IMPLEMENTACION DE CONTROLES POSTERIOR A UN PROCESO DE REINGENIERIA

CAPITULO 3

CONTROLES RELATIVOS A LOS SISTEMAS

3.1 Controles de Acceso lógico

3.1.1 Necesidad de los controles

3.1.2 Identificación de Usuarios

3.1.3 Suspensión de Permisos

3.1.4 Acceso a Datos

3.1.5 Acceso a Programas y Utilitarios

3.1.6 Controles de Aplicación

3.1.7 Controles de Actividades del Programador de Sistemas

3.1.7.1 Casos Reales sobre accesos no autorizados a sistemas informáticos y, fraudes - **El Pentágono, Citibank y Barings Bank of London, Universidad Spring Arbor de Michigan y Proinco de Ecuador.**

3.2 Control de Cambios

3.2.1 Razones para establecer un Control de Cambios

3.2.2 Procedimiento de Control de Cambios

3.2.3 Modelo de Formato para Control de Cambios

3.3 Producción y Operaciones

3.3.1 Criterios a aplicarse en los controles de Producción y Operaciones.

3.3.2 Procedimientos de la función de Producción y Operaciones.

CAPITULO 4

RESPALDOS Y RECUPERACION DE PROGRAMAS

4.1 Procedimiento de Respaldos y Recuperación de Programas

4.2 Procedimiento de Almacenamiento de Medios Magnéticos

4.3 Modelos de Formato para Control, Recuperación y Almacenamiento de Respaldos.

CAPITULO 5

CONTROLES APLICADOS EN LA ADMINISTRACION DEL PERSONAL

5.1 Objetivo de los Controles Administrativos

5.2 Contratación y término de Contratos

5.3 Políticas Administrativas

5.3.1 Vacaciones

5.3.2 Entrenamiento

5.3.3 Uso de Recursos Computacionales

- **CONCLUSIONES**
- **RECOMENDACIONES**
- **BIBLIOGRAFIA**

AGRADECIMIENTO

Mi Mami

Econ. Carlos Izurieta

Jenny Anchundia de Andrade

Washington Rodríguez

Carlos A. García

Victor M. Serrano

Oscar Ponce de León

GRACIAS

A todos ellos…….. por su apoyo emocional, su predisposición y colaboración para la culminación de este trabajo.

Y un agradecimiento muy especial a Dios, quién me ha dado la fortaleza necesaria para superar todos los obstáculos.

DEDICATORIA

A mi Mami…

****

ahora la medallita estará completa...

INTRODUCCION

En un proceso de Reingeniería luego de su implantación, los controles no quedan establecidos, por cuanto la Reingeniería se concentra básicamente en nuevos e innovadores diseños de los procesos, buscando un marcado, dramático y notorio incremento en la productividad, eficiencia y utilidades de las empresas, sin contar con el diseño de controles en los procesos. Por lo tanto debe someterse a un análisis para la **Implementación de Controles básicos e indispensables** y con mayor énfasis en el área de Procesamiento de Datos. El no hacerlo provocará seguramente fallas o desvíos en los nuevos procesos, sin que podamos determinarlos o auscultarlos oportunamente y evitar fallas o errores. Estos lineamientos una vez desarrollados, deben ser aplicados por toda la empresa y principalmente por el personal que labora en el área de sistemas.

El objeto de este trabajo no es enseñarle a hacer una reingeniería ni tampoco el de explicar su metodología. El objeto de este trabajo es el de mostrarle que hay un **"más allá"** luego de una reingeniería y estos son los controles y seguridades sobre los cuales se centra este trabajo. Mi intención es **mostrarle los puntos de alerta** de las áreas que corren " mayormente " un peligro inminente, y una forma lo menos técnica posible para **explicar al administrador de empresas, las formas de prevenirlos mediante la Implementación de los controles y seguridades de los datos.**

Es importante dar a conocer también al administrador de empresas que si bien aunque no sea un experto en sistemas computacionales, debe "conocer" cuales son básicamente los puntos que debiera concentrarse y obtener información detallada del experto en sistemas de su empresa.

Finalmente, si el administrador de empresas lidera un colegio, universidad, industria, banca o empresa comercial, este trabajo le ayudará en mucho, ya que aplica para cualquier tipo de empresa. Su enfoque está dado mayormente al área de procesamiento y afines, pero sus conceptos pueden extenderse inclusive al resto de áreas.

CAPITULO 1 : *GENERALIDADES*

1.1 **Objetivo de la Reingeniería**

Mucho se ha dicho sobre lo que es y no es la reingeniería. Entre lo que se ha dicho que es la reingeniería, tenemos que es un programa o una metodología que busca un cambio radical, no buscan mejoras incrementales, ni tampoco solo la automatización, ni sólo la organización, ni solo la reducción de tamaño, ni solo la calidad.

Se define a la Reingeniería de Procesos como un enfoque "equilibrado" que contiene elementos de los programas más tradicionales de mejoras, aunque no es un programa "más" de mejora, ya que la reingeniería es mucho más. Busca avances decisivos en medidas importantes que afectan el rendimiento. Busca metas multifacéticas, tanto en calidad, costos, rapidez, flexibilidad, satisfacción del cliente, precisión; todas ellas simultáneamente y no una en especial. La Reingeniería toma como punto de vista los "procesos" y se centra en ellos para re-diseñarlos y por tanto su perspectiva no es funcional ni organizacional.

Por lo antes explicado y por lo que ya ustedes deben conocer de Reingeniería, esta busca enderezar el proceso, quitándole lo serpentino del mismo. Para ello define que un proceso tiene fronteras y que en cada frontera tiene al menos un control, por lo tanto tendrá mínimo dos controles en el proceso, uno para la persona que hace el traspaso y otra para la que recibe lo cual para la Reingeniería es inconcebible. El establecimiento de controles a su manera de ver, perjudica el flujo del proceso ya que incorporan actividades que al punto de esta metodología, No agregan valor.

La definición de reingeniería espera producir la optimización del flujo del trabajo y de la productividad en una organización midiendo ambas en función de los *resultados del negocio*: incremento de rentabilidad, participación de mercados, rendimiento sobre la inversión, capital social y activos. También la reingeniería se puede medir por reducción de costo total o unitario.

La Reingeniería de procesos establece una correlación explícita entre los resultados del negocio (que son de interés para los altos ejecutivos que optan por este programa), y los resultados del proceso: rapidez, precisión y reducción del tiempo del proceso (que el equipo de reingeniería trata de optimizar).
Sin establecer este vínculo deliberado, cuantificable, entre el fin y los medios, es decir, entre los resultados del negocio y los resultados del proceso; los programas de reingeniería estarían condenados al fracaso.

Finalmente la Reingeniería responde a la evolución de las tendencias en el ambiente de los negocios donde fallan programas de mejora incremental más tradicionales. En muchos casos, sólo la reingeniería promete un cambio suficientemente rápido y radical para mantenerse a tono con el cambiante ambiente de los negocios.

1.2 **Objetivo de los Controles**

El Control es uno de los pilares en que se fundamenta la administración. Un concepto simple de lo que significa el control sería el de la "medición de resultados actuales y pasados, en relación con los esperados, ya sea total o parcialmente, con el fin de corregir, mejorar y formular nuevos planes". En sí el control busca recolectar sistemáticamente datos para conocer la realización de los planes.

Con los avances tecnológicos y el éxito que tienen los sistemas de comunicación, es posible en muchos casos obtener una "retroalimentación" de las informaciones que resultan del control mismo, y utilizarlas para que la acción correctiva se inicie de forma automática, con lo cual, no hay que esperar hasta que se produzcan íntegramente los resultados para poner en obra la acción correctiva: un procedimiento previamente establecido, va corrigiendo la acción constantemente, con base en esos resultados, sin necesidad de detenerla.

Los controles pueden ser automáticos, manuales o una combinación de ambos. Para tener una idea de las formas en que se presentan los controles tenemos el siguiente

ejemplo: Se ha fijado como estándar de temperatura en un local determinado que ésta debe sostenerse entre los 20° y 22° centígrados. En un sistema de control manual hay que visualizar en qué momento el termómetro baje de los 20°C o pase de los 22°C para ajustar la ventilación a fin de cumplir con los estándares señalados.
En un sistema de control automático, al llegar la temperatura a menos de 20° o a más de 22°C automáticamente cambia la calefacción, manteniendo así constantemente la temperatura en el nivel deseado.

En el campo administrativo es posible obtener las mismas aplicaciones, por ejemplo: en inventarios que se requieren puntos de reposición, al llegar al mismo automáticamente se generan los pedidos necesarios para que no falten los elementos indispensables mientras se consume la existencia. Este ejemplo realizado en forma manual, requiere de igual forma un control manual de los niveles de existencias y puntos de reposición.

Luego de esta breve explicación de lo que es el “control”, definimos entonces que el objetivo de los controles es el de proporcionar a la empresa, un elemento de seguimiento y detección de desvíos o fallas en los procesos. Se crean con el fin de asegurar los elementos tales como:

-Seguridad, oportunidad y exactitud de la información de acuerdo a los requerimientos de la empresa.

-Aplicación de medidas de protección y control sobre los datos almacenados o de los programas utilizados en el centro de procesamiento como son los microcomputadores de la empresa.

-El diseño de seguridades físicas y administrativas que conlleven al apoyo de las medidas de control para el centro de procesamiento y otros entes que operen con datos oficiales.

-Que los datos oficiales de la empresa sean accesados por personal autorizado expresamente y con atribuciones específicas, mediante la ejecución de un proceso

autorizado que refleje un producto final confiable con base a la aplicación de los procesos diseñados.

-El personal con atribuciones, los datos oficiales (datos formales) y procesos autorizados forman parte de todo un **sistema de formalidad** de la institución, los cuales son continuamente examinados, revisados y aprobados por los mecanismos de control de la empresa y que operan recurrentemente bajo los esquemas de seguridad y control que se apliquen.

-Los procesos, datos y programas que funcionen en una empresa deben llevar siempre una tendencia hacia la formalización (ya sea por los usuarios, auditoría interna, sistemas, control interno, capacitación y otros) cuando estos sean relevantes para la empresa, y cuando su procesamiento ocurra continuamente así como su permanencia. De esta forma se asegura el cumplimiento de todas las normas, políticas y procedimientos y controles establecidos en la Institución.

-Analizar las posibles inversiones necesarias para dar cumplimiento a las normas y procedimientos destinados para seguridad y control de datos; evaluándose con criterio de los beneficios que serían obtenidos por la inversión, y contemplando en todo momento los intereses de la empresa que deben ser salvaguardados.

CAPITULO 2: *SEGURIDAD FISICA*

2.1 **Objetivo de la Seguridad Física**

El objetivo es el de proteger los sistemas tanto en la parte de hardware, software, documentación y medios magnéticos de los riesgos por pérdidas, extravíos o por daños físicos. Así mismo de los potenciales riesgos se pueden dar en el acceso de personal no autorizado sin los controles adecuados de seguridad física; en los incendios; en las interrupciones de energía eléctrica; en inundaciones por filtraciones de agua y, en los controles de acceso lógico.

2.2 **Aspectos que involucran la Seguridad Física**

La seguridad física involucra como mínimo los siguientes aspectos:

- Control de Acceso
- Seguridad contra Incendios
- Suministro de Energía
- Aire Acondicionado
- Detección de Agua
- Guardias de Seguridad
- Telecomunicaciones

2.2.1 Control de Acceso

Aunque la inversión en sistemas de control de acceso no debe ser necesariamente onerosa como la implantación de vidrios a pruebas de balas, guardias armados las 24 horas del día o cámaras de video; las empresas si deben contemplar controles adecuadamente razonables para evitar el acceso de individuos e incluso de personal “no autorizado” al centro de procesamiento o a las áreas de manejo de datos o información oficial y exclusiva.

GUARDIAS DE SEGURIDAD

CAMARA DE SEGURIDAD

ALARMAS DE SEGURIDAD
keypad

PROTECCION DE PERIMETROS
CON SENSORES

LECTOR DE HUELLAS
DACTILARES

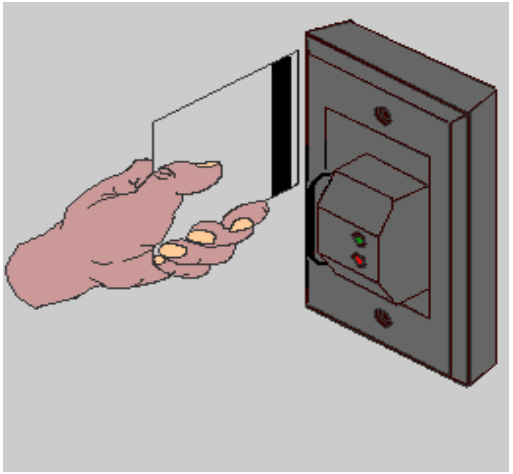
CERRRADURAS

DETECTORES DE MOVIMIENTO

PROTECCIONES PARA
VENTANAS

TARJETAS DE CONTROL
DE ACCESO

Estos sistemas de Seguridad deben contemplar el uso de claves de seguridad a ser ingresadas a través de un componente electrónico ubicada en cada área o por medio del uso de una tarjeta plástica codificada. La asignación de claves debe estar dada por el representante del área de sistemas y deberán ser modificadas periódicamente para evitar cualquier infiltración dentro del archivo maestro de claves o el otorgamiento de las mismas entre usuarios.



Cabe indicar que debe haber para el efecto una interrelación entre cada área que responsabiliza a un individuo a través del uso de una clave, y el área de control que asigna y controla las claves emitidas a los usuarios. El no conocer sobre el despido, renuncia o ausencia de un personal determinado durante un tiempo específico o permanente provocaría que el proceso de control de acceso no tenga éxito por daños provocados por actos de sabotaje, robos, asaltos, etc.

Los accesos también deben ser otorgados sobre la base de la necesidad mínima y dependiendo de los casos bajo la supervisión del Responsable de Sistemas.

Cuando se reasigne personal a otras funciones en las que no requieran del acceso que tenían previamente autorizado; el permiso debe ser revocado una vez que la persona sea reasignada en sus funciones. Así mismo en el periodo de vacaciones del personal debe aplicarse este mismo concepto.

Las movilizaciones de equipos o medios magnéticos deben ser realizadas sólo por personal autorizado y deben seguir el procedimiento de control de movilizaciones de equipos. El guardia de seguridad debe asegurarse que las movilizaciones de equipos o medios magnéticos tanto de ingreso como de egreso se efectúen con las autorizaciones del caso.

El personal que corresponda a la categoría de visitantes y que requieran movilizarse por el centro de procesamiento o afines deberán utilizar una tarjeta que indique su calidad de “visitantes” y estar siempre escoltados o supervisados por personal de la institución y su ingreso y salida debe quedar registrado en una bitácora del área.

La limpieza y aseo del centro de procesamiento y afines debe efectuarse en presencia del personal de la institución. Dicho personal de limpieza debe ingresar previo a la identificación ante el guardia de seguridad quien debe constatar su

nombre dentro del registro del personal externo a la empresa y el horario autorizado para su acceso.
Debe prohibirse el ingreso de personal con maletas o bolsos u objetos que no fueran los que constituyan o sirvan para su labor de limpieza y aseo.

Las tarjetas de acceso a áreas restringidas así como las tarjetas de visitantes deben ser reportadas inmediatamente en el caso de perdidas, al personal de seguridad y al Responsable de sistemas a fin de revocar el uso de dichas tarjetas.

Para casos de emergencia, el personal de seguridad debe tener las llaves del centro de procesamiento y de las oficinas. Estas deben conservarse en sobre sellado, bajo seguridad y revisado periódicamente por Auditoría.

Los horarios de ingreso y salida del personal así como de equipos y medios magnéticos debe ser revisados por el personal de Auditoría periódicamente y comprobado que los movimientos de equipos se hayan efectuado de acuerdo a los controles establecidos y que, el ingreso y salida del personal se haya efectuado en el horario establecido y con los permisos respectivos para entradas o salidas fuera de horario.

Es importante que las empresas prevean la obtención de una póliza que resguarde pérdidas o daños de sus activos fijos.

2.2.2 Seguridad contra Incendios

El centro de procesamiento y afines debe poseer detectores de humo los cuales deben activarse de forma automática al momento de una emanación considerable de humo. Estos dispositivos deben probarse regularmente para corroborar su funcionamiento. En caso de ser detectores de incendios con prolongación automática de agua, deben ubicarse en áreas lejos de los equipos y material no recuperable por contacto con agua.

ALARMA CONTRA INCENDIOS

SISTEMA DE PROLONGACION AUTOMATICA DE AGUA

DETECTORES DE HUMO

El centro de procesamiento debe disponer de suficientes extintores de incendios portables y que deben ser probados periódicamente a fin de que estos puedan funcionar en los casos de emergencias.

EXTINTORES DE INCENDIOS

Debe hacerse una revisión visual de su presurización procediendo a enviar a cargar o descargar el extintor al centro de mantenimiento respectivo.

Así mismo debe señalizarse el área de tal forma que se especifique las áreas en que se prohibe fumar o utilizar material combustible.

Los extintores a ser usados varían de acuerdo a la clase de incendio que se presenten. Tenemos para ello incendios tipo A, B, C y D. Los incendios de Tipo A, se producen en combustibles sólidos corrientes como la madera, textiles, basura, etc. El fuego de esta clase, agrieta el material, origina brasas, deja ceniza y se propaga de afuera hacia adentro. Se le combate preferentemente con agentes de extinción a base de agua.

Los incendios de tipo B se producen en líquidos inflamables: gasolina, aceites, pinturas, grasa, etc. Se caracteriza porque el fuego se produce sólo en superficie. Para combatirlos debemos, preferentemente eliminar el oxígeno que está en contacto y se requiere de agentes de extinción que cumplan ese fin.

Los incendios de tipo C, se producen en equipos eléctricos conectados, aunque este tipo de incendios se produce en materiales sólidos o líquidos, han merecido clasificación especial por el peligro que implica la corriente eléctrica. Se emplean agentes de extinción NO CONDUCTORES DE ELECTRICIDAD.

Los incendios de tipo D se producen en metales livianos, productos químicos, farmacéuticos, etc. Al entrar en combustión estos materiales generan su propio oxígeno; al ser atacados con agentes extintores ordinarios producen violentas reacciones, llegando inclusive a la explosión. Se los combate, preferentemente con agentes extintores especiales como el polvo químico.

A continuación un cuadro explicativo de los tipos de fuegos y tipos de extintores a usarse en cada uno.

CLASE DE FUEGO		**EXTINTOR**					
CLASE	**TIPO DE MATERIAL COMBUSTIBLE**	**AGUA**	**ESPUMA**	**CO2**	**POLVO BC**	**POLVO ABC**	**AGENTES ESPECIALES**
A	Madera, trapos, papel, etc. Sólidos en general	●	●	△	△	●	×
B	Líquidos inflamables o sólidos de bajo punto de fusión.	×	●	●	●	●	△
C	Equipo eléctrico vivo o conectado	×	×	●	●	●	△
D	Materiales, productos químicos, etc.	×	×	×	△	△	●
● Adecuado para el tipo/ incendio			△ Puede usarse	× No debe usarse en este tipo /incendios			

El centro de procesamiento y afines debe ser estructurado con equipos, muebles y material no inflamable. Es preferible la no-utilización de cortinas en el centro de procesamiento. El equipamiento eléctrico como cables, deberá ser instalado y elaborado por personal altamente calificado.

Los interruptores de energía deben estar separados por secciones y uno que permita el corte completo del suministro de energía para casos de emergencia, los mismos que deben estar protegidos para evitar su manipulación accidental.

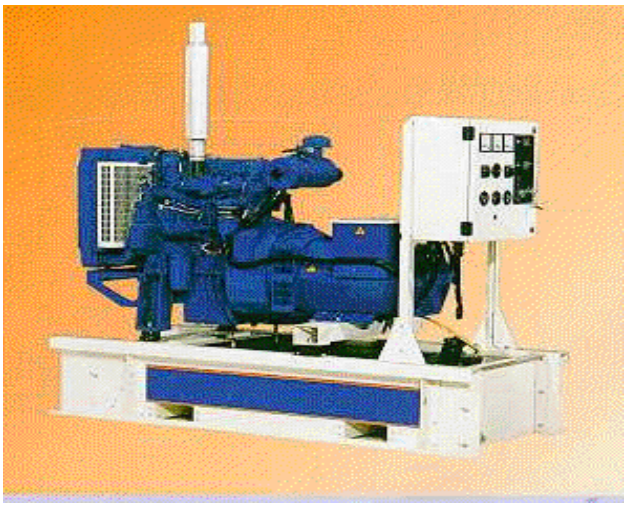
Por ningún motivo se debe fumar en el área de procesamiento. Cualquier material de fácil combustión, como hojas, manuales, formularios, deberá estar ubicados lejos de las zonas calientes y del posible contacto con elementos inflamables.

2.2.3 Suministro de Energía

-Toda empresa debe poseer un **UPS** (**U**ninterruptable **P**ower **S**upply/Fuente Ininterrumpida de Energía) para protegerse de cualquier suspensión o caída del suministro eléctrico.

UPS

-Adicionalmente al UPS debe existir un Generador de Energía a ser utilizado en casos de emergencia también, el cual debe ser probado periódicamente a fin de asegurar su operación.



GENERADOR DE ENERGIA

-Tanto el Generador de energía como el UPS deben proyectarse a ser utilizados hasta el 70% de su carga.

-Cabe indicar que el UPS está en constante funcionamiento, no sólo para soportar la ausencia de luz por un periodo determinado sino también en intermitencias o picos eléctricos. Es importante hacer una correcta evaluación de las especificaciones que debe tener un UPS antes de adquirirlo a fin de que este soporte todos los equipos del centro de procesamiento y afines. Esta evaluación debe estar a cargo del Responsable de Sistemas.

-Los equipos deben ser mantenidos regularmente.

-La energía del centro de procesamiento y afines debe ser exclusiva y no compartida con otras áreas.

-En casos de emergencias es importante que el personal del centro de procesamiento esté familiarizado con los procesos respectivos a fin de qué, al momento de trabajar sólo con energía brindada por el UPS, los equipos no indispensables sean apagados, a fin de alargar el tiempo de suministro alterno de energía.

-Como herramienta de emergencia, se debe contar siempre con linternas a pilas.

2.2.4 Aire Acondicionado

-El centro de procesamiento debe ser mantenido a una temperatura entre 18-19°C, con una humedad entre el 45%-50%.

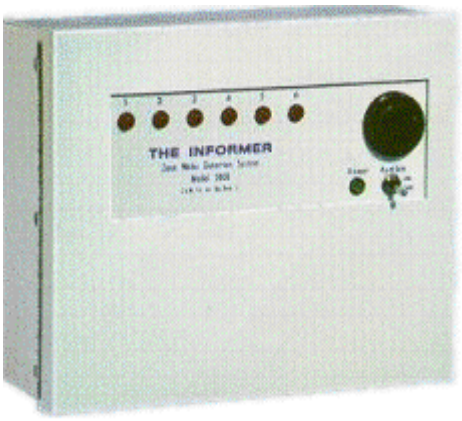
MODELOS DE AIRE ACONDICIONADO

-Para el centro de procesamiento debe existir independiente del sistema central de aire acondicionado, dos equipos de aire acondicionado “especiales” de los cuales uno actúe como respaldo del otro cuando este no pueda operar correctamente. La característica de estos equipos no es la común de los aires acondicionados normales. Estos equipos principalmente acondicionan automáticamente la temperatura, la humedad, controlan el fluido de aire y son silenciosos, evitando de esta forma, daños en las computadoras y demás equipos que conforman el centro de procesamiento.

-En casos de contingencias en las cuales no se cuente con la operatividad del acondicionador de aire principal y a falta del equipo de respaldo; podrían mantenerse disponibles ventiladores de pedestales a fin de refrescar los equipos principales mientras dure la emergencia.

2.2.5 Detección de Agua

Es muy raro que una empresa utilice detectores de agua en sus centros de procesamiento no por su ineficacia sino por falta de conocimiento sobre la existencia de estos tipos de equipos. Estos dispositivos son importantísimos para mantener al centro de procesamiento, lejos de filtraciones de agua, principalmente en los puntos débiles, como son los lugares cercanos a los equipos de aire acondicionado.



SENSOR DE AGUA Y HUMEDAD

DETECTOR AUDIBLE DE AGUA

-Estos dispositivos pueden ser detectores de agua por sonido o por sensibilidad. Se pueden usar individualmente de acuerdo a las necesidades de cada empresa o pueden combinarse, es decir; pueden usarse en ciertos sectores claves los sensores de agua y humedad (lugares donde se ubiquen equipos acondicionadores de aire) y en otros pueden usarse los detectores audibles (cercanos a griferías o ductos de agua).

-Las alarmas deben ser mantenidas y probadas periódicamente para asegurar su operación.

-De forma complementaria a los sistemas automáticos, se puede detectar visualmente filtraciones o emanaciones de agua en los pisos falsos, tumbados o paredes.

2.2.6 Guardias de Seguridad

-Los Guardias de Seguridad deben asegurar la vigilancia permanente de las oficinas y principalmente del centro de procesamiento y afines. Ninguna persona no autorizada podrá ingresar al centro de procesamiento sin el permiso respectivo.

-Deberán también verificar que el personal de visita se encuentre en el piso y con la persona visitada. De igual forma el egreso de visitantes debe quedar registrado

y deberá ser controlado a través de las tarjetas de visita y del registro de firma y hora de salida por parte del visitante.

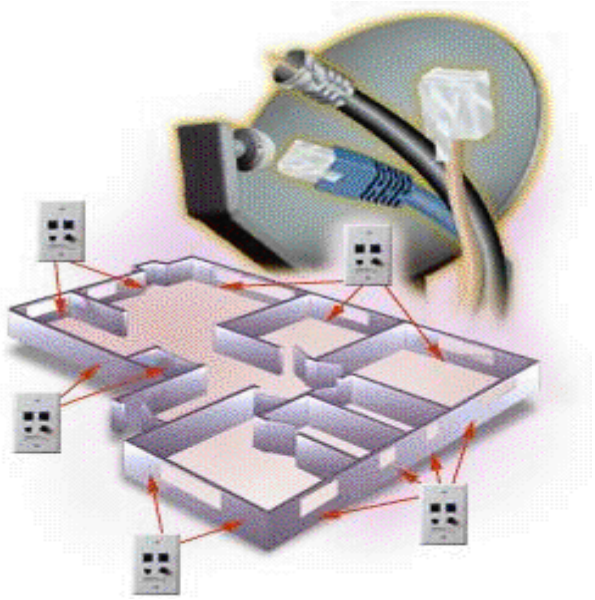
-Dependiendo de las dimensiones de la empresa y de la sensibilidad de la información que manejen, se suelen establecer cámaras de seguridad por pisos o sectores, las cuales son monitoreadas por grupo de guardias de seguridad en los sitios de control destinados para el efecto.

2.2.7 Telecomunicaciones

Se define a las comunicaciones como el arte y la ciencia de “Comunicar”. Este simple concepto se extiende a las telecomunicaciones, las cuales consisten en “Comunicar” a través de alguna distancia, utilizando medios electrónicos, eléctricos, ópticos, por cable, fibra o electromagnéticamente. Las telecomunicaciones son sencillamente, medios de transmisión, recepción e intercambio de señales.

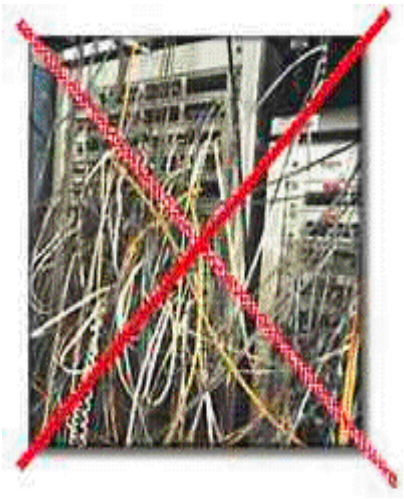
-Entre las seguridades que deben observarse en el ámbito de telecomunicaciones están los Cables de comunicaciones y eléctricos deben mantenerse de forma protegida para asegurar que funcionen adecuadamente.

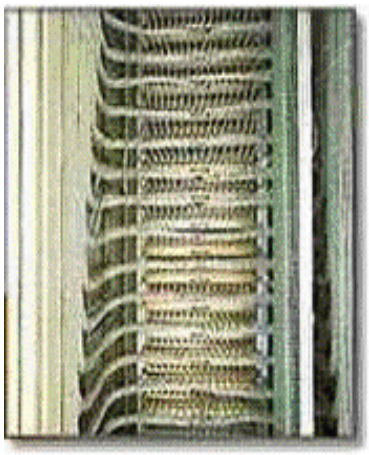
-Los equipos de comunicación como módems, nodos, controladores, servidores, etc. deben estar protegidos dentro del lugar físico donde se encuentren y en un ambiente acorde a las especificaciones técnicas proporcionadas por el manufacturador y/o proveedor del equipo.



-En toda la empresa y principalmente en el centro de procesamiento, los cables eléctricos deben estar dentro de canaletas o tuberías de plástico que es un material no conductor de energía eléctrica. Para el caso de cables de redes (transmisor de voz y datos, generalmente se utilizan tuberías metálicas).

-Los cables, sean estos eléctricos o no, deben estar en sitios perfectamente señalados para el efecto y ordenados, utilizando los elementos necesarios que se encuentran en el mercado para su protección contra circuitos o daños producidos por negligencia, agua, roedores, etc.





-Actualmente las empresas dedicadas al diseño de ambientes, proporcionan paredes movibles las cuales tienen integrado en la panelería, las canaletas para cables. Es importante recalcar que este tipo de panelería debe ser usada fuera del área de procesamiento, ya que generalmente el material que las recubre es de tela, por tanto de fácil combustión.

Si bien es cierto que el Administrador de empresas encargará al Responsable de Sistemas de su empresa la ejecución o instalación de cableado eléctrico o estructurado (para redes), no es menos cierto que debe conocer sobre cuales serán los puntos que deben cubrirse en este tipo de instalaciones:

-Instalación eléctrica: Proyecto y ejecución de obra civil, tendido de ductos (plástico), tendido de cables. Provisión e instalación de: tomacorrientes, tableros, supresores de pico (estabilizadores de tensión-UPS), etc.

-Cableado Estructurado: Proyecto y ejecución de obra civil, tendido de ductos (metálico o plástico), tendido de canaletas, tendido de cables de voz y datos. Provisión e instalación de: gabinetes, conectores, patcheras, hubs, ruteadores, etc. provisión e instalación de equipamiento informático y su correspondiente software.

-Servicio de mantenimiento de redes: Puede incluir todo el equipamiento informático (Servidores, computadoras personales, impresoras, etc.), como así también el chequeo y corrección de problemas en el tendido de la red y sus componentes activos. En instalaciones preexistentes, se ofrece el Servicio de Certificación de la Red.

CAPITULO 3: *CONTROLES RELATIVOS A LOS SISTEMAS*

3.1 **Controles de Acceso lógico**

3.1.1 **Necesidad de los controles**

Los Controles de Acceso lógico son de vital importancia ya que permiten proteger los recursos tales como programas, archivos, transacciones, comandos, utilitarios, etc.

Definiremos los lineamientos para implementar los mecanismos de control sobre el acceso lógico tanto local como remoto, a los recursos del centro de procesamiento de datos y afines.

-A nivel general, los permisos de acceso deben estar basados en la necesidad del usuario por conocer la información. Esto implica que los permisos deben ser respaldados y justificados de acuerdo a la función que desempeña el usuario.

-En casos de emergencia en que los recursos suelen estar desprotegidos y, en las que se requiere que otra persona diferente a la autorizada efectúe un acceso lógico, deberá hacerlo siempre bajo adecuada supervisión. Posterior a la emergencia deberá darse de baja ese usuario y clave o reemplazada con una nueva clave por seguridad.

-Los sistemas de control de acceso lógico deben contemplar las violaciones al mismo. Mantener un registro histórico de todos los accesos inclusive de los intentos fallidos o violaciones de su seguridad debe producirse en forma automática.

-Las claves de acceso deben resguardarse en sobres debidamente sellados y guardados en caja fuerte. En casos de emergencia, el responsable de la caja fuerte bajo autorización del Responsable de Sistemas, podrá entregar a quien este último indique, la clave que está resguardada. Deberá mantenerse un

registro de los accesos a estas claves respaldadas y las autorizaciones respectivas.

-Los usuarios son responsables de las claves que tienen asignadas. Por ningún motivo debe divulgarse o intercambiarse claves con otros usuarios. Cualquier resultado de no-cumplimiento de este punto, quedará exclusivamente bajo responsabilidad del usuario respectivo.

-La empresa debe establecer un ente que se encargue de administrar las seguridades, usuarios y claves. Las funciones asignadas será la de controlar y mantener actualizada la lista de usuarios y claves asignadas a los diferentes recursos y de establecer políticas de cambios periódicos a fin de evitar desviaciones en las seguridades de los recursos.

3.1.2 **Identificación de Usuarios**

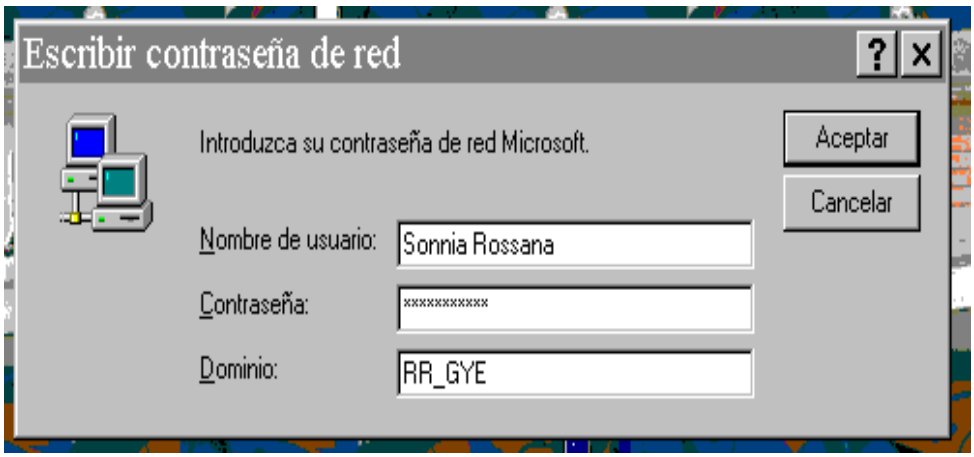
-Los usuarios no deberán nunca compartir sus identificaciones como usuarios y sus claves o contraseñas. Cada nuevo usuario debe ser solicitado y justificado al Responsable de sistemas y una vez aprobado, deberá ser canalizado a través del Administrador de seguridades para su asignación y control respectivo.

-Es importante que el Responsable de Sistemas informe tanto al solicitante como al Administrador de Seguridades, cuales son los tipos accesos que tendrá el nuevo usuario, así como también los no accesos, los cuales inclusive podría abarcar hasta restricciones a nivel de terminales.

-Ningún usuario puede crearse sin su correspondiente clave o contraseña (password) ya que este constituye el único medio de control de seguridades.

-Las claves deben consistir como mínimo de 6 caracteres alfanuméricos (números y letras), los cuales serán elegidos por el usuario. En otras ocasiones y dependiendo de los recursos a los que se tendrá acceso, las claves son

asignadas directamente por el Administrador de seguridades e informadas al usuario, ejm.: usuarios de red y claves de red.



-Es importante que el Administrador de usuarios no tenga dentro de sus registros la misma clave para otros usuarios. De producirse este caso, deberá cambiarse la clave inmediatamente e informado al usuario respectivo de la nueva clave. También debe en este caso tomar en cuenta los siguientes factores:

*No deben existir claves de diferentes usuarios con caracteres iguales en las mismas posiciones, ejm: 123SRRG y 123LRRG.

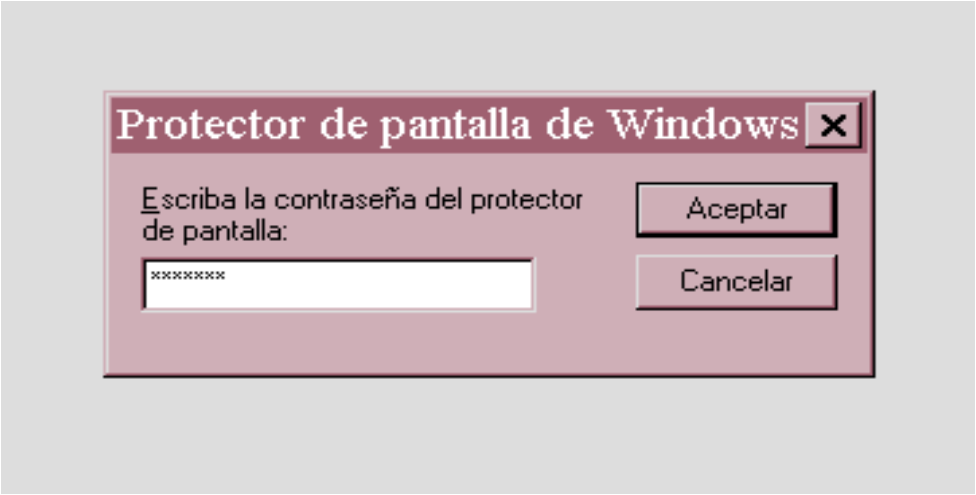
*Debe estipularse la cantidad de caracteres numéricos a usarse en la clave.

*Debe estipularse la cantidad máxima de caracteres.

-Las claves deberán ser cambiadas mínimo cada 30 días. Para los casos de claves de usuarios altamente sensitivos deberá evaluarse un tiempo mayor de cambio.

-Los intentos fallidos deberían ser máximo en un total de tres con clave incorrecta. Cumplidos los tres intentos fallidos, el usuario debe quedar inhibido. Estos intentos deben quedar registrados en el sistema para su posterior control.

-Las claves no deben visualizarse. Su almacenamiento debe ser en forma encriptada (codificada).



-Cada acceso a cada recurso debe contener una clave específica y no repetirse.

-Si el usuario considera el cambio de su clave por perdida de su confidencialidad, debe solicitar al Administrador de seguridad, la asignación de una nueva clave inmediatamente.

-Hay programas que contienen usuario y clave por default (defecto) para facilitar su instalación. Esta debe cambiarse una vez que el programa haya sido instalado.

-Las claves deben respaldarse en sobres de seguridad y deberán realizarse pruebas aleatorias para verificar su autenticidad y actualidad.

3.1.3 **Suspensión de Permisos**

Los permisos deben ser suspendidos por las siguientes causas:

-Cuando los empleados se ausenten por Vacaciones.

-Cuando su usuario y clave no haya sido utilizado por un lapso de 30 días.

-A evaluación del Administrador de seguridades y Responsable de Sistemas por accesos en fines de semana y feriados.

-Cuando supere los intentos máximos de accesos fallidos a recursos asignados o no.

En cualquiera de estos casos se debe analizar e investigar los motivos y para rehabilitar el usuario, deberán solicitarse las autorizaciones nuevamente, dependiendo del tipo de suspensión aplicada. Para el caso de suspensiones por inactividad del sistema, este debe solicitar la re-entrada de la clave nuevamente.

3.1.4 **Acceso a Datos**

-Los datos serán almacenados en medios magnéticos tales como disquetes, cartuchos o cintas. A estos datos, solo podrá accesar el personal autorizado.
-La información impresa debe clasificarse de acuerdo a su seguridad.

-En caso de accesos fallidos a datos, el sistema debe mantener dicha información en detalle con el nombre del usuario, fecha, aplicación, archivos, etc. a los que se pretendía accesar, así como también el número de intentos.

-De igual forma el sistema debiera llevar un control sobre los intentos exitosos posteriores a varios intentos fallidos. Estos pueden manejarse a través de logs (archivos de actividades cronológicas) de seguridad que deben ser revisados periódicamente por el Administrador de seguridad.

-Las empresas deben diseñar el procedimiento que les permita asegurar con éxito el Control de las seguridades de accesos a datos.

3.1.5 **Acceso a Programas y Utilitarios**

Los accesos a programas y utilitarios deben estar segmentado de acuerdo al perfil del usuario. La clasificación general es:

- Los usuarios del sistema
- Los programadores del sistema y,
- Personal de producción.

Los **usuarios del sistema** son los que podrán generar transacciones reales, o usar las funciones del sistema en producción. Podrán también accesar a los archivos generados por el sistema producto de las transacciones.

Los **programadores** solo deben tener acceso al ambiente de pruebas o desarrollo. No deben tener acceso a transacciones reales o a accesar a funciones del sistema en producción.

-El **personal de producción**, debe asegurarse que acceda solo a la información definida para cada usuario. Podrá efectuar las tareas definidas para el área de producción pero previniendo el acceso a datos mediante cualquier tipo de herramienta de programación o a través de programas de aplicación.

-Las bibliotecas de los programas y utilitarios deben estar separadas tanto para desarrollo como para producción.

-Es importante que los programas en desarrollo también sean mantenidos a nivel de versión y con los datos de fecha, hora y usuario que lo desarrolló. Es vital mantener al menos la última y penúltima actualización, de esta forma en caso de reversión se podrá ir a cualquiera de las dos últimas versiones.

-En caso de ser necesario, sí se puede permitir el acceso de bibliotecas del ambiente de desarrollo tanto al usuario del sistema como al personal de producción.

-Antes de que un sistema sea pasado a producción debe efectuarse una evaluación del nivel de seguridades que brinda ese programa o utilitario. Es importante que un Auditor de Sistemas y el responsable de Control Interno verifique para determinar si el sistema cumple con las especificaciones técnicas y contiene las seguridades y controles adecuados.

-Los cambios que se efectúen posteriores a programas en producción deben efectuarse de acuerdo al Control de Cambios.

3.1.6 **Controles de Aplicación**

Los Controles de Aplicación se constituyen en aquellos enfocados a controles por los usuarios y controles por los sistemas. Los controles por los usuarios están dados sobre los datos de entrada, datos fijos, ítems rechazados o en espera, datos de salida. Los controles por los sistemas se enfocan en los datos de entrada, ítems en espera, y sobre el procesamiento.

Los controles **por los usuarios** se refieren a la responsabilidad que el mismo debe tener en la preparación y aprobación de las transacciones (datos de entrada); en la modificación de datos fijos en los archivos maestros y de tablas del sistema responsabilizándose por la integridad y exactitud de los mismos (datos fijos); en el control de las transacciones rechazadas o en suspenso, las cuales deben ser corregidas inmediatamente de acuerdo a su fecha contable (ítems rechazados y en suspenso) y finalmente es el responsable de los errores o desviaciones presentadas y detectadas en los **datos de salidas.**

Los Controles por los sistemas son aquellos que proveen y garantizan que los datos ingresados son digitados íntegramente (datos de entrada); que los ítems rechazados y en suspenso se identifiquen correctamente y se mantengan

pendientes de una solución (ítems rechazados y en espera); y finalmente que el sistema posea mecanismos de control del procesamiento para asegurar que la información fue procesada con los archivos de datos correctos y además brindando a través de las diferentes etapas del procesamiento, un seguimiento de la transacción que permita mantener una adecuada evidencia de auditoría (sobre el procesamiento).

Entre los diferentes **controles por los sistemas** se pueden citar los de **entrada de datos**, los cuales están dados mediante la generación de controles por transacciones, controles por totales, controles por secuencia, controles por tamaño de registro, verificación de clave, etc. Estos controles no deben ser seleccionados sino mas bien aplicados todos, ya que tienen una función específica durante todo el trayecto de la operación de entrada.

- Con los Controles por transacciones se establece una aprobación de la misma antes de su procesamiento, esto en aprobaciones automatizadas.

- Para aprobaciones manuales es preferible que esta sea dada al final del procesamiento o cuando la transacción ya está completa, **ejm.:** Cuando se efectúa un ingreso de una compra en el sistema de compras y la aprobación del pago de la misma se realiza antes de dicho ingreso al sistema, mediante firma en un documento; no se estará seguro de que el ingreso se haya efectuado de forma correcta con las cantidades, proveedor y demás datos de la transacción original. Para evitar fraudes, es importante en este caso aprobar o firmar una vez que la transacción haya sido completada, es decir al final.

- Existe otro tipo de controles que van dirigidos al mantenimiento de la información, respecto de cambios de ítems, precios, cantidades, etc.

- Con los Controles por Totales se establece un registro que asegure que todas las transacciones ingresadas sean totalizadas.

- Los Controles por Secuencia son aquellos que automáticamente o manualmente va generando una secuencia del registro ya sea a nivel de formularios pre-numerados o a través de una secuencia generada automáticamente por documento que se ingresa.

- Los Controles de tamaño de Registro confirman que la longitud del mensaje quede registrada de acuerdo a los parámetros técnicos establecidos y se evite la transmisión de información no contemplada en la transacción. En algunos casos también puede evaluarse la necesidad de transmisión de la información de forma codificada la cual hará más difícil el descifrar la información. Esto último es muy usado cuando la información es altamente sensitiva.

- Los Controles de Aplicación deben en todo caso asegurar que los usuarios accesen o afecten sólo lo autorizado y definido para cada uno de ellos.

3.1.7 **Controles de Actividades del Programador de Sistemas.**

Las Actividades del programador de sistemas deben asegurar que el programa diseñado cumpla con los requerimientos solicitados, seguridades e inviolabilidad del caso. El Responsable de sistemas se encargará de verificar antes de que el programa sea puesto en producción, de que el programador haya documentado debidamente el programa o cambio, que se hayan efectuado las rutinas de validación y verificación y de que se hayan completado las pruebas del sistema.

Es importante que se realicen verificaciones de las entradas y salidas de datos para todos los registros y que sea imposible la manipulación de algún registro en particular, por ejm.: Los programadores de aplicaciones bancarias (cuentas corrientes o ahorros) podrían programar débitos o créditos a cuentas sin que estas sean detectadas a simple vista. Es vital que se implante un mecanismo de control y verificación que certifique que el programa en mención cumple con los requerimientos solicitados y las seguridades del caso.

3.1.7.1 **Casos Reales sobre accesos no autorizados a sistemas informáticos y fraude - El Pentágono, Citibank, Banco Barings de Londres, Universidad Spring Arbor de Michigan y Proinco-Ecuador**

Caso 1: Acceso al Sistema del Pentágono.

Debido a las implicancias políticas y estratégicas que vivió EE.UU. en la crisis con IRAK, la noticia se divulgó enseguida. El subsecretario de Defensa, John Hamre, se apresuró a desmentir que el acceso del hacker al Pentágono, haya sido efectuado a sus sistemas secretos. Puntualizó que si hubieron entradas, pero estas fueron a la red de información no clasificada. Así mismo trató de visualizar el ataque como "un juego" según sus expresiones, con el propósito de quitarle lo dramático de la situación.

A los pocos días del ataque, fue detenido finalmente el joven sospechoso de haber entrado ilegalmente a las computadoras del Pentágono. El pirata parece ser que era un israelí llamado **Edhud Tenebaum** de 18 años cuyo nombre ficticio (nick) es "el analista" y que entró desde las computadoras y la red de su escuela para no dejar rastros personales de su paseo virtual por las instalaciones militares americanas.

Además del Pentágono, el joven habría pirateado a otros diversos organismos de Israel y otros tantos de los Estados Unidos. Las informaciones contrastadas recogidas por estos dos países habrían dirigido finalmente a descubrir la identidad del joven.

Además de "el analista" también se detuvieron a un grupo de jóvenes que supuestamente colaboraron en su entrada al sistema del Pentágono. Una vez que se descubrió esta entrada, los responsables

de la misma pusieron tras la pista del pirata informático a un total de 47 agentes del FBI.

Pero producto de este caso, apareció un documental sumamente detallado por Discovery Channel durante los primeros meses del año 98 donde se indicaba que el mismo departamento de Defensa, ya había sido atacado por un hacker en el **año de 1994** pero que por razones de seguridad en dicho momento, el problema fue poco divulgado.

Como este caso, existen muchos más que han sido presentados a público en general sobre fraudes informáticos a entidades financieras, en la cual los piratas informáticos accesan a las computadoras centrales de las mismas, manipulando saldos de las cuentas bancarias a su favor mediante un no tan complejo método, pero con un gran grupo de gente especializada en este tipo de fraudes. Conviene entonces que conjuntamente con los avances tecnológicos, las empresas se preparen y, preparen sus sistemas, invirtiendo en tecnología de punta que permita disminuir los riesgos y en muchos casos eliminarlos por completo.

Caso 2: Fraude a Citibank

Este caso es el único documentado en la historia de los robos a bancos a través de sus sistemas. El robo lo ejecutó un pirata informático de nombre **Vladimir Levin**, de nacionalidad Rusa, quién ingenió y diseñó el más conocido robo de la historia **en 1994** por un monto de 10 millones de dólares del Banco Citibank.

Este caso tuvo un gran despliegue publicitario tanto en Estados Unidos como en Europa. La forma de operar de este hacker (pirata informático) era accesando al sistema del Citibank y asignando

millones de dólares desde varias cuentas de clientes en diferentes oficinas de Citibank alrededor del mundo, a las cuentas de sus cómplices ubicados en: California, Israel, Finlandia, Alemania, Paises Bajos y Suiza. Todo esto lo hacía desde San Petersburgo en Rusia y sin separarse de su teclado. Fue arrestado por la Interpol en el año de 1995.

Este caso es extraordinario, no solo por el monto de dinero que fue robado ni el método utilizado, sino por el revuelo que causó en la comunidad Financiera y a la Industria de Seguridad del Internet.

Con este caso, se renovaron preguntas acerca de como el crimen informático prevalece y porqué el sector financiero y comercial son adversos a reportarlos.

Al respecto surgieron en su momento comentarios tanto del sector financiero como de los fiscales e Investigadores del caso. Por su lado el sector bancario a través de sus representantes indicó que el incidente de Citibank fue una casualidad y que de acuerdo a la ley, el sector financiero debe reportar las pérdidas experimentadas por estos casos y que, el sugerir que ellos esconden información es un error. Por otro lado los fiscales e Investigadores se oponen a estas declaraciones indicando que el caso no fue simple casualidad y, que en las experiencias adquiridas trabajando con el sector financiero y comercial sucede que, cuando ellos ven problemas, los niegan y cubren todas las evidencias de lo que pasó con el propósito de evitar perder la confianza que el público deposita en la industria, y también para evitar tener problemas con sus superiores.

Actualmente el FBI de Nueva York desde el caso de Citibank indican que han podido incursionar en el sector privado en aproximadamente

500 compañías, y aunque no han tenido una gran respuesta, saben que el camino que siguen es el correcto para proteger a las empresas.

Los crímenes cometidos a través de computadoras se extienden más allá del robo de dinero en efectivo o a través de tarjetas de crédito. También se propagan grandemente a robo de secretos comerciales y estrategias corporativas.

Finalmente, Citibank expresó a través de Amy Dates, vocera del Banco; que a pesar de este incidente, no perdieron un solo cliente y que se alegran de haber tomado muy seriamente el suceso y que trabajarán con la justicia en forma vigorosa para determinar a los responsables de estos actos.

Caso 3: Fraude a Barings Bank of London

En Febrero de **1995**, El banco con más años en Londres, Barings Bank se vino abajo con pérdidas de más de Un Billón de dólares. El escándalo estremeció al mundo bancario internacional ya que se produjo por un empleado del Banco de nombre **Nicholas (Nick) William Leeson** de 28 años, quién se desempeñaba como Trader (negociante) del Banco y quién fue culpado por el gran desastre. Actualmente y después de haber permanecido en las cárceles de Alemania, fue extraditado a Singapour donde se sigue el proceso. Leeson fue el único envuelto en el colapso de Barings Bank, aunque los investigadores señalan que los Ejecutivos del Banco fueron también culpables.

El caso ha sido analizado por políticos, investigadores y gente de la banca internacional, y todos coinciden en que el error estuvo en el mismo banco, al permitirle a Lesson iniciar y terminar una operación sin ningún tipo de control o supervisión de sus actividades. El era director tanto del front-desk es decir responsables de las

operaciones; como del back-office es decir de la evaluación diaria de los compromisos efectuados, es decir, el nivel de **riesgos adquiridos**. *En otras palabras, la misma persona debía tomar las decisiones y controlar esas decisiones para impedir que se corriesen demasiados riesgos*.

En definitiva, la caída del Banco Británico se debió a pérdidas acumuladas por malas negociaciones de Leeson. El estudio de dos oficiales investigadores reveló que el derrumbamiento de Barings Bank se debió realmente a la "Incompetencia" en la Administración y la falta de vigilancia en tres importantes áreas donde se cometieron equivocaciones mayores y estas fueron: Sistemas, Supervisión y Control Interno.

En las tres áreas se descuido completamente la importancia del control. Y se indica la "importancia del control" puesto que Barings Bank tenía Auditores internos pero no se dio importancia a los informes presentados por dichos auditores. Era evidente que sus funcionarios no tenían el conocimiento y destrezas necesarias para cubrir cada parte del negocio. Barings Bank contaba con información, pero no fue usada por negligencia.

Y todo ello parece cierto, ya que la dirección londinense del Barings estaba informada de las operaciones que realizaba Leeson, ya que transfirió fuertes sumas durante los dos meses anteriores a la caída del banco (400 millones de libras prestados por cerca de veinte bancos japoneses). Quizá Nick Leeson mintió sobre las verdaderas razones por las que pedía estas transferencias, sin embargo, parece extraño la falta de curiosidad de los directivos en cuanto al destino de importantes sumas de dinero.

Realmente la catástrofe de Barings pudo ser evitada. Reportes de Auditoría Interna del Banco en el **año de 1994** (un año antes del suceso) mencionaron la necesidad de cambios en la operación del Banco. Si este reporte se le hubiera dado la importancia del caso, el derrumbe hubiera sido advertido e impedido ya que, los auditores expresaron en su informe claramente el peligro de que, Nick Leeson tenga ambas responsabilidades en la negociación, así como también su habilidad para infringir el sistema del banco. Los Administradores del Banco ávidos del dinero fácil producto de las negociaciones, no siguieron estas recomendaciones y las consecuencias fueron dramáticas.

Caso 4: Fraude a la Universidad (cristiana) Spring Arbor en Michigan.

En Mayo de **1995** se desató otro escándalo por Fraude. Esta vez le tocó a la Universidad Spring Arbor ubicada en Michigan. El acusado: **John Bennett** de 57 años, cristiano evangélico que disfrutaba de una reputación intachable en los círculos altruistas de Filadelfia.

La forma de operar de Bennett consistía en aplicar el sistema clásico de Pirámide de Ponzi, el cual permitió a Charles Ponzi despojar de su dinero a varias personas de Boston las cuales perdieron todos sus ahorros. Ponzi convencía a la gente de entregar su dinero a cambio de darles un rédito del 50% al término de tres meses. Con los fondos de quienes se animaban a invertir, Ponzi saldaba las cuentas que se iban venciendo, pero la mayoría de los primeros "beneficiados" re-invertían sus ganancias. Como era de esperarse, la gigantesca pirámide acabó por venirse abajo y miles de personas fueron estafadas.

El sistema de Bennett en consecuencia era una pirámide, la cual fue descubierta por Albert Meyer, un profesor de contabilidad de la universidad de Spring Arbor y en la cual también era contador. Meyer vio en los estados de cuenta de la Universidad, transferencias altas de dinero a una cuenta bancaria perteneciente a una fundación llamada Herencia de valores. Investigando el caso, Meyer fue informado, que Herencia de Valores era una fundación que les servía de intermediaria entre la Universidad y la Fundación Nueva Era (con sede en Pennsylvania) de la cual Bennett era su Director. Bennett indicaba a las instituciones incautas que él repartía dinero de benefactores anónimos. Así si una institución sin fines de lucro reunía cierta cantidad en donativos como era el caso de la Universidad Spring Arbor, "los benefactores" se comprometían a aportar una suma igual.

Al conocer Meyer esta información, sus dudas respecto a si era o no una pirámide de Ponzi, quedaron despejadas. Luego de pasar un tiempo en el cual él seguía investigando el tema y conversando con varios funcionarios de Spring Arbor, esta recibió su dinero con el rédito ofrecido. En estas circunstancias, la Universidad no podía desconfiar cuando ellos recibían su dinero crecido y puntualmente, sencillamente lo tomaban como un préstamo sin garantía, el cual siempre era devuelto puntualmente.

Meyer entonces agudizó más sus investigaciones e incluso llegó a la máxima administración de la Universidad a exponer su preocupación, pero como respuesta obtuvo de que " fue duro hacer crecer los fondos y que no necesitaban de su intromisión". A pesar de ello, Meyer solicitó al Servicio de Recaudación fiscal copias de las declaraciones de impuestos. Aquí pudo observar que Bennett a pesar de recibir a manos llenas las inversiones, no había ningún registro de ellas.

Luego de la serie de investigaciones y consultas que realizó Meyer, se descubrió completamente el Fraude. Bennett fue acusado de fraude financiero y de transferir indebidamente más de 4,2 millones de dólares de las cuentas de la fundación, a la de sus propios negocios. Las pérdidas estimadas ascienden a más de 100 millones de dólares.

Caso 5: Proinco Sociedad Financiera S.A (Ecuador)

En el mes de junio de 1999 se descubrió un perjuicio de más de cinco millones de sucres contra Proinco Sociedad Financiera S.A., por parte de un sujeto que utilizó ilícitamente la tarjeta mastercard gas # 550141007500776. Aunque no significó mucho dinero, esté caso fue un ejemplo de como se estafó a esta entidad ecuatoriana con la utilización de una tarjeta que por error no había sido anulada.

Este caso no es el único ni será el último de muchas formas de fraudes con dinero plástico que se producen a nivel mundial y del cual nuestro país no es la excepción. Existen movimientos especializados para fraudes con dinero plástico, que van desde montaje de cajeros falsos, clonación de tarjetas, hasta la compra de números de cuentas de poco movimiento para sustraer el dinero sin ser detectado fácilmente. Estos grupos trabajan regularmente con personal insertado en las mismas instituciones a las que les realizan los fraudes.

Estas anomalías suelen ser detectados sólo cuando el cliente presenta su reclamo a la institución financiera, sin embargo, muchos de estos casos no son solucionados debido a la ausencia de control en los procesos. Normalmente la misma persona que comete el fraude es quién recibe el reclamo o quién lo procesa, lo cual difícilmente permite detectar los fraudes.

3.2 Control de Cambios

3.2.1 **Razones para establecer un Control de Cambios**

Es importantísimo el determinar mecanismos para dar cumplimiento a un Control de cambios efectuados en cualquier elemento del ambiente de producción como pueden ser programas, equipos, utilitarios, etc. Con esto se da una estructura de formalidad a la administración de los cambios a fin de que estos sean evaluados técnicamente y a nivel de empresa o negocio y, para que los cambios sean incorporados de forma consistente con la respectiva autorización del Responsable de sistemas.

Así mismo el control de cambios se completa con el análisis de impacto en el usuario final el cual debe estar en pleno conocimiento de los mismos. Estos riesgos deben ser evaluados y analizados con antelación.

El control de cambios es una herramienta fundamental para mantener registro cronológico de lo que está sucediendo en nuestro sistema computacional o sus dispositivos. No solo es un medio de información que permite actualizar la documentación técnica sino también permite la toma de decisiones respecto a la solución de fallas o inconsistencias presentadas posterior a las implementaciones de dichos cambios.

Como ejemplo se cita un caso sencillo en el área de facturación de una empresa que no contempla el control de cambios. Por efectos de las leyes impositivas una empresa decide eliminar de la facturación la Retención en la Fuente. Dicho cambio es solicitado por el Gerente Administrativo al Gerente de sistemas. El cambio se realiza y en la siguiente facturación ya no consta el valor de la retención en la fuente, pero se determina que el Subtotal más el Impuesto al Valor Agregado no coincide con el Total de la factura.

El Gerente Administrativo comunica al Gerente de sistemas el particular y este último busca al programador que realizó el cambio para exponerle el problema. El programador no está, se encuentra de vacaciones. ¿Cuál considera usted que

es el resultado de este caso?. Pues muchos, pérdida de tiempo, falta de documentación, imposibilidad de delegación del trabajo a otro programador por falta de información, retrasos en la facturación, costos por incumplimiento de facturación, afectación en el flujo de caja y muchos innumerables problemas más. Ahora la solución del problema era realmente sencilla si se contaba con la información del Cambio que había realizado el programador, cuyo trabajo pasó a producción sin la supervisión y aprobación debida. El problema fue que el programador al estructurar un nuevo algoritmo para el campo Total factura, tomó solamente el campo del Subtotal y eliminó el campo de retenciones y lamentablemente el campo del I.V.A también. Estos inconvenientes podrían haberse solucionado llevando un Control de los Cambios.

3.2.2 **Procedimiento de Control de Cambios**

Para el caso de los cambios en programas o utilitarios se seguirá el siguiente procedimiento.

-Recepción del requerimiento por parte del usuario autorizado.

- Evaluación del impacto a causarse con el cambio.

- Aprobación de usuario de los riesgos e impacto a causarse con el cambio.

- Ejecución del cambio en ambiente de desarrollo.

- Definición de pruebas del cambio solicitado.

- Pruebas del cambio por personal de desarrollo en ambiente de desarrollo.

- Auditoría de sistemas al cambio a realizarse.

- Control Interno del cambio a realizarse.

- Depuración del cambio luego de auditoría y control interno.

- Pruebas del cambio por parte de los usuarios, en ambiente de desarrollo.

-Aprobación formal del Usuario en el registro de control de cambios.

- Aprobación formal del Responsable de Sistemas en el registro de control de cambios.

-Determinación de Instrucciones y criterios por escrito, necesarios para la correcta transferencia al ambiente de producción y su reversión en caso de que sea necesario ejecutarlo.

-Determinación de lugar, fecha, hora, recursos físicos y humanos requeridos para la implementación del cambio en el ambiente de producción.

Para el caso de cambios en equipos (hardware) se seguirá el siguiente procedimiento.

-Recepción del requerimiento por parte del usuario autorizado.

-Evaluación del impacto a causarse con el cambio

-Aprobación de usuario de los riesgos e impacto a causarse con el cambio.

-Definición de pruebas del cambio solicitado

-Determinación de Instrucciones y criterios por escrito, necesarios para el correcto cambio de hardware.

-Determinación de lugar, fecha, hora, recursos físicos y humanos requeridos para la implementación del cambio en el ambiente de producción.

-Ejecución del cambio.

-Aprobación formal del Usuario en el registro de control de cambios.

-Entrenamiento al usuario

-Actualización del inventario de equipos

-Actualización del inventario de configuración de equipos y de los planos de la sala de computación.

-Revisión de contratos de mantenimiento y garantías para los equipos, de tal manera que se asegure el soporte necesario para la configuración efectuada.

3.2.3 **Modelo de Formato para Control de Cambios**

EJEMPLO DE FORMULARIO DE CONTROL DE CAMBIOS
Nombre de la Aplicación Afectada:
Nombre del proceso(s) afectado(s):

Descripción: Condición actual Fecha:	***Observaciones***
Descripción: Condición después del cambio / creación	***Observaciones***

Beneficios/Motivos del Cambio	*Propuesto por:*

Aprobado Usuario (nombre, fecha, firma, y comentarios)
Aprobado por:

PROBADO EN DESARROLLO *POR*	*AUTORIZADO POR* *Gerencia de Sistemas*	*Lugar y fecha de implementación* *Hora:*
…….. *Firma* *Nombre:*	……... *Firma y Sello*	*Recursos Requeridos:*

Acompañe a este formulario, la información técnica respectiva al cambio /creación.

3.3 **Producción y Operaciones**

3.3.1 **Criterios a aplicarse en los controles de Producción y Operaciones**

Los criterios están dados en la operación de normas sólidas, consistentes, confiables y seguras que permitan entregar el servicio con la mayor calidad.

Estos criterios serán aplicados a los aspectos organizativos, de programación, seguimiento de la producción, medios de almacenamiento, documentación y administración de problemas.

3.3.2 **Procedimientos de la función de Producción y Operaciones.**

Para el caso de la Organización del área de producción y operaciones se contemplará lo siguiente:

- El personal de operación no deberá desempeñar ningún rol en la creación o modificación de programas o aplicaciones o de sistemas.

- No deberá tener responsabilidades de actualización del sistema operativo.

- No deberá tener acceso como usuario a aplicaciones específicas.

-Deben tener una descripción del cargo y funciones específicas y ser adecuadamente entrenado para cumplir con sus responsabilidades.

-Deberá contar con adecuada supervisión para asegurar el correcto cumplimiento de sus deberes.

Para el caso de la Planeación y seguimiento de la producción se contemplará lo siguiente:

-Solo las tareas autorizadas serán procesadas con datos de producción, minimizando así el riesgo de omisión y con un orden y planificación predecible.

-Es preferible que las actividades de planeación de carga, ejecución y seguimiento de procesos sean lo mas automatizado posible.

-En casos de que la intervención del operador sea inevitable, deben entregarse instrucciones precisas para las actividades a realizar, las cuales deben ser registradas y analizadas posteriormente.

-En caso de resultados emergentes, se deberá contar con procedimientos de contingencia para dar respuesta a dichos resultados.

-La planeación de los procesos debe considerar la prioridad de este entre las diferentes aplicaciones.

-Deben implantarse controles para prevenir o detectar la ejecución de tareas no autorizadas por la planeación de la producción.

-Para los casos en que usuarios requieran de tareas no establecidas o incluidas dentro de la planeación de la producción, se debe establecer un procedimiento de excepción adecuadamente controlado y con las autorizaciones correspondientes.

-El ambiente de producción y los procedimientos de operaciones deberán garantizar que sea utilizada la versión correcta de programas y los archivos respectivos.

Para el caso de la Protección de medios de almacenamiento se contemplará lo siguiente:

-Operaciones, es responsable de que los datos almacenados en medios magnéticos se encuentren adecuadamente protegidos, controlados y que sean auditables.

-Para controlar la seguridad física de medios tales como cintas, cartuchos y disquetes, estos deben ser almacenados en un área protegida, existiendo un registro de la ubicación de todos los medios magnéticos que son utilizados en el área de sistemas.

-Deberán registrar todos los ingresos y salidas de medios magnéticos de la instalación.

-Los medios magnéticos almacenados deberán debidamente etiquetados con su contenido, fechas y orden cronológico.

Para el caso de la documentación se contemplará lo siguiente:

-Una planeación o cartilla diaria, paso a paso de las actividades normales del operador.

-Una planeación o cartilla diaria de los procesos con inicio y fin de cada operación.

-Los procedimientos de contingencia para los procesos

-Los procedimientos de contingencia para las fallas de hardware, software, telecomunicaciones.

-Las instrucciones en el manejo de medios magnéticos y registros de aquellos que ingresan o son retirados de la sala.

-El registro de problemas del área de operaciones

-El registro de accesos a la sala de computación.

-El responsable del área de sistemas debe asegurar que toda la documentación requerida para las operaciones esté completa, correcta y actualizada.

Para el caso de la administración de problemas se contemplará lo siguiente:

-Todas las fallas operacionales e incidentes anormales, deberían ser registrados en un Reporte de Problemas, con los detalles de hora, tipo de problema, síntomas y las acciones iniciales realizadas. Cada reporte deberá ser identificado en forma única y se deberá asignar lo más rápidamente posible la responsabilidad para su investigación y resolución.

-Mantener un registro de los problemas el cual deberá ser revisado periódicamente por el Responsable de sistemas.

-Todas las llamadas que requieran el soporte de proveedores o personal de sistemas, deben ser registradas con información del tiempo de respuesta de tales llamadas y las acciones tomadas, para su análisis posterior.

-Debe existir un procedimiento de revisión regular que incluya un análisis de tendencia de los problemas y permita asegurar que todos son resueltos.

-Se debería considerar la evidencia registrada en el sistema de administración de problemas, a objeto de tomar decisiones relativas a la oportunidad que se realice el mantenimiento de rutina y reemplazo de equipamiento.

-Todas las soluciones identificadas como cambios a ser incorporadas en el ambiente de producción, deberán ser registradas, seguidas y manejadas por los procedimientos de control de cambio. Adicionalmente se deberá registrar el origen de la solución, identificando cual fue el problema o falla.

-Informar a todos los usuarios afectados por el impacto de los problemas identificados y de los progresos obtenidos en la solución del problema.

CAPITULO 4: *RESPALDOS Y RECUPERACION DE PROGRAMAS*

4.1 **Procedimiento de Respaldos y Recuperación de Programas**

-Los Respaldos deberán ser efectuados de acuerdo a la periodicidad dependiente de su contenido. Es importante que se mantengan respaldos diarios, semanales, quincenales y mensuales de información altamente sensitiva. Para el análisis de la periodicidad del respaldo debe tomarse en cuenta el volumen de información perdida en caso de contingencia y la fecha del último respaldo. Por ejemplo, si el respaldo se hace diariamente y surge una contingencia un día miércoles, se perderá información no respaldada equivalente a un sólo día, partiendo de la existencia del respaldo diario del día martes.

-Los sistemas operativos y programas en general deben ser guardados en su versión original y la que se utiliza en producción.

-En caso de cambios se requiere que se mantengan respaldadas siempre las versiones originales, la versión antes del cambio y la versión producto del cambio, asemejándose a un esquema generacional de abuelo, padre e hijo.

4.2 **Procedimiento de Almacenamiento de Medios Magnéticos**

-Los respaldos de datos y programas de alta sensibilidad deben siempre mantenerse en bóvedas externas, a prueba de fuego. Se escogerán sitios de preferencia uno en la ciudad donde opera la empresa pero distanciada de la misma, y otra fuera de la ciudad. Una copia de los archivos claves puede ser mantenida dentro de las instalaciones de la empresa con las debidas seguridades, para permitir su utilización en procesos de recuperación.

-Adicionalmente se deben contemplar controles asociados al transporte de dichos respaldos. Estos controles pueden estar dados por uso de valijas con llave, registros de movimientos de los respaldos hacia y desde las bóvedas de seguridad o caja fuerte y el Uso de vehículos de seguridad donde sea apropiado.

-Los medios magnéticos deben ser etiquetados adecuadamente de tal forma que permita su obtención y fácil identificación y recuperación de los archivos requeridos.

-Normalmente los respaldos que son requeridos y que se considerarían como información altamente sensitiva son:

*Programas elaborados por la propia empresa

*Programas adquiridos mediante licencia y que sean sujetos a actualizaciones permanentemente y/o customizaciones.

*Archivos de Datos: Información contable, financiera, administrativa, de compras, y de producción y otros que la empresa estime sensitivos.

-Los procedimientos de respaldos deben ser continuamente probados de tal forma que se compruebe la efectividad de los mismos mediante su restauración y verificación.

-Así mismo se debe evaluar periódicamente los sitios de respaldo, su facilidad de acceso y los procedimientos de control de acceso a los medios magnéticos almacenados.

-Al menos anualmente deben ser revisadas las cintas, cartuchos y disquetes mantenidos por largos periodos de tiempo en las bóvedas de seguridad. Deben ser probados para constatar su operación.

-Adicionalmente, deben establecerse todos los requisitos que sean necesarios para implementar los controles básicos en la recuperación de programas o datos. Estos serán de responsabilidad del analista que desarrolló el programa, o del usuario en el caso de recuperación de Datos. Es importante que el Administrador de Seguridad de Datos asesore en estos requisitos.

-Junto con el almacenamiento magnético de programas, debe considerarse el almacenamiento de documentación que corresponda a los procedimientos de

operaciones para ejecución de respaldos, Procedimientos para recuperación de fallas menores usando los respaldos de la instalación, Procedimientos de recuperación de fallas mayores usando los respaldos externos, Procedimientos de Respaldos luego de la Recuperación por fallas menores y mayores (retorno a la normalidad).

4.3 **Modelos de Formato Control, Recuperación y Almacenamiento de Respaldos.**

EJEMPLO DE FORMULARIO DE CONTROL Y ALMACENAMIENTO DE RESPALDOS		
Obtención del Respaldo (Lugar y fecha)		
Hora		
Identificación del Respaldo		
Detalle-contenido		
Responsable Obtención Respaldo		
Firma		
Medio de Respaldo y cantidad		
Firma de Jefe de Area responsable de obtención de respaldo		
ACUSE DE RECIBO DEL RESPONSABLE DE SEGURIDAD DE RESPALDOS		
Sitio1 Entrega de respaldo (Fecha)		
Responsable de Recepción		
Hora de recepción		
Firma		
Sitio2 Entrega de respaldo (Fecha)		
Responsable de Recepción		
Hora de recepción		
Firma		
Sitio3 Entrega de respaldo (Fecha)		
Responsable de Recepción		
Hora de recepción		
Firma		
ACUSE DE RECIBO DEL RESPONSABLE DE SEGURIDAD DE RESPALDOS		
Sitio1 Entrega de respaldo (Fecha)		
Responsable de Recepción		
Hora de recepción		
Firma		
Sitio2 Entrega de respaldo (Fecha)		
Responsable de Recepciòn		
Hora de recepciòn		
Firma		
Sitio3 Entrega de respaldo (Fecha)		
Responsable de Recepción		
Hora de recepción		
Firma		

Sitio1= En las instalaciones **Sitio2=** Sitio externo local **Sitio3=** Sitio externo otra ciudad

EJEMPLO DE FORMULARIO DE RECUPERACION DE RESPALDOS			
Solicitado para: Actualización ☐ Restauración☐		Lugar y Fecha:	
Respaldo Obtenido en	Lugar:	Fecha:	Hora:
Identificación del Respaldo			
Detalle-contenido			
Medio de Respaldo			
Ubicación del respaldo: Sitio1, Sitio2, Sitio3			
Solicitado Por		Firma:	
Solicitado A		Firma:	
Custodio que entrega (Nombre)		Firma:	

CAPITULO 5

CONTROLES APLICADOS EN LA ADMINISTRACION DEL PERSONAL.

La administración de personal es un área en la que confluyen varias disciplinas; incluye conceptos de psicología industrial y organizacional, ingeniería industrial, derecho laboral, ingeniería de seguridad, medicina laboral, ingeniería de sistemas, etc. Los temas son diversos como diversas resultan las disciplinas mencionadas anteriormente. Por tanto la Administración de personal se refiere tanto a aspectos internos de la organización como a externos o ambientales.

Podremos entonces definir que la Administración de personal consta de subsistemas independientes como se indica en el cuadro a continuación:

Subsistemas de Administración de Personal.	**Capítulos Abarcados**
Alimentación de RRHH	• Planificación de Recursos Humanos. • Reclutamiento de personal • Selección de personal
Aplicación de RRHH	• Descripción y análisis de cargos • Evaluación de desempeño humano
Mantenimiento de RRHH	• Compensación • Beneficios sociales • Higiene y seguridad • Relaciones laborales
Desarrollo de RRHH	• Capacitación y desarrollo de personal • Desarrollo Organizacional
Control de RRHH	• Base de datos y sistemas de información. • Auditoría de Recursos Humanos

Estos subsistemas están estrechamente interrelacionados y son interdependientes, pero a pesar de ello no existe una forma única de establecerlos, ya que eso va acorde con la empresa y dependiendo de diversos factores como son los organizacionales, humanos y tecnológicos.

Para el efecto, se crean políticas o reglas que permiten dirigir las funciones y asegurar que estas se realicen de acuerdo con los objetivos deseados.

Algunas de estas reglas se crean para establecer “Controles Administrativos” cuya orientación es impedir que los empleados desempeñen funciones que no le pertenecen o pongan en peligro el éxito de funciones específicas.

Los Controles aplicados a la Administración de personal se centran en todos los subsistemas y principalmente en los temas de los cuales se hablará en el transcurso de este capítulo.

5.1 **Objetivo de los Controles Administrativos**

Este capítulo trata sobre los controles que deben establecerse en los puntos sensitivos del área administrativa y a los cuales se va a centrar la temática, como son el personal, su contratación, vacaciones, entre otros.

5.2 **Contratación y término de Contratos**

El proceso de Reclutamiento y Contratación del personal así como de servicios externos debe estar perfectamente evaluado. Los contratos deberán contener integrado en sus cláusulas, las políticas y normas de seguridad de datos que lleva a cabo la empresa.

El personal de servicio externo deberá ser evaluado de acuerdo a los mismos criterios de seguridad aplicados para el personal permanente de la empresa.

Cuando un empleado interno o externo deja de prestar servicios, debe suspenderse las autorizaciones que este tenga tanto de acceso lógico como físico a las instalaciones, sistemas o datos. El ejecutivo principal del área a la que pertenecía el empleado es el responsable de informar de acuerdo a las políticas que establezca la empresa, la ausencia permanente del empleado.

El Departamento Administrativo por su parte deberá revocar todos los permisos de acceso que haya tenido el empleado, así como recuperar las tarjetas magnéticas de acceso y credenciales de la empresa e inhabilitarlas. Deberá verificarse la

devolución de toda la documentación de carácter confidencial que haya sido manejada por el empleado.

5.3 **Políticas Administrativas**

5.3.1 **Vacaciones**

El personal que deba tomar vacaciones y principalmente del área de sistemas de la empresa, lo realizará conforme a las disposiciones internas. Se sugiere que dicho personal no haya dejado de tomar por propia voluntad sus vacaciones por un periodo de 2 años. Algunos fraudes informáticos tienden a descubrirse cuando quienes los comenten toman vacaciones; tiempo en el cual no tienen acceso al sistema o son reemplazados mientras duran sus vacaciones. Cabe indicar al Administrador de Empresas que este es un punto de seguridad básica que debe tomar muy en cuenta dentro de los controles administrativos.

5.3.2 Entrenamiento

El personal de sistemas debe acogerse al plan de entrenamiento que la empresa tenga, siguiendo los estándares y procedimientos de seguridad de datos y a los aspectos específicos de seguridad de su puesto de trabajo.

5.3.2 Uso de Recursos Computacionales

El uso de recursos computacionales para asuntos personales debe quedar prohibido.

El software que cada usuario opere debe ser asignado de acuerdo a su utilización y el cual debe constar con las licencias respectivas.

Los empleados deben estar familiarizados con el almacenamiento de datos de carácter sensitivo o confidencial.

Cabe indicar que cada usuario es responsable por el equipo asignado, software utilizado, datos contenidos en él y utilitarios que opere.

La empresa debe establecer políticas y reglamentos claros respecto del uso de software ilegal (sin licencia) y los no correspondientes a los estándares de la empresa. De igual forma la empresa debe establecer un uso y propiedad claramente establecidas sobre los programas elaborados o desarrollados por personal interno, lo cual normalmente se deja reglamentado dentro de los contratos de trabajo.

- **CONCLUSIONES**

- **Todo proceso de la empresa debe contener actividades de control y seguridad.** Cualquier proceso de la empresa con o sin la aplicación de Reingeniería no puede permanecer sin los controles y seguridades tanto en sus datos como en sus componentes.

- **La ausencia de controles se presenta SIEMPRE en un proceso Reingeniado y CASI SIEMPRE en procesos sin ningún tipo de aplicación de herramientas de mejoras de la eficiencia y productividad.** La Reingeniería es una herramienta metodológica excelente, viable y con grandes resultados y mejoras dramáticas, pero no es menos cierto que deja a los procesos frágiles y débiles, ya que, en su afán de eliminar actividades que no agregan valor; crean un proceso ausente de controles satisfactorios y por consiguiente indispensables. De igual forma, procesos que no hayan pasado por Reingeniería pueden presentar ausencias de controles si estos no han sido considerados estratégicamente.

- **El modelamiento del comportamiento humano no es SUFICIENTE para asegurar niveles de controles y seguridades satisfactorias**. Existen muchos precursores de nuevas técnicas y metodologías dirigidas al modelamiento del comportamiento humano y opuestos a los controles y seguridades habituales. El modelamiento humano no es "suficiente" para asegurar que no se cometerán errores o fraudes en los procesos. El modelamiento humano aplica en temas marketeros, estratégicos y de relaciones humanas en los cuales son muy útiles, pero estos no aplican en términos operativos y de seguridades.

-**Finalmente, los beneficios de tener un sistema de seguridad nunca podrán ser medidos completamente, porque la mayoría de las empresas no sabrán realmente "CUANDO" alguien tratará de quebrantar sus seguridades.** Sin embargo, es fácil determinar objetivamente que los beneficios serán grandes, producto de los costos evitados. Es entonces, en estas circunstancias, donde los sistemas de seguridad son **"Invaluables.** Las únicas ventajas y desventajas que podrían usted encontrar en los

sistemas de seguridad están dadas en la **alternativa** de seguridad que usted escoja e implemente, la cual le brindará mayor o menor seguridad a sus procesos. La otra alternativa que se puede ofrecer, es la de sencillamente no tener ningún sistema de seguridad; lo cual resultaría absolutamente negligente.

- **RECOMENDACIONES**

◊ El administrador de empresas debe recordar que los procesos manuales o automáticos deben ser controlados adecuadamente y suficientemente sin caer en la negligencia o en el exceso. Aquí en este trabajo se ha brindado una herramienta que le permita al menos poder elaborar una lista de los puntos débiles en su empresa y saber que debe controlarlos. Usted cree que todo en su empresa marcha bien y no necesita absolutamente nada de lo sugerido en este trabajo? Si su respuesta es afirmativa, le recomiendo que lea el trabajo nuevamente si ya lo leyó; luego reúnase con su ejecutivo de Sistemas que es el mayormente involucrado en la implantación de controles y seguridades de datos, y pídale que le cuente detalladamente que hace cada área de departamento de sistemas. Le aseguro, que se quedará usted sorprendido de conocer que puede aplicar cada punto de su lista y de que podrá entrar a ese fabuloso mundo; que era antes desconocido e inentendible por usted.

◊ El administrador de empresas debe estudiar todas las alternativas y, si elige la Reingeniería; debe saber qué el nuevo proceso rediseñado **debe** equilibrarlo con una implantación de controles y seguridades suficientes y satisfactorias. Talvez no podrá efectuarlo con el mismo personal de Reingeniería, ya que los conceptos de Reingeniería y controles no comulgan mucho que digamos. Recomiendo entonces que el administrador consulte a su responsable de Sistemas y a su responsable de Reingeniería para llegar a un acuerdo tanto a nivel de productividad y eficiencia del proceso como también de sus seguridades.

◊ El Administrador de Empresas debe involucrarse más en todos los procesos de su empresa, tanto administrativos, operativos y de sistemas. Solo así tendrá una idea total de como se une cada eslabón de la cadena de procesos de su empresa.

◊ No importa cuanto usted invierta en seguridad de sistemas para proteger sus redes, componentes o datos, nunca piense que será una cantidad **"suficiente"** ya que siempre los adelantos tecnológicos exigen más para mantener fuera a los intrusos. Con esto entonces no verá la adquisición de seguridad como un gasto, sino como una **inversión**.

BIBLIOGRAFIA

-Seguridad de Datos, Metodología Price Waterhouse Coopers 1992

-Plan de Contingencias, Metodología Price Waterhouse Coopers 1997

-Como Hacer Reingeniería, Raymond L. Manganelly y Mark M. Klein

-Administración de Recursos Humanos, Idalberto Chiavenato 1994

-Administración de Empresas (teoría y práctica, segunda parte), Agustin Reyes Ponce 1994.

-Revista "Mundo Informático" Edición Abril 1998

-Revista "Selecciones" Edición Junio 1996

-Diario el Universo "Sección Sucesos" Julio-5-1999

Sitios de Internet para consultas:

Detectores de agua	http://www.cam.surf1.com
Extintores de incendio	http://www.pp.okstate.edu/ehs/modules/apw.htm
Acondicionadores de aire	http://www.liebert.com/products
Fuentes Ininterrumpidas de poder (UPS)	http://www.exide.com
Cableado	http://www.wit-sa.com.ar http://www.sidicom.net
Sistemas de seguridad	http://protectiontech.com/
Caso de fraude al Citibank	http://www.infowar.com http://www.discovery-channel.com/area/technology/hackers/levin.html
Caso de fraude al Baring Bank de Londres.	http://www.imd.ch/pub/pfm_9601.html http://www.fsa.ulaval.ca/personnel/vernag/PUB/Barings.E%20.html
Caso fraude a la Universidad Spring Arbor de Michigan.	http://cgi.pathfinder.com/time/magazine/archive/1995/950529/950529.scandal.html
Sistema de Fraude Piramidal.	http://cnet.bigpond.com/Briefs/Guidebook/Crime/ss03a.html

DATOS DEL AUTOR

Nombre	Sonnia Rosado García
Edad	28 años
Título Universitario	Ingeniera Comercial (Administradora de Empresas)
Correo Electrónico	sonnia_ros@hotmail.com srosado@uole.com
País/Ciudad	ECUADOR/Guayaquil

Experiencia en procesos de Reingeniería, Calidad Total, Planes de Contingencia y Seguridades Físicas.