este Trabajo



Anexo A – Interfaz de Usuario.

ANEXO B

Estructura de Base de Datos

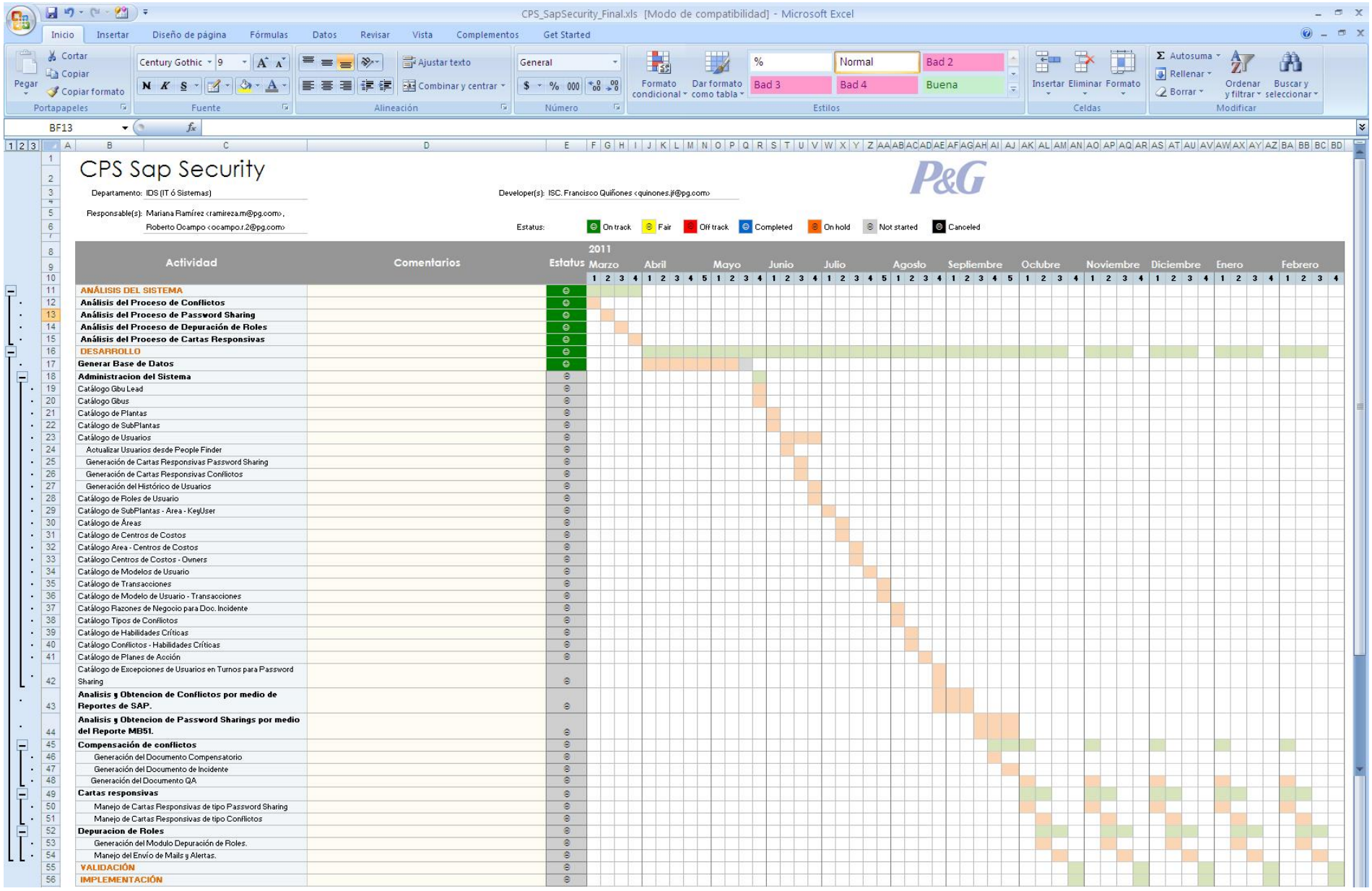


Anexo B – Estructura de Base de Datos.

ANEXO C

CPS SAP Security
(Control Process Shedule):

Control de Flujo de Trabajo para el Sistema SAP Security



Anexo C – CPS Sap Security.