PROYECTO DE TRABAJO DE GRADO
PROPUESTA DE ESTRUCTURACIÓN DE PERFILES Y PROCEDIMIENTOS A PARTIR DE UN ANÁLISIS DE RIESGOS DE SEGURIDAD SOBRE LA ADMINISTRACIÓN DE PERFILES DEL MÓDULO "ENTERPRISE PORTALS" DEL GRUPO NUTRESA.

Estudiante : Esteban Betancur Londoño **Cédula: 15370864**
Teléfono(s): 4221070-3655406 **Id: 000010851**
E-mail : tebito84@gmail.com **Programa: Ingeniería Informática**

Director: María Teresa Villegas Moreno **Cédula:** 42789356
Teléfono(s): 3251529
E-mail : Maria.Villegas@une.com.co
Empresa: UNE EPM TELECOMUNICACIONES S.A.

FACULTAD DE INGENIERÍA INFORMÁTICA
UNIVERSIDAD PONTIFICIA BOLIVARIANA
29/11/2013
MEDELLÍN

PROPUESTA DE ESTRUCTURACIÓN DE PERFILES Y PROCEDIMIENTOS A PARTIR DE UN ANÁLISIS DE RIESGOS DE SEGURIDAD SOBRE LA ADMINISTRACIÓN DE PERFILES DEL MÓDULO "ENTERPRISE PORTALS" DEL GRUPO NUTRESA.

Primera revisión
Recibió: _____
Fecha: _____
Lectura y asignación de evaluador en comité #: _____
Fecha: _____
Recomendación: _____
Reprobado: _ Aplazado: _ Aprobado: _
Comité #: _____ Firma responsable: _____ Fecha: _____
Comentarios:
_____
_____
_____
_____
_____
_____
_____

Segunda revisión
Recibió: _____
Fecha: _____
Lectura y asignación de evaluador en comité #: _____
Fecha: _____
Recomendación: _____
Reprobado: _ Aplazado: _ Aprobado: _
Comité #: _____ Firma responsable: _____ Fecha: _____
Comentarios:
_____
_____
_____
_____
_____
_____
_____
_____

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: en seguridad un activo de información es todo recurso informático que se encuentra en una compañía. Dentro de estos se tienen en cuenta: recursos de información (bases de datos, manuales, documentación, etc), recursos de software (aplicaciones, sistemas operativos, herramientas de desarrollo), recursos físicos, servicios (servicios informáticos y de comunicaciones, utilitarios generales como iluminación energía eléctrica, planta de emergencia) y por último y no menos importante, las personas. Dentro de los recursos físicos se contemplan: equipamiento informático (procesadores, monitores, portátiles, etc), equipos de comunicaciones (routers, máquinas de faxs, etc), medios magnéticos (cintas, cds, disquetes, dvds, etc), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado, etc), mobiliario.

APO: Advanced Planning and Optimization es un modulo de SAP que permite planificar y optimizar funcionalidades en diferentes procesos de negocio de planeación de la demanda, planeación del suministro, ajuste del suministro y la demanda y administración del transporte.

BACK OFFICE: es la parte de las empresas donde tienen lugar las tareas destinadas a gestionar la propia empresa y con las cuales el cliente no necesita contacto directo. Por ejemplo: el departamento de informática y comunicaciones que hace que funcionen los ordenadores, redes y teléfonos, el departamento de recursos humanos, el de contabilidad, etc.

BASC: Business Aliance for Secure Commerce es una alianza empresarial internacional que promueve un comercio seguro en cooperación con gobiernos y organismos internacionales. Está constituida como una organización sin ánimo de lucro, con la denominación “World BASC Organization” bajo las leyes del estado de Delaware, Estados Unidos de América. Es un sistema integral de gestión y administración de la seguridad y control de todas las actividades de la compañía.

BI: Business Intelligence se refiere al uso de datos en una empresa para facilitar la toma de decisiones. Abarca la comprensión del funcionamiento actual de la

empresa, bien como la anticipación de acontecimientos futuros, con el objetivo de ofrecer conocimientos para respaldar las decisiones empresariales.

DENIAL OF SERVICE (DOS): el denial of service o denegación de servicio es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

DENIAL OF SERVICE: ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios.

ERP: Enterprise resource planning son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios.

ICONTEC: el Instituto Colombiano de Normas Técnicas y Certificación es un organismo de carácter privado, sin ánimo de lucro que está conformado por la vinculación voluntaria de representantes del gobierno nacional, de los sectores privados de la producción, distribución y consumo, el sector tecnológico en sus diferentes ramas y por todas aquellas personas jurídicas que tengan interés en pertenecer. Además es la principal fuente de certificación en normas ISO.

MOHP: Modelo Operativo Homologado de Procesos es un conjunto de procesos, sub-procesos y flujos de actividades. Incluye la identificación de políticas a definir, indicadores de gestión y resultados de desempeño de procesos. Es una estructura que reúne los modelos de procesos de los negocios que hacen parte del Grupo Nutresa S.A.S, reflejando todos los segmentos de las industrias que se tienen. Es importante resaltar que el MOHP no define estructuras organizacionales, cargos, roles ni funciones.

NPDI: New product development and introduction es un término para describir el proceso completo para traer un nuevo producto o servicio al Mercado.

PWC (PricewaterhouseCoopers): es la mayor firma de servicios profesionales del mundo.

SAP: (*Systeme, Anwendungen und Produkte*) (Sistemas, Aplicaciones y Productos), con sede en Walldorf (Alemania), es el segundo proveedor de software empresarial en el mundo, después de Oracle. 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 está más allá de toda duda.

TRASHING: consiste en rastrear en las papeleras información, contraseñas o directorios. Esta técnica tiene una parte física y virtual, ya que la búsqueda de papeleras no solo consiste en buscar físicamente documentos en papel, también puede ser en la papelera de reciclaje del sistema operativo.

WORKFLOW: es la automatización de procesos del negocios, en un todo o parte, en los cuales documentos, información o tareas son pasadas de un participante (maquina o humano) a otro para realizar una acción, de acuerdo a un conjunto de reglas.

RESUMEN

A continuación se presenta un análisis y evaluación de riesgos para el portal de Grupo Nutresa basándose en las metodologías establecidas en la Norma Técnica Colombiana de gestión del riesgo 5254 y en la norma ISO 31000, para identificar los riesgos fundamentales a los que está expuesto actualmente, sus posibles causas y proponer controles, tales como la definición de procedimientos para la administración de perfiles del portal.

PALABRAS CLAVES: EVALUACIÓN DE RIESGOS; ANÁLISIS DE RIESGOS; CAUSAS; CONTROLES; ISO 31000; NTC 5254; PROCEDIMIENTOS; PORTAL SAP; GRUPO NUTRESA; PERFILES.

INTRODUCCIÓN

El propósito de este trabajo es realizar el primer análisis de riesgos en el ámbito de procesos de tecnología para el sistema colaborativo "*Enterprise Portals*" del Grupo Nutresa, utilizando los procedimientos basados en las mejores prácticas presentadas en la norma ISO 31000 ya adoptados en el Grupo Nutresa.

En el mundo de hoy la tecnología es uno de los elementos de mayor influencia en el desarrollo de los procesos normales de las compañías, la utilización de la misma se ha convertido en la principal forma de apalancamiento en la mejora de los procesos y el mundo de internet se ha convertido en el punto de afluencia de estos. De allí que las empresas, inviertan más recursos en la implementación de portales que permitan el acceso a ellas y a su portafolio de servicios, en un mercado de internautas que cada día va aumentando.

Con esta inversión en mente y entendiendo que el mundo del internet posee una diferente gama de vulnerabilidades, las empresas de hoy entienden que exponer sus servicios a través de este medio conlleva un riesgo y que este debe ser analizado, cuantificado, estudiado y en su finalidad controlado.

De allí la importancia de los resultados que se presentan en este trabajo y de las recomendaciones identificadas.

Este trabajo tiene como columna vertebral las diferentes fases del análisis del riesgo que plantean la Norma Técnica Colombiana 5254 y la ISO 31000, además de la experiencia adquirida por el área de riesgos de Grupo Nutresa en sus diferentes análisis dentro de las compañías que conforman el Grupo y las experiencias vividas por los equipos de Portales, Seguridad y Operaciones en el día a día.

OBJETIVO GENERAL

Proponer una estructura de perfiles y procedimientos, para mejorar la seguridad en los permisos de los usuarios en el sistema colaborativo "*Enterprise Portals*" del Grupo Nutresa, a partir de un análisis de riesgos según las mejores prácticas presentadas en la norma ISO 31000.

OBJETIVOS ESPECÍFICOS.

- Identificar las vulnerabilidades de los perfiles de los usuarios, para conocer el nivel de riesgo actual por medio de un análisis de este.
- Jerarquizar las vulnerabilidades de los perfiles de los usuarios, para seleccionar cuales enfrentar.
- Realizar una propuesta de mejores prácticas para la administración y definición de roles para los usuarios que tienen acceso al portal del Grupo Nutresa.
- Diseñar una estructura de perfiles para mitigar los riesgos dentro de la estructura de perfiles actual del modulo *Enterprise Portals* del Grupo Nutresa.
- Realizar un análisis final para rectificar los resultados.

ANTECEDENTES

Origen de la Idea.

Actualmente el Grupo Nutresa se encuentra inmerso en un proyecto empresarial llamado EVEREST, cuyo inicio se dio en el año de 2006; básicamente este se enfoca en el montaje de todas las compañías del Grupo Nutresa en el sistema de información SAP.

Actualmente el Grupo Nutresa se encuentra dividido en:

Figura 1. División Grupo Nutresa

Fuente: http://www.gruponutresa.com/es/content/estructura-del-grupo.

Para la implementación de dicho proyecto y posterior operación se requiere contar con una estructuración de roles para cada tipo de cargo, lo cual permite a cada uno de los usuarios desempeñar su labor de forma controlada y eficaz sin realizar actividades que no le competen, ya sea por desconocimiento o negligencia (cerca de 4000 usuarios internos y 15000 externos).

El sistema de información SAP en el Grupo Nutresa trabaja sobre 6 módulos específicos:

ERP (Enterprise Resource Planning): Planeación de Recursos Empresariales.

APO (Advanced Planning and Optimization): Logística Avanzada.

BI (Business Inteligence): Inteligencia de Negocios, la cual está constituida de dos sub-módulos llamados:

BW (Business Warehouse): Bodega de datos
BO (Business Objects): Sistema de explotación de la bodega de datos.

NPDI (New Product Development and Introduction): Desarrollo e Introducción de Nuevos Productos.

EP (*Enterprise Portals*): Portal Empresarial.

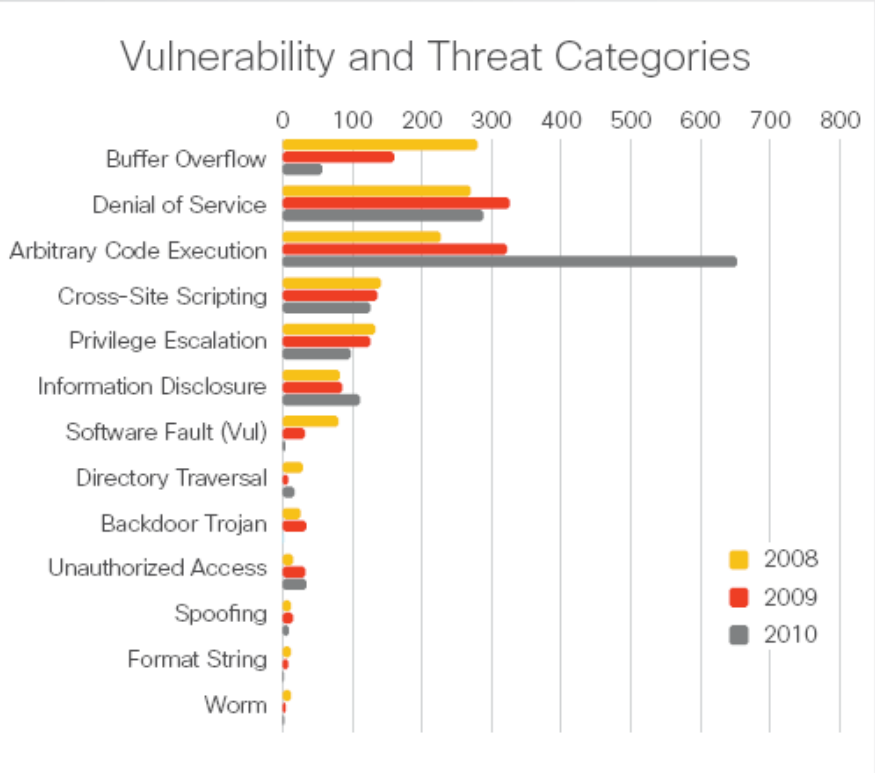
Además de la magnitud del proyecto y el grupo empresarial, estas compañías transfieren una gran cantidad de información (financiera, contable, administrativa, publicitaria, de mercadeo, estratégica, de ventas, presupuestal, comercial, logística, etc.) clasificada no solo como pública, mucha de esta información es considerada como confidencial, o privada, convirtiéndose en presa deseada para atacantes informáticos y vulnerable a la gran diversidad de riesgos (modificación o pérdida de información, modificación o pérdida de servicio o malware: virus, troyanos, gusanos, rootkits, backdoors, etc.) generados por las técnicas actuales (ingeniería social, ingeniería social inversa, trashing, ataques de monitorización, ataques de autenticación, Denial of Service (DOS), ataques de modificación – daño, etc).

Figura 2. Estadísticas de vulnerabilidad según lenguaje de programación Web a Marzo de 2010

	ASP	ASPX	CFM	DO	JSP	PHP	PL
Websites having had at least one serious* vulnerability	74%	73%	86%	77%	80%	80%	88%
Websites currently with at least one serious* vulnerability	57%	58%	54%	56%	59%	63%	75%
Avg. # of serious* vulnerabilities per website during the WhiteHat Sentinel assessment lifetime	25	18.7	34.3	19.9	25.8	26.6	44.8
Avg. # of serious* severity unresolved vulnerabilities per website	8.9	6.2	8.6	5.5	9.6	8.3	11.8

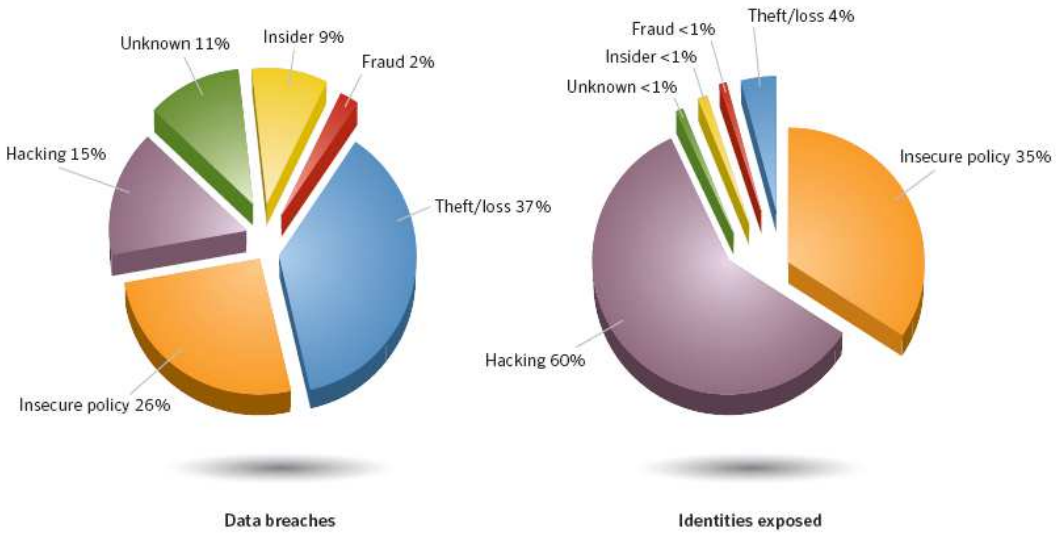
Fuente WhiteHat Website Security Statistics Report, 9° Edición, Primavera 2010.
*** El lenguaje utilizado por el modulo Enterprise Portals de Grupo Nutresa es JSP**

Figura 3. Estadísticas de vulnerabilidades y amenazas



Fuente: Cisco 2010 Annual Security Report

Figura 4. Brechas de datos e identidad expuesta



Fuente Symantec Internet Security Threat Report Trends for 2009

Debido a que el medio presenta tantas oportunidades, formas y facilidades para explotar las vulnerabilidades más comunes, es de vital importancia estudiar las posibles debilidades y riesgos que puedan ser atacados y generar planes de acción que mitiguen, y en menor medida identifiquen las vulnerabilidades de los diferentes sistemas del Grupo Nutresa. Como se menciona anteriormente el proyecto busca implementar perfiles de usuario para su control; en el portal empresarial se identifican tres grupos de usuarios generales: Clientes (internos y externos a nivel nacional e internacional), proveedores y vendedores. Desde el año 2006 hasta el año 2012 eproyecto ha implementado soluciones a estos perfiles basándose en el objetivo de prestar disponibilidad; sin embargo con la evolución del mismo y los análisis realizados por los analistas de seguridad y por los analistas de portal, se han ido identificando ciertas falencias en los roles específicos de esta solución, generando riesgos latentes en la seguridad informática. Adicionalmente existen riesgos administrativos ya que no se identifican procedimientos claros y documentados para la administración de dichos roles, al igual que la existencia de dificultades en la gestión del conocimiento, principalmente en la transferencia del mismo, ya que no se tienen instructivos documentados que apoyen dicha solución.

A raíz de la identificación de estas problemáticas se plantea la realización de esta tesis cuyo objetivo es realizar un análisis de riesgos, documentarlo, categorizarlo y analizarlo, documentar procedimientos e instructivos para el modelo implementado en el Portal de Clientes, Proveedores y Vendedores para el Grupo Nutresa, ya que este es la puerta de entrada de los usuarios externos a la compañía.

Marco teórico y estado del arte.

A comienzos de la creación de las redes, los servicios prestados por las mismas eran servicios muy limitados (correo electrónico y compartición de impresoras) adicionalmente su uso era más para un público especializado como eran los estudiantes e investigadores universitarios así mismo como usuarios corporativos, y es por esta razón y la poca madurez del tema que la seguridad de la información no era de mucha importancia[1]; pero ahora, cuando millones de ciudadanos comunes, de edades, intereses y culturas diversas usan redes para sus transacciones bancarias, compras, declaraciones de impuestos, consultas e incluso socializaciones y reuniones, la seguridad de la información se ha transformado en la necesidad de proteger la integridad, confiabilidad, confidencialidad y disponibilidad tanto de la información como de sus usuarios.

Es gracias a la necesidad de las organizaciones y los grandes países de proteger sus redes y sistemas de información, que la seguridad en redes comienza a tomar fuerza, sin embargo la necesidad de proteger la red físicamente y la transmisión de los datos eran sus principales objetivos. Es en estos momentos en que la seguridad en redes comienza a incluir aspectos que no se consideraban anteriormente, aspectos como el monitoreo de redes, respaldos y la importancia de una buena planeación, se descubre que "la seguridad que puede lograse por medio técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados"[2]. No obstante no es hasta los eventos del 9-11[3], que la importancia de la información toma un marco mucho más amplio dentro de las compañías; el vuelco provocado por la pérdida de información, dinero y personal implicó una reestructuración en las metodologías de protección, mejorar las metodologías de recuperación contra desastres, incluir procesos de protección de activos intangibles; la gestión de la seguridad y del conocimiento comenzaron a tener un espacio en los proyectos empresariales y el pensamiento "extremista" de los analistas de seguridad tomo mayor forma y fue de mejor recepción por los líderes empresariales.

Igualmente en los años 90 las empresas requerían de sistemas que les permitirán administrar todos sus procesos, no solo de manufactura como lo conseguían

[1] TANENBAUM, Andrew S. Redes de computadoras. Cuarta edición. México: Guillermo Trujado Mendoza, 2003, p 721.

[2] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology - Code of practice for information security management. ISO/IEC 17799:2000(E). 2000. p 7.

[3] 9-11: Se refiere a los atentados del 11 de Septiembre de 2001 a las Torres Gemelas en el Centro Internacional de Comercio (World Trade Center).

sistemas de años anteriores como el MRP (*Manufacturing Resource Planning*). Es en medio de esta búsqueda que los sistemas debían evolucionar, aumentando la cantidad de servicios que pudieran proveer a las empresas para un proceso unificado. Es cuando los sistemas ERP (Enterprise Resource Planning) entran en el panorama empresarial, profetizando un mejor futuro para las empresas, su rendimiento y capacidad de toma de decisión.

Objetivos de un sistema ERP:

"1. Optimización de los procesos empresariales.

2. Acceso a información confiable, precisa y oportuna.

3. La posibilidad de compartir información entre todos los componentes de la organización.

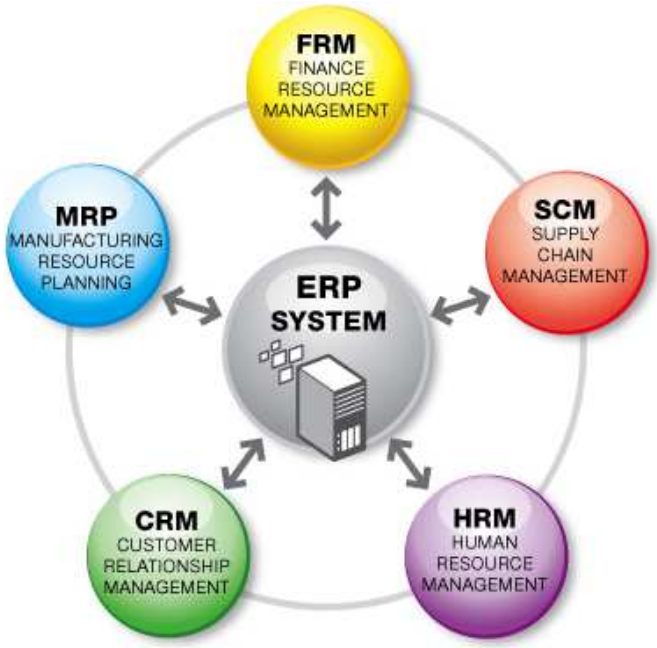
4. Eliminación de datos y operaciones innecesarias.

5. Reducción de tiempos y de los costes de los procesos."[4]

Sin embargo, es precisamente el objetivo principal del ERP, "otorgar apoyo a los clientes del negocio, tiempos rápidos de respuesta a sus problemas así como un eficiente manejo de información que permita la toma oportuna de decisiones y disminución de los costos totales de operación"[5], el que lleva a que estos sistemas no sean suficientes para grandes empresas como las del día de hoy, ahora las empresas requieren de sistemas que no solo mejoren la producción, sino que garanticen un mejor entendimiento, relación y atención del cliente, una optimización constante de los procesos de producción y mejores herramientas para la toma de decisiones y es por esto que las empresas productoras de ERP decidieron realizar módulos o ampliaciones a los sistemas actuales generando especializaciones de estos temas. Estos sistemas son llamados sistemas colaborativos, precisamente porque estos apoyan o colaboran con los sistemas ERP para otorgar mayor calidad y cantidad de servicios.

[4] http://www.wikilearning.com/monografia/planeacion_de_recursos_empresariales/11812-3
[5] Ibid

Figura 5. Constitución de un sistema ERP



Fuente: http://www.extolcorp.com/solution/sea_ecerp.html

En el mundo existen diferentes ERP, entre ellos se encuentra un sistema llamado SAP[6], este se constituye de dos grandes módulos: funcionales, conocidos como módulos que permiten la función general de la empresa; y de estructura técnica llamados SAP Netweaver, "conocidos como aplicaciones orientadas a servicios y a la integración… incorporan un bajo costo con una gran flexibilidad, una mejor integración con las aplicaciones y construcción en estándares para asegurar la futura interoperación"[7]. Estos módulos tienen sus submódulos respectivos:

Funcionales:

- SAP ERP (Enterprise Resource Planning)
- SAP CRM (Customer Relationship Management)
- SAP SRM (Supplier Relationship Management)
- SAP PLM (Product Lifecycle Management)
- SAP SCM (Supply Chain Management)

De estructura técnica:

- People Integration

[6] SAP: (*Systeme, Anwendungen und Produkte*) (Sistemas, Aplicaciones y Productos)
[7] http://es.wikipedia.org/wiki/SAP_NetWeaver

    - SAP MI (Mobile Infrastructure)
    - SAP EP (Enterprise Portal)
    - SAP KM (Knowledge Management)
- Information Integration
    - SAP BI (Business Intelligence)
    - SAP MDM (Master Data Management)
- Process Integration
    - SAP XI (Exchange Infrastructure)
    - SAP BPM (Business Process Management)
- Application platform
    - ABAP Stack
    - Java Stack
- Composite Application Framework
- Lifecycle Management
- Integración con MS .net
- Integración con IBM Websphere

Las empresas de hoy, en su constante búsqueda de mejorar y automatizar sus procesos, además de incrementar su productividad y ganancias, han encontrado en los sistemas informáticos, como el ERP, grandes aliados, sin embargo estos sistemas también representan un riesgo, ya que en el ambiente informático encontramos grandes amenazas que son explotadas por criminales cibernéticos. Ante tales amenazas los países del mundo debieron buscar mecanismos legales para enfrentarlas y a su vez mitigarlas. Así pues apoyándose en el Pacto Internacional de Derechos Económicos, Sociales y Culturales, de Derechos Civiles de la ONU los países unidos a este, lograron encontrar una base para fundamentar leyes en contra del crimen cibernético.

En el caso de Colombia, por medio de la ley 74 de 1968 se incorporo a dicho pacto[8], y por medio de leyes que la apoyan y complementan[9] es que los grandes líderes en las empresas, aquellos que promulgan el cambio, encuentran ayuda a grandes desafíos y a la protección de sus activos. La problemática principal en nuestro país, no es como en los demás, los enemigos principales de las comunicaciones en el exterior son estudiantes, en Colombia hay una modalidad extra en las categorías de abusadores, los grupos al margen de la ley.

En consecuencia a esta problemática informático-social, las empresas con el fin de proteger su información y sus empleados, se encuentran en una constante búsqueda y mejoramiento de sus procedimientos, procesos y administración,

[8] http://www.informatica-juridica.com/legislacion/colombia.asp
[9] Ley 1273 de enero 5 de 2009, Artículo 269: Acceso abusivo a un sistema informático.

apoyándose en diferentes modelos como ITIL[10] y COBIT[11] para documentar e implementar mejores estrategias de recuperación de desastres y mecanismos de backup. En resultado a esta búsqueda se encuentran instituciones que facilitan el entendimiento de las normas, como lo son el ICONTEC, empresas reguladoras como la BASC (Business Aliance for Secure Commerce)[12], firmas consultoras (Price WaterHouse Coopers, Deloitte), que proveen servicios de auditorías para lograr ser certificadas por el ICONTEC en los estándares internacionales.

Dentro del Grupo Nutresa existe un centro de servicios compartidos para prestar soporte a los procesos que son generales para todas las compañías, y se llama Servicios Nutresa S.A.S; en éste, se encuentra la Gerencia de Tecnologías de la Información, y en ella la Dirección de Infraestructura de la cual depende la jefatura de Seguridad de la Información, es aquí donde la seguridad es planteada y todas las políticas y los estudios de las mismas son desarrollados.

Dentro de las responsabilidades del área de Seguridad de la información se encuentran:

- Diseñar estrategia y plan de seguridad
- Desarrollar y actualizar políticas, procedimientos y estándares de IT
- Desarrollar funcionalidad de aplicaciones / sistemas / seguridades
- Brindar seguridad a la información
- Definir requerimientos para la seguridad de la información
- Implementar los requerimientos para la seguridad de la información
- Auditar/probar la seguridad de los sistemas de información
- Administrar los planes de contingencia en los sistemas de IT

Con el fin de responder a estas responsabilidades, se han implementado medidas de aseguramiento y un monitoreo de las actividades y procesos que se manejan en la empresa. De esta manera, se encuentran ciertas necesidades a las que se ha respondido conforme fueron detectadas o dependiendo de su criticidad.

En el año 2006 inició el proyecto Everest. Básicamente este se enfoca en el montaje de todas las compañías del Grupo Nutresa (alrededor de 48 empresas), en el sistema de información SAP, y con este el montaje de un portal empresarial para el manejo de sus clientes proveedores y vendedores.

[10] ITIL (Information Technology Infrastructure Library): La Biblioteca de Infraestructura de Tecnologías de Información documenta las Mejores Prácticas para la Administración de Servicios de TI.

[11] COBIT (Control Objectives for Information and related Technology): Los Objetivos de Control para la Información y Tecnologías Relacionadas, son el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan.

[12] BASC: es una alianza empresarial internacional que promueve un comercio seguro en cooperación con gobiernos y organismos internacionales.

EP Portal Empresarial:

Los portales empresariales nacen en los años 90 con el gran apogeo de portales WEB como AOL, Altavista, Excite y Yahoo. Estas páginas contenían una gran variedad de servicios que no fueron desapercibidos por las grandes empresas, encontrando en esta herramienta una gran posibilidad de divulgación de información mucho más eficiente y sencilla. Con el crecimiento de la idea la aparición de la Intranet fortaleció los servicios ya prestados y aumento el portafolio para los usuarios internos de la compañía.

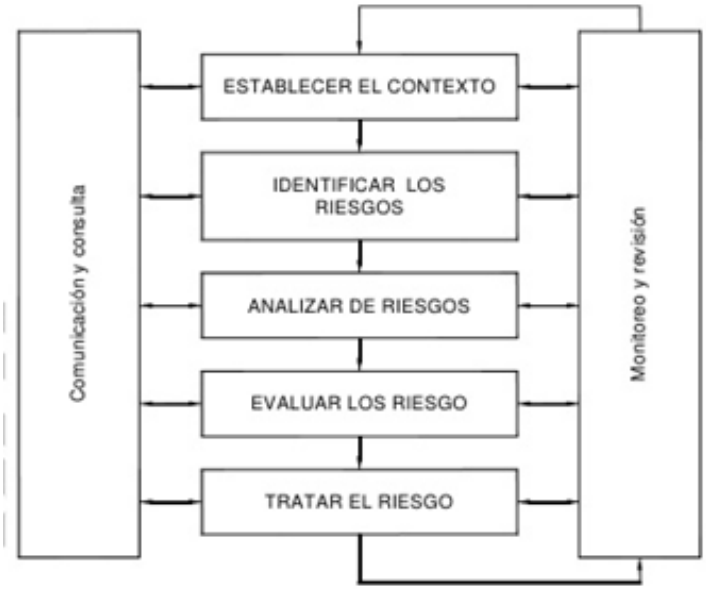
Los portales empresariales no solo se enfocaron en los usuarios internos, sino que también se les extendieron servicios a clientes, proveedores y usuarios externos que requerían de una mejor y más eficiente atención. Ahora los portales empresariales representan un activo de gran valor para las empresas ya que son entrada de pedidos, comunicados para los empleados, clientes y proveedores.

DESCRIPCIÓN DE LA METODOLOGÍA

La metodología utilizada para este proyecto está basada en los lineamientos y guías establecidos en la Norma Técnica Colombiana de gestión del riesgo 5254 que “es una traducción idéntica de la norma técnica Australiana AS/NZ 4360:2004 de amplia aceptación y reconocimiento a nivel mundial para la gestión de riesgos independiente de la industria o el negocio que desee emplearla”, la cual posteriormente fue reemplazada por la ISO 31000 dado que esta amplía la norma australiana enfocando su interés adicionalmente en el diseño, implementación, mantenimiento y mejoramiento de los procesos de administración de riesgos.

Estas normas y estándar establecen el siguiente esquema para el proceso de gestión de riesgos:

Figura 6. Proceso de Gestión del Riesgo



Fuente: Norma Técnica Colombiana (NTC) 5254

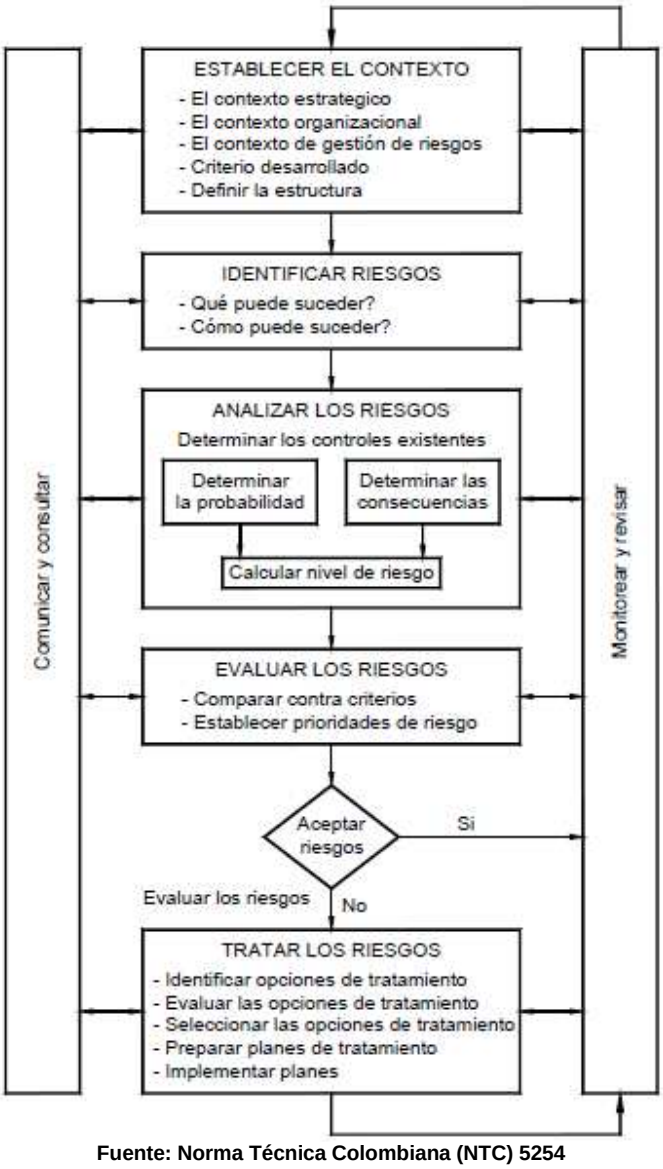
Siguiendo este esquema, el proceso de análisis de gestión del riesgo para el portal de Grupo Nutresa se divide en 7 etapas:

- Comunicación y consulta.
- Establecer el contexto.
- Identificar los riesgos.
- Analizar los riesgos.

- Evaluar los riesgos.
- Tratar el riesgo.
- Monitoreo y revisión

Cada uno de estos elementos posee un proceso detallado:

Figura 7. Proceso de gestión del riesgo (ampliado)



Fuente: Norma Técnica Colombiana (NTC) 5254

Con esta claridad se desprende el desarrollo de las etapas en detalle para la gestión y administración del riesgo del portal de Grupo Nutresa.

1. COMUNICAR Y CONSULTAR

El propósito de esta etapa del proceso es informar, consultar y mantener informado a todos los equipos, áreas o grupo de personas interesados en la evolución o desarrollo de cada una de las etapas: “Comunicar y consultar con las partes interesadas, internas y externas, según sea apropiado, en cada etapa del proceso de gestión del riesgo y con relación al proceso en conjunto”.

El proceso de gestión de análisis de riesgos inicia con una serie de reuniones o entrevistas donde a cada una de las áreas (riesgos, centro de competencias, operaciones y seguridad), se les da a conocer el interés por hacer este proceso. Su vinculación con el proyecto se dio en cada una de las etapas, donde su participación fue vital para identificar, escoger, analizar y concretar los diferentes riesgos y controles, actuales y futuros, que permitieron la realización de todo este análisis.

2. ESTABLECER EL CONTEXTO

“El establecimiento del contexto es necesario para definir los parámetros básicos dentro de los cuales deben administrarse los riesgos y para proveer una guía para las decisiones dentro de estudios de administración de riesgos más detallados. Esto establece el alcance para el resto del proceso de administración de riesgos. Deben incluirse el ambiente interno y externo y sus interfaces correspondientes.”

El establecimiento del contexto implica tener de acotar el alcance de todo lo que se vaya a analizar dentro del proceso, es literalmente “poner en contexto”, enmarcar para tener claridad dentro de que rangos de análisis se estará enfocados.

En gran medida el establecimiento del contexto para este proyecto se dio a conocer en el capítulo “Antecedentes”, sin embargo el Grupo Nutresa posee un proceso de análisis de riesgos ya previamente establecido enfocado en los procesos de producción y distribución de alimentos. Este proceso se toma como base para este análisis y se presentan cambios dado que el enfoque del mundo de la tecnología presenta características diferenciales representativas.

3. IDENTIFICAR RIESGOS

Para determinar claramente el proceso del análisis del riesgo se debe realizar una breve explicación de ¿qué es un riesgo?:

El riego es definido de diferentes maneras por distintos autores:

Según la real academia de la lengua española el término riesgo proviene del italiano *risico* o *rischio* que, a su vez, tiene origen en el árabe clásico *rizq* ("lo que depara la providencia"). El término hace referencia a la proximidad o contingencia de un posible daño.[13] [14]

Según GARP[15], La palabra riesgo se deriva del latín *risicare* que significa atreverse, en este sentido el riesgo es más una elección que un destino al que nos debemos resignar. [16]

Sin embargo el riesgo también puede ser definido según el tema y la aplicación del mismo:

La OHSAS (Occupational Health & Safety Advisory Services) define el riesgo como el producto de la probabilidad de que una amenaza resulte en un evento adverso, multiplicado por la severidad de dicho evento.[17]

Según la ISO 27005 para términos de seguridad informática: El potencial de que una amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos y de esta manera causar daño a la organización.[18]

Para términos financieros es definido como la volatilidad inesperada de los resultados, y esto puede incluir tanto resultados potenciales mejores de lo esperado como peores.[19]

Sin embargo es importante tener presente que la Gestión Integral de Riesgos adoptada por Grupo Nutresa, que es el foco de estudio, se basa en la Norma Técnica Colombiana NTC 5254 (AS/NZS 4360 e ISO 31000) como se indica anteriormente, y la definición establecida en la ISO 31000, sería la definitiva. Esta definición determina que el riesgo es "el efecto de la incertidumbre en los objetivos", lo que no centraliza el significado en solo impactos negativos, sino que abarca o infiere que el riesgo puede tener impactos tanto negativos como positivos. "La ISO 31000 reconoce que todos operamos o vivimos en un mundo incierto. Cada vez que tratamos de lograr un objetivo, siempre hay una posibilidad de que no logremos el objetivo que estamos buscando conseguir. Cada paso que

[13] Definición de riesgo - Qué es, Significado y Concepto http://definicion.de/riesgo/#ixzz2SRHBQXwv
[14] http://buscon.rae.es/drae/srv/search?val=riesgo
[15] GARP : Global Association of Risk Professionals
[16] Definiciones de riesgo ISO 31000 SesColombia 1 de 4 - http://www.youtube.com/watch?v=E7bNwBruR9I
[17] An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006
[18] ISO/IEC 27005:2008
[19] http://en.wikipedia.org/wiki/Risk

tomamos para lograr este objetivo involucra incertidumbre. Cada paso tiene un elemento de riesgo que necesita ser administrado. En pocas palabras, riesgo es la posibilidad que haya una desviación, positiva o negativa, de los objetivos que pretendemos obtener"[20].

Bajo este entendimiento y esta definición se debe comprender que el propósito de la ISO 31000:2009 es proveer los principios y guías genéricas sobre la administración del riesgo. Busca proveer un paradigma universal y reconocido para las compañías y practicantes que emplean procesos de administración del riesgo y así reemplazar los incalculables estándares, metodologías y paradigmas que existen y que difieren de industria a industria, temas relacionados y regiones.[21]

Para identificar el riesgo es importante plantear dos cuestionamientos:

¿Qué puede suceder? Es identificar claramente la fuente del riesgo, que, cuando y donde es lo que me puede suceder para que la posibilidad del logro de los objetivos, se vea potencializado o disminuido.

¿Cómo puede suceder? Además de tener claro el que, cuando y donde, es muy importante identificar el cómo, el medio, el por qué se puede presentar ese riesgo. En otras palabras es identificar claramente la causa o el motivo por el cual se presenta este riesgo.

Dado que el Grupo Nutresa ya poseía un listado base de riesgos generalmente el procedimiento a seguir es tomar este listado y evaluar el "Qué" (fuente) y él "Cómo" (Causa) de estos. De esta manera se tomó como base la lista de 73 riesgos generales ya analizados y definidos por el equipo de riesgos del Grupo Nutresa:

ANEXO 1. Matriz de Riesgos Grupo Nutresa.

Dado que la matriz está concebida para todo tipo de proceso del Grupo Nutresa, la cuarta compañía más grande en el sector de alimentos de Latino América en términos de capitalización bursátil, los riesgos que se encuentran en esta matriz están enfocados en el proceso principal del grupo, producción de alimentos, el cual es apalancado por empresas dedicadas a la comercialización de estos productos y a la prestación de servicios de Back Office. Los riesgos encontrados en esta matriz son de carácter general y pueden ser aplicados a cualquier proceso del grupo indiferentemente de su naturaleza.

[20] http://www.praxiom.com/iso-31000-terms.htm#2.1_Risk
[21] http://en.wikipedia.org/wiki/ISO_31000

El análisis que se realizó para este proyecto, es para un proceso que no produce alimentos, en otras palabras colaborativo, que apalanca la movilidad, la toma de decisiones y la generación de valor frente a la operación general del negocio.

Cada uno de estos riesgos se revisó, analizó y compartió con los tres equipos directamente involucrados con el módulo de portales.

Equipo Funcional: Equipo encargado de recibir, entender, transformar, modelar, implementar, soportar y mejorar los diferentes servicios y procesos soportados en el portal.

Equipo de Operaciones: Equipo encargado de soportar, diseñar, implementar, administrar y mejorar los diferentes procesos de infraestructura técnica.

Equipo de Seguridad: Equipo encargado de soportar, diseñar, implementar, administrar y mejorar los diferentes procesos de seguridad de la información.

De estas reuniones y análisis, cada uno de los equipos seleccionó los riesgos que consideran, afectan de manera directa sus procesos y pueden generar oportunidades de mejora o corrección. El equipo funcional determinó que 36 riesgos de los 73 son relevantes para su operación mientras que el equipo de operaciones determinó 34 y el equipo de seguridad 35, indicando así un total de 105 riesgos a revisar en detalle.

ANEXO 2. Matriz de riesgos específicos por equipo.

Posteriormente al análisis anterior y un estudio con el equipo de riesgos, se propuso a cada equipo tomar de cada uno de su listado 5 riesgos críticos a enfrentar y analizar en profundidad, así que del total de 105 riesgos identificados, el análisis total se realizará con 15 riesgos:

Tabla 1. Riesgos Funcionales

Riesgos	Descripción del riesgo
Afectación por equipos de apoyo	Dependencia de actividades a realizar por los terceros o partes involucradas para la ejecución de los proyectos o procesos que generan retrasos en los mismos.
Fallas en la comunicación interna	No transmisión oportuna de información relevante para la toma de decisiones
Fuga de talento	Retiro, incapacidad o muerte de personal clave para la organización sin que esta cuente con un reemplazo establecido; ej: Accidente de avión en el que vayan varios ejecutivos
Insatisfacción de la demanda	Incapacidad para responder a la demanda

Retraso	Situación que genera incumplimiento en el programa de producción.

Tabla 2. Riesgos de Operaciones

Riesgos	Descripción del riesgo
Ataque de un cracker	Intrusión de personas ajenas a la organización, en los sistemas de información, con el propósito de causar daños y manipular la información en beneficio propio. La diferencia con HACKER es que este último hace intrusión pero no con fines delictivos
Colapso en los sistemas de información	No dejar evidencia escrita de todas y cada una de las modificaciones realizadas a un software determinado
Fallas en el sistema de información	Problemas en el procesamiento electrónico de datos por contaminación con virus y gusanos informáticos
Obsolescencia	Plataforma informática inadecuada para las necesidades de los usuarios
Selección inadecuada de asociados de negocio	Fallas, errores u omisiones en la evaluación de proveedores, contratistas y demás asociados que colaboren con el normal desarrollo de la actividad

Tabla 3. Riesgos de Seguridad

Riesgos	Descripción del riesgo
Ataque de un cracker	Intrusión de personas ajenas a la organización, en los sistemas de información, con el propósito de causar daños y manipular la información en beneficio propio. La diferencia con HACKER es que este último hace intrusión pero no con fines delictivos
Fallas en el sistema de información	Problemas en el procesamiento electrónico de datos por contaminación con virus y gusanos informáticos
Fuga de información	Entrega de información restringida de la Empresa a terceros por parte de algún empleado
Obsolescencia	Plataforma informática inadecuada para las necesidades de los usuarios
Sabotaje	Acción delictiva subrepticia, tendiente a interrumpir o afectar sensiblemente la operación normal de un sistema, mediante la afectación violenta o no sobre los equipos o procesos, realizada por personal dentro de una empresa u organización.

La metodología utilizada en el Grupo Nutresa indica que se debe realizar un análisis donde se debe tomar cada riesgo, determinar la fuente que genera el riesgo, sus posibles causas o motivos, las consecuencias que genera la materialización de dicho riesgo y por último los controles actuales que se tienen para mitigar dicho riesgo; esto nos ayuda a determinar la gravedad de que este se materialice.

Estos riesgos fueron consolidados en una sola lista de 12 riesgos generales a estudiar:

Tabla 4. Riesgos consolidados

Riesgo	Descripción
Ataque de un cracker	Intrusión de personas ajenas a la organización, en los sistemas de información, con el propósito de causar daños y manipular la información en beneficio propio. La diferencia con HACKER es que este último hace intrusión pero no con fines delictivos
Colapso en los sistemas de información	No dejar evidencia escrita de todas y cada una de las modificaciones realizadas a un software determinado
Fallas en el sistema de información	Problemas en el procesamiento electrónico de datos por contaminación con virus y gusanos informáticos
Interrupción de la operación	Paros en la producción, en el proceso por agentes internos o externos
Obsolescencia	Plataforma informática inadecuada para las necesidades de los usuarios
Afectación por equipos de apoyo	Dependencia de actividades a realizar por los terceros o partes involucradas para la ejecución de los proyectos o procesos que generan retrasos en los mismos.
Fallas en la comunicación interna	No transmisión oportuna de información relevante para la toma de decisiones
Fuga de talento	Retiro, incapacidad o muerte de personal clave para la organización sin que esta cuente con un reemplazo establecido; ej: Accidente de avión en el que vayan varios ejecutivos
Insatisfacción de la demanda	Incapacidad para responder a la demanda
Retraso	Situación que genera incumplimiento en el programa de producción.
Fuga de información	Entrega de información restringida de la Empresa a terceros por parte de algún empleado
Sabotaje	Acción delictiva subrepticia, tendiente a interrumpir o afectar sensiblemente la operación normal de un sistema, mediante la afectación violenta o no sobre los equipos o procesos, realizada por personal dentro de una empresa u organización.

Estos 12 riesgos se analizaron en detalle y se detectó que 7 eran realmente riesgos, mientras que los demás se redefinieron para efectos de este proceso como causas.

Tabla 5. Riesgos finales

Código	Riesgo
R1	Suplantación de identidad
R2	Fuga de información
R3	Sabotaje
R4	Pérdida de Dinero
R5	Afectación a la marca
R6	Reprocesos
R7	Fraude

De este análisis se realizó una identificación de las posibles causas o amenazas del medio y de la realidad del negocio que pueden materializar dichos riesgos:

ANEXO 3. Matriz Causa Riesgos

Posteriormente se tomaron los principales activos ya definidos por el Grupo Nutresa y se identificaron cuales de estos riesgos afectaban estos activos. Esta matriz se convierte en la base para los siguientes análisis.

ANEXO 4. Matriz causa riesgo activo.

4. ANALIZAR LOS RIESGOS.

El análisis del riesgo se desarrolla con el objetivo de entender el mismo. Este entendimiento se fundamenta en tomar las fuentes, considerar sus consecuencias o impactos e identificar la probabilidad o frecuencia de que estas hayan ocurrido, estén ocurriendo o puedan ocurrir.

Estos análisis se pueden realizar de tres modos:

Cualitativo: El análisis cualitativo emplea palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la posibilidad de que estas consecuencias ocurran. Estas escalas pueden adaptarse o ajustarse según las circunstancias, y se pueden emplear diferentes descripciones para diferentes riesgos.

Semi cuantitativo: En el análisis semi cuantitativo, se asignan valores a escalas cualitativas como las descritas anteriormente. No es obligatorio que el número asignado a cada descripción tenga una relación exacta con la magnitud real de las consecuencias o posibilidad. Los números se pueden combinar mediante cualquier fórmula de entre una variedad de ellas, siempre y cuando el sistema usado para priorización sea compatible con el sistema escogido para asignar números y combinarlos. El objetivo es producir una priorización más detallada de la que se logra generalmente en el análisis cualitativo, y no sugerir cualquier valor realista del riesgo tal como se intenta en el análisis cuantitativo.

Cuantitativo: El análisis cuantitativo emplea valores numéricos (en lugar de las escalas descriptivas empleadas en los análisis, cualitativo y semi cuantitativo), tanto para las consecuencias como para la posibilidad a partir de datos de una variedad de fuentes. La calidad del análisis depende de la exactitud y de la integridad de los valores numéricos empleados.

Apoyándonos en los análisis previos realizados para proyectos de análisis de riesgos en procesos del grupo, dado que no existen estadísticos de los eventos que se están analizando en este proyecto y nos basamos en las diferentes experiencias de las áreas involucradas, el modo de análisis utilizado fue el semi cuantitativo.

El análisis fue realizado en tres fases. La fase de análisis de la probabilidad de ocurrencia, de impacto y la determinación del factor del riesgo.

4.1 ANÁLISIS DE PROBABILIDAD.

Para realizar el análisis de probabilidad de ocurrencia se determinaron dos insumos vitales:

a. Matriz causa-riesgo-activo (Anexo 4)
b. Escala de probabilidad.

Tabla 6. Escala de Probabilidad

ESCALA DE PROBABILIDAD		
Valor	**Probabilidad**	**Definición**
0	**----------**	
1	**Remoto**	Muy baja probabilidad de ocurrencia: a. No se ha presentado en el último año pero se ha presentado alguna vez en la historia de la compañía. b. Puede suceder alguna vez en los próximos 5 años c. Se cumple gestión legal
2	**Posible**	Limitada probabilidad de ocurrencia a. Ha sucedido una vez en el último año o b. Puede suceder solo una vez, en el próximo año.
3	**Frecuente**	Significativa probabilidad de ocurrencia a. Sucede o ha sucedido dos veces en el último año o b. Puede suceder dos veces en el próximo año.
4	**Recurrente**	Alta probabilidad de ocurrencia a. Ocurre más de tres veces en el último año o b. Puede suceder tres veces en el próximo año.
5	**Constante**	Muy Alta probabilidad de ocurrencia a. Ocurre más de 4 veces en el último año o b. Puede suceder 4 veces en el próximo año.

La escala de probabilidad fue obtenida de la información utilizada para los análisis de riesgos de Grupo Nutresa. Esta escala fue tomada como base y ajustada de acuerdo al conocimiento de probabilidad de ciertos escenarios que se identificaron en la Matriz causa-riesgo-activo. Luego de esto se determino la probabilidad por cada riesgo en dos escenarios específicos: Análisis de probabilidad sin control y análisis de probabilidad con control. Esta información se determinó realizando un análisis de la frecuencia que se ha presentado en los 5 años que lleva el portal de Grupo Nutresa en funcionamiento:

ANEXO 5. Matriz causa-riesgo-activo-probabilidad SC

ANEXO 6. Matriz causa-riesgo-activo-probabilidad CC

4.2. ANÁLISIS DE IMPACTO Y FACTOR DEL RIESGO.

La escala de impacto no fue modificada y proviene de la información utilizada para los análisis de riesgos de Grupo Nutresa:

Tabla 7. Escala de Impacto

ESCALA DE IMPACTO						
Valor	**Gravedad**	**Humano**	**Financiero (EBITDA)**	**Información**	**Reputación**	**Medio Ambiente**
0	**----------**					
1	**Insignificante**	Lesiones menores sin incapacidad	<5%	Recuperable dentro del área	Conocimiento interno sin consecuencias	Afectación ambiental leve recuperable
2	**Leve**	Lesiones con incapacidad, pero sin secuelas	>5 y <15%	Recuperable dentro de la compañía	Conocimiento interno con consecuencias	Afectación ambiental leve no recuperable
3	**Grave**	Lesiones con secuelas, pero sin invalidez	>15 y <20%	Recuperable fuera de la compañía	Conocimiento externo sin consecuencias	Afectación ambiental grave recuperable
4	**Crítico**	Invalidez o la muerte	>20%	Irrecuperable	Conocimiento externo con consecuencias	Afectación ambiental grave no recuperable

Luego se toma el anexo 5 y se determino por cada uno de los riesgos el impacto. En esta etapa se realizó un análisis del riesgo sin control:

ANEXO 7. Matriz causa-riesgo-activo-probabilidad-impacto SC.

Posteriormente se verificó cada uno de los riesgos y se analizaron los controles actuales:

ANEXO 8. Matriz causa-riesgo-activo-probabilidad-impacto CC.

4.3. LA DETERMINACIÓN DEL FACTOR DEL RIESGO

Con la probabilidad y frecuencia determinada se calcula el factor del riesgo multiplicando ambos elementos de cada uno de los activos identificados y así realizar una evaluación del riesgo y determinar la gravedad de la materialización del mismo:

ANEXO 9. Matriz de factor de riesgos.

5. EVALUAR LOS RIESGOS

La evaluación del riesgo es tomar decisiones sobre los resultados obtenidos en el análisis realizado previamente. Es el proceso en el que se toman todos los elementos posibles que nos permitan determinar qué hacer con estos riesgos detectados y los valores de evaluación identificados. En esta etapa se deben comparar los riesgos sin control y los resultados del riesgo residual y de esta manera determinar la prioridad de los riesgos y las acciones a tomar.

Para efectos de este proyecto la evaluación del riesgo se realizo en 2 análisis:

5.1 COMPARACIÓN SIN CONTROL VS CON CONTROL:

Se realizó un comparativo entre los riesgos sin control contra el riesgo con control o residual. Esta comparación permite identificar que los diferentes controles actuales reducen los valores identificados en el análisis sin control y determinar si los controles actuales realmente están realizando un efecto o no, en el proceso. El análisis de los 876 escenarios detectados arrojo como resultado:

Cantidad de riesgos por evaluación:

Tabla 8. Cantidad de riesgos sin control

Evaluación del Riesgo Sin Control	Riesgos por Evaluación Sin Control
8	238
20	638

Total general	**876**

Tabla 9. Cantidad de riesgos con control

Evaluación del Riesgo Con Control	Riesgos por Evaluación Con Control
1	187
2	412
3	40
4	34
5	51
6	16
8	13
10	62
15	24
16	1
20	36
Total general	**876**

Se realizó un análisis de efectividad del control por medio de una fórmula de porcentaje:

$$\%\ de\ Efectividad = \frac{ESC - ECC}{ESC} * 100$$

Donde:

ESC= valor de evaluación sin control
ECC = valor de evaluación con control

Esto aplicado al Anexo 9 nos arrojo los siguientes resultados:

Tabla 10. Porcentaje de efectividad

Efectividad del control	Riesgos por % Efectividad
0%	38

20%	1
25%	40
38%	8
50%	71
60%	11
75%	188
80%	25
85%	40
88%	58
90%	267
95%	129
Total general	**876**

Con esto podemos determinar que si el porcentaje de efectividad es muy bajo, el control no está teniendo efecto o no existe en lo absoluto. Este análisis facilitará la toma de decisión de que riesgos serán los enfrentados, evaluados y/o asumidos.

5.2 IDENTIFICACIÓN DE CONTROLES.

Para la identificación de los riesgos que requieren ser evaluados se realiza la matriz de aceptabilidad. Esta matriz de aceptabilidad, es una matriz 5X4 donde se determina por medio de un análisis del valor de gravedad del impacto cuanto será el valor de aceptación para verificar que riesgos serán asumidos, enfrentados o trasladados. La matriz de aceptabilidad se divide en 4 zonas de colores donde dependiendo del valor de la evaluación del riesgo es su color.

Verde: Riesgos que pueden ser asumidos.
Amarillo: Riesgos que pueden ser asumidos pero deben ser revisados.
Naranja: Riesgos que deben ser revisados y establecer un control para enfrentarlos.
Rojo: Riesgos que deben ser revisados inmediatamente y se les debe determinar un control o si serán trasladados.

Para el análisis de riesgos del Grupo Nutresa se determinó la siguiente escala de aceptabilidad:

Verde: Riesgos que su evaluación esté entre 1 y 4.
Amarillo: Riesgos que su evaluación esté entre 5 y 9.
Naranja: Riesgos que su evaluación esté entre 10 y 14.
Rojo: Riesgos que evaluación este entre 15 y 20.

Tabla 11. Matriz de aceptabilidad

MATRIZ DE ACEPTABILIDAD						
4	Grave	4	8	12	16	20
3	Moderado	3	6	9	12	15
2	Leve	2	4	6	8	10
1	Insignificante	1	2	3	4	5
		Remoto	**Ocasional**	**Moderado**	**Frecuente**	**Constante**
		1	**2**	**3**	**4**	**5**

Con este análisis se marcaron los riesgos con la escala determinada en la matriz de aceptabilidad y se decidió revisar de manera prioritaria aquellos que estuvieran en las franjas naranja y roja. En otras palabras aquellos que estuvieran entre 10 y 20 en su evaluación del riesgo. De acuerdo a esta determinación, las causas a enfrentar para mitigar los riesgos que resultaron del análisis son:

ANEXO 10. Causas que requieren controles.

Cada una de estas causas se analizó con la realidad del negocio y se le estableció un control específico que permitiera su mitigación.

ANEXO 11. Controles propuestos.

Dado que uno de los objetivos de este proyecto es realizar una propuesta de mejores prácticas para la administración y definición de roles para los usuarios

que tienen acceso al portal del Grupo Nutresa, solo nos enfocaremos en los siguientes controles:

Documentación de Procedimiento de Administración de perfiles de portal en el Back End. [22]

Documentación de Procedimiento de Administración de perfiles de portal en el Portal.

PROPUESTA DE DEFINICIÓN DE ROLES.

Para desarrollar el tema de definición de roles primero debemos entender el modelo funcional. El esquema funcional de portales se basa en 4 grandes elementos:

Iviews: Son el elemento más pequeño pero más importante de el esquema, este es el elemento que incluye el servicio. Pueden ser Web Dynpro[23], transacciones SAP, páginas Web, entre otros elementos.

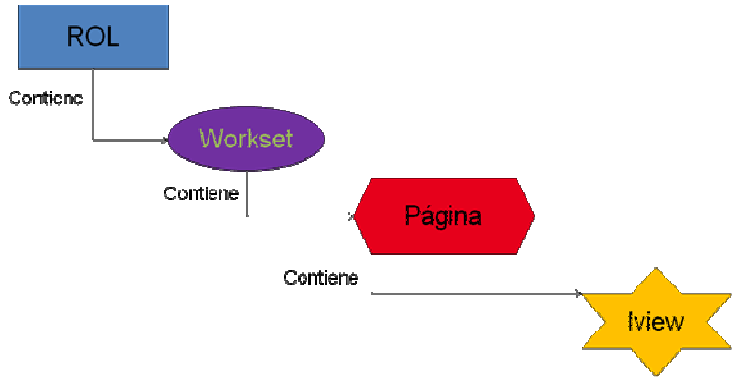
Páginas: Son la estructura donde se agrupan las Iview y permiten hacer reportes de actividades.

Workset: Son la estructura donde se agrupan las páginas. Es el segundo elemento más importante del esquema, ya que esta determina la visualización de las Iview: donde y en qué orden. Estas determinan el punto de entrada que significa que por esta es que se accede al servicio.

Roles: Son los que agrupan los workset. Este es el elemento que se entrega al equipo de seguridad para estructurar toda la seguridad de portal.

[22] BACK END: Para el portal de Grupo Nutresa "Back End" es cualquier sistema que esté detrás de la capa de visualización presentada por el portal y del cual este extrae información para el servicio en particular.
[23] Web Dynpro: Es un modelo de programación SAP para interfases de usuarios y provee soporte cuando se desarrolla en aplicaciones de negocio con presentación Web.

Figura 8. Modelo Funcional



Hay que tener en cuenta que un ROL en el portal es diferente a un ROL en un sistema SAP, también llamado sistema núcleo o “core”, fuente o “source”, o simplemente productivo y a su vez diferente a un ROL de negocio:

ROL de portal (ROL EP): es un contenedor de objetos del portal como worksets, páginas y iViews. Un ROL EP debe estar obligatoriamente incluido en un Grupo de portal (GRP EP) dado a una definición de negocio. Los ROLES EP pueden ser asignados directamente a los usuarios sin embargo no se realiza dicha acción dado que son elementos muy ligados a las acciones de los funcionales y son considerados de su administración.

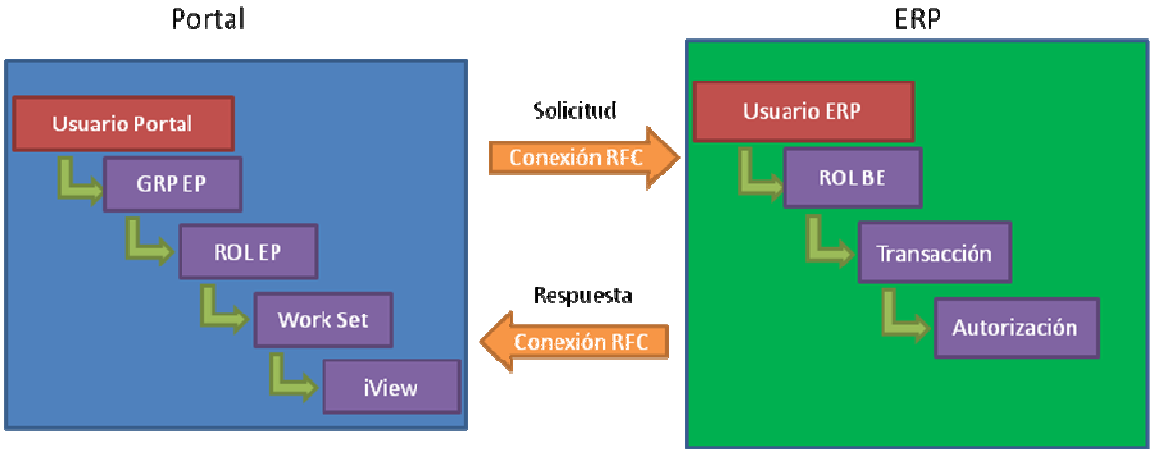
ROL Sistema Back End (ROL BE): es un contenedor de objetos de autorización que permiten la conectividad entre el portal y el sistema Back End, final o fuente. En este se incluyen las transacciones o las autorizaciones necesarias para correr un proceso, consultar un dato o extraer información del sistema.

Rol de Negocio (ROL GN): es la relación que se da entre el ROL BE con el GRP EP. Estos no son configurados en el sistema, son mantenidos y administrados directamente en un archivo de Excel y existen para darle mayor claridad a las asignaciones de los usuarios, tanto a los analistas de portal como a los analistas de seguridad y administradores de negocio.

1. MODELO ACTUAL DE SEGURIDAD.

El modelo actual consta de 3 elementos: usuario, GRP EP y ROL BE. De acuerdo a esto el usuario debe estar creado tanto en el sistema Back End como en el Portal, dado que muchos de los servicios prestados requieren de validaciones contra el sistema Back End:

Figura 9. Esquema de funcionamiento



Nota: RFC (Remote Function Call o Remote Procedure Call (RPC)) es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

En la actualidad en el portal de Grupo Nutresa se cuenta con los siguientes servicios:

ANEXO 12. Servicios del Portal

Dentro de estos servicios se logro identificar una condición especial con el tema de toma de pedidos en línea; para efectos del montaje del portal de clientes se implementó la tienda del portal de SAP (Internet Sales), dentro de la configuración del sistema se dejo "quemada" o estática la contraseña de conexión con el sistema ERP, tema que obliga a que todos los clientes y vendedores, que requieran de este servicio, sean usuarios de tipo "servicio" en el sistema ERP.

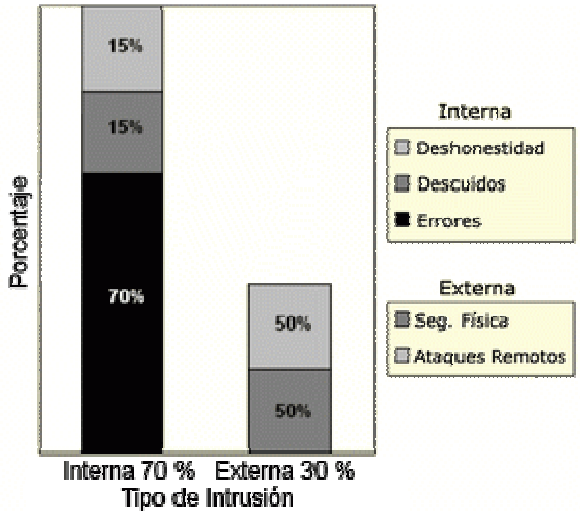
Usuario tipo Servicio: "Es propicio para su utilización por parte de usuarios que requieren acceso anónimo. No respetan las normas de expiración de contraseña y la misma solo puede ser cambiada por el administrador del sistema. Las autorizaciones que se le otorguen al mismo deben ser mínimas y restringidas específicamente a la necesidad por la que se creó el usuario. Su uso no es recomendable salvo necesidad específica, ya que son accesibles mediante SAP GUI."[24] Esto indica que el riesgo que un usuario ingrese al sistema ERP con la contraseña definida por Grupo Nutresa es alta y pueda generar una suplantación de identidad y acceder a los servicios de un cliente o vendedor sin autorización.

Se debe tener en cuenta que el riesgo hacia el exterior de la compañía es menor dado que los sistemas Back End no están expuestos a internet, su único medio de ingreso es a través del portal y este no posee dicha configuración, en otras palabras, cuando el usuario ingresa al portal este debe ingresar la contraseña ya

[24] http://www.seguridadsap.com/sap/tipos-de-usuario-en-sap/

cambiada y configurada, no la definida por Grupo Nutresa. Adicionalmente debe poseer instalado en su máquina el SAPgui[25] y a su vez el SAP Logon[26] de Grupo Nutresa lo que lo hace más complejo de realizar. El riesgo se identifica más puntualmente para los usuarios internos ya que estos poseen ingreso a la red, generalmente poseen el SAPgui instalado y el SAP Logon en sus máquinas de trabajo. Es importante tener en cuenta estos elementos, dado que el pensamiento general es considerar que los incidentes informáticos son causados por elementos externos y esto se da gracias a la confianza que se le otorga al empleado, sin embargo las estadísticas contradicen esta teoría:

Figura 10. Tipos de Intrusión



Fuente: http://www.cybsec.com

"Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar."[27]

Dado a esto se debe estudiar el modelo de seguridad actual y los conceptos que se poseen sobre el mismo para entender cuáles son los puntos a mejorar y

[25] SAP GUI: es el cliente universal de SAP para acceder a las funcionalidades de SAP en las aplicaciones de SAP tales como SAP ERP, SAP Business Suite, SAP Business Intelligence. http://scn.sap.com/community/gui

[26] SAP Logon: es el programa de windows que se utiliza para ingresar en un sistema SAP en sistemas operativos Windows. Este media entre el sistema SAP y la interfaz de usuarios. El SAP Logon muestra una lista de los sistemas SAP disponibles y automáticamente selecciona los servidores con el mejor tiempo de respuesta actual.
http://help.sap.com/saphelp_470/helpdata/en/c4/3a6466505211d189550000e829fbbd/content.htm

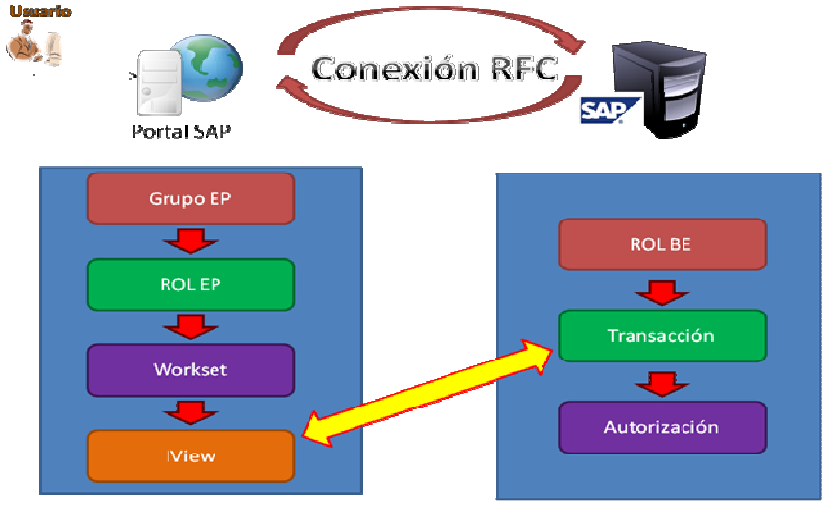
[27] http://www.segu-info.com.ar/amenazashumanas/amenazashumanas.htm

establecer un modelo que mitigue esta situación y permita establecer las autorizaciones tal como lo recomiendan los expertos.

1.1 MODELO DE AUTORIZACIONES ACTUAL:

El proceso de implementación del portal adoptó el concepto donde obligatoriamente un servicio expuesto en el portal debía poseer una transacción asociada en el sistema Back End (servicios tipo ITS[28]), en otras palabras, si por medio del portal se quisiera consultar la cartera, el servicio debería conectar con el sistema Back End a la transacción SAP asociada para este fin y utilizar todas las autorizaciones que implican ejecutar dicha transacción.

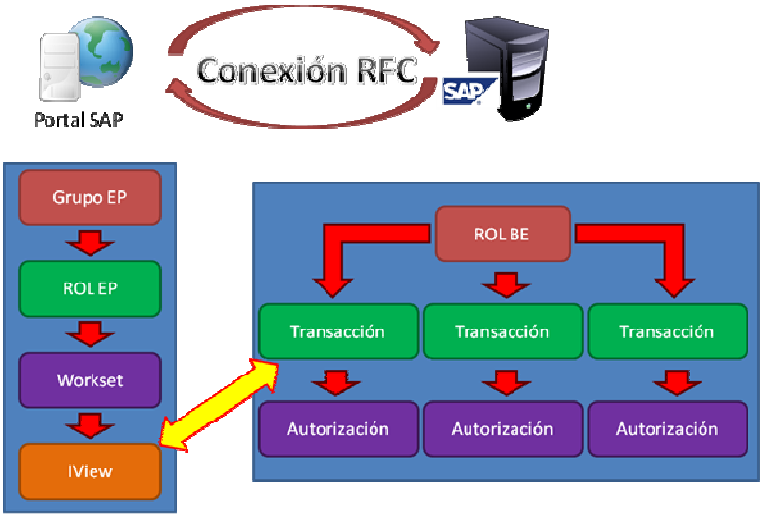
Figura 11. Concepto de ITS en SAP.



Este concepto implica que si se tiene asignada esta transacción y esta está agrupada con otras transacciones, además de asignarle al usuario en el sistema Back End la transacción necesaria, se asignan más permisos de los necesarios en el sistema.

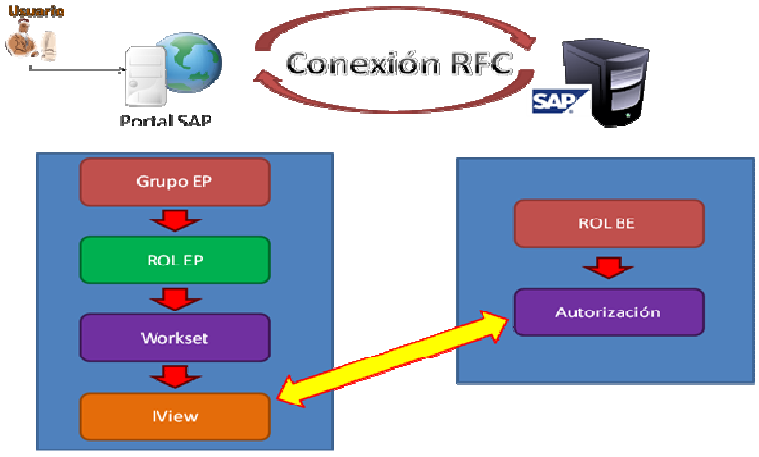
[28] ITS: Internet Transaction Services, este tipo de aplicaciones son usadas para representar pantallas transacciones SAP en pantalla como páginas web (HTML) en internet.

Figura 12. Esquema Rol BE



Después de varias investigaciones y de varias pruebas, se identificó que este concepto no era necesario para todos los servicios y que no es necesario tener la transacción asociada en los sistemas Back End para un servicio como tal. Esto se debe a que muchos de los servicios son consultas construidas de manera particular o a la medida, lo que hace que simplemente se necesite traer ciertos elementos del sistema Back End, no la transacción completa. Esto implica dentro del esquema, que en estos casos el servicio no apunte contra la transacción sino que solicite autorización sobre los elementos que conforman este servicio, en otras palabras, si deseo ver la factura en un reporte de cartera debo solicitar autorización sobre las tablas del modulo de cartera que poseen este campo:

Figura 13. Esquema ROL BE (Autorización)



Con estas oportunidades de mejora identificadas se sugiere el siguiente modelo de seguridad.

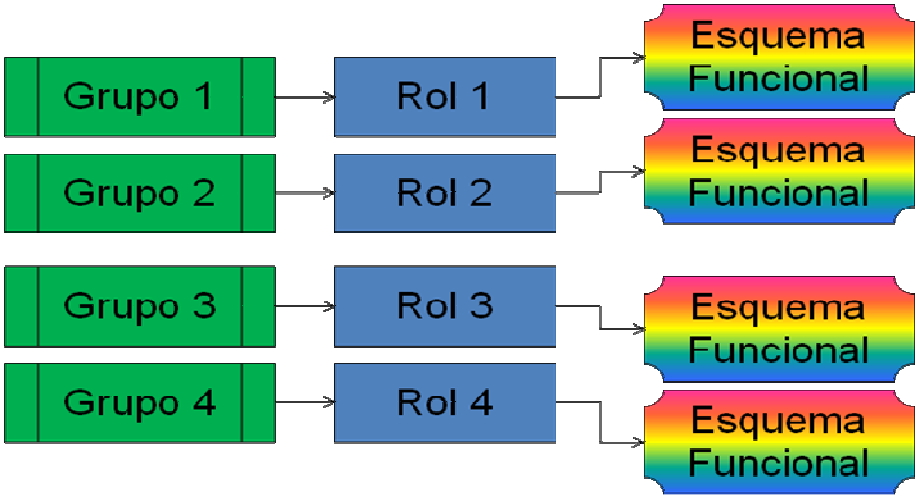
2. MODELO DE SEGURIDAD DE ROLES SIMPLES.

Como se estableció anteriormente el modelo de seguridad consta de Grupos en el portal y roles en los diferentes Back End para funcionar. Actualmente se tienen una gran variedad de Grupos en el portal implementados, 67 grupos en total.

Esto significa que tenemos 67 grupos simples. Sin embargo estos grupos pueden contener 1 o más ROLES EP. Se propone separar estos servicios y crear un grupo por ROL EP para tener grupos simples que nos faciliten la relación servicio – GRP EP.

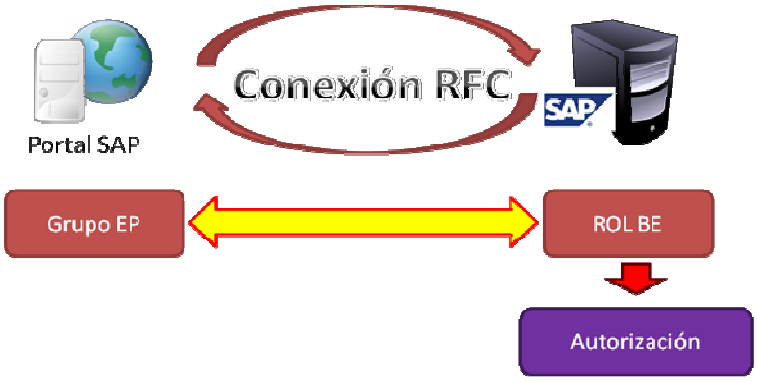
Para tal fin se propone que para la seguridad del Portal de Grupo Nutresa se relacionen los 67 grupos de la siguiente manera:

Figura 14. Esquema de Roles Simples



Adicionalmente se sugiere llevar este esquema incluso hasta los sistemas Back End, asignando un ROL BE que posea todas las autorizaciones necesarias para ejecutar el proceso:

Figura 15. Esquema de Roles Simples Extendido



Con esta extensión, se genera una relación directa y clara entre los accesos que se habilitarán en la herramienta portal y los diferentes Back End.

Con esta extensión se establecería una relación directa entre el servicio o aplicación con su ROL EP, su GRP EP y su ROL BE. Este esquema le permite al equipo funcional, administradores de negocios y equipo de seguridad identificar de manera más clara cada servicio y diseñar los ROLES GN con los servicios necesarios sin tener mayor conocimiento técnico del sistema.

Con la adopción de este concepto eliminamos el conflicto de asignaciones adicionales y concentramos las autorizaciones exclusivamente al servicio específico, tal como se establece en la definición de usuario tipo servicio.

Sin embargo cuando el servicio es una ITS, se conserva el conflicto, se sugiere realizar una estructuración de los ROLES BE para que estos solo posean la transacción que se requiere para el servicio. Es entendible que esto genere un conflicto con la mejor practica que establece que una transacción solo debe estar en un ROL BE, pero se garantiza la relación única entre el Back End y el portal, una mejor administración y adicionalmente elimina el conflicto de exceso de autorizaciones, lo que se considera una ganancia significativa frente a la situación actual.

Una vez aplicadas las recomendaciones establecidas anteriormente el resultado final se puede observar en la siguiente matriz:

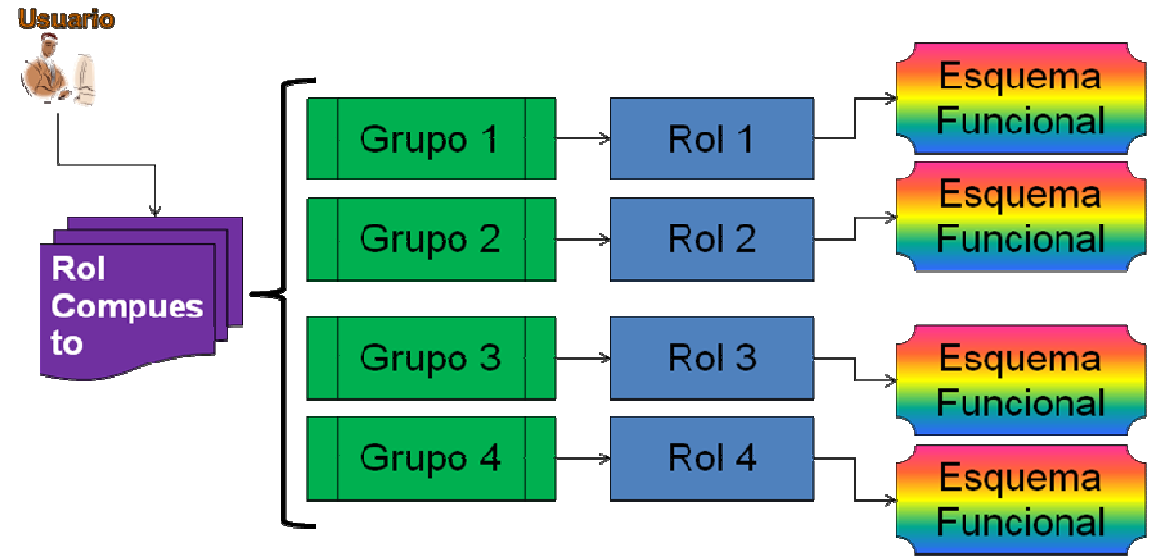
ANEXO 13. Matriz de seguridad de Roles Simples

Como se mencionó anteriormente los grupos están constituidos por varios Roles. Este esquema se debe conservar dado que esto es lo que constituye los Roles GN actuales. Para conservar esta estructura se definen los roles compuestos.

3. MODELO DE SEGURIDAD DE ROLES COMPUESTOS.

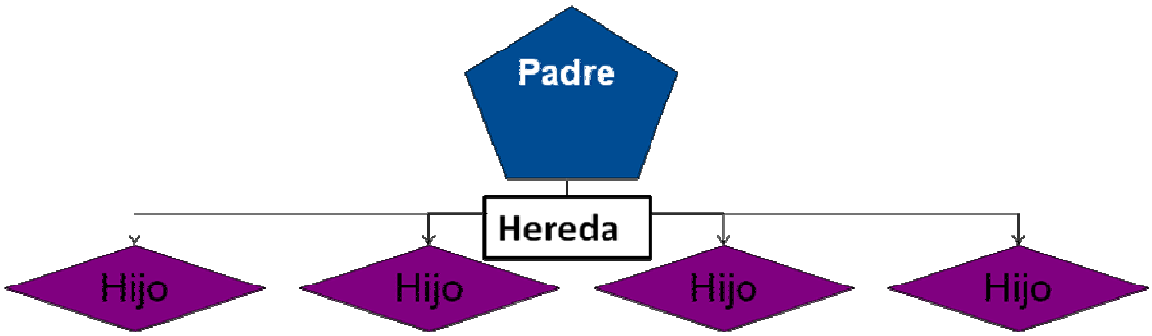
El objetivo del modelo de seguridad de roles compuestos es agrupar los roles simples para minimizar el número de asignaciones en el sistema, esto simplifica potencialmente la administración y adicionalmente permite un acercamiento más tangible a los ROLES GN.

Figura 16. Modelo de Rol Compuesto



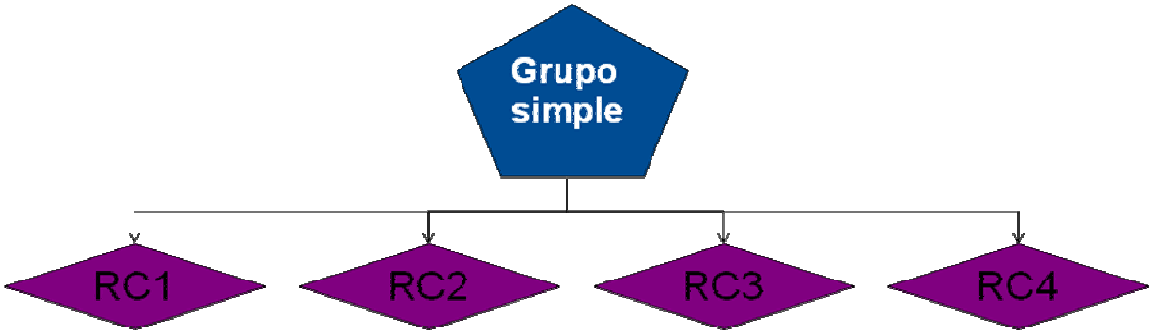
Para entender el funcionamiento de un Rol compuesto debemos aclarar el concepto de lo que es la herencia. Según la definición de la Real Academia de la Lengua la herencia son “Rasgo o rasgos morales, científicos, ideológicos, etc., que, habiendo caracterizado a alguien, continúan advirtiéndose en sus descendientes o continuadores”. En otras palabras la herencia es la facultad de poseer las características o propiedades de su progenitor:

Figura 17. Concepto de herencia



Los roles compuestos la propiedad de la herencia. El rol compuesto hereda todos los permisos que poseen los grupos simples, en otras palabras cuando un rol compuesto agrupa muchos roles simples, este está heredando las propiedades de cada uno haciendo esto al rol simple el padre y el rol compuesto el hijo:

Figura 18. Herencia en roles compuestos



Es importante tener en cuenta que las necesidades de cada negocio son diferentes, esto quiere decir que un negocio solo debe tener acceso a la información de su negocio, así como también un rol compuesto para un negocio puede poseer grupos simples diferentes a otro; a este fenómeno lo llamamos segmentación.

Figura 19. Segmentación por información

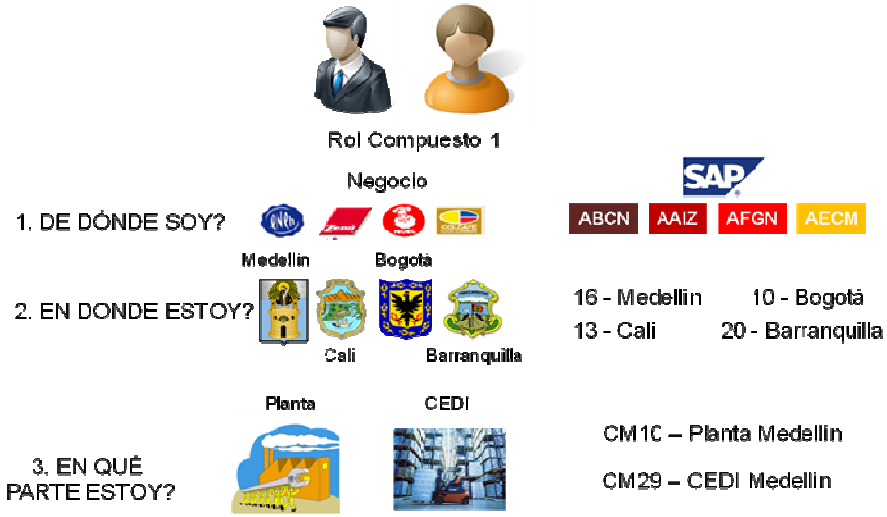
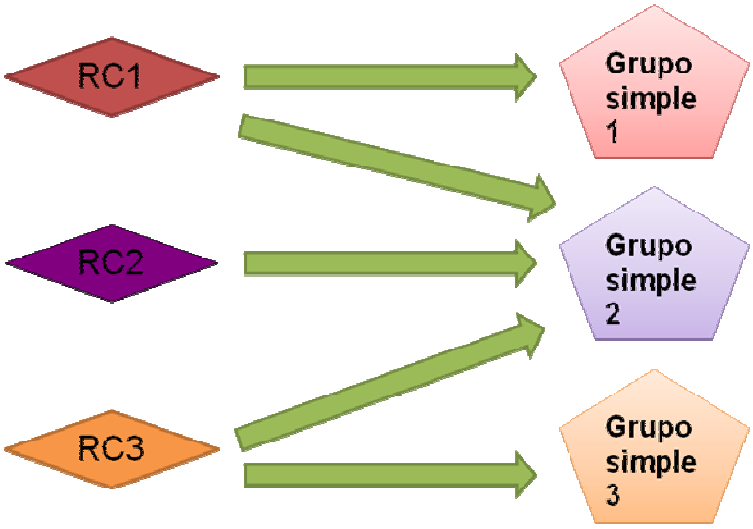


Figura 20. Segmentación por servicio



Aplicando estos conceptos al Anexo 13 obtenemos la agrupación de los grupos simples en roles compuestos y el acercamiento que deseamos al ROL GN.

ANEXO 14. Matriz de seguridad de Roles Compuestos

4. NOMENCLATURA

4.1. OBJETOS DE PORTAL.

El estándar de identificación de Objetos de portal es de máx. 20 caracteres:

Z_XX_YY_ZZA_BBBBBBBB = 20 caracteres

Los objetos deben tener la siguiente nomenclatura:

Tabla 12. Nomenclatura objetos de portal

Posición	Número de caracteres	Valor	Descripción	Carácter
1-2	2	Z_	Diferencia el objeto definido por Grupo Nutresa de los estándar definidos por SAP	Fijo

Posición	Número de caracteres	Valor	Descripción	Carácter
3-5	3	XX	Identifica el módulo del sistema al cual tendrá acceso el objeto asociado, reemplazar XX por alguno de los siguientes valores según corresponda: EP_: Enterprise Portals R3_: Enterprise Resource Planning BI_: Business Intelligence NP_: New Product Development and Introduction SC_: Supply Chain Management BC_: Basis Components LN_: Lotus Notes Nótese que el carácter "_" hace parte de la descripción del tipo.	Variable
6-8	3	YY	Identifica el tipo objeto de portal al cual se asocia, reemplazar YY por alguno de los siguientes valores según corresponda: WK_: Workset IW_: Iview PG_: Página RL_: Rol GR_: Grupo CP_: Carpeta TD_: Traducción TP_: Transporte Nótese que el carácter "_" hace parte de la descripción del tipo.	Variable
9-10	2	ZZ	Identifica el módulo del portal al cual se asocia el objeto, reemplazar ZZ por alguno de los siguientes valores según corresponda: CL: Cliente PR: Proveedor IN: Interno	Variable
11-12	2	A	Identifica la categoría del modulo del portal al cual se asocia el objeto, reemplazar A por alguno de los siguientes valores según corresponda: N_: Nacional I_: Internacional T_: Interno	Variable

Posición	Número de caracteres	Valor	Descripción	Carácter
			Nótese que el carácter "_" hace parte de la descripción del tipo.	
13-20	8	BBBBBBBB	Nombre corto para describir el servicio que se proveerá con el objeto asociado.	Libre

4.2. ROLES SIMPLES.

Los roles simples de portal en los sistemas Back End pueden tener o no transacciones. Son la única excepción en el sistema que puede contener transacciones ya asignadas en el sistema ERP.

Los roles simples deben tener la siguiente nomenclatura:

Tabla 13. Nomenclatura roles simples

Posición	Número de caracteres	Valor	Descripción	Carácter
1	2	Z_	Diferencia el grupo de actividad definido por el Grupo NUTRESA de los estándar definidos por SAP	Fijo
3-5	3	EP_	Identifica que el grupo de actividad pertenece al modulo Enterprise Portals.	Fijo
6-12	7	A…D	En 7 caractéres se debe especificar la actividad principal del Rol. Ej: Crear, modificar, borrar entre otros.	Libre
13	1	"_"	Carácter especial fijo	"_"
14-27	14	A…D	En el resto del campo se debe colocar servicio al cual está asignado el Rol hasta donde alcance en 14 caracteres ej: Gestionar ventas directas, comprar materiales y servicios, dar conformidad de pagos. Entre otros.	Libre
28	1	"_"	Caracter especial fijo	"_"
29-30	2	XX	Últimos 2 caracteres: descripción del tipo de rol: Maestro, básico, segmentado, donde XX es: 00 = Maestro NS = No segmentado BA = Básico	

Posición	Número de caracteres	Valor	Descripción	Carácter
			01…0n = Segmentado	

4.3. ROLES COMPUESTOS.

Los roles compuestos del portal contienen todos los roles simples que requiera un usuario para ejecutar sin problemas sus funciones en los sistemas Back End y sistema portal con su segmentación respectiva.

Los roles compuestos deben tener la siguiente nomenclatura:

Tabla 14. Nomenclatura Roles compuestos

Posición	Número de caracteres	Valor	Descripción	Carácter
1	2	Z_	Diferencia el grupo de actividad compuesto definido por el Grupo NUTRESA de los estándar definidos por SAP	Fijo
3-5	3	RC_	Identifica que el grupo de actividad es un grupo de actividad/rol compuesto.	Fijo
6-12	7	A…D	En 7 caracteres se debe especificar el código del rol en papel al que se asocia el grupo de actividad compuesto Ej: ROLEP01, ROLEP02, etc.	Libre
13	1	"_"	Carácter especial fijo	"_"
14-16	3	XXX	Identifica el tipo de usuario al que está asociado el grupo / rol compuesto. Reemplazar XXX por alguno de los valores siguientes según corresponda: CLI: Cliente PRV: Proveedor VEN: Vendedor ADM: Administrador GDC: Gestión Documental	Variable
17	1	"_"	Carácter especial fijo	"_"
18-26	8	A…D	En 8 caracteres se debe especificar la clasificación del tipo de usuario al que esta asociado el grupo/rol compuesto Ej: NACIONAL, INTERNAL, EJECUTIV, etc.	Libre

<table>
<tr><th>Posición</th><th>Número de caracteres</th><th>Valor</th><th>Descripción</th><th>Carácter</th></tr>
<tr><td>17</td><td>1</td><td>“_”</td><td>Carácter especial fijo</td><td>“_”</td></tr>
<tr><td>-30</td><td>4</td><td>ABCD</td><td>Identifica a que compañía está asociada la segmentación incluida dentro del grupo / rol compuesto. Reemplazar ABCD por alguno de los valores siguientes según corresponda:

<table><tr><th>Empresa</th><th>Código</th></tr><tr><td>Blue Ribbon Product S.A</td><td>AABR</td></tr><tr><td>Ernest Berart S.A.</td><td>AAEB</td></tr><tr><td>Alimenticia Hermo de Venezuela</td><td>AAHV</td></tr><tr><td>Industria Alimentos ZENU S.A.S</td><td>AAIZ</td></tr><tr><td>Alimentos Cárnicos S.A.S</td><td>AANN</td></tr><tr><td>Setas Colombianas S.A</td><td>AASE</td></tr><tr><td>Alimentos Cárnicos Zona Franca</td><td>AAZF</td></tr><tr><td>Compañía Nac Chocolate DCR S.A</td><td>ABCC</td></tr><tr><td>Compañía Nac Chocolates S.A.S</td><td>ABCN</td></tr><tr><td>Compañía cacao PERÚ S.A</td><td>ABCP</td></tr><tr><td>Compañía Nac Choc PERÚ S.A</td><td>ABFP</td></tr><tr><td>Nutresa S.A de C.V</td><td>ABNU</td></tr><tr><td>Serer S.A de C.V</td><td>ABSR</td></tr><tr><td>Prod Alimenticios Doria S.A.S</td><td>ACDR</td></tr><tr><td>Pastas COMARRICO S.A</td><td>ACPA</td></tr><tr><td>Alimentos de CO S.A (Meals)</td><td>ADML</td></tr><tr><td>Industrias Aliadas S.A.</td><td>AEAL</td></tr><tr><td>Tropical Coffee Company S.A.S</td><td>AEBS</td></tr><tr><td>Ind Colombiana de Café S.A.S</td><td>AECM</td></tr><tr><td>Compañía galletas NOEL CR S.A</td><td>AFCG</td></tr><tr><td>F. Foods INC</td><td>AFFF</td></tr><tr><td>Compañía Galletas NOEL S.A.S</td><td>AFGN</td></tr><tr><td>Molinos Santa Marta S.A.S</td><td>AFMS</td></tr><tr><td>Distrib Tropical Nicaragua</td><td>AFPN</td></tr><tr><td>Galletas de Pozuelo Panamá S.A</td><td>AFPP</td></tr><tr><td>Galletas de Pozuelo DCR S.A</td><td>AFPZ</td></tr><tr><td>Cordialsa NOEL de Venezuela</td><td>AFVI</td></tr><tr><td>Cordialsa Boricua S.A</td><td>AGBC</td></tr></table></td><td>Variable</td></tr>
</table>

Posición	Número de caracteres	Valor	Descripción		Carácter
			Cordialsa CR S.A Costa Rica	AGCD	
			Cordialsa Colombia S.A.S	AGCO	
			Cordialsa Ecuador	AGEC	
			Cordialsa Guatemala	AGGC	
			Cordialsa Honduras	AGHC	
			La Recetta Sol Gastron. Int SA	AGLR	
			Cordialsa Mexico S.A de C.V	AGMC	
			Cordialsa Nicaragua S.A.	AGNC	
			Novaventa S.A	AGNO	
			Cordialsa Panamá	AGPC	
			Cordialsa Salvador	AGSC	
			Cordialsa USA INC	AGUC	
			Dulces de Colombia S.A.S	CBDU	
			Inversiones Saronis S.A	FAIS	
			Proveg Investments S.A.	FDRE	
			Distribuidora Maple S.A	FHDM	
			F. Holdings LLC	FHFH	
			Grupo Nutresa S.A.S	FHIA	
			Inversiones Maple S.A.	FHIM	
			Inversiones Proveg S.A.	FHIP	
			Portafolio de Alimentos	FHPR	
			Valores Nacionales S.A.S	FHVN	
			Fundación Grupo Nutresa S.A.S	LJFI	
			Litoempaques S.A.S	MFLT	
			Gestión Cargo Zona Franca SAS	SAGZ	
			Servicios Nutresa S.A.S	SISS	

ESTADO FINAL: PROPUESTAS DE PROCEDIMIENTOS DE ADMINISTRACIÓN DE PERFILES DE PORTAL.

Nota: como se mencionó anteriormente la palabra administración implica creación, modificación y eliminación de perfiles de portal.

Premisas:

1. Las pruebas de seguridad se realizan ingresando por el portal de desarrollo.

2. La creación y ajustes de ROLES BE se realizan en el sistema 120 de cada Back End (Excepción Business Intelligence)

3. La creación de usuarios y asignación de permisos se realizan en el sistema SOLMAN[29].

4. Las pruebas de seguridad en calidad se realizan en el portal de calidad y en el mandante 200 de cada Back End (Excepción Business Intelligence que no posee ambiente de calidad)

[29] SOLMAN: Solution Manager es una plataforma central, integral punto a punto cuya función es permitir a los clientes de SAP adaptarse a nuevos desarrollos de manera más ágil, administrar el ciclo de vida de las aplicaciones y correr soluciones SAP.

1. PROCEDIMIENTO DE CREACIÓN DE PERFILES DE PORTAL

Figura 21. Procedimiento de creación de perfiles de portal (1)

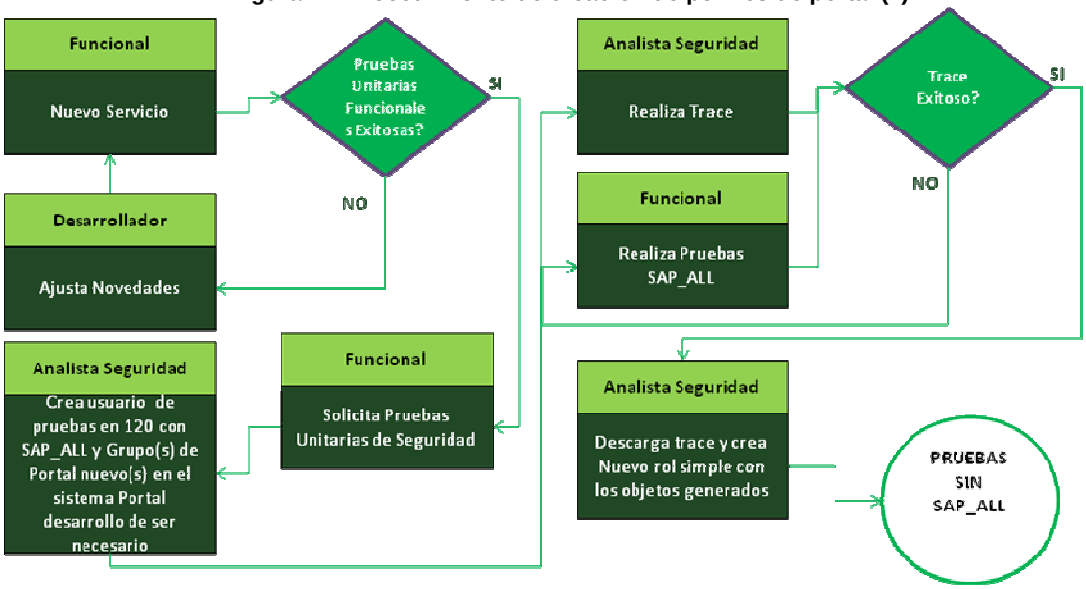
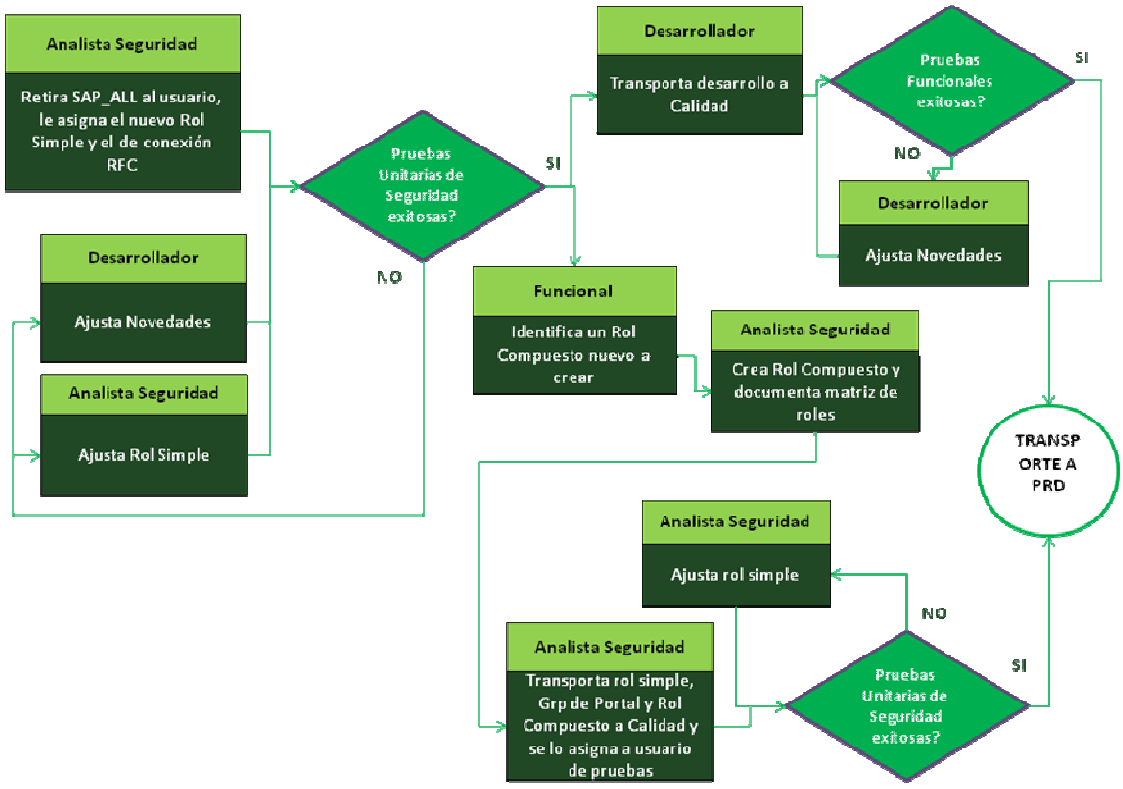


Figura 22. Procedimiento de creación de perfiles de portal (2)



2. PROCEDIMIENTO DE MODIFICACIÓN DE PERFILES DE PORTAL

Figura 23. Procedimiento de modificación de perfiles de portal (1)

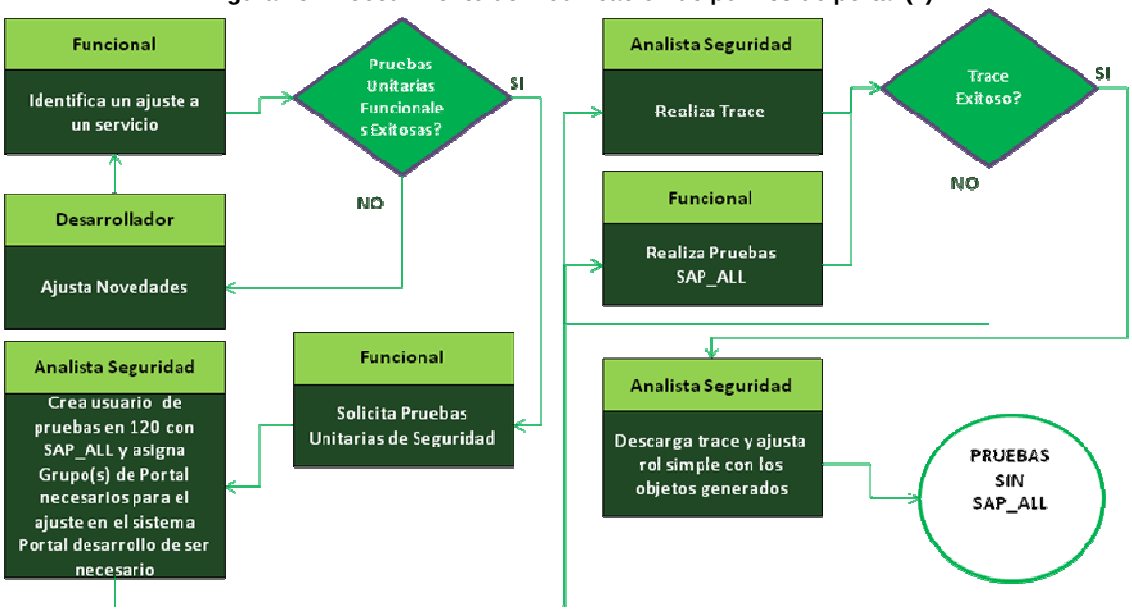
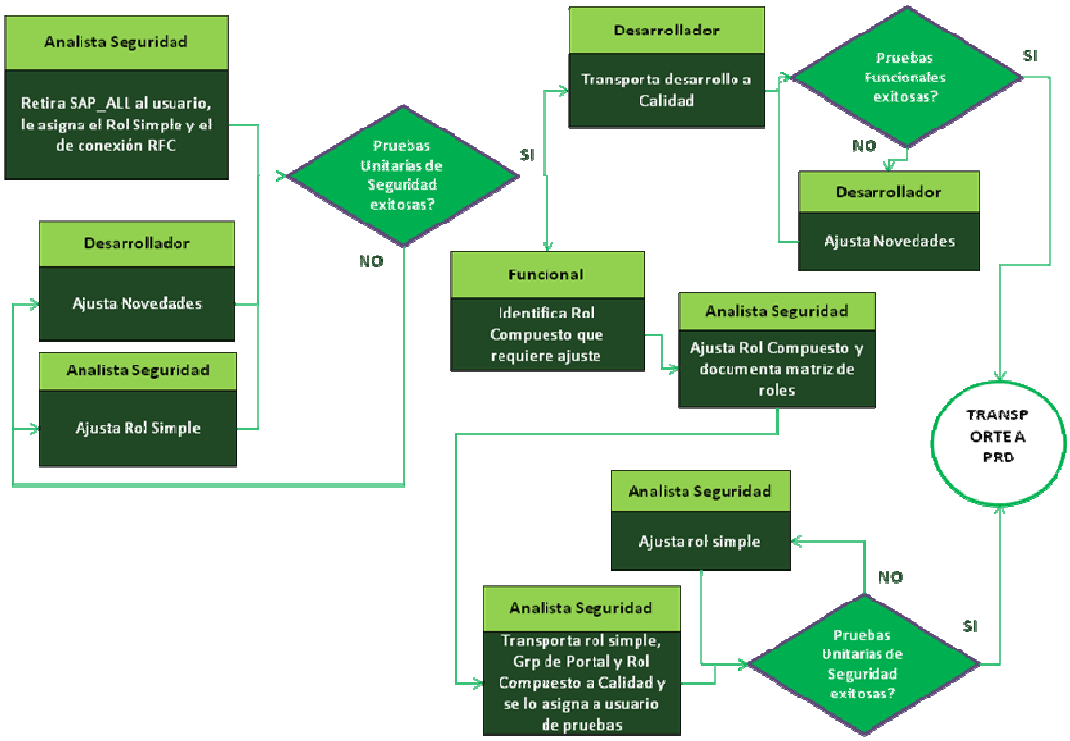
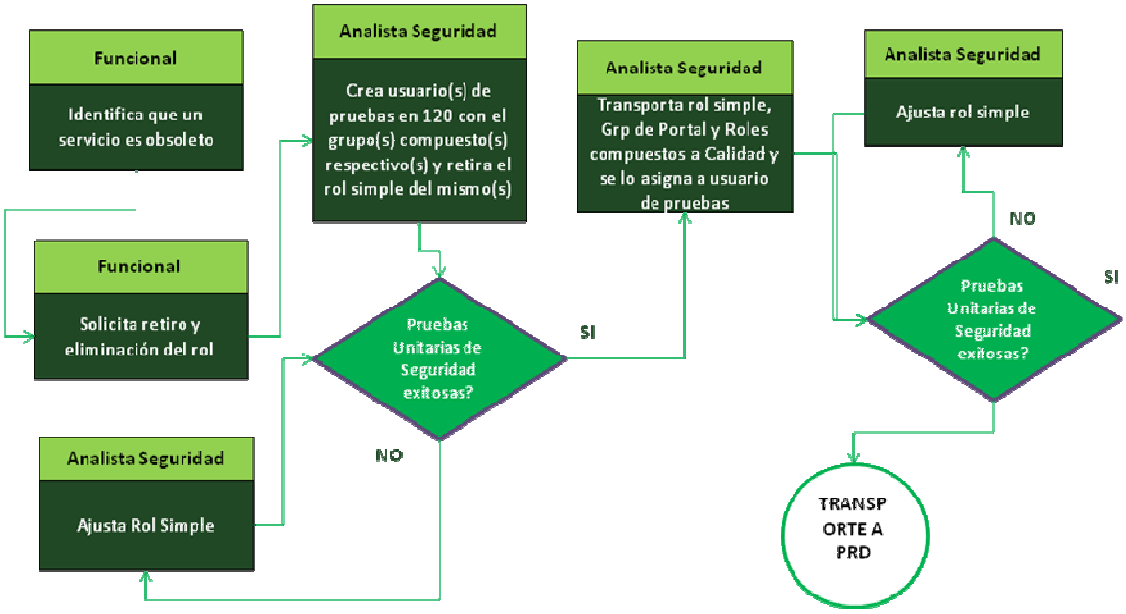


Figura 24. Procedimiento de modificación de perfiles de portal (2)



3. PROCEDIMIENTO DE ELIMINACIÓN DE PERFILES DE PORTAL

Figura 25. Procedimiento de Eliminación de perfiles de portal



CONCLUSIONES.

El presente trabajo de grado exploró la utilización de las recomendaciones indicadas en la Norma Técnica Colombiana 5254 y la ISO 31000, guiándose por las experiencias y lineamientos establecidos por el área de riesgos de Grupo Nutresa para el análisis de riesgos en el portal de Grupo Nutresa.

Al aplicar las distintas recomendaciones, se identificó que la aplicación de la metodología utilizada por el Grupo Nutresa debía realizársele ciertas modificaciones dado que, la utilización de la metodología, está enfocada en procesos de producción de alimentos, y los procesos de TI deben ser analizados de manera distinta.

Con esta metodología ajustada se lograron detectar varias mejoras y elementos a destacar dentro de los modelos utilizados actualmente para la administración del sistema y la interacción que se presenta dentro de los equipos de trabajo.

Es importante anotar que al ya tener unas experiencias y modo de trabajo para el levantamiento de riesgos en el Grupo Nutresa, salirse del estado de confort de esta metodología implicó un esfuerzo adicional, dado que adaptar la metodología sin salirse de los límites establecidos por la misma no fue fácil de lograr.

Con este trabajo de tesis se logró identificar que las metodologías para la obtención de datos por medio de entrevista generalmente pueden llevar mucho tiempo, sobre todo cuando la prioridad de la ejecución de esta actividad no es la más alta. Coordinar los tiempos es complejo, de igual manera lograr una participación activa de los miembros del equipo.

El tener poca información estadística implicó basarse en las experiencias de los miembros del equipo, lo que no es información 100% fidedigna, lo que lleva a que los resultados de esta tesis sean de carácter cualitativo.

Varios de los riesgos de mayor valoración identificados para análisis que se estimaban fueran clasificados dentro del esquema de ataques informáticos, fueron clasificados dentro de elementos de comunicación, claridad de procedimientos y elementos de trabajo en equipo, otorgando una visión diferente sobre la realidad e inclinando la balanza a realizar acciones a nivel administrativo y no técnico. Esto significa que para lograr un mejor desempeño sobre los procesos actuales del portal, se requiere de un mayor compromiso por parte de los involucrados en los diferentes procesos, así como un análisis más exhaustivo sobre los procedimientos actuales.

El análisis del riesgo es un proceso que puede llegar a ser de mucha profundidad, de allí que el alcance del mismo debe ser claramente establecido desde el inicio, ya que en el camino se pueden identificar muchas fuentes de riesgo que pueden desviar el objeto de análisis.

El análisis del control del riesgo cuando se detecta que la fuente del mismo es la carencia o ausencia de un elemento es más simple de realizar, el control se fundamenta en suplir esa ausencia, sin embargo cuando la causa es la no utilización de un elemento o la mala utilización del mismo, los controles suelen ser de carácter más administrativo, lo que implica un alto compromiso de los participantes en el proceso.

BIBLIOGRAFÍA

Antonio Vieyra, G. C. (s.f.). *ASAP MODELO DE IMPLANTACIÓN DE SAP R/3*. Recuperado el 24 de Enero de 2010, de http://innovaar.net/uriel/wp-content/uploads/2008/11/asap-modelo-de-implatancion-sap-r3.doc
C. S. (2010). *Cisco 2010 Annual Security Report.* Reporte Anual, San Jose.

CORPONOR. (s.f.). *RESUMEN NORMA TECNICA COLOMBIANA NTC 5254.* Recuperado el 16 de Noviembre de 2013, de http://www.corponor.gov.co/: http://www.corponor.gov.co/NORMATIVIDAD/NORMA%20TECNICA/Norma%20T%E9cnica%20NTC%205254.pdf

G. S.-I. (s.f.). *Segu-Info*. Recuperado el 28 de 10 de 2011, de Noticias de Seguridad Informática: www.segu-info.com.ar/blogger/blogger.htm

Gil Sepúlveda, V., & Teruel García, X. (s.f.). *Hackers y Virus Informativos Historia de la informática*. Recuperado el 29 de Mayo de 2007, de Xavier Teruel: Pagina de Inicio:
http://personals.ac.upc.edu/xteruel/fib/asig/asai/presentacion.hackers.y.virus.pdf

Grupo Nutresa S.A. (s.f.). *Estructura del grupo | Grupo Nutresa. Compañía de fabricación y comercialización de alimentos*. Recuperado el 22 de Noviembre de 2013, de http://www.gruponutresa.com/es/content/estructura-del-grupo.

ISO. (s.f.). *ISO*. Obtenido de ISO 31000:
http://www.iso.org/iso/home/standards/iso31000.htm

Núñez Sandoval, A. (s.f.). *Estándares de seguridad en la información*. Recuperado el 29 de Mayo de 2007, de Enter@te:
http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

Off, F., & Linkies, M. (2006). *SAP Security and Authorizations* (Primera Edición ed.). Alemania: Galileo Press.

Olivares, J. (s.f.). *Actualización ISO/IEC 17799:2005 (E) En el año del Profesional de la Información*. Recuperado el 2007 de Mayo de 29, de Universidad Tecnica Federico Santa Maria:
http://cibsi05.inf.utfsm.cl/presentaciones/empresas/Neosecure.pdf

P. P. (s.f.). *Internet y la World Wide Web*. Recuperado el 27 de 05 de 2007, de Para Libros Medios: http://www.paralibros.com/passim/p20-tec/pg2052ci.htm

Ramírez, A. O. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, Vol. 16, No. 2* , 56-66.

Raymond, E. (s.f.). *Historia del hacking - Historias de hackers y hackeos*. Recuperado el 29 de Mayo de 2007, de La Covacha Underground: http://www.lcu.com.ar/historia/

S. C. (2010). *Symantec Internet Security Threat Report.* Mountain View.

SAP. (s.f.). *SAP - PLM Software | Product Lifecycle Management Solution*. Recuperado el 31 de 10 de 2011, de SAP PRODUCT LIFECYCLE MANAGEMENT (PLM): http://www.sap.com/solutions/business-suite/plm/pdf/BWP_NPDI_PLM_White_Paper.pdf

SAP. (s.f.). *Web Dynpro Architecture (SAP Library - Web Dynpro for ABAP)*. Recuperado el 23 de Noviembre de 2013, de http://help.sap.com/saphelp_nw04/helpdata/en/a5/1a1e3e7181b60ae10000000a114084/content.htm

Siles Peláez, R. (2002). *Analisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados.* Argentina.

Tanenbaum, A. S. (2003). *Redes de computadoras.* (G. Trujado Mendoza, Trad.) Mexico: Prentice- Hall.

W. F. (s.f.). *Wikipedia*. Obtenido de Wikipedia: www.wikipedia.com

WhiteHat Security, I. (2010). *WhiteHat Website Security Statistic Report* (Novena edición ed.). Santa Clara.

ANEXOS