UNIVERSIDAD DE BUENOS AIRES

Facultad de Ingeniería

Implantación de Sistemas (75.17)

Trabajo Práctico
Auditoría

Empresa Seleccionada: CEFAS S.A.

Integrantes

Ariel Diskenstein 83389
Christian Tagliapietra 80515
Gonzalo Soriano 84468
Sebastian D'Agostino 85155

2° Cuatrimestre 2010

Presentación de la empresa:

Misión

CEFAS SA es una empresa minera, de alcance nacional e internacional, con una política empresaria ética y responsable, comprometida con sus clientes, su gente y con la sociedad; cuya misión es Desarrollar, Producir y Comercializar productos de destacado valor para los sectores de la Construcción, la Industria y el Agro.

Hace especial hincapié en el valor que tienen sus empleados, los cuales ellos mismo definen como el activo más valioso de la empresa. A su vez, están convencidos que el cuidado del medio ambiente y de las condiciones de trabajo contribuirán al engrandecimiento de la empresa y al mejoramiento de la sociedad.

Historia

CEFAS SA nace en 1995 como parte de un destacado grupo empresario con gran experiencia en la Industria de la Construcción y la producción de cemento, que toma a su cargo la fabricación y comercialización de cal El Milagro en dos fábricas ubicadas en la provincia de Córdoba.
En 1997, adquiere canteras, plantas fabriles en Olavarría, provincia de Buenos Aires y las marcas de cal hidráulica Lougas y Feitis.
Un año más tarde amplía su campo de acción incorporando tres fábricas y canteras de cal aérea ubicadas en las provincias de Córdoba, Mendoza y San Juan, así como las prestigiosas marcas Sublime y Malagueño.
Asimismo se incorporan a la empresa yacimientos de sulfato de calcio, carbonato de calcio y carbonatos de calcio y magnesio e instalaciones fabriles en Zapala provincia de Neuquén.
Finalmente en el año 2009 se inaugura un nuevo establecimiento ubicado también en la provincia de San Juan en la pequeña localidad de Cienaguita, dicha planta cuenta con el horno de calcinación mas grande de sudamérica ampliando la capacidad de producción en 500 toneladas diarias.

Negocio

Actualmente trabajan cerca de 500 empleados y con una producción aproximada de 1000 toneladas por día es uno de los principales proveedores de cal en el país.

La empresa cuenta en la actualidad con cinco plantas de fabricación de cales y otros productos derivados situadas en:

- Olavarría, provincia de Buenos Aires.
- Quilpo, provincia de Córdoba.
- Los Berros, provincia de San Juan.
- CIenaguita, provincia de San Juan.
- Zapala, provincia de Neuquén.

A las cuales deben sumarse los depósitos ubicados en:

- Estación Sola, Ciudad Autónoma de Buenos Aires.
- Haedo, Ciudad de Haedo, provincia de Buenos Aires.

La estratégica ubicación de sus plantas y depósitos garantiza una logística de óptimos costos y alto grado de eficacia.

La producción se divide en distintos tipos de cales que finalmente se venden en 3 mercados distintos:
Construcción: es un material básico para las terminaciones de las obras.
Industrial: Es un insumo utilizado en diversas industrias siendo las más destacadas las siderurgias, el tratamiento de aguas y los ingenios azucareros.
Agro: Como fertilizante de suelos principalmente dedicados a la soja.

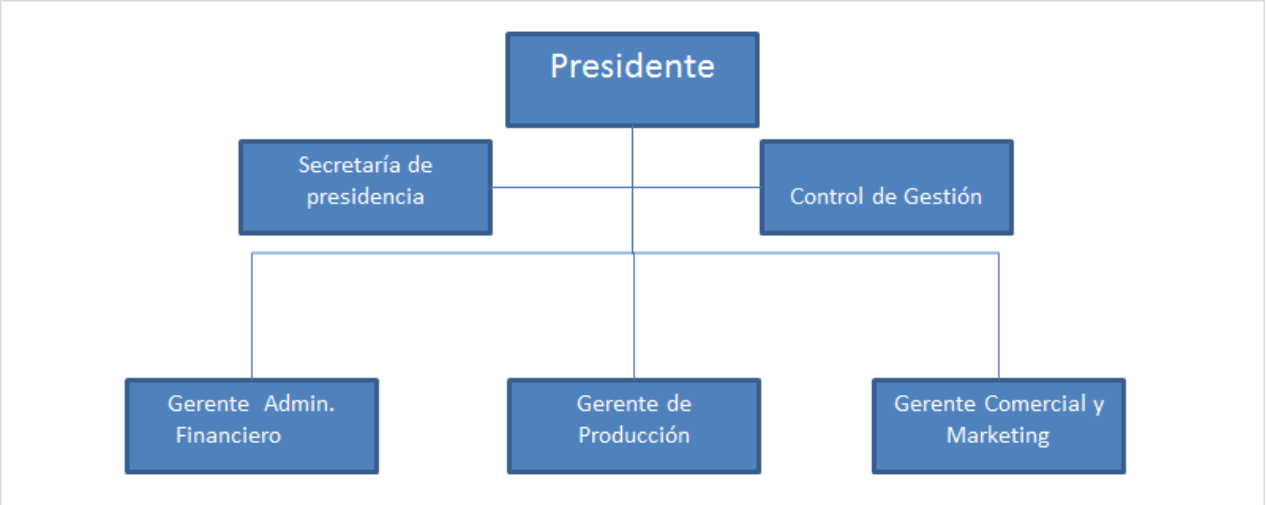
Actualmente se exportan de las distintas unidades de negocio materiales a Chile y Uruguay

Organigrama

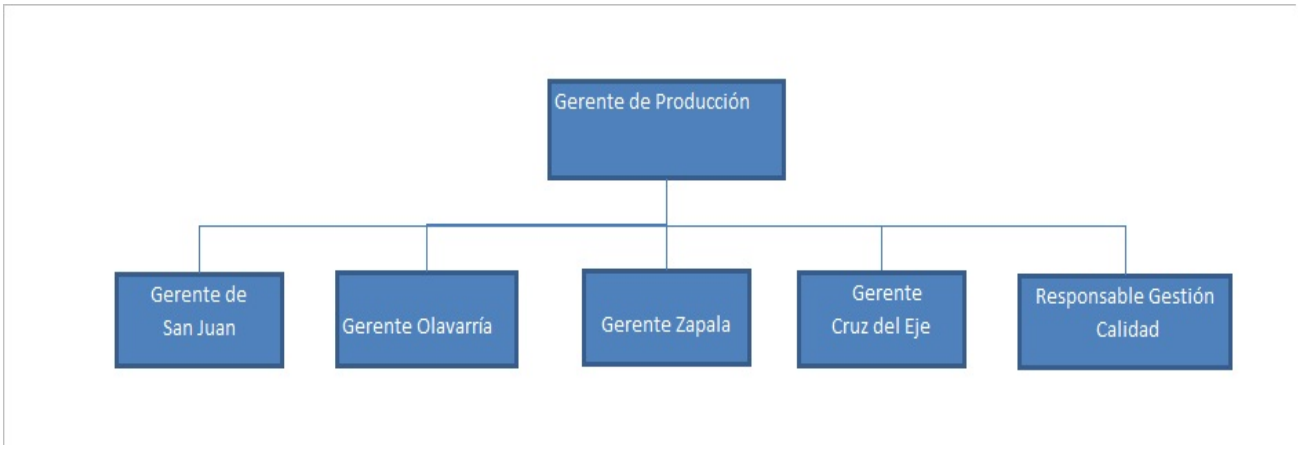
A continuación se presenta el organigrama de la empresa. Debido a su complejidad se presenta una versión prescindiendo de poner todos los centros de producción ya que tienen una estructura similar.
Para que sea comprendido correctamente El mismo se divide en las siguientes partes:

1) Alta dirección
2) Gerencia de producción
3) Gerencia Administrativo Financiera
4) Gerencia de Mercadeo y Logística
5) Planta de Producción.

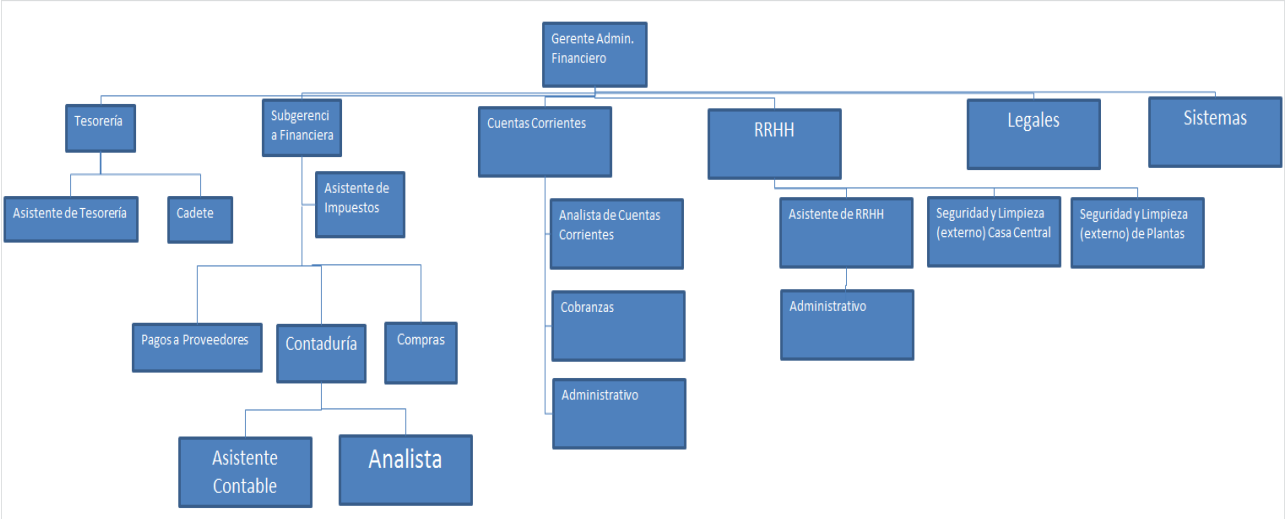
1) Alta Dirección



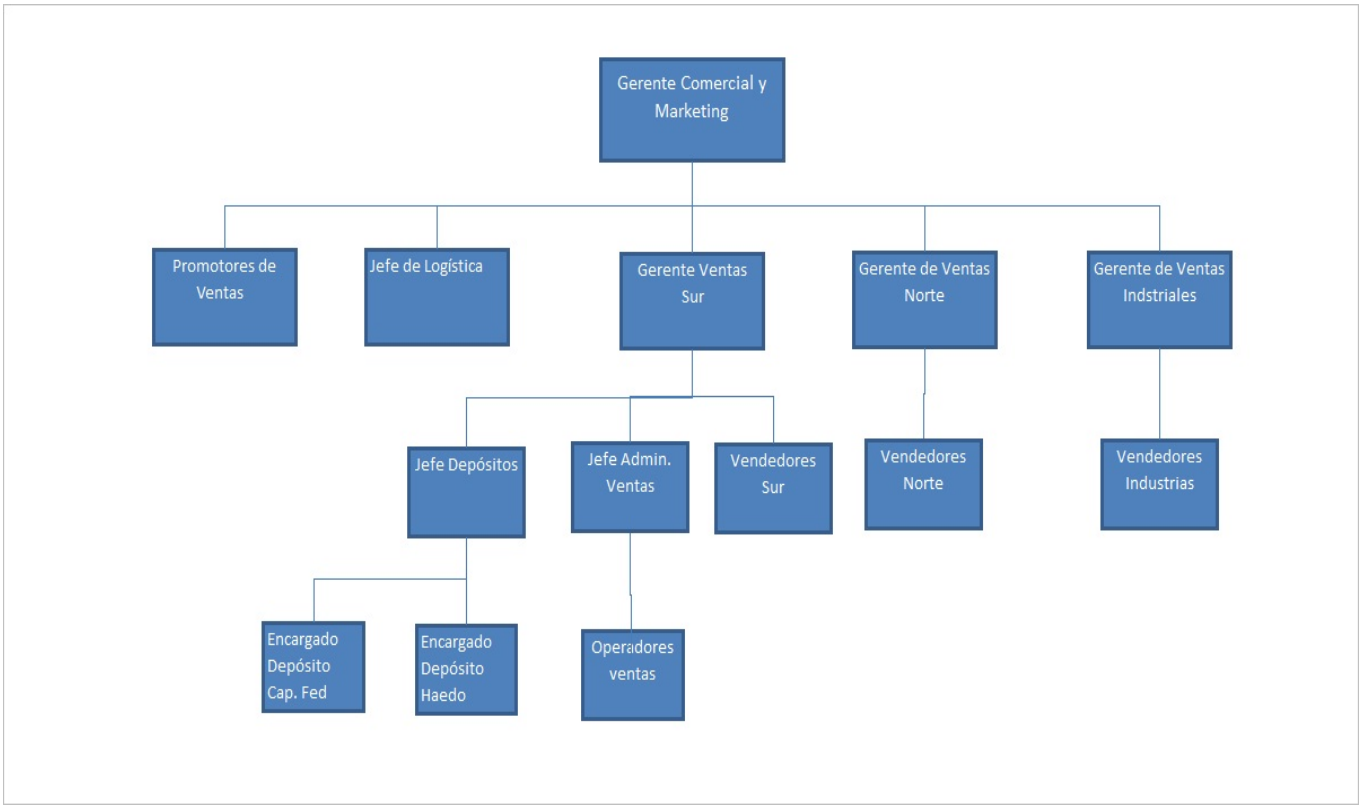
2) Gerencia de producción



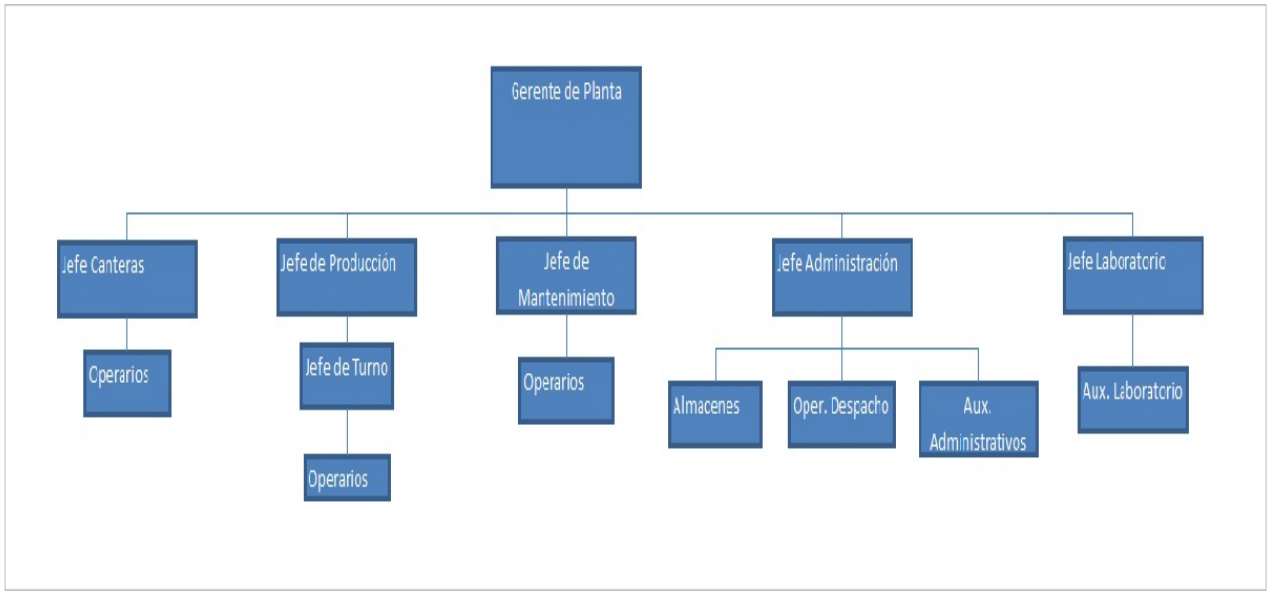
3) Gerencia Administrativo Financiera



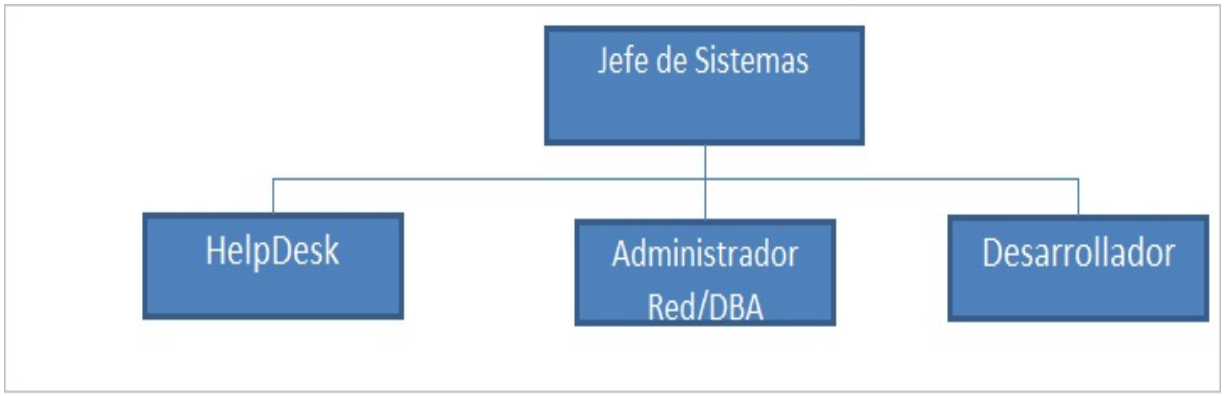
4) Gerencia de Comercial y Marketing



5) Planta de producción, se pone como ejemplo el establecimiento ubicado en la zona de Olavarría. El resto de las plantas, tiene una distribución similar.



6) Área de Sistemas



Infraestructura tecnológica

En el data center de las oficinas centrales se encuentra el servidor AS400 punto central de la gestión de la empresa. Adicionalmente existen servidores de plataforma x86 Intel para ofrecer servicio de e-mail, proxy para regular el acceso a internet, hosting de la web y archivos compartidos.
Los controles de acceso a los archivos e inicio de sesión en las PC se realizan mediante una infraestructura LDAP (Active Directory).
La seguridad con la red externa se limita con un firewall.
Los establecimientos de producción se comunican con las oficinas centrales mediante enlaces satelitales provistos por Global Crossing. Los mismos son lentos por lo tanto obligan a restringir el tráfico de Internet y priorizar el uso del sistema de gestión. Debido a la ubicación geográfica de las fábricas por el momento esta es la única forma de conexión confiable disponible.

Principales aplicaciones en producción

- **J.D. Edwards:** Sistema de gestión y planificación empresarial dedicado a la administración centralizada de toda la organización. Se caracteriza por ser altamente escalable, configurable y personalizable.
  Se encuentra instalado sobre una plataforma mainframe AS400. Actualmente se encuentran implementados los módulos de: contabilidad, finanzas, ventas, logística, compras, cuentas a pagar, cuentas a cobrar, almacenes e inventarios.

- **Condor:** Sistema para la administración de personal y RRHH, se encuentra instalado bajo Windows server 2003 con Oracle como base de datos. La administración y soporte de esta aplicación se encuentra totalmente tercerizada.

- **Administración de documentos ISO 9001***:* Sistema para administrar registros de la gestión de calidad. Estos documentos están almacenados en bases de datos bajo Lotus Domino. Esta plataforma permite que los registros puedan editarse de forma colaborativa o siguiendo algún workflow con un bajo tiempo de desarrollo.

- **Pesaje:** Las oficinas de despachos ubicadas en los establecimientos de producción cuentan con *sistemas de pesaje* para camiones externos a JDE.

- **Datawarehouse:** Se encuentra en desarrollo un datawarehouse para mejorar las decisiones estratégicas, comerciales y de marketing.

Planes de producción y mantenimiento: son manejados por pequeños sistemas instalados en las respectivas PCs de los jefes de cada área. Actualmente esos programas no son ni administrados ni se brinda soporte, de parte del área de sistemas.

Auditoría área de sistemas

Segregación de tareas en el área de sistemas:

Situación Actual	Riesgo Detectado	Posibles Consecuencias	Recomendación	Probabilidad de Ocurrencia
Incompatibilidad de funciones	Ante la ausencia del administrador de la red/DBA o jefe de sistemas, el help desk tiene acceso a los servidores y a los ambientes de producción para realizar alguna tarea puntual.	Accesos no autorizados y/o falta de capacitación para la administración de los sistemas y por ende potenciales problemas en los ambientes de producción o algún servidor.	Incorporar más personal y definir políticas ante la ausencia de algún integrante del equipo.	Medio
No existe un procedimiento de baja de usuarios	Accesos de ex empleados luego de su egreso.	Fraude o fuga de información.	Documentar el proceso de baja e informar sobre la importancia de que sea al momento de la desvinculación.	Alto
El desarrollador tiene acceso total al ambiente de producción.	Acceso no autorizado a información sensible.	Robo o fuga de información.	El acceso al ambiente de producción debe ser por Perfiles y el Desarrollador no debe tener un acceso total.	Alto
No hay controles de acceso al datacenter	La llave que abre la puerta, esta en poder de todo el personal de sistemas, no existen registros de ingresos y egresos.	Sabotaje de parte del propio personal sin posibilidad de determinar quien lo realizó.	Instalar cerraduras para el ingreso con controles de acceso biométricos. Instalar cámaras de seguridad.	Medio

Procedimientos de cambios de los programas:

Situación Actual	Riesgo Detectado	Posibles Consecuencias	Recomendación	Probabilidad de Ocurrencia
Procedimiento de cambio de los programas	No existe un procedimiento para el paso de ambiente de desarrollo a producción.	Errores en los programas a la hora de realizar ventas. Perjuicio económico	Desarrollar los manuales correspondientes	Bajo

Acceso general a los datos o programas de aplicación:

Situación Actual	Riesgo Detectado	Posibles Consecuencias	Recomendación	Probabilidad de Ocurrencia
Las contraseñas de todos los servidores se encuentran almacenadas en una base de datos encriptada.	Las contraseñas que desencriptan dicha base no se encuentran documentadas.	En caso de desvinculación de las personas que saben las contraseñas pueden quedar inutilizados los sistemas.	Documentar dichas contraseñas y entregárselas a la dirección de la empresa.	Media
Las contraseñas tienen una longitud mínima de 6 caracteres. Alfanuméricas y con al menos una mayúscula.	La longitud de 6 caracteres favorece el ataque por fuerza bruta.	Robo de contraseña, accesos no autorizados	Aumentar la longitud mínima a 8 caracteres.	Baja
Las contraseñas de acceso a la red caducan a los 30 días.	Ninguno	Ninguno	Ninguno	
Las sesiones de windows y de JDE se bloquean o cierran luego de 15 minutos de inactividad.	Ninguno	Ninguno	Ninguno	
Accesos VPN abiertos 24 hs	Accesos por VPN fuera del horario laboral.	- Accesos no permitidos y cambios sin autorización. - La red queda expuesta con ausencia de personal de sistemas.	Restringir el horario de acceso por usuario según la tarea que desarrollen. Los administradores mantienen acceso 24 hs.	Media
Accesos VPN solo con contraseña. (PPTP)	Los accesos tipo PPTP solo requieren contraseña (no certificados). Esto permite conectarse desde cualquier PC	Ingreso desde PCs con virus, falta de actualizaciones o no revisadas por el area de sistemas. Ingreso de personas no autorizadas con fines maliciosos.	Implementar la infraestructura de certificados digitales y cambiar el tipo de conexión a L2TP (contraseña y certificados).	Alta
Los perfiles de un usuario los define su respectivo gerente. Los perfiles quedan documentados.	Ninguno	Ninguno	Ninguno	

Publicación de estados de Cta Cte del cliente, bajo protocolo HTTP	Los clientes inician sesión en la web de la empresa para chequear el estado de sus cuentas bajo un protocolo no seguro (http).	Se puede interceptar la contraseña ya que la misma viaja en texto plano y así acceder a información confidencial.	Implementar protocolo SSL (HTTPS web segura)	Alto
La instalación de software no es sensitivamente controlada.	Los usuarios tienen permiso de administrador sobre la PC en la que trabajan, permitiendo la instalación de programas pagos sin licencia o maliciosos.	- Perjuicio económico ante entidades de software legal. - Posibilidad infección de virus o spyware y su posible propagación por la red de la empresa.	Restringir la instalación de software, estableciendo perfiles para acceso a la red.	Medio
Acceso a internet controlado y auditado a través de un proxy.	Ninguno	Ninguno	Ninguno	
No hay auditoría de acceso a archivos.	No existe control de auditoría sobre el acceso a archivos. Los accesos por parte de los administradores no quedan registrados.	Acceso a archivos confidenciales por personas no autorizadas. Fuga de información y problemas para determinar el responsable de una modificación o eliminación de un archivo	Habilitar el control de auditoría	Bajo
Existencia de firewall, antivirus y control de actualizaciones de windows.	Ninguno	Ninguno	Ninguno	
Se permite una sola sesión de JD Edwards por usuario	Ninguno	Ninguno	Ninguno	

Plan de continuidad de procesamiento:

Situación Actual	Riesgo Detectado	Posibles Consecuencias	Recomendación	Probabilidad de Ocurrencia
Las cintas de backup se encuentran en el mismo edificio que el datacenter.	En caso de existir un siniestro grave (incendio) las cintas se dañarían junto con los servidores	Backup inutilizado, pérdida total de los datos.	Disponer de copias de las cintas fuera del edificio.	Alto

Se realizan pruebas de restauración de backups	Ninguno	Ninguno	Ninguno	
No existe un plan de contingencia documentado	Caída del sistema por un tiempo prolongado.	Perjuicio económico	Desarrollar el plan de respuesta ante incidentes.	Medio
Existe Backup de SO y aplicaciones.	Ninguno	Ninguno	Ninguno	

Informe Sintético

Obejtivo

El objetivo de esta auditoría consiste en realizar una revisión de los principales procedimientos de seguridad de la empresa para efectuar un análisis con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información y de esta forma poder determinar los controles necesarios para llevarlos a cabo.

Alcance

Controles generales de la compañía y propios del área de Sistemas.

Metodología

Relevamiento de las operaciones del área de Sistemas para lo cual se realizaron entrevistas a personal de la empresa y mediante la observación de la práctica operativa del área.

Diagnóstico/Conclusión

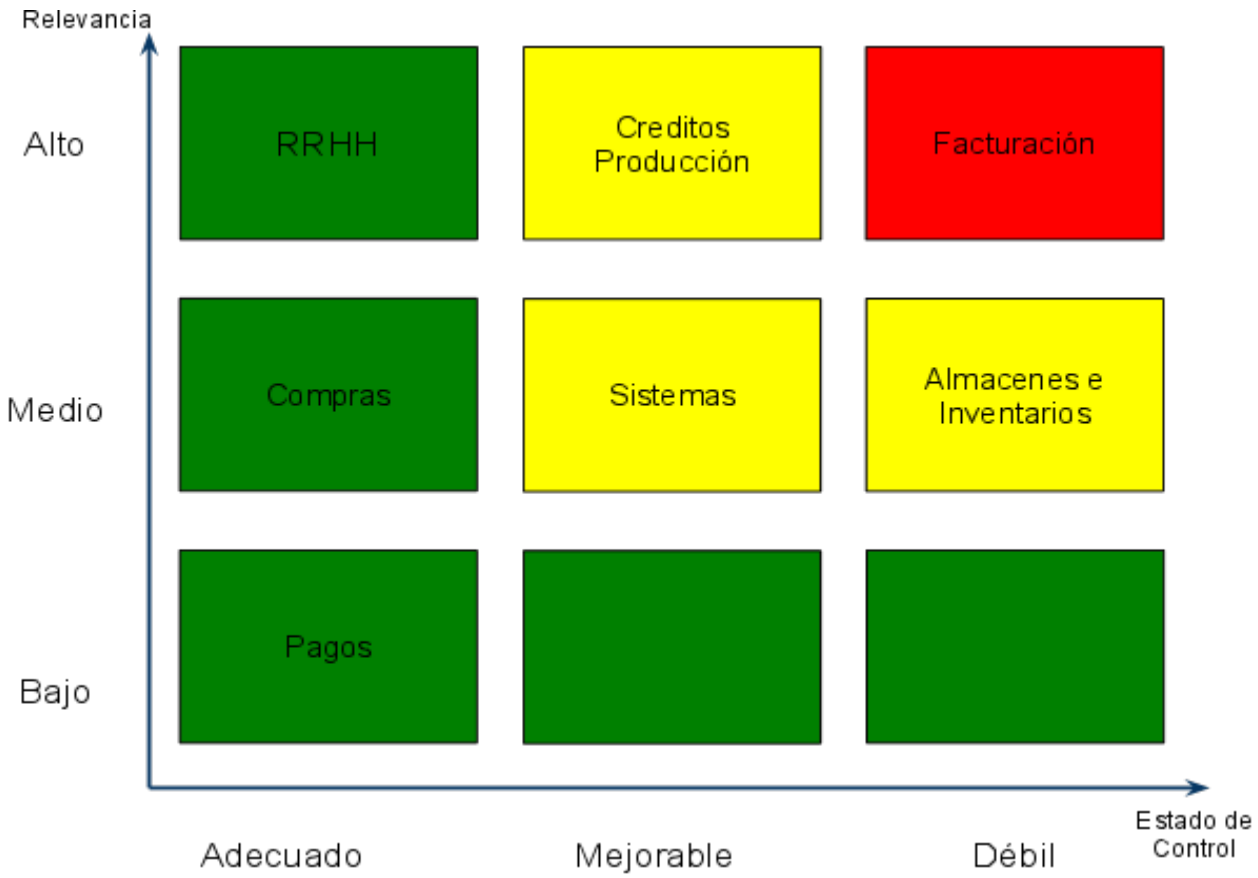
A partir del relevamiento realizado encontramos algunos puntos en los cuales se podrían mejorar los controles para satisfacer una mejor integridad y confidencialidad de la información.

- Los desarrolladores tienen acceso total al ambiente de Producción, lo que podría producir que éstos modifiquen datos reales por lo que se deberían implementar los controles pertinentes para que esto no ocurra y, de ser necesario, crear un nuevo perfil.
- No existe un procedimiento para la baja de usuario, por lo que los ex empleados de la compañía siguen teniendo acceso a los datos reales lo que compromete la confidencialidad de la información. Debe crearse un procedimiento para la baja de

usuarios ni bien abandonan la empresa e implementarse una interfaz temporal que dé de baja a todos los ex empleados.

- Para acceder a las contraseñas de los servidores es necesario desencriptar una base datos con una contraseña que no se encuentra documentada y ante la eventual renuncia, fallecimiento o despido de quien la posee se perderán las contraseñas de los servidores. Por esto es recomendable que esa contraseña se persista en algún medio seguro y accesible solo por personal de Alto Rango.
- Ante la ocurrencia de un siniestro grabe se pueden perder los backups y las copias de seguridad por lo que la empresa perdería toda la información necesaria para llevar adelante el día a día. Es recomendable que las copias de seguridad se almacenen fuera del edificio en el que se encuentran los backups.

Mapa de Riesgos:



Auditoría de aplicación de sistema de Facturación

Debido a la importancia dentro de la organización decidimos auditar el sistema de facturación destinado a las ventas locales. Adicionalmente dentro de la empresa existen distintas formas de ventas (exportación, por anticipos, entre otras), pero gracias a que esta abarca el 90% de los despachos nos centraremos en esta modalidad.

Sectores intervinientes:

Administración de ventas, créditos, despachos.

Descripción del proceso:

El circuito comienza con la carga de un pedido de parte de administración de ventas respetando la orden de compra recibida a través de correo electrónico de parte del cliente. Este pedido se ingresa de manera automática en un estado retenido (inhabilitado para despachos). Cada pedido consta de: número de cliente, planta desde donde se despachará, las cantidades y el precios.
Luego la orden ingresada aparece en la pantalla del analista de créditos asignado a ese cliente, y en base a la evaluación de su nivel de crédito consumido junto a la condición de venta particular arreglada en el pedido se decide si se libera o no. En caso que se libere queda disponible para ser facturado y despachado. En caso contrario se avisa al cliente, al vendedor y administrativo de ventas correspondiente para realizar una nueva negociación o solicitar que se depositen valores para aumentar el nivel de crédito.
Una vez habilitado el pedido, el transporte del cliente se acerca hacia la planta o centro de distribución para retirar la mercadería. Luego que se carga el camión, la oficina de despachos a partir del pedido liberado genera la factura y remitos correspondientes que le entrega al transportista. Los pedidos pueden ser en unidades cerradas y contadas como bolsas, o a granel requiriendo este último tipo realizar un pesaje del transporte para saber el total de la carga y así realizar los ajustes correspondientes en la factura para que reflejen lo finalmente despachado.
Una vez que cierra la jornada se produce en un proceso batch el cierre diario de ventas, alimentándose la contabilidad y sumando la deuda correspondiente en la cuenta corriente del cliente.
En caso de falta de disponibilidad del sistema, los operadores de despachos confeccionan remitos manuales. Cuando el sistema retorna realizan las facturaciones pendientes. En primer lugar se genera el despacho con los datos de lo que anteriormente salió, luego le asignan los números de remito manual y se imprimen las facturas.

Auditoría de la aplicación de facturación:

Situación en el sistema actual	Riesgo detectado	Consecuencia posible	Oportunidad de mejora	Probabilidad de ocurrencia
Los administrativos de ventas y créditos	Adulteración de pedidos para	Violar los criterios de asignación de	Bloquear las modificaciones al	Alta

pueden modificar los precios del pedido luego de la aprobación del mismo.	cumplir con los criterios de asignación de Créditos, y después se modifiquen para reflejar las ventas reales.	Créditos.	cliente como el precio y la cantidad de artículos comprados una vez aprobado el pedido.	
Los operadores de despachos conservan en su cola de impresión las facturas y remitos.	Los operadores pueden disponer de múltiples copias de una misma factura o remito.	Problemas ante inspecciones impositivas. Posiblidad de error cuando hay muchas facturas impresas.	Eliminar automáticamente las facturas de la cola de impresión y diseñar un manual para reimpresiones, que involucre las autorizaciones correspondientes.	Media
Créditos puede ingresar clientes nuevos.	Creación de clientes falsos o duplicados.	Mal control de la situación crediticia de los clientes, por lo que se les podría asignar un crédito mayor al estipulado.	Permitir que solo un departamento cree Clientes o los tenga que aprobar para poder asignarles créditos	Medio
Los registros de pesaje son externos a JDE mediante un sistema no seguro.	Alteración a propósito de los registros de pesaje. Permitiendo que el personal robe mercadería. Errores funcionales del sistema de pesaje.	Pérdida económica por salidas de material no registradas.	Diseñar e implementar una interfase con JDE que permita ingresar los registros de pesaje directamente en el sistema.	Bajo
El stock real disponible, nunca refleja el existente en el sistema.	Desconocimiento preciso de la existencia de material en los almacenes	Comprometerse con un cliente y no poder cumplirle. Incapacidad de detectar un robo o faltante de mercadería	Actualización del stock en forma on-line.	Bajo
El menú para ingresar remitos manuales permite el cambio de cualquier número de remito en la factura luego de impresa.	Modificación de los remitos asociados a una factura.	Que se omita la facturación de remitos por asignarlos a una factura pagada o se vuelva a facturar un remito.	Bloquear las modificaciones a las facturas una vez impresas.	Medio
El limite de crédito puede ser cambiado y no hay registro de los cambios.	Modificaciones indebidas al límite de crédito de un cliente.	Aumento del límite de crédito a un cliente moroso sin registro del responsable.	Registrar todos los cambios hechos sobre el límite de crédito de un cliente guardando el nuevo valor ingresado, la fecha y el usuario que lo realizó.	Alto

No hay autorizaciones de parte del departamento de créditos para la emisión de NC y ND.	Falta del control crediticio.	Autorizar un pedido que no cumpla con el límite de crédito o perder una venta por más que cumpla con todos los requisitos.	Requerir autorizaciones por parte del departamento de créditos para la emisión de NC y ND.	Medio
No existen controles sobre el precio ingresado en el pedido.	Adrede o por error se cargue mal un precio en un pedido.	Pérdida de la compañía por dejar de vender un producto (al ser muy caro) o venderlo a un precio menor que el costo.	Implementar el módulo de administración de precios que tiene JDE, permitiendo que los mismos sean redefinidos solo por los gerentes de ventas.	Alta
Los pedidos que por cualquier motivo se terminan cancelando o anulando no siempre son anulados en el sistema.	No reflejar en el sistema, una operación cancelada con un cliente.	- Perder ventas por suponer que un cliente no cuenta con el crédito necesario por tener pedidos pendientes. - Errores en los despachos. Los operadores toman por error el pedido que no fue cerrado en el sistema y pueden facturar y despachar un pedido cancelado.	Incluir dentro del Manual de Normas y Procedimientos la cancelación en el Sistema, además de implementar alertas al responsable y su superior ante pedidos pendientes con un lapso mayor a 15 días.	Medio

Informe sintético:

Objetivo:
Revisión de los procedimientos de facturación, identificando riesgos posibles de mitigar y diagnosticar la situación encontrada.

Alcance:
La auditoría abarca desde que se ingresa el pedido al sistema hasta que se despacha desde algunos de los establecimientos de producción, pasando por el control de créditos, la facturación, y el pesaje de camiones

Metodología:
Se realizo la auditoría a partir de entrevistar a usuarios de sistema, y realizar operaciones en el entorno de prueba y desarrollo disponible.

Diagnóstico/Conclusión

A partir del relevamiento realizado encontramos algunos puntos en los cuales se podrían mejorar los controles para satisfacer una mejor integridad y confidencialidad de la información.

- El sistema permite que los sectores de Créditos y Ventas accedan a la misma información, por lo que existe posibilidad que administración de ventas pueda elevar el nivel de crédito de los clientes logrando permitir despachos teniendo una deuda que pase el límite permitido por Créditos.
- No existe una administración de Precios fijada por el Sistema, por lo que en forma accidental o intencional la empresa puede vender artículos a un precio distinto del establecido y perder plata.
- Existe la posibilidad de tener múltiples copias de una factura, por lo que ante una posible inspección de la DGI podrían aplicarse multas.
- No hay autorización del departamento de Créditos para la emisión de Notas de Crédito o Débito, por lo que un vendedor podría crearlas para mejorar circunstancialmente la situación crediticia de un cliente y así violar el control de Créditos.

Plan de Trabajo Oracle

Riesgos y posibles consecuencias	**Objetivos de Control**	**Controles a Identificar**	**Pruebas a Efectuar**
No tener registros sobre cualquier operación en las BD.	Verificar el estado de auditoría de la BD.	- Consulta si la Auditoría esta habilitada - Observar las tablas de auditoría y verificar que tengan información valida.	Realizar cambios en los datos y en los usuarios y ver que se reflejen en los registros de auditoría. Ejecutar: -Select user_id, session_id, sample_time from sys.wrh$_active_session_history; -Select userid, action#, returncode, timestamp# from sys.aud$ -Select userif, action#, timestamp#, logoff$time from aud$;

No detectar intrusiones ni cambios de configuración realizadas por una persona no autorizada.	Determinar si la base de datos loguea eventos de inicio de sesión, modificación de datos y los mismos no pueden sobreescribirse.	Verificar que la base de auditoría no puede sobreescribirse.	Verificar que la Base de Datos esté en modo ARCHIVELOG (la opción incorrecta es NONARCHIVELOG) Ejecutar la consulta SQL que devuelve el modo en que se encuentra la base: SELECT VALUE V$PARAMETER WHERE FROM NAME="archiv_log_start";
Intrusión	Prevenir accesos no autorizados	- Verificar si hubo ataques por fuerza bruta o diccionario a cuentas de usuario - Consultar ataques a la cuenta SYS - Verificar fortaleza de la contraseña.	- Verificar si hubo ataques por fuerza bruta o diccionario a cuentas de usuario - Consultar ataques a la cuenta SYS - Consultar las tablas de registo de sesión, los horarios de los mismos y las IPs de procedencia. Ejecutar los siguientes querys: -select userid, action#, returncode, timestamp# from sys.aud$; -select name, lcount from users$ where lcount>0; -select name, ltime from user$ where astatus=4;
Intrusión/robo de información	Determinar si el sistema es vulnerable a fallas de seguridad conocidas públicamente.	Verificar la correcta aplicación de parches de seguridad.	Ejecutar el exploit de AUTH_ALTER_SESSION Ejecutar: -Select userid, action#, returncode, timestamp# from SYS.AUC$
Intrusión/robo de información	Buscar inconsistencias en los datos. Buscar usuarios creados por atacantes.	Consultar usuarios, roles, usuarios con función de DBA, cuentas bloqueadas, tiempos de expire de los passwords Verificar que se guarden los hash de los passwords y no los passwords en texto plano.	Verificar que los usuarios creados correspondan a los usuarios autorizados. Verificar si los permisos asignados a cada usuario poseen los privilegios correspondientes a la definición de su rol. Verificar si existen cuentas incorrectamente bloqueadas.

			Verificar si los tiempos de expiración de las sesiones se corresponden con las políticas de la empresa. Ejecutar: - Select user#, name, astatus, password, ctime, ptime, ltime from sys.user$ where type#=1; - Select u.name as grantee, u2.name as role from sys.user$ u, sys.user$ u2, sys.sysauth$ a where u.user#=a.grantee# and privilege#=u2.user#;
Borrado de información	Determinar si existen tablas o información eliminada.	Revisar los DataBlocks de la Base de Datos Oracle	Buscar en los Oracle Data Blocks: - Registros eliminados - Localizar bloques asignados a tablas - Seguimiento de objetos creados y eliminados - Localizar tablas eliminadas - Localizar funciones eliminadas - Revisar las tablas RECYCLEBIN$ y OBJ$ Ejecutar: - select u.name, r.original_name, r.obj#, r.droptime, r.dropscn from sys.recyclebin$ r, sys.user$ u where r.owner#=u.user#;
Intrusión	Disminuir riesgos de accesos no autorizados.	Estado de seguridad de los SID de las bases.	- Buscar conectarse a la BD con el SID por default o con el nombre del servidor.
Intrusión/ robo de información	Impedir la ejecución de codigo arbitrario por parte de un atacante e inyecciones de SQL	Determinar la existencia de librerías que puedan estar ejecutando código malicioso	- Revisar librerías. - Revisar triggers al encendido, inicio y terminación de sesión
Inseguridad de datos durante transmisión	Proveer métodos de encriptación robustos	Revisar si se usa el paquete Oracle Advanced Security	- Efectuar pruebas de ataques contra los algoritmos DES, 3-DES, etc soportados por DBMS_OBFUSCATION_TOO

			LKIT - Verificar encriptación de la transmisión