UNVERSIDAD POLITECNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERIA DE SISTEMAS

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

TEMA:

AUDITORÍA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA LA EMPRESA DE ALIMENTOS "ITALIMENTOS CIA. LTDA."

AUTORES:

CHRISTIAN MIGUEL CADME RUIZ.

DIEGO FABIAN DUQUE POZO

DIRECTOR:

ING. RODOLFO BOJORQUE.

2011-2012

CUENCA - ECUADOR

Ing. Rodolfo Bojorque

Certifica

Que el presente informe de monografía fue desarrollado por los estudiantes Christian Miguel Cadme Ruiz y Diego Fabián Duque Pozo, bajo mi supervisión, en base a ellos, autorizo la presentación de la misma.

Cuenca, Abril del 2011

Ing. Rodolfo Bojorque

Director de tesis

Responsabilidad

El análisis de los conceptos y las ideas vertidas en la presente tesis son de total responsabilidad de los autores, y autorizamos a la Universidad Politécnica Salesiana el uso de la misma con fines académicos.

Cuenca, 13 de abril del 2011

Christian Cadme.

Diego Duque.

Dedicatoria

Este proyecto de tesis está dedicado muy especialmente a mi familia, quienes me han sabido apoyar incondicionalmente para la culminación de mi carrera profesional. A todos las personas que me han ayudado a ser una mejor persona y profesional en el proceso de mi vida.

Christian Miguel Cadme Ruiz.

Agradecimientos

A Dios por brindarme salud y la capacidad de cumplir mis metas en la vida. De manera muy especial a mis padres por la confianza y el apoyo que me han otorgado en todo momento. A mi compañero de tesis por el apoyo a la culminación de nuestro proyecto de tesis. A las personas que me han extendido su mano cuando yo los necesitaba. Al jefe de sistemas por brindarnos la ayuda e información necesaria para culminar nuestro proyecto. Al director de carrera por apoyarnos con las revisiones graduales de nuestro proyecto de tesis.

Christian Miguel Cadme Ruiz.

Dedicatoria

La presente tesis le dedico con mucho amor a mi madre Enma Pozo que vive una lucha abnegada de todos los días y más contra su enfermedad donde nunca se rindió y supo salir adelante, eso me ayudo mucho para la culminación de mi carrera, gracias madrecita, a mi padre Cesar Duque que me brindó todo su apoyo cuando más lo necesitaba, sus consejos sus retos que supieron dar la ayuda necesaria para resolver con énfasis los problemas que se daban, a mis hermanos Rodrigo, Paola, Carlos que con el apoyo de ustedes pude continuar con mis estudios, y lo fundamental con sus buenos ánimos en los momentos difíciles de mi vida, a mi novia Katty que con su apoyo incondicional supe valorar mis estudios y sus concejos de vida, a mis tías, primos, sobrinos familiares en general y amigos que supieron darme la luz para culminar esta etapa estudiantil. GRACIAS A TODOS…

Diego Fabián Duque Pozo.

Agradecimiento

Quiero agradecer primero a mi Dios que fue el que me guió todo éste camino lleno de batallas y continuas luchas ante adversidades que se pusieron en ésta etapa de estudio, Al Sr Lautaro Jetón Gerente de Italimentos por prestarnos su empresa para el estudio respectivo, a mi compañero de tesis por haber confiado en mis conocimientos para la realización de ésta auditoría, a mi director de tesis Rodolfo Bojorque por sus conocimientos a la hora de dirigirnos y sus consejos al momento de poner en práctica, al Ing. Cristian Baculima por facilitarnos los activos para la realización de la auditoria informática realizada en sus instalaciones y el tiempo que nos brindó a nosotros para la contestación de las preguntas. GRACIAS TOTALES….

Diego Fabián Duque Pozo.

INDICE

CAPITULO 1

"Descripción de Italimentos Cía. Ltda."

1.1 Reseña histórica

"ITALIMENTOS es una empresa caracterizada desde su origen por su responsabilidad social, espíritu innovador y vanguardista que se ha ubicado como líder de su rama, siempre buscando en todos sus productos, la más alta calidad con el uso de las mejores materias primas, con procesos definidos en todos los pasos, para lograr un producto final de excelente sabor y calidad, que llene las expectativas de nuestros consumidores en todo el país.

ITALIMENTOS tuvo como instalaciones iniciales un pequeño local ubicado en el sector de Yanuncay de la ciudad de Cuenca, en el cual un personal de 4 colaboradores se elaboraban artesanalmente salchichas y chorizos, así como también se comercializaban chuletas y carnes crudas, teniendo como destino final la ciudad de Cuenca y algunas zonas de la provincia de El Oro." *La Figura 1.1.1 muestra la fábrica en sus inicios.*[1]

Figura 1.1.1. Primera fábrica establecida por Don Lautaro Jetón.[2]

"Debido a la acogida entre sus clientes y colaboradores, surgió la necesidad de un nombre que se identificara, y es así como en el mes de Febrero de 1989, nace EMBUTIDOS LA ITALIANA." [1] *La Figura 1.1.2 muestra algunos de los productos ofrecidos por la empresa.*

1 http://www.laitaliana.com.ec/index.php?mod=empresa&id=3
[2] http://www.youtube.com/watch?v=DG1arVmq6SE&feature=player_embedded

Figura 1.1.2 Muestra de algunos productos.[3]

Poco a poco la aceptación por sus productos fue creciendo, debido a que siempre se ha cumplido el compromiso de ofrecer a sus consumidores productos de la mejor calidad y a precios accesibles. *La Figura 1.1.3 muestra las instalaciones de producción de embutidos en la actualidad*

Figura 1.1.3 Centro de procesamiento de Embutidos.[2]

"De la crisis surge grandes oportunidades y es así que en la segunda mitad de la década de los 90, época marcada por innumerables problemas para el país, la italiana, afrontó los riesgos con responsabilidad, inteligencia y dinamismo, para salir airosa y fortalecida, ubicándose como una empresa líder en la región y con una participación de mercado importante a nivel nacional." *La siguiente Figura 1.1.4 muestra los logos utilizados durante el transcurso de brindar servicios por Italimentos.*

Figura 1.1.4 Logos utilizados desde 1988 hasta la actualidad. [3]

[3] http://www.youtube.com/watch?v=DG1arVmq6SE&feature=player_embedded

1.1.1 Misión

"Alimentar y servir con satisfacción."

1.1.2 Visión

"Ser **líderes** a nivel Nacional en la producción y comercialización de **alimentos sanos y nutritivos** en su segmento, con productos elaborados con la más alta tecnología de acuerdo a normas de **calidad** reconocidas internacionalmente, **respetuosos del medio ambiente** y de nuestro entorno, contribuyendo al desarrollo del país, con un equipo de trabajo comprometedor e **innovador** que satisfaga adecuadamente las necesidades de nuestros consumidores." [4]

1.1.3 Ubicación geográfica

Debido a su crecimiento, en el año 1997 se ve la necesidad de ampliar sus instalaciones, y para tal fin, se adquieren terrenos ubicados en el parque industrial, sector de Machangara, en Cuenca donde luego de un largo periodo de diseño y construcción, en el que intervino un numeroso equipo de expertos tanto nacionales como extranjeros se pone al servicio de la comunidad su nueva Planta Industrial el 7 de Diciembre del 2002.

Esta Planta es considerada como una de las más modernas del país por su diseño y facilidades técnicas, así como por la maquinaria alemana de última generación con la que ha sido dotada, llenando así los requisitos de infraestructura necesarias para cumplir las BPM[4]. *La Figura 1.1.3.1 nos muestra la ubicación actual empresa.*

[4] BPM: Buena Practica de Manufactura.

Figura 1.1.3.1. Ubicación actual de Italimentos Cía. Ltda.[5]

1.1.4 Estructura organizacional

La empresa de Italimentos, tiene delimitado sus funciones y obligaciones mediante una estructura organizacional, en la cual se ocupan cargos dependiendo de sus labores dentro y fuera de la organización. *Véase anexo A.*

1.1.4.1 Departamento comercial

Este departamento es muy amplio y de diversas funciones en su trabajo por lo tanto su jerarquía arranca desde el subgerente comercial donde se divide en:

1.1.4.1.1 Sub-Gerente comercial

- Jefe de ventas
    - Supervisores de ventas
        - Vendedores
        - Vendedores de mostradores
- Jefe de distribución

[5] http://maps.google.es/

    - Supervisor de distribución
        - Auxiliar de distribución
        - Operarios de distribución
- Jefe de marketing
    - Trade
        - Mercaderistas
    - Diseñador
        - Auxiliar de diseño

1.1.4.2 Ejecutiva de cuentas

Este departamento realiza un conjunto de actividades necesarias para hacer llegar al consumidor los productos realizados por la empresa y realiza las siguientes funciones:

1.1.4.2.1 Planificación y control

Se precisa, en un tiempo en concreto, las acciones futuras para posteriormente comparar los resultados actuales con resultados históricos para sacar conclusiones de esta comparación.

1.1.4.2.2 Estudio de mercado

Se proporciona información que permite a la dirección de la empresa fijar sus objetivos y tomar decisiones sobre puntos seguros. Este estudio de mercado utiliza diversas fuentes de información y técnicas de recogida de datos para intentar determinar las preferencias de compra de los consumidores.

1.1.4.2.3 Promoción y publicidad del producto

Mediante la publicidad se da a conocer el producto al cliente, se informa de sus características y se destaca el principal atributo que lo diferencia de la competencia. Con

esto se pretende incrementar las ventas.

1.1.4.2.4 Ventas

Organiza la venta directa y la relación con intermediarios. A través de la venta, la empresa consigue sus ingresos o facturación con el objetivo de compensar los gastos de producción y obtener ganancias.

1.1.4.3 Departamento de producción

En este departamento, la fábrica de Italimentos, constituida como la mejor empresa por su producción se encargo de dividir el departamento para que sus productos surjan en el mercado por esto se vio la manera de jerarquizar el departamento de la siguiente manera:

- Jefe de aseguramiento a la calidad
  - Coordinador BPM
    - Operador de limpieza
  - Laboratorista
    - Operador de calidad
  - Inspectores
- Jefe de mantenimiento
  - Auxiliar de mantenimiento
- Supervisores de planta
  - Coordinador de planta
  - Operarios

Para la empresa, se considera uno de los departamentos más importantes, ya que se

realizan métodos adecuados para la elaboración de productos, para ello se debe suministrar al departamento: mano de obra, equipos, instalaciones, materiales, materia prima y herramientas requeridas.

1.1.4.3.1 Ingeniería del producto

Se diseña el producto que se va a comercializar, tomando en cuenta especificaciones para cada una de ellas. Al elaborar el producto se realizan pruebas de calidad para comprobar que el producto cumpla con el objetivo para el cual fue elaborado.

1.1.4.3.2 Ingeniería de planta

Se toma en cuenta especificaciones requeridas para el adecuado mantenimiento y control de equipo.

1.1.4.3.3 Ingeniería Industrial

Se investiga medidas de trabajo necesarias, así como la distribución física de la planta y equipos.

1.1.4.3.4 Planeación y control de la producción

Se establece estándares necesarios para respetar especificaciones, de producciones requeridas en cuanto a calidad, se regula la producción y el stock de la materia prima. También se realiza informes referentes de los avances de producción para garantizar que se está cumpliendo un horario fijo.

1.1.4.3.5 Abastecimiento

Depende de un adecuado tráfico de mercancías para que la materia prima llegue en un horario fijo. Se tiene un control de inventarios, verificando que las compras locales e internacionales sean las más apropiadas.

1.1.4.3.6 Control de calidad

Es el producto final con sus debidas características de calidad por el cual se satisface las expectativas del cliente. Se toma en cuenta las normas y especificaciones requeridas, realizando pruebas de verificación del producto.

1.1.4.3.7 Fabricación

Se realiza el proceso de transformación necesaria para la obtención del producto final.

1.1.4.4 Departamento financiero

En este departamento es muy amplio ya que interactúan varios tipos de personal de suma importancia para la fábrica ya que aquí abarca la parte financiera dividiéndose jerárquicamente en:

- Contador general
    - Auxiliares contables
- Jefe de cartera
    - Recaudador
        - Tesorería
        - Auxiliar de tesorería y recaudación
    - Auxiliares de cartera
- Contador de costos

En este departamento se centra en diversas actividades donde sobresalen el establecer los estados financieros de la organización a la vez se mostrara a continuación las diversas tareas que se efectúan en la fábrica de Italimentos.

- Elegir los proyectos que se efectuaran en la empresa y que son los más adecuados.
- Proponer cuales serán las necesidades financieras en la fábrica.
- Recaudar todos los montos efectuados por días y hacer sus respectivos balances.
- La determinación de activos de la empresa.

- Comprobar el plagio que se suscite en el cobro por día de los productos vendidos.

- Realizar los cobros respectivos a los vendedores por rutas.

1.1.4.5 Departamento de investigación y desarrollo

En este departamento interactúan dos tipos de empleados que son de suma importancia en la empresa estos empleados son los:

- Supervisores de planta

    - Operarios

En este departamento, se encargan de fomentar la investigación y desarrollo de nuevos productos alimenticios, ya que cuanta con una infraestructura adecuada, personal calificado y tecnología para aplicaciones generales. Las principales funciones que se realizan son:

- Desarrollo de productos de Investigación aplicados al campo de la industria alimenticia.

- Desarrollo de productos que solucionen necesidades de la industria alimenticia ecuatoriana con productos altamente competitivos.

- Evaluación de nuevas alternativas para la elaboración de productos producidos por Italimentos.

- Elaboración de fichas técnicas de los productos en investigación y desarrollo.

- Trabajo conjunto con diferentes clientes para el desarrollo de aplicaciones particulares, para futuros procesos productivos de alimentos.

- Estudio de ingredientes y formulación.

- Fijación del objetivo concreto, para obtener una mejora adicional o una rebaja de

costos, hasta formar un producto nuevo.

- Buscar información como: composición e ingredientes de productos similares, composición nutricional y propiedades de los ingredientes, aditivos, etc.

- Especificación de alternativas de formulación y selección de la mejor.

1.1.5 Arquitectura de hardware

1.1.5.1 Topología de la red

La red informática de la empresa "Italimentos Cía. Ltda." se compone del siguiente equipamiento:

- 90 PC's distribuidos en la empresa ubicada en el parque Industrial de Cuenca
- 7 servidores divididos en:
  - 1 servidor de base de datos
  - 1 servidor de internet-proxy
  - 1 terminal server
  - 1 servidor de dominio
  - 1 servidor de desarrollo
  - 1 servidor de base de datos de respaldo
  - 1 servidor de aplicaciones
- Cable UTP categoría 5
- 3 enlaces de fibra óptica que se interconectan switch
- 2 switch 3Com_Baseline-Switch-2948 de 48 puertos cada uno conectados en

cascada

- 3 switch 3Com_Baseline-Switch-2948 de 24 puertos cada uno
- 1 antena de transmisión inalámbrica DIR-300 que provee internet pero no acceso a la red de la empresa
- Conexión a internet que provee empresa “Punto net”

1.1.5.2 Conexiones externas de la sede

Las conexiones externas en la fábrica de Italimentos, tiene como proveedor de servicios de red a la empresa Puntonet, que se encarga de la parte de enlaces y conexiones hacia el exterior, dando soporte cuando existan problemas relacionados con redes.

Mediante un router, propiedad de “Punto net”, se tiene conexiones al exterior hacia diferentes establecimientos comerciales, propiedad de “Italimentos Cía. Ltda.” tales como:

- Italdeli, sector Av. Solano
- Italdeli sector San Sebastián
- Italdeli, sector Virgen de Fátima
- Granja, sector Paute
- Italdeli, Quito
- Italdeli, Guayaquil

1.1.5.3 Servidores

1.1.5.3.1 Servidor de base de datos

Provee servicios de base de datos a otros programas u otras computadoras, este servidor está definido por el modelo cliente servidor. Hace referencia a aquellas computadoras que esta dedicadas a ejecutar y prestar servicios.

La base de datos maneja grandes cantidades de información que deben estar seguras, tiene un SGBD[6] que proporciona una herramienta de apoyo a la toma de decisiones, al mismo tiempo que proporciona transacciones de usuarios y así se tiene una información actualizada y consistente.

1.1.5.3.2 Servidor de internet-proxy

Permite enviar mensajes electrónicos de unos usuarios a otros con independencia de la red. El protocolo que se está usando es el SMTP[7] para el envío de correos y el protocolo POP3[8] para el recibo de correos.

1.1.5.3.3Terminal server

Permite a uno o más usuarios, acceder de forma remota a través de la red, a aplicaciones o información contenida en un servidor. Este modelo ayuda a mejorar las prestaciones de los clientes, ya que este servidor se encarga de procesas la información y ejecutar la aplicaciones, dejando a los clientes la tarea de desplegar la gráfica y el sonido.

1.1.5.3.4 Servidor de dominio

Proporciona resolución de nombre para la red TCP/IP[9], hace posible que los usuarios de PC's cliente, utilicen nombres en lugar de direcciones IP automáticas para identificar hosts remotos. El servidor de dominio proporciona un método para asignar un nombre descriptivo a una PC o servicio a otros datos asociados como una dirección IP.

1.1.5.3.5 Servidor de desarrollo

Se guarda la información del nuevo sistema que se está realizando para la empresa, la información está centralizada en este servidor y todos los días la información se actualiza.

1.1.5.3.6 Servidor de aplicaciones

Proporciona servicios de aplicación y gestiona la página web de la empresa así como las funciones del negocio y acceso a datos de aplicación, permitiendo el procesamiento de

[6] SGDB: Sistema de Gestor de Base de Datos.
[7] SMTP: Simple Mail Transfer Protocol.
[8] POP3: Post Office Protocol.
[9] TCP/IP: Transmission Control Protocol / Internet Protocol.

datos sobre la aplicación cliente. Con este servidor de mantiene la integridad de los datos y códigos y su configuración está centralizada haciéndolas más seguras y eficientes.

1.2 Equipamiento

1.2.1 Características de los servidores

Las características de hardware y software que tiene cada servidor es:

- **Servidor de Base de Datos**
  - Procesador Intel Xeon CuadCore 3.00Ghz X2
  - Sistema Operativo Microsoft Windows Server 2003 R2 Standar Edition
  - Service Pack 2
  - Memoria RAM de 2 Gb
  - Con acceso a internet
  - Disco Duro de 140Gb
- **Servidor de internet-proxy**
  - Procesador Dual 3.0 Ghz Intel Pentium III
  - Sistema Operativo Centos
  - Service Pack 2
  - Memoria RAM de 2 Gb
  - Con acceso a internet
  - Disco Duro de 140Gb

- **Terminal Server**
    - Procesador Intel Xeon DualCore X1
- **Servidor de Dominio**
    - Dual 3.0Ghz Intel Pentium III
    - Sistema Operativo Microsoft Windows Server 2003 R2 Standar Edition
    - Service Pack 2
    - Memoria RAM de 2Gb
    - Sin acceso a internet
    - Disco Duro de 140Gb
- **Servidor de Desarrollo**
    - Procesador Intel Xeon 2.4Ghz
    - Sistema Operativo Microsoft Windows Server Enterprise 2008
    - Service Pack 2
    - Sin acceso a internet
    - Memoria RAM de 2Gb
    - Disco Duro de 280Gb
- **Servidor de Aplicaciones**
    - Procesador Intel Xeon 2.00Ghz X2

- Sistema Operativo Microsoft Windows Server 2003 Standar Edition
- Service Pack 2
- Con acceso a internet
- Memoria RAM de 2Gb
- 2 Discos Duros de 20Gb c/u

1.2.2 Características de los PC's

La empresa está distribuida en once departamentos, de los cuales están dispersas del siguiente modo:

- 14% en el departamento administrativo.
- 1% en el departamento de calidad.
- 4% en el departamento comercial
- 7% en el departamento de compras
- 19% en el departamento financiero
- 2% en gerencia general
- 5% en el departamento de gestión humana
- 1% en el departamento de gestión y desarrollo
- 17% en el departamento de producción
- 30% en el departamento de sistemas

CAPITULO 2

"Revisión de conceptos de seguridad informática"

2.1 Norma ISO[10] 27001

La norma ISO/IEC 27001 que en siglas significa Technology Security Techniques viene a ser la evolución del estándar de buenas prácticas ISO creado en 1995, para lo cual su creación conlleva un progreso certificable llamado estándar 27001. Este tipo de certificación facilitará a la Seguridad Informática al momento de establecer, implantar, operar, supervisar, mantener, mejorar un SGSI[11].

2.1.1 Funcionamiento de la norma ISO 27001

Es un sistema de gestión para la seguridad de información que sirve para brindar soporte de los datos que se encuentran registrados en la organización. Para ello se implementa un SGSI con estándar 27001 para el cuidado de la información brindando confidencialidad, disponibilidad e integridad de los datos para el buen uso de la información y no divulgación del mismo en Organizaciones ya sean grandes o pequeñas.

2.1.1.1 Confidencialidad de datos

Es cuando un usuario o empleado de la empresa garantice seguridad al momento de ingresar a la información, no divulgando dicha información a personas ajenas a la empresa; con ello se busca conseguir una seguridad donde los que puedan acceder a los datos son los administradores del sistema o la misma gerencia.

2.1.1.2 Disponibilidad de datos

La disponibilidad de datos es el acceder a la información de la empresa al tiempo o la hora que sea con el fin que los usuarios alteren, actualicen, respalden los datos útiles y no tener pérdidas financieras o de personal.

2.1.1.3 Integridad de datos

La integridad de datos hace referencia a que los datos no pueden ser alterados por ningún tipo de personal, solo por la alta dirección, para ello deben de tener un tipo de seguridad que ayude al manejo debido de los datos para beneficio propio de la empresa.

10 ISO: International Organization for Standardization.
11 SGSI: Sistema de Gestión de Seguridad de Información.

2.1.2 Origen de la norma ISO 27001.

1995 BS[12] 7799 Parte 1 Código de buenas prácticas.

1998 BS 7799 Parte 2 Especificación de SGSI.

1999 BS7799 Revisión de la parte 1 y parte 2.

2000 BS7799 Parte 1 Se adopta como ISO.

2002 BS7799 Revisión de la Parte 2.

2005 ISO/IEC 17799 Revisión de la ISO 17799.

2005 ISO/IEC 27001 Parte 2 Se adopta como ISO.

2.1.3 Beneficios de la norma ISO 27001

"Demuestra la garantía independiente de los controles internos y cumple los requisitos de Gestión Corporativa y de continuidad de la actividad comercial.

Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.

"Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.

Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información." [13]

Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.

El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora." [14]

12 BS: Based.

13 http://es.wikipedia.org/wiki/ISO/IEC_27001

2.1.4 Pasos para la certificación

2.1.4.1 Elegir la norma

Se elige la norma para luego poder realizar una solicitud correspondiente, para bajar de la página web de la ISO 27001 para poder leer y entender la misma.

2.1.4.2 Contactar

Es necesario ponerse en contacto con los trabajadores de la certificación donde sus requerimientos son los más importantes para una buena entrega del estándar con ello se pondrá de acuerdo del precio y el tiempo que se supone será evaluado.

2.1.4.3 Cita con el equipo de evaluación

Se conoce a la persona responsable de que el certificado sea entregado con todas las normas correspondientes a este estándar dando la confianza de profesionalismo ante todo en el trabajo que realiza y en los conocimientos que posee para un buen desempeño de la certificación.

2.1.4.4 Considerar la formación

Si se desea ampliar los conocimientos del estándar, se debe disponer de talleres, seminarios donde la función es adaptar los conocimientos que se han pedido que se aplique en la certificación y así no tener problemas en el desarrollo de algún sistema de seguridad en cualquier organización.

2.1.4.5 Revisión y evaluación

Se realiza una análisis de los procesos operativos del sistema de gestión de seguridad informática, por ende cualquier problema que se realice se debe satisfacer antes de la evaluación formal, una vez resuelto el problema se llevara la evaluación exclusiva en la organización.

---

14 http://www.bsigroup.es/certificacion-y-auditoría/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISO 27001/

2.1.4.6 Certificación y mucho más

Concluida la evaluación se emite un certificado de registro que se explica hasta donde llega la certificación, este certificado lleva una validez de tres años y el responsable de la entrega visitará constantemente para ayuda como garantía que cumpla los requisitos y el apoyo continuo de los sistemas.

2.1.5 Contenido de la norma ISO 27001

2.1.5.1 Introducción

En la introducción se indicará todo lo que se va abarcar en la Norma ISO 27001 con el fin que el lector comprenda hasta dónde llegará sus objetivos y funciones de ésta tesis.

2.1.5.2 Objeto

En el objeto de la Norma ISO 27001 se propone abarcar hasta qué punto puede ayudar éste tipo de estándar en la organización que se va a auditar, se basa mucho en lo que es el Anexo A donde va ser el alcance de nuestra tesis.

2.1.5.3 Referencias normativas

Aquí interviene de donde no más se logró sacar la información, es decir, si se obtuvo también de otras ISO y qué específicamente se alcanzó de dichas referencias.

2.1.5.4 Términos y definiciones

Aquí se coloca cada uno de los términos importantes que se den en la Norma ISO 27001 como su respectiva definición de cada uno de los términos propiamente escritos.

2.1.5.5 Sistema de gestión de la seguridad de la información

En este sistema se abarca todo acerca de la seguridad de la información en la parte específica de lo que es la gestión, que intervienen en ésta política y que no más necesita para encontrar la solución más adecuada para su respectiva auditoría.

2.1.5.6 Responsabilidad de la dirección

La dirección debe estar atenta a lo que ocurra con las auditorías, ya que con ello pueden tomar medidas para poder prevenir posibles fallos en la seguridad informática. La

dirección debe también racionalizar el uso de los activos informáticos y para ello se realizan actividades que ayudan al auditor a tomar decisiones

2.1.5.7 Auditorías internas de SGSI

El objetivo primordial de este tipo de auditoría de SGSI es averiguar si hay algo que se está realizando mal, de manera objetiva. El auditor interno debe ser una persona capacitada y atenta a lo que está ocurriendo en la empresa, debe poder descubrir si algo se hace mal dentro de su empresa de trabajo. Si se realiza un buen trabajo, correctivo o preventivo, entonces la auditoría interna de SGSI mejorará su seguridad.

2.1.5.8 Revisión del SGSI por la dirección

Este paso es muy importante, ya que la dirección también debe formar parte en el proyecto, para lo cual se realizan reuniones planificadas para dar puntos de vista y recomendaciones. La revisión por parte de la dirección esta desarrolladamente con ese objetivo, ya que el estándar requiere que la dirección examine todos los hechos importantes que se van encontrando en el transcurso del tiempo. Al momento que se ha realizado éste paso, entonces se decidirán las mejoras que se implementaran.

2.1.5.9 Mejora de SGSI

Mediante la mejora continua del SGSI, se evitarán que se produzcan errores y para ello se desarrollaran medidas preventivas, que representan una forma de corregir las cosas antes que se generen problemas. Similares a las medidas preventivas existen las medidas correctivas que corrigen un problema cuando éste ya sucedió

2.1.5.10 Anexo A. Resumen de controles

Para este caso, el anexo que se va a cumplir, es el anexo A. Este anexo es, probablemente, el anexo mas nombrado de todas las normas de gestión El objetivo del anexo A contiene los siguientes puntos:

- A.5 Política de la seguridad
- A.7 Gestión de activos
- A.8 Seguridad relacionada con el personal
- A.9 Seguridad física y de entorno

• A.11 Control de Acceso
• A.13 Estrategias de Solución

Como podemos observar en los puntos, el anexo A, no solamente se centra en las tecnologías de la información; también incluye seguridad física, protección legal, gestión de recursos, etc.

2.1.5.11 Bibliografía.

Aquí se citan todas las referencias visitadas para consultas o copias ya sean: libros, revistas, páginas web, etc.

La Norma ISO 27001 implementa un modelo plan do check act o también llamado ciclo de demming para establecer, implementar, monitorear, revisar y mantener un SGSI.

2.1.6 Ciclo de demming

2.1.6.1 Planificar

Incluyen determinar metas, objetivos y determinar métodos para alcanzar las metas estas son:

- Definición de Políticas y Objetivos.
- Determinación Del Alcance.
- Valoración de Activos.
- Análisis de Riesgo.
- Gestionar los Riesgos.
- Seleccionar los controles ISO 17799:2005.

2.1.6.2 Hacer

Incluyen asegurar la educación y el entrenamiento e implementar el trabajo estas son:

- Definir e Implementar Plan de Gestión de Riesgo.
- Implementar Controles Seleccionados y sus Indicadores.
- Implementar el Sistema de Gestión.

2.1.6.3 Chequear

- Consiste en verificar los efectos de la implementación estos son:
- Revisión Gerencial.
- Desarrollar Procesos de Monitorización.
- Revisar Regularmente el SGSI.
- Revisar los Niveles de Riesgo.
- Auditar Internamente el SGSI.

2.1.6.4 Actuar

Consiste en tomar la acción apropiada esto son:

- Implementar las Mejoras
- Adoptar Acciones Preventivas y Correctivas
- Comunicar Acciones y Resultados
- Verificar que las Mejoras Cumplen al Objetivo

2.2 Piratas informáticos

"Su actividad consiste en la copia ilegal de programas, rompiendo sus sistemas de protección y licencias. Luego estos se distribuyen de manera abierta a través de internet, CD's, etc."[15]

2.2.1 Hackers

Hacker es un vocablo utilizado por los informáticos para referirse a un experto en varias o alguna rama técnica relacionada con la informática tales como: programación, redes de computadora, sistemas operativos, etc. Es una persona apasionada por descubrir o aprender nuevas cosas y entender el funcionamiento de estos para bien o mal. Pueden romper seguridades en los sistemas de una empresa por diversión o explorar datos privados, pero la ética hacker no permite divulgar esos datos privados ya que sería un acto de vandalismo.

15 http://hecman.jimdo.com/hacker-ycracker/clasificacion-de-crackers/

2.2.2 Cracker

Es una persona con grandes conocimientos informáticos y con un propósito de luchar en contra de lo que está prohibido, empieza a investigar la forma de bloquear o traspasar protecciones hasta lograr su objetivo. Los crackers usan programas propios o bajados del internet gratuitamente, con esos programas se intenta desbloquear claves de acceso con generadores automáticos de claves.

Se distinguen varios tipos de crackers:

2.2.2.1 Lammer

Es una persona con poco conocimientos informáticos, que consiguen herramientas ya creadas para atacar ordenadores. Ejecutan aplicaciones sin saber que están causando grandes daños.

2.2.2.2 Trasher

Son personas que buscan en la basura y en papeleras números de tarjetas de crédito, claves de acceso, cuentas bancarias, etc; para cometer estafas y actividades fraudulentas a través de internet.

2.2.2.3 Insiders

Crackers corporativos, empleados de las empresas que las atacan desde dentro, movidos usualmente con motivos de venganza.

2.2.2.4 Activos Informáticos

Son los bienes de una organización, que se encuentran relacionadas de manera directa o indirecta con la actividad informática, entre los cuales se encuentran:

Información mecanizada, es decir, no tienen documentos fuentes que los generen

- Medios de comunicación que se utilizan para la transmisión de datos, tales como: redes, correo electrónico, etc.
- Medios magnéticos y ópticos de almacenamiento de información como: cintas, discos, etc.

- Programas y aplicaciones de la empresa, ya sea desarrollados por la misma, o adquiridos por terceros.
- Manuales, procedimientos y reglamentaciones afines al área informática.

2.3 Vulnerabilidad

Las vulnerabilidades son errores que permiten realizar acciones desde afuera, sin permiso del administrador del equipo, incluso se puede suplantar a un usuario en común Actualmente existen muchas amenazas que tratan de acceder remotamente a ordenadores, ya sea para hacerlos servidores ilegales o robar información privada.

2.4 Seguridad informática

La seguridad informática garantiza que la información privada de una empresa, sea físico o lógico esté solo al alcance de las personas con suficientes privilegios para realizar acciones que se les ha otorgado mediante políticas dadas por la empresa.

En definitiva, la seguridad informática nos ayuda a proteger la integridad y la privacidad de la información almacenada en un sistema informático o bien sea un activo informático

2.4.1 Seguridad física

Mediante la seguridad física se evita el acceso no autorizado, daños o intromisiones en las instalaciones y a la información de la organización; ya que los servicios de procesamiento de información deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados.

2.4.2 Seguridad física del edificio

Aquí se intenta minimizar el riesgo que personas ingresen a algunos recursos informáticos específicos, con el objetivo de asegurar los activos. Así mismo, se trata de que el centro de procesamiento de datos [16] esté ubicado en un lugar seguro, sin vulnerabilidades de accesos a los mismos.

16 Centro de Procesamiento de Datos: Cuartos de Servidores.

Deberían existir políticas de seguridad bien planteadas, diseñadas y desarrolladas que cubran la gran mayoría de aspectos para que exista un verdadero SGSI, así mismo deberían existir planes de seguridad que ayuden a tomar decisiones seguras para cuando exista un acceso físico no autorizado a algún recurso informático de la empresa.

2.4.3 Control de accesos

Todos los sitios en donde se encuentren sistemas de procesamiento de datos informáticos o de almacenamiento, deben estar protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo, registro de entradas y salidas, guardias de seguridad, detectores metálicos, etc.

2.4.4 Seguridad en el acceso a la información

En la seguridad en el acceso a la información es muy importante que toda los datos de la empresa sean sumamente protegidos por tipos de riesgos que constantemente se interceptan en la Organización, poniendo en peligro la información precisa que sea divulgada causando graves problemas en todo tipo de trabajo, por eso se ve factible colocar o implementar herramientas o estándares como una forma de protección para dichos problemas, esas herramientas estarán jugando el papel protector de la empresa y así no ser divulgado por personas que no pertenecen a la organización.´

2.4.5 Seguridad en las estaciones de trabajo

En este tipo de seguridad no se deben de confundir que una estación de trabajo es una PC por ende toda la información que se produce en la empresa es importante, para ello se restringen varios tipos de entretenimientos, páginas web que no intervienen en el uso general de la empresa, para un buen funcionamiento en su trabajo viéndose de tal manera se verificara algunos restricciones importantes que se realiza en este tipo de seguridad para no tener problemas en posteriores informaciones acerca del trabajo que se emplean en la organización.

- Las computadoras de trabajo no deben tener instalado ningún otro software como juegos o cualquier otro software de entretenimiento que no sea el licenciado y requerido para que el usuario desarrolle su trabajo.

- Todos los equipos deben contar con software antivirus instalado y activo así como la última actualización del mismo y la definición de virus.
- Queda estrictamente prohibido emplear cualquiera configuración manual como dirección IP, DNS[17], puerta de enlace o default Gateway, rutas estáticas, etc; en las estaciones de trabajo de los usuarios, deben ser configuradas para obtener una dirección IP automáticamente.
- Siempre se deben de escanear los discos flexibles y cualquier archivo o medio electrónico de transmisión antes del acceso a la información contenida en ellos.
- Respaldar periódicamente los datos de aplicaciones y configuraciones, y almacenarlos en un lugar seguro.
- Solo el personal autorizado del área de informática puede efectuar cambios en la configuración siempre y cuando se justifique.
- Queda estrictamente prohibido que los usuarios remuevan o agreguen componentes tanto de software como de hardware a los equipos.
- "Queda estrictamente prohibido que los usuarios cambien el equipo del lugar al que han sido asignados.
- Los equipos deben configurarse para que empleen el protocolo TCP/IP y debe removerse cualquier otro protocolo innecesario."[18]

2.5 Integridad de la información

La integridad de la información se basa en que ninguna persona no autorizada puede hacer uso de cambios o modificaciones en el sistema ya sea con fin propio para beneficiar o perjudicar a la organización, es por eso que se tiene una herramienta para este tipo de problemas haciendo que cada personal de la empresa posea una firma digital en donde el que ingresa sea procesado y sea la persona que al ingresar la única culpable en el desarrollo del sistema hablando de la parte informática específicamente.

17 DNS: Domain Name System.
18 http://cert.salud.gob.mx/Estacionesdetrabajo.html

2.6 Copias de seguridad

Se le denomina copias de seguridad a todo tipo de respaldo que se realiza con el fin de desempeñar una breve recuperación de los datos y restaurar el original después de que se prevenga las pérdidas totales de la información importante en cualquier organización o archivos importantes para su bien común.

2.7 Soporte de almacenamiento

Se establece que el dueño de un archivo informático no pueda modificar los permisos que está bajo un control de accesos obligatorio, para lo cual a cada usuario, dato, etc se le asigna una etiqueta o un nivel de seguridad jerárquico y una categoría Cada usuario puede tener acceso a un solo tipo de información. También se verifica que la información este debidamente etiquetada con un nombre informativo.

2.7.1 Guardado de información

Se verifica que la información se guarde en formatos establecidos por políticas y como debe estar encriptado dicha información, dependiendo de la importancia de cada uno de ellas. Cada cambio que se realice debe estar registrado en un historial de cambios tales como fecha, hora, cambios realizados y por quien; para que así poder registrar malos entendidos en algún cambio realizado.

2.8 Acceso a la información

Se asegura que se limite el acceso desde un ordenador a información privada ya sea por medios de autenticación Si verifica contraseñas y tiempos de vida de cada contraseña, así como un registro de los cambios a la información y por quien han sido modificados. Se verifica firewalls para restricción de puertos que no se estén usando y que sea registren vulnerabilidades en dichos puertos.

2.9 Restauración de datos

Se verifica si se es posible recuperar información perdida en un sistema de información, y si se gestiona estas pérdidas y cuál fue el motivo por el que dicha información se

elimino. Mediante el respaldo de información se asegura de haber guardado la información de manera correcta sin modificaciones.

2.10 Servidor

Un servidor es una computadora que da servicio a otros ordenadores llamados clientes.

También se suele denominar a un servidor como una aplicación informática que realiza ciertas tareas en beneficio de otras aplicaciones cliente. Ofrece servicio de acceso a archivos o información, permite almacenar y acceder a archivos de una computadora y servicios de aplicaciones que los realiza el usuario final. *La figura 2.11.1 muestra un ejemplo de cómo está conformado un servidor y sus clientes.*

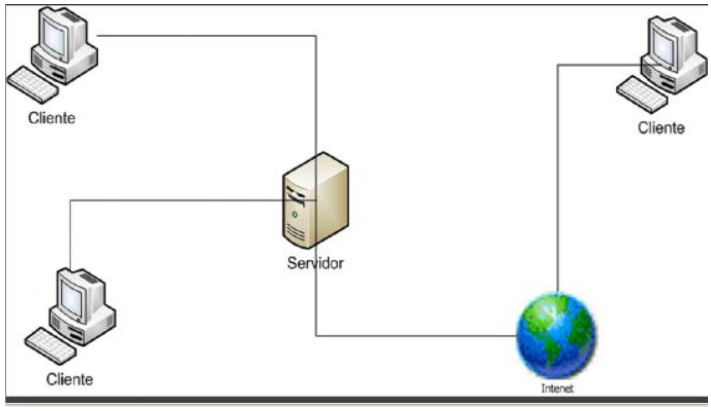


Figura 2.11.1. Modelo de Cliente-Servidor[19]

2.11 Virus informático

Los virus informáticos son programas de software que se ejecutan y se propagan localmente, realizando copias de sí mismo en otro programa o documento, infectando otros ordenadores.

2.11.1 Características

La principal característica es el consumo de recursos que ocasionan problemas tales como la pérdida de productividad, que la PC no este 100% funcionando, pérdida de

19 http://mipc.elrincontecnologico.com/2008/12/definicin-de-servidor.html

información, etc. Otra característica es tienen la posibilidad de replicarse por todo el ordenador ya sea localmente o por medio de redes que no tienen seguridades adecuadas.

2.11.2 Acciones de los virus

Los virus pueden causar diferentes acciones como:

- Unirse con un programa instalado en la computadora permitiendo la propagación
- Mostrar en la pantalla mensajes o imágenes humorísticas pero molestas
- Hacer lento la computadora o bloquear la misma
- Eliminar información importante almacenada en el disco, a veces impidiendo el funcionamiento de la computadora
- Reducir el espacio de almacenamiento en el disco
- Molestar al usuario cerrando ventanas, moviendo el ratón, etc.

2.11.3 Métodos de propagación

Un virus puede propagarse por medio del usuario que acepta o de forma involuntaria instala el virus, o si no, el virus actúa replicándose por la red; de esta manera el sistema operativo comienza a sufrir una serie de comportamientos no deseados, y esos comportamientos pueden dar pista que existe un virus.

Las contaminaciones más frecuentes realizadas por el usuario se encuentran:

- Mensajes que ejecutan automáticamente programas
- Ingeniería social, mensajes como <<Ejecute este programa y gane un premio>>
- Entrada de información infectada en discos de otros usuarios
- Instalación de software que contienen programas maliciosos
- Por unidades extraíbles de almacenamiento infectadas

2.11.4 Métodos de protección y tipos

Existen métodos para disminuir o reducir el riesgo de infección o reproducción de los virus como:

2.11.4.1 Antivirus

Son programas que tratan de descubrir huellas dejadas por software malicioso para así detectarlo, eliminarlo o contenerlo en cuarentena para evitar su reproducción Intenta tener controlado el sistema de intrusos como medida de seguridad.

2.11.4.1.1 Tipos de vacunas

Puede existir varios tipos de vacunas, entre ellos:

- **Solo detección:** Solo actualizan archivos infectados pero no pueden eliminarlos o desinfectarlos.
- **Detección y desinfección:** Detectan archivos infectados y pueden desinfectarlos.
- **Detección y aborto de la acción:** Detectan archivos infectados y detiene las acciones del mismo.
- **Comparación de firmas:** Comparan las firmas de los archivos infectados para conocer si estos están infectados.
- **Comparación de firmas de archivo:** Compara las firmas de los atributos guardados en la computadora.
- **Métodos heurísticos:** Se usa métodos heurísticos para comparar archivos, puede como no ser la mejor alternativa.
- **Invocado por el usuario:** Se activan por petición del usuario.

2.11.4.2 Sistemas operativos mas atacados

Las plataformas mas atacadas por virus informáticos son los sistemas de Windows. Al respecto con los sistemas de GNU/Linux[20], BSD[21], Solaris, Mac OS X[22], tienen mayor seguridad por sus privilegios en los sistemas.

2.12 Copias de seguridad

Son llamadas también backup, son respaldos de información con el fin de que puedan utilizare para restaurar información modificada accidentalmente o después de una

20 GNU: Sistemas Operativos Libres.
21BSD: Berkeley Software Distribution.
22 OSX: Sistema Operativo Desarrollado por Apple Inc.

pérdida de datos, según datos estadísticos el 66% de usuarios de internet han sufrido una pérdida grave de la información. Fundamentalmente son útiles para 2 cosas:

- Recuperación de información ante una catástrofe informática
- Recuperación una pequeña cantidad de información que se pudieron haber eliminado accidentalmente o corrompido.

2.12.1 Elección de datos

Se debe decidir de qué información estará compuesta la copia de seguridad, si se copia muchos datos redundantes se agota la capacidad de almacenamiento y es muy demorado. Si no se realiza una copia de seguridad, se podrá perder información crítica. A continuación se muestra algunas observaciones para las copias de seguridad:

- **Archivos a copiar:** Copiar solo los archivos que se hayan modificado
- **Deposito del sistema de ficheros:** Copiar el sistema de ficheros que tienen los ficheros copiados, conocido como copia de seguridad particionada en bruto.
- **Control de cambios**: Gestionar los cambios en los archivos por fechas de modificación
- **Incremental a nivel de bloque:** Copiar los bloques físicos que han sufrido algún cambio.
- **Incremental o diferencias binaria:** Copiar los bloques con variaciones binarias que sufren los ficheros.
- **Versionando el sistema de ficheros:** Se mantiene atento a los cambios del fichero y crea estos cambios accesibles a usuario.

2.12.2 Copias de seguridad de datos en uso

Cuando una computadora esta en uso, se ejecuta la copia de seguridad, incluyendo la posibilidad de que haya ficheros abiertos o trabajando sobre ellos. Si un fichero está abierto, el contenido posiblemente no se refleje en lo que el usuario ve.

CAPITULO 3

"Auditoría de políticas de seguridad"

3.1 Consideraciones

La empresa Italimentos posee dos personas encargadas en el departamento de sistemas para la administración de servidores y para solucionar problemas que vayan ocurriendo dentro o fuera de la empresa, ya que Italimentos tiene locales Italdeli[23] ubicados en los sectores de:

- San Sebastián
- La Salle
- Virgen de Fátima
- Parque Industrial
- Quito
- Guayaquil.

Se tiene el caso en que en ninguno de estos sectores se tiene documentos físicos o compartidos por una red LAN[24] o WAN[25], que determinen un tipo de políticas de seguridad o planes de seguridad a seguir cuando exista una catástrofe informática. Al momento que existe un problema el encargado de sistemas de Italimentos va al sector donde ocurrió el problema o a veces se realiza un escritorio remoto[26] para solucionar dichos inconvenientes.

3.1.1 Departamento de sistemas

En el departamento de Sistemas está a cargo de toda la parte informática de la empresa siendo ésta área una ayuda importante para continuidad del servicio, confidencialidad de los datos y la integridad del mismo.

23 Italdeli: local comercial perteneciente a Italimentos
24 LAN: Local Area Network
25 WAN: Wide Area Network
26 Escritorio remoto: Tomar el control de una PC por una red de forma remota.

Este departamento apoya, a la vez, de forma computacional a las actividades que posee toda la organización, ya sea la gerencia, departamentos y otras áreas que utilizan recursos informáticos, realizando el mantenimiento y la administración de las redes, sistemas y equipos computacionales de la empresa.

Recopila la información, como a su vez actualiza y mantiene los datos de los productos que posee la empresa con la finalidad de que esté al servicio de cada departamento.

3.1.1.1 Ubicación

El Departamento de Sistemas se encuentra ubicado en el segundo piso y compartiendo su área con el departamento de cartera, provocando un espacio físico muy reducido para sus labores diarias. *La figura 3.1.1.1.1 muestra como está estructurada el área de sistemas y cartera.*

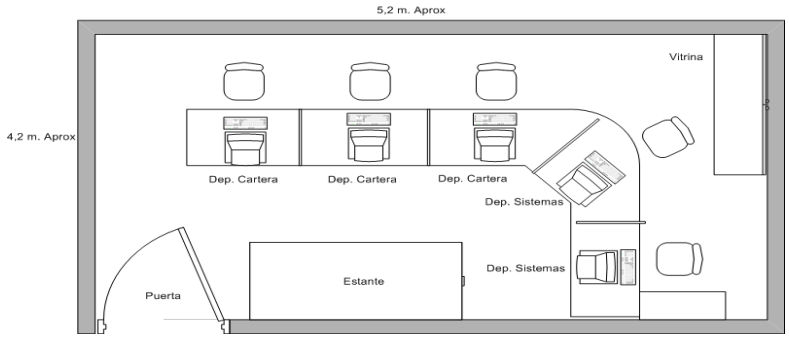


Figura 3.1.1.1.1. Estructura del departamento de sistemas y cartera

El departamento de contabilidad unido con Sistemas provoca un espacio limitado laboral y de atención al usuario. *La figura 3.1.1.1.2 y 3.1.1.1.3 muestra la unión de los dos departamentos.*

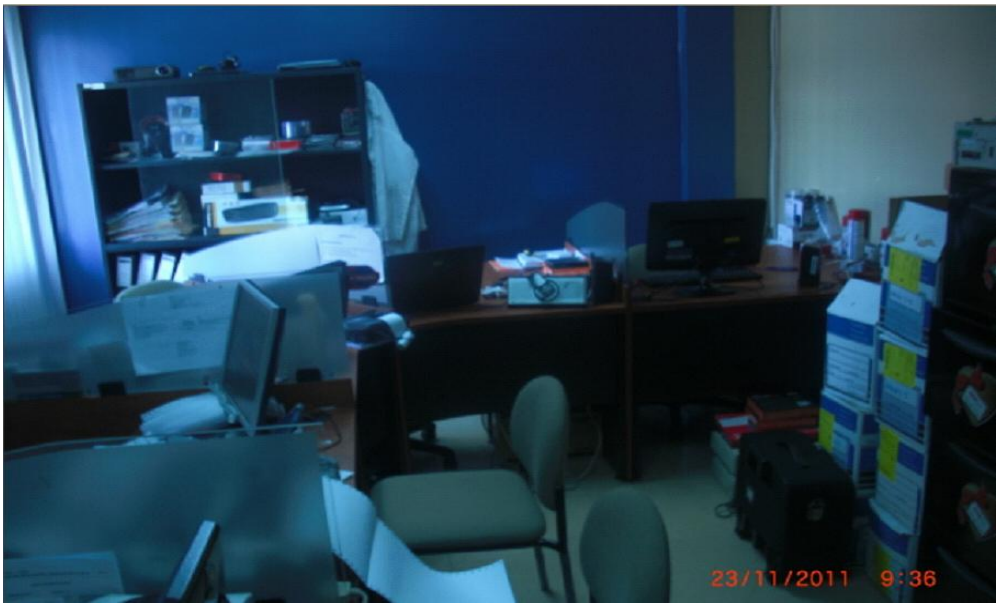


Figura 3.1.1.1.2. Departamento de Sistemas y Cartera

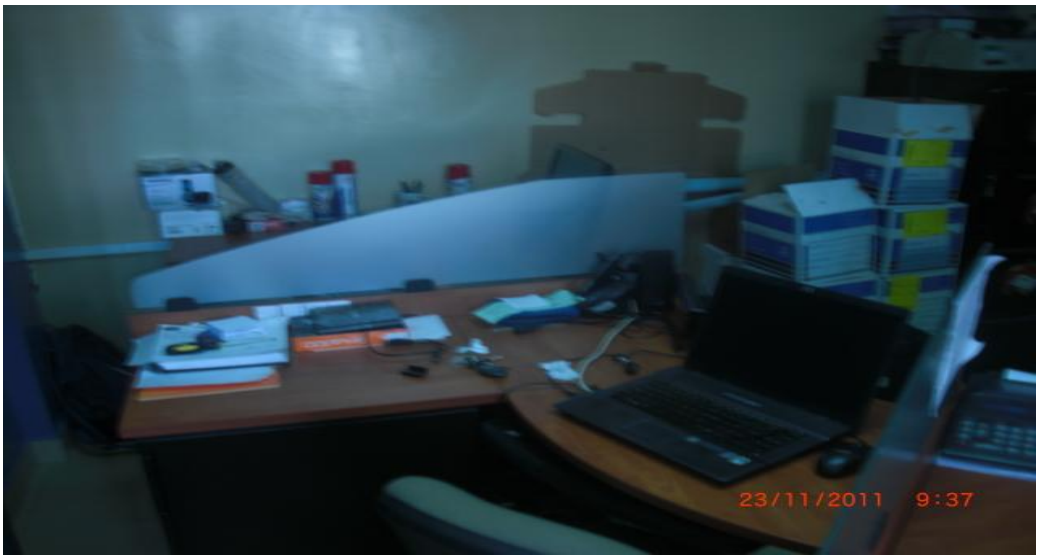


Figura 3.1.1.1.3. Departamento de Sistemas y Cartera

3.1.2 Servidor

Un servidor es una computadora que da servicio a otros ordenadores llamados clientes, también se suele denominar a un servidor como una aplicación informática que realiza ciertas tareas en beneficio de otras aplicaciones cliente. Ofrece servicio de acceso a archivos o información, permite almacenar y acceder a archivos de una computadora y

servicios de aplicaciones que los realiza el usuario final. *La figura 3.1.2.1 muestra el rack con los servidores de Italimentos Cía. Ltda.*

Figura 3.1.2.1. Rack con servidores de Italimentos

3.1.2.1 Cuarto de servidores

En el cuarto de servidores es un lugar muy importante para la empresa ya que se almacena toda la información de la organización además de solventar otros servicios que la fábrica posee.

En el cuarto de servidores o centro de procesamiento de datos se actualiza la información precisa de la empresa siendo aporte fundamental para la integridad de los datos, es decir, sin este tipo de procesamiento la divulgación de la información sería muy a menudo y no tendrían confidencialidad en el momento de intercambiar la información con los usuarios finales.

3.1.2.2 Cuarto de servidores de Italimentos

En la empresa de Italimentos poseen 6 servidores con sus debidas características de hardware y software:

- **Servidor de base de datos**
    - Procesador Intel Xeon CuadCore 3.00Ghz X2
    - Sistema Operativo Microsoft Windows Server 2003 R2 Standar Edition
    - Service Pack 2
    - Memoria RAM de 2 Gb
    - Con acceso a internet
    - Disco Duro de 140Gb
    - IP27: 192.168.1XX.XXX
- **Servidor de internet-proxy**
    - Procesador Dual 3.0 Ghz Intel Pentium III
    - Sistema Operativo Centos
    - Service Pack 2
    - Memoria RAM de 2 Gb
    - Con acceso a internet
    - Disco Duro de 140Gb
    - IP: 192.168.1XX.XXX
- **Terminal server**

27 IP: Internet Protocol

- Procesador Intel Xeon DualCore X1 de 2.33Ghz
- Sistema Operativo Microsoft Windows Server 2003 R2
- Service Pack 2
- Sin acceso a internet
- Memoria RAM de 2GB
- Disco Duro de 80Gb
- IP: 192.168.1XX,XXX

- **Servidor de dominio**
  - Dual 3.0Ghz Intel Pentium III
  - Sistema Operativo Microsoft Windows Server 2003 R2 Standar Edition
  - Service Pack 2
  - Memoria RAM de 2Gb
  - Sin acceso a internet
  - Disco Duro de 140Gb
  - IP: 192.168.1XX.XXX

- **Servidor de desarrollo**
  - Procesador Intel Xeon 2.4Ghz
  - Sistema Operativo Microsoft Windows Server Enterprise 2008

- Service Pack 2
- Sin acceso a internet
- Memoria RAM de 2Gb
- Disco Duro de 280Gb
- IP: 192.168.1XX.XXX

- **Servidor de aplicaciones**
  - Procesador Intel Xeon 2.00Ghz X2
  - Sistema Operativo Microsoft Windows Server 2003 Standar Edition
  - Service Pack 2
  - Con acceso a internet
  - Memoria RAM de 2Gb
  - 2 Discos Duros de 20Gb c/u
  - IP: 192.168.1XX.XXX
- **Base de datos de respaldo**
  - Procesador Intel Xeon CuadCore 3.00Ghz X2
  - Sistema operativo Microsoft Windows Server 2003 R2
  - Service Pack 2
  - Con acceso a internet

- Memoria RAM de 2GB
- Disco Duro de 140 GB
- IP: 192.168.1XX.XXX

Nota: Estos servidores están operando hasta 14 de Noviembre de 2011 por lo cual se tiene planificado dar de baja el Servidor de Dominio antes de terminar el año 2011.

3.1.2.3 Administrador del sistema

Es una persona profesional capaz de solucionar todos los problemas de recursos informáticos que posee la empresa. Este profesional debe ejecutar, mantener, operar y asegurar el correcto funcionamiento informático o de red de computadoras con el fin de que no se de ningún problema posteriores en el sistema de la empresa.

3.1.2.4 Administradores del sistema en Italimentos

En la empresa de Italimentos los administradores del sistema racionalizan los recursos informáticos como a su vez brindan mantenimiento y operan la seguridad que tiene cada uno de los equipos actualizando antivirus, formateando PC's [28], brindando internet en cada uno de los usuarios que trabajan en la empresa y respaldando en cada uno de los servidores que posee la fábrica.

3.2 Medidas, controles, procedimientos, normas y estándares de seguridad.

Se realizó un cuestionario al jefe de sistemas con un total de dieciséis preguntas para las cuales a cada una de ellas se resolvió con la respectiva entrevista al mismo. *Véase Anexo B.*

3.2.1 Medidas

28 PC: Computadora Personal

En la entrevista con el jefe de sistemas se dio a entender que no existen medidas en un documento físico o en un medio de almacenamiento por lo cual sus medidas son tomadas en base al tiempo transcurrido y son requeridas al momento de realizar una acción ya sea de mantenimiento o rutina. Cuando un activo informático va a ser desechado, se reutilizan las partes que sirven siendo esto una medida preventiva para cuando ocurra algún problema de hardware, por ende la empresa de Italimentos posee una bodega donde se almacena los recursos no útiles para la organización. *La figura 3.2.1.1 muestra la bodega de almacenamiento de los recursos informáticos inactivos.*

Figura 3.2.1.1. Bodega de recursos informáticos inactivos.

En la bodega los recursos informáticos que funcionen serán donados y los que no funcionan serán desechados o reciclados, pero no hay una fecha específica para dichas acciones.

3.2.2 Controles

No existen procedimientos escritos para notificación y gestión de incidencias, en donde, los problemas que ocurre se los resuelve en ese momento. Para los controles de acceso físico y lógico a la información se da privilegios de solo lectura, solo escritura o lectura-escritura, para los controles lógicos se va abrir una cuenta llamada “tesis” bajo el

dominio[29] de Italimentos con la dirección IP 192.168.10.210 y se nos otorgará distintos privilegios de usuario para la auditoría, el sistema operativo cliente usado es Microsoft Windows XP y Linux Ubuntu 11.04. *La figura 3.2.2.1 y 3.2.2.2 muestra las configuraciones de las características*

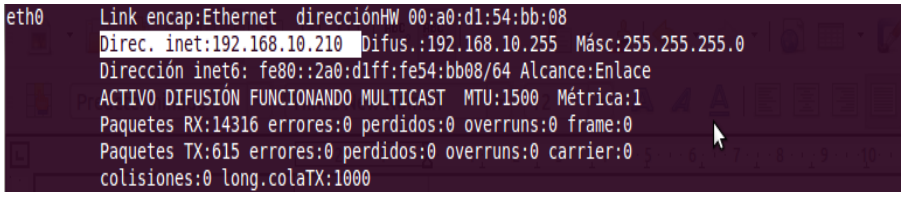


Figura 3.2.2.1. Dirección IP

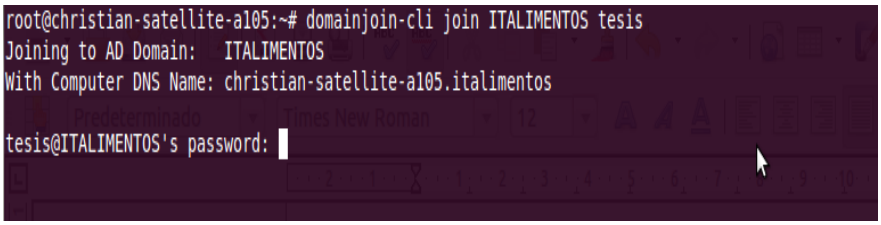


Figura 3.2.2.2. Usuario tesis, bajo el dominio de ITALIMENTOS

3.2.3 Procedimientos

Los problemas que más ocurren y los más críticos es en el servidor de aplicaciones, puesto que los programas y tareas existentes en este servidor se quedan estancadas y los administradores detallan los pasos para solucionar los problemas:

- Reciben la llamada de fallo en el sistema
- Se dirige al cuarto de servidores ubicado en el tercer piso
- Conecta un monitor, teclado y ratón al servidor
- Se registra con el debido usuario y contraseña
- Cierra la aplicación que está dando problemas
- Vuelve abrir la aplicación que da los servicios

29 Dominio: Nombre de una red

- Cierra la sesión.

En casos extremos cuando no existe una solución, se comunica a todo el personal que no habrá sistema por unos minutos, entonces eso lleva a un reinicio físico del servidor que tarda varios minutos en volver a brindar los servicios. Con los demás servidores no existen muchos casos sobre problemas.

Cuando existen problemas en máquinas de usuarios los procedimientos que siguen los encargados de sistemas es:

- Reciben la llamada de fallo de su PC
- Una persona encargada va a revisar el equipo a la estación de trabajo del usuario
- Se revisa el posible error
- Si con todas las posibles soluciones no hay reparar la PC, entonces se desconecta y va al departamento de sistemas.
- En el departamento de sistemas o cuarto de servidores, se abre la computadora y se prueba posibles soluciones con hardware y software.
- Al realizar la reparación, la PC vuelve a su debida estación de trabajo

Para estas reparaciones no existe un historial de incidentes o documentos, que detallen pasos a seguir sino que las soluciones se las realiza en el momento que falla una PC.

Cuando se adquiere un nuevo equipo de hardware o software, no existe una política escrita en un documento pero se tiene un inventario y realizan el siguiente procedimiento:

- Recursos humanos realiza el pedido al departamento de sistemas
- El departamento de sistemas realiza el pedido al proveedor de hardware o software

- La factura de los recursos a adquirir se dirige al departamento de cartera
- Se obtiene los recursos y entra a producción

3.2.4 Normas y estándares de seguridad

Para el caso del departamento de sistemas, no existen documentos físicos o almacenados que detallen normas o estándares de seguridad, sino que el administrador de sistemas, realiza actividades acordes se vayan dando fallos sin seguir un procedimiento escrito.

3.3 Contraseñas

Una contraseña es una clave el cual sirve como un candado para poder proteger algunos datos u otro tipo de archivos que se encuentren, ya sea, en una cuenta de correo electrónico, redes sociales, bancaria, una PC, etc. Esta clave solamente el usuario conoce y solo el usuario puede cambiarla, salvo casos o normas empresariales. Pero existen personas que realizan programas para poder descifrar estas claves y poder tener acceso a la información que se encuentre resguardada en la cuenta.

3.3.1 Contraseñas en Italimentos

En Italimentos, no existe un documento físico o almacenado que defina un estándar para definir las contraseñas a nivel de usuario, sino que cada usuario define su propia contraseña y es responsable de su propia computadora.

A nivel de servidores, existe un estándar dado por el propio sistema operativo que debe tener mayúsculas, minúsculas, números, símbolos especiales y una longitud de más de ocho caracteres.

3.3.2 Periodo de vida de contraseñas

Existe una política definida por el departamento de sistemas, pero no descrita en un documento, que cada usuario debe cambiar su contraseña cada dos o tres meses y la clave en los servidores no varía ya que el nivel de complejidad de las contraseñas es muy alto para cambiar cada cierto tiempo. Al momento de realizar mantenimientos a los

recursos informáticos, no se puede acceder a algunas computadoras ya que no se tiene la clave de ingreso del usuario responsable de la computadora.

3.3.3 Estructura

El departamento define a los usuarios que se establezcan una contraseña mayor a cuatro caracteres, ya que no existe una estructura que detalle una contraseña segura. "Cada usuario registra su contraseña de manera privada y el usuario es responsable de mantener la privacidad de su clave personal."[30]

3.4 Privilegios del Personal

Existe una diferencia entre derecho y privilegio, por lo cual:

- Un derecho autoriza a un usuario o a un grupo de usuarios a realizar determinadas operaciones sobre un servidor o estación de trabajo, ya sea, de manera física o por medio de una red.

- Un privilegio es una marca asociada a cada recurso de la red como: ficheros archivos, impresoras, etc.; que regulan a los usuarios a acceder a estos de manera física o por una red.

De esta forma, el derecho se refiere a operaciones propias del sistema operativo como el derecho a realizar copias de seguridad, pero un permiso seria el permiso leer un archivo en concreto. La asignación de los privilegios se los puede realizar en dos fases:

1. Se determina el permiso de acceso sobre el servicio de red para poderse conectar a un recurso en específico. Esto evita que se puedan abrir otras unidades remotas de red sobre las cual no se tenga privilegios.

2. Deben configurarse los permisos sobre ficheros y directorios que se tiene sobre la red.

30 http://www.metroblog.com/privacy

3.4.1 Privilegios en Italimentos

En Italimentos los más altos privilegios para poder realizar acciones son la gerencia y el departamento de sistemas. Existen carpetas compartidas a las que se pueden acceder a nivel de usuario, permitiendo ver información de otros departamentos. Para la asignación de privilegios estos se realizan a nivel de usuario, en el cual existen tres tipos de privilegios los que constan usuarios finales, administradores y gerencia.

3.4.1.1 Usuarios finales

Lo usuarios finales no pueden instalar ningún tipo de aplicación ni modificar configuraciones en sus estaciones de trabajo, pero tienen acceso a información específica en la red. Dentro de este tipo de usuario se encuentra:

- Asistente de gerencia
- Medico
- Enfermera
- Gerente financiero
- Contador general
- Auxiliares contables
- Jefe de cartera
- Recaudador
- Auxiliares contables
- Tesorería
- Auxiliares de tesorería y recaudadores
- Jefe administrativo

- Coordinador administrativo
- Recepcionista
- Operadores administrativos
- Auxiliares de gestión humana
- Operarios de RRHH
- Coordinador de compras
- Bodeguero
- Operario de bodega

La información que se encuentra en las carpetas compartidas es pública para todos los departamentos que se encuentran con este tipo de privilegios

3.4.1.2 Administradores

Los usuarios administradores pueden instalar aplicaciones en las estaciones de trabajo y realizar modificaciones en la configuración de sus computadoras. Dentro de este tipo de usuario se encuentra:

- Coordinador de seguridad industrial
- Contador de costos
- Jefe de gestión humana
- Jefe de sistemas
- Auxiliar de soporte de sistemas

3.4.1.3 Gerencia

Los usuarios con privilegios de gerencia, pueden realizar instalaciones de software y acceder a cualquier información en la red y a la aplicación de cámaras de seguridad de la empresa. Dentro de este grupo se encuentra:

- Gerencia
- Jefe de compras

3.5 Cifrado de información

El cifrado de la información describe todas las técnicas que permiten cifrar mensajes o hacerlos inentendibles sin recurrir a una acción específica. La criptografía se basa en la aritmética, en el caso de un texto, consiste en transformar las letras en una serie de números y luego realizar cálculos para:

- Modificarlos y hacerlos incomprensibles
- Asegurarse que el receptor pueda descifrarlos

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado y generalmente las claves pueden ser:

- Claves simétricas: son claves que se usan para el cifrado y descifrado.
- Claves asimétricas: son claves que se usan para el cifrado y otras claves para el descifrado.

3.5.1 Cifrado de información en Italimentos

En Italimentos la información más importante de los servidores se guarda semanalmente en una medio de almacenamiento óptico DVD, estos respaldos se guardan en un archivo con extensión .Zip y al momento de abrir pide un nombre de usuario y contraseña seguras. El programa usado para realizar estas copias de seguridad se llama FBackup 4.6 que es una herramienta que ayuda a realizar dichos respaldos de información de la base de datos y de usuarios críticos.

La base de datos realiza también un respaldo de información utilizando los recursos del mismo servidor, ya que no posee un respaldo externo o servidor de base de datos de respaldo, pero existe copias de seguridad en medios de almacenamiento DVD´s que solo pueden ser abiertos en el servidor de base de datos.

No existe un cifrado de información que este contenida en un medio de almacenamiento como USB, disco duro o una partición de un disco duro, por lo cual cualquiera podría ver la información.

3.5.2 FBackup 4.6

FBackup 4.6 es un software gratis que ayuda a realizar copias de seguridad y su uso puede ser personal o comercial. Este programa protege datos importantes haciendo automáticamente copias de seguridad a cualquier dispositivo de almacenamiento local o en red. Los datos respaldados pueden ser comprimidos en varios formatos o se puede hacer una copia de seguridad exacta de los archivos originales.

La aplicación es compatible con sistemas operativos Microsoft Vista, XP, 2008/2003/2000 server y tiene una interfaz sencilla y que va guiando al operario mediante un asistente que le va realizando preguntas:

- Donde desea guardar la copia de seguridad
- Que desea respaldar
- Como desea realizar la copia de seguridad: copia comprimida .Zip, copia de seguridad espejo sin comprensión.
- Cada cuando desea realizar el respaldo.

La figura 3.6.2.1 muestra la aplicación FBackup usada para realizar copias de seguridad

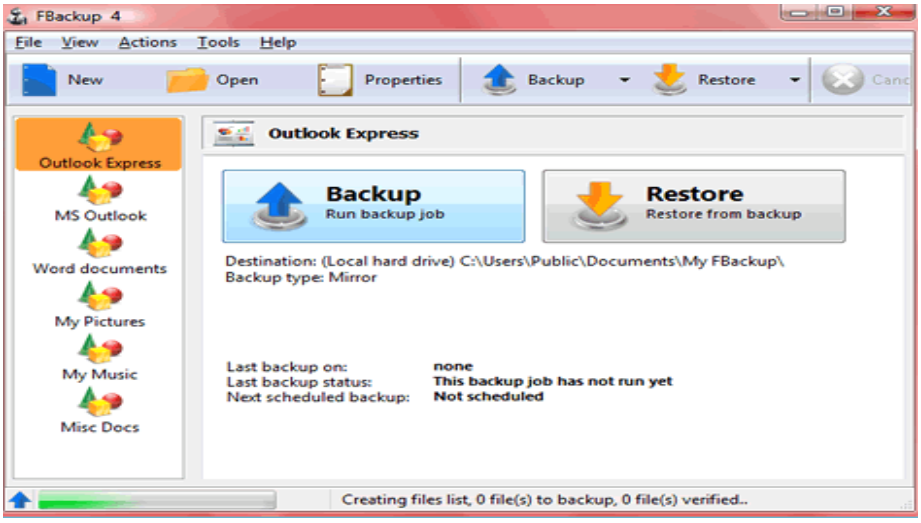


Figura 3.6.2.1. Aplicación FBackup 4.6

Cuando ya se define una tarea de respaldo, se puede iniciar manualmente presionando el botón Backup o presionando la tecla F, o si ya se tiene una tarea programada entonces la tarea de realizar la copia de seguridad se la realizara automáticamente.

CAPITULO 4

"Auditoría de la gestión de activos informáticos"

4.1 Inventario de soportes y actualizaciones

Cada soporte informático está identificado mediante un código único, puede por fecha de respaldo o por un código dado por una normativa. Este identificador también puede estar representado gráficamente mediante un código de barras para facilitar su control y lectura, siempre que sea físicamente posible.

En cada soporte físico inventariado se queda adherida una etiqueta con el código de barras u otro método de etiquetado. El inventario de soportes informáticos detalla la fecha de adquisición, proveedor, características del elemento, destino que se le da, estado en que se encuentra; en caso que sea un desecho se debe obtener la fecha y causa. Así mismo se ha de constar la valoración que le ha otorgado el responsable de seguridad de ficheros [31] y sistemas. La gestión de soportes informáticos debe estar regulada en un artículo para todos los niveles de seguridad alto, medio y bajo. La relación del personal que se encuentra en un mismo lugar que las copias de seguridad, se debe tener un espacio restringido de acceso a las mismas ya que pueden contener información de carácter personal o datos importantes para la empresa. Las tablas 4.1.1, 4.1.2, 4.1.3 muestran varios ejemplos que puede tomar cualquier organización para registrar un inventario de soportes

ORGANIZACIÓN X				
06-010-00	**INVENTARIO DE SOPORTES**		**VERSIÓN**	
ELABORADO POR	**FECHA**	**APROBADO POR**	**FECHA**	
ALTAS			**BAJAS**	
No. Soporte	Tipo de información	Fecha	motivo	Fecha

Tabla 4.1.1. Inventario de soportes.

31 Ficheros: Conjunto de bits almacenado en un dispositivo.

ORGANIZACIÓN X							
02-010-00		**INVENTARIO DE HARDWARE**				**VERSIÓN**	
ELABORADO POR		**FECHA**	**APROBADO POR**			**FECHA**	
Equipo	Marca	Modelo	Serie	Sistema Operativo	Fecha de instalación	Uso	Ubicación

Tabla 4.1.2. Inventario para hardware.

ELABORADO POR			**FECHA**	**APROBADO POR**		**FECHA**
Aplicación	Versión	Modulo	Función	Lenguaje	Fecha de creación	Fecha de modificación

Tabla 4.1.2. Inventario para software de desarrollo externo.

ORGANIZACIÓN X						
02-020-00		**INVENTARIO DE SOFTWARE DE DESARROLLO INTERNO**				**VERSIÓN**
ELABORADO POR		**FECHA**	**APROBADO POR**			**FECHA**
APLICACIÓN	VERSIÓN	MODULO	FUNCIÓN	LENGUAJE	FECHA CREACIÓN	FECHA ULTIMA MODIFICACIÓN

Tabla 4.1.2. Inventario para software de desarrollo interno.

ORGANIZACIÓN X						
02-020-00		**INVENTARIO DE SOFTWARE COMERCIAL**			**VERSIÓN**	
ELABORADO POR		**FECHA**	**APROBADO POR**		**FECHA**	
Aplicación	Versión	Modulo	Función	Lenguaje	Fecha de creación	Fecha última modificación

Tabla 4.1.2. Inventario para software comercial.

4.1.1 Inventario de soportes y actualizaciones en Italimentos

En Italimentos se realiza un inventario de recursos informáticos, solo lo que son: CPU, monitores e impresoras, puesto que los demás recursos informáticos son tomados como gastos. Existe el departamento de compras en el cual se registra todos los elementos informáticos adquiridos sean: hardware, software comercial, repuestos; para entrar a producción en la empresa. Para el software libre no se tiene un inventario puesto que eso se puede descargar libremente de internet y no pasa por el departamento de compras o recepción de recursos, sino que pasa directamente a producción si es necesario.

4.1.1.1 Inventario de hardware

En el departamento de sistemas, tiene un inventario en un documento de Microsoft Office Excel 2007 que se actualiza una o dos veces cada año, este inventario está almacenado en la computadora del jefe de sistemas y compartida con ciertos usuarios, pero este documento está cifrado para poder ingresar con nombre de usuario y contraseña. El inventario de recursos informáticos consta de las siguientes características:

- Tipo PC: Indica si el equipo es servidor, laptop o escritorio.

- Responsable: Indica cual es el usuario responsable del equipo.
- Nueva IP tipo C: Indica la IP del equipo.
- Nombre: Indica el nombre del equipo.
- Departamento: Indica dentro de que departamento se encuentra el equipo.
- Usuario: Indica cual es la cuenta de usuario del equipo.
- Password: Indica que password tiene el equipo. Esta opción no está para todos los usuarios.
- Año: Indica el año de fabricación del equipo.
- Microprocesador: Indica la velocidad del microprocesador.
- RAM: Indica la velocidad de memoria.
- HHDD: Indica la capacidad del disco duro.
- Estado USB: Indica si los puertos USB están activos o inhabilitados.
- Unidades externas: Indica si el equipo posee unidades externas.
- Más características: Otras características que se encuentre al equipo.
- Observaciones: Observaciones que se dé al equipo en producción.
- Ciudad: En que ciudad o sector se encuentra el equipo.
- Srv Squid: Indica dentro de que grupo de proxy se encuentra el equipo.
- Ratón: Indica que tipo de ratón se encuentra conectada al equipo. Esta característica ya no se realiza actualmente.

- Teclado: Indica que tipo de teclado se encuentra conectado al equipo. Esta característica ya no se realiza últimamente.

- Código Monitor: Indica el número de serie del monitor y código asignado por Italimentos.

- Código CPU: Indica el número de serie del equipo y código asignado por Italimentos.

- Impresora: Indica que tipo de impresora se encuentra conectado al equipo. Si no existe impresora se deja en blanco.

- Teléfono: Indica el número de teléfono del usuario del equipo. Si no existe se deja en blanco.

- Mantenimiento Software: Indica si se han dado mantenimientos de software.

- Mantenimiento de Hardware: Indica si se han dado mantenimientos de hardware.

El departamento de sistemas tiene un formato usado para movimientos o bajas de equipos de cómputo. *Véase Anexo C.1.*

4.1.1.2 Inventario de software

En Italimentos no existe un inventario de software comercial o libre que posee la organización, pero existe un inventario que describe solo el sistema operativo que tiene cada computadora en la empresa..

4.1.1.3 Inventarios de soportes de copias de seguridad

En la empresa o departamento de sistemas no existe un inventario de soportes de las copias de seguridad. Anteriormente se realizaba la copia en un medio de almacenamiento DVD y se iba apilando en un estuche dentro de una vitrina en el departamento de sistemas y cartera.

Estas copias de seguridad, están etiquetadas físicamente por fechas, con un marcador de CD u otra herramienta de sellado y tienen un orden lógico en su almacenamiento ya que

la ultima copia de seguridad realizada es la primera en encontrarse en el estuche de almacenamiento de copias. *La figura 4.1.1.3.1 muestra el estuche de almacenamiento de copias de seguridad.*

Figura 4.1.1.3.1. Estuche de almacenamiento de copias de seguridad.

Ahora las copias de seguridad se realizan dentro del mismo servidor, pero no realiza un registro detallado indicando que días se realizaron las copias de seguridad y que información se ha respaldado.

4.2 Registro y actualización de entrada y salida de información

El controlar toda la documentación e información que se recibe y emite, en papel o formato electrónico, se debería regir bajo un reglamento dado por un comité dentro de la empresa. El registro de entrada y salida de datos, soportes, información, documentos, etc. debería ser un proceso fundamental para organismos públicos y privados.

Las oficinas dentro de una empresa reciben numerosa documentación, información y solicitudes en diferentes formatos, para explotarlas de la mejor manera; toda esta información debe clasificarse, registrarse e incluirse un sello de control para poder distribuirla y entregarla de forma automática a cada destinatario, el cual puede aceptar, rechazar o trasladar el registro recibido.

Además, se debe poder explotar de la mejor manera la información registrada a través de informes y estadísticas para conocer a que parte se dirige la mayoría de la información y cuál es el objetivo de la misma.

Para conocer más sobre lo que está ocurriendo es necesario identificar las funciones y servicios de los sistemas de información, clasificarlos, identificar los flujos de información y situar los posibles puntos de entrada y salida de datos e información. Para esos puntos de entrada y salida se debe garantizar tres componentes de seguridad:

- Integridad
- Disponibilidad
- Confidencialidad

En las entradas y salidas de información se deben identificar qué nivel de protección se aplica sobre los sistemas, ya que se puede implementar sistemas de registro log32, o se pueden usar herramientas que ayuden a gestionar los registros para minimizar tiempos en los tramites de recepción y emisión.

4.2.1 Registro y actualización de entrada y salida de información en Italimentos

En Italimentos no se lleva un control de entrada y salida de información, ya que no se tiene definida una política que clasifique el tipo de información: restringido, gerencial, publica, etc. Esta información se recibe o emite por distintos medios de transmisión, sean: CD´s, DVD's, memorias flash, teléfonos móviles, etc. Dependiendo de la información que se desee emitir o recibir, se realiza o no un cifrado de información. Pero no existe una política que defina que información debe o no ir cifrada, y en que medio se debe transmitir.

La mayoría de PC's de la empresa están bloqueadas los puertos USB con el objetivo que los usuarios no puedan llevar información al exterior o ingresar información, virus y

32 Log: Registro de eventos realizados en una computadora

otros programas ajenos a la empresa. Solo un grupo de usuarios pueden grabar información en medios de almacenamiento y trasladarla hacia un lugar en específico.

Existe un registro sobre un inventario cuando una PC, monitor o impresora se trasladan hacia otra estación de trabajo. Antes de que la PC entre a producción con el nuevo usuario, se realiza un formateo de la computadora a bajo nivel, eliminando todo rastro de información y registros con el fin de evitar que se pueda recuperar información dentro de la misma.

Del mismo modo cuando un disco duro se cambia a otra estación de trabajo, se realiza un formato a bajo nivel, eliminando todo rastro de información. Estas acciones están comprobadas puesto que el mismo jefe de sistemas, utilizando herramientas, no ha logrado recuperar información como medida de seguridad.

4.3 Copias de seguridad y recuperación de datos

Las copias de seguridad tienen dos objetivos que son muy importantes:

- Permiten la restauración de archivos individuales, se da este caso cuando un usuario borra un archivo accidentalmente o se corrompe y pide restaurarlo desde su último respaldo.

- Permiten la restauración completa de archivos completos, por la situación que sea, el administrador observa que un hardware que era parte productiva del centro de datos, ahora es un hardware sin funcionamiento. Aquí se puede perder gran cantidad de datos o perderlos todos.

En la actualidad los datos cambian y para el diseño de un procedimiento de respaldo se realizan por dos razones;

- Una copia de seguridad es un reflejo de los datos.

- Los datos que cambian con poca frecuencia se respaldan a menudo, pero los datos que cambian regularmente deben ser copiados frecuentemente.

4.3.1 Tipos de respaldos

4.3.1.1 Respaldos completos

Es un respaldo donde cada archivo es escrito con su archivo copia, realizando modificaciones en todos los ficheros sobre escritos, si los datos a respaldar nunca cambian entonces cada respaldo creado será una copia exacta del original. El respaldo completo no verifica para ver si un archivo ha cambiado desde el ultimo respaldo, sino que escribe ciegamente todo lo que respalda, haya sido modificada o no.

4.3.1.2 Respaldos incrementales

Los respaldos incrementales primero revisan para ver si la fecha de modificación de un archivo es más reciente que la fecha del último respaldo. Si no lo es, se puede saltar dicho respaldo. Si la fecha de modificación es más reciente, el archivo ha sido modificado y se debería realizar la copia. La principal ventaja es que copian mucho más rápido que un respaldo completo.

4.3.1.3 Respaldos diferenciales

Es similar al respaldo incremental, realizando copias cuando archivos han sido modificados. Estos respaldos son acumulativos, una vez que el archivo ha sido modificado continuo siendo incluido en todos los próximos respaldos. Cada uno de estos respaldos tiene todos los archivos modificados, haciendo posible una restauración completa con el último respaldo completo y el último diferencial.

4.3.2 Copias de seguridad y respaldos en Italimentos

En Italimentos las copias de seguridad se realizan semanalmente para todos los usuarios, para ello se realizaron tareas programadas automáticas en las computadoras para que se realice respaldos cada semana, pero a petición de ciertos usuarios la información se respalda de forma manual. Estos respaldos se los hace en carpetas compartidas en una red interna, en la cual cada usuario solo puede ingresar a ciertas carpetas y guardar su información, pero otros usuarios pueden ver dicha información si los ficheros no están cifrados con usuario y contraseña.

Para la base de datos que contiene información critica e importante se realiza respaldos, en el propio servidor, utilizando una aplicación llamada SQLServer. Para los respaldos de información de usuarios críticos se utiliza la aplicación FBackup 4.6 la cual se programa para que realice respaldos automáticos cada dos días a la 01:30am para no interrumpir los servicios al siguiente día. Los administradores de sistemas realizaron las configuraciones en la herramienta FBackup 4.6, para realizar copias de seguridad incrementales, de tal manera que se realizan actualizaciones de la información y sobre-escribiendo la información antigua. Para observar el cuestionario realizado al jefe de sistemas y conocer las acciones que se realiza en Italimentos de acorde a la gestión de activos informáticos. *Véase el Anexo C.2.*

4.4 Lugar de almacenamiento de copias de seguridad

Estos lugares de almacenamiento es importante que sean lugares muy seguros, ya que deben tener protección suficiente contra catástrofes como incendios, inundaciones, terremotos, robos, etc. Existen muchas estrategias para copias de seguridad de los datos, incluso algunas gratuitas, pero es importante encontrar un método de plan de copia de seguridad en un medio seguro de almacenamiento tales como:

4.4.1 Tipos de almacenamiento

4.4.1.1 Disco duro

El almacenamiento de una copia de seguridad en un lugar distinto del original asegura de que los datos no se pierdan. Adjuntar otro disco duro a la unidad original del sistema para almacenar la copia de seguridad es una solución ya que se tiene el respaldo inmediato después de una catástrofe informática. *La figura 4.4.1.1.1 muestra un disco duro de PC.*

Figura 4.4.1.1.1. Disco duro.

4.4.1.2 DVD

La mayoría de veces las copias de seguridad son quemadas en DVD+R/RW o DVD-R/RW33. Los DVD tienen una larga vida y garantizan que la copia de seguridad de los datos estará disponible para su recuperación cuando sea necesario. *La figura 4.4.1.2.1 muestra un DVD.*

Figura 4.4.1.2.1. DVD

4.4.1.3 Unidades de cinta

El almacenamiento de los datos de copia de seguridad en cintas tradicionales, es un método eficaz para las empresas ya que los datos son grabados y trasladados a un lugar seguro. *La figura 4.4.1.3.1 muestra una unidad de cinta de respaldo marca hp.*

33 DVD+R/RW o DVD-R/RW: Digital Versatile Disc Grabable Writable or Re Writable

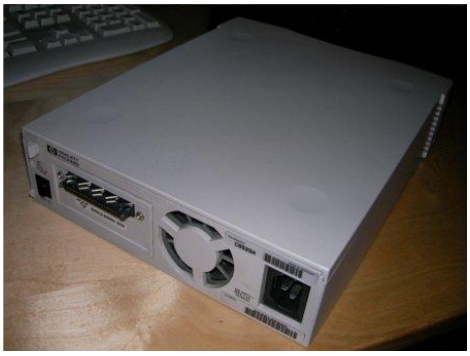


Figura 4.4.1.3.1. Cintas de respaldo marca hp.

4.4.1.4 A través de la red local

Los administradores del sistema, deberían mantener una política para realizar copias de seguridad de un ordenador a otro ordenador o de un servidor a través de la red local. De esta manera los datos de copia de seguridad, en un ordenador o servidor, almacenan las copias de seguridad de otro ordenador o servidor.

4.4.1.5 Almacenamiento en línea

Mediante internet se puede almacenar copias de seguridad de datos en línea a través de la web34, ya que internet presenta un lugar seguro, lejano y una avanzada solución de almacenamiento de los datos de copias de seguridad en un equipo remoto ya que se puede desactivar el servidor web para hacer inaccesible el ingreso la información. Se debe tomar en cuenta que la información debe estar encriptado o hacer uso de nuevas tecnologías como es el https[35].

4.4.1.6 Flash memory:

Estos dispositivos USB o Firewire[36] son comúnmente usados para el traslado de información de manera segura a diferentes partes. Estos medios de almacenamiento son muy utilizados para llevar información de manera inmediata y responder ante un problema informático de manera rápida y segura. *La figura 4.4.1.6.1 muestra una unidad de almacenamiento USB marca kingston.*

34 Web: Medio de comunicación a través de la red
35 https: Hiper Text Transfer Protocol Secure
36 Firewire: Bus serial de apple, similar al USB.

Figura 4.4.6.1. USB marca kingston

4.4.1.7 Discos extraíbles

Llamados también Jazz-unidades, unidades ZIP [37] y discos REV[38] extraíbles, son todas las cintas de almacenamiento de datos de la misma manera que los discos flexibles. La única diferencia que pueden almacenar datos en un rango de 100Mb hasta 40Gb. *La figura 4.4.1.7.1 muestra una unidad jazz.*

Figura 4.4.1.7.1. Unidad Jazz

4.4.2 Lugar de almacenamiento de copias de seguridad en Italimentos

En la empresa, las copias de seguridad solían ser quemadas en DVD's y guardadas en un estuche dentro de una vitrina, estas copias solían ser quemadas cada semana respaldando la información crítica e importante para solucionar problemas cuando existía una catástrofe informática.

37 Unidad ZIP: Zone Information Protocol para comprensión de archivos.
38 Discos REV: Medio de almacenamiento secundario extraíble

Actualmente, las copias de seguridad de los usuarios se las realiza en el disco duro de 140 Gb que se encuentra dentro del mismo servidor de base de datos mediante una herramienta de software llamada FBackup versión 4.6, la cual realiza copias de seguridad en un archivo con extensión .zip. El servidor de base de datos se encuentra dentro de un rack[39], junto con otros servidores en un cuarto de servidores. *La figura 4.4.2.1 muestra el cuarto de servidores donde se encuentra el rack de servidores de Italimentos.*

Figura 4.4.2.1. Cuarto de servidores con el rack.

4.5 Etiquetado de los activos

El etiquetado de los activos informáticos permite realizar informes que ayudarán a identificar, realizar seguimientos, asegurar y recuperar los equipos de forma más fácil y sencilla. La forma más sencilla de realizar un seguimiento de los activos de hardware es etiquetarlos cuando estos entran a producción, en la que la etiqueta se imprime en cada activo y esta permite recuperar información importante para las actualizaciones de los inventarios.

Los informes sobre los activos ayudan a integrar, desechar o reutilizar los activos informáticos en la empresa, ya que los informes pueden ser entregados cada día, cada

[39] Rack: Estructura para soporte de servidores

semana o cada mes, y es una herramienta útil de seguimiento para identificar y tomar decisiones.

Este proceso de etiquetado en los medios de almacenamiento masivo, como copias de seguridad, debe ser consistente con los objetivos dados para dichos activos informáticos. El etiquetado permite ahorrar tiempo en la implementación, reduciendo el costo de monitoreo de activos, para ello se usan etiquetas de identificación de propiedad que pueden estar en el chasis de las computadoras, en la caja de embalaje o también disponibles sobre la BIOS [40]. Al personalizar los activos informáticos, la empresa reduce considerablemente sus costos totales de propiedad y aseguran el máximo nivel de calidad.

4.5.1 Beneficios

La creación y etiquetado de activos permite ahorrar tiempos de implementación y costos de monitoreo con el etiquetado físico de los equipos, eliminando atrasos de producción y costos de administración al permitir que las etiquetas se puedan administrar internamente en un inventario de etiquetas.

4.5.2 Características

Las características principales al etiquetar activos informáticos son:

- Ahorrar tiempo de implementación y costos de monitoreo
- Colocar etiquetas a una lista especifica de activos fijos informáticos
- crear y fijar etiquetas estándar o predefinidas por la empresa

4.5.3 Etiquetado de los activos en Italimentos

En Italimentos el departamento de compras se encarga de etiquetar los activos y de los inventarios de la empresa, el departamento de sistemas solo se encarga de realizar la petición de un nuevo recurso informático. Para los activos informáticos solo se etiqueta monitores, CPU e impresoras, puesto que los demás recursos son tomados como gastos

40 BIOS: Basic Input/Output System

pequeños en la empresa. Al momento de etiquetar un nuevo recurso se toma el número de serie, con código de barras, del activo y se etiqueta un código establecido por Italimentos. *La figura 4.5.3.1 muestra el antiguo sello de etiquetado establecido por el sistema antiguo.*

Figura 4.5.3.1. Sello antiguo de activos de Italimentos

La figura 4.5.3.2 muestra el nuevo sello de etiquetado usado por el nuevo sistema de Italimentos.

Figura 4.5.3.2. Sello nuevo de activos de Italimentos

4.6 Medidas a adoptar cuando un soporta va a ser desechado o reutilizado

Una de las vías más peligrosas para que la información salga de una empresa es en el desecho físico de discos, cintas o cualquier otro soporte. Normalmente se suelen enviar a la basura sin tomar las debidas precauciones, ya que en muchos casos estos desechos

contienen información importante y, en muchas ocasiones, puede ser recuperada por expertos que pueden comercializar la información obtenida en un soporte.

Para ello se debe tener un reglamento con medidas de seguridad cuando un soporte, con información de nivel medio o alta, va a ser desechado o bien vaya a ser reutilizado. En un reglamento se debe tener por escrito las medidas de seguridad para impedir cualquier tipo de recuperación posterior de información almacenada en un soporte. Todo esto se debe realizar antes que se elimine de un inventario de soportes.

No se debe olvidar que existen herramientas de software muy poderosas que logran recuperar información que pareciera que esta borrada, para ello se emplean técnicas de eliminación permanente de información en soportes de almacenamiento como: utilización de des magnetizadores para soportes magnéticos, la grabación con varias pasadas con un contenido aleatorio para que no se pueda ver el contenido anterior o hasta la destrucción física del soporte. *La tabla 3.6.1 muestra un ejemplo a utilizar para el desecho o reutilización de soportes.*

<table>
<tr><td colspan="4">ORGANIZACIÓN X</td></tr>
<tr><td>04-020-00</td><td colspan="2">PROCEDIMIENTO DE DESECHO Y REUTILIZACIÓN DE SOPORTES</td><td>VERSIÓN</td></tr>
<tr><td>ELABORADO POR</td><td>PECHA</td><td>APROBADO POR</td><td>FECHA</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Aplicable a:

ORGANIZACIÓN X

Ámbito:

Contenido:</td></tr>
</table>

Tabla 3.6.1. Plantilla para desecho o reutilización de soportes

4.6.1 Ámbito

El ámbito para aplicar el procedimiento de desecho y reutilización de soportes es para todas las áreas, divisiones, departamentos, servicios, directivos, empleados y entidades o profesionales contratados por la empresa.

4.6.2 Contenido

Se requiere adoptar medidas adecuadas cuando un soporte va a ser desechado o reutilizado, en función de los datos que contenga en soporte: magnético, óptico, PDA[41], teléfono móvil o papel; para proceder a su destrucción. En el contenido se pone el tipo de información que posee el soporte para dar la mejor solución a una reutilización o desecho, bien sea desde una PC hasta un CD o DVD. Cada vez que se realice una acción se debe registrar en un inventario de soportes.

4.6.3 Medidas a adoptar cuando un soporte va a ser desechado o reutilizado en Italimentos

El departamento de sistemas no tiene una política descrita en un documento que detalle los procedimientos a realizar cuando un soporte va a ser desechado o reutilizado, pero al dar de baja un activo informático se reutiliza las partes que funcionen para tener de soporte cuando otra PC no funcione. Todos los activos informáticos que están dados de baja, están almacenados en bodega de recursos informáticos y no pueden ser desechados, reciclados o donarlos porque se necesita la autorización de un notario para dichas acciones. *La figura 4.6.3.1 muestra la bodega de recursos informáticos inactivos.*

Figura 4.6.3.1. Bodega de recursos informáticos inactivos.

[41] PDA: Asistente Personal Digital

Al ser desechado un soporte informático, primero se aseguran de borrar la información almacenada para evitar recuperar la información, posterior al desecho del recurso informático inactivo.

4.7 Cuentas de usuario

Las cuentas de Usuario son la vía de acceso principal al sistema para la gente que trabaja en cualquier parte de un gestor de activos, estas cuentas aíslan al usuario del entorno impidiendo que pueda causar daños al sistema o a otros usuarios, y pidiendo que se pueda personalizar su entorno sin que esto afecte al resto de los empleados.

Cada empleado que acceda al sistema propio al que está trabajando debería tener una sola cuenta de usuario, esto nos ayuda averiguar quién está haciendo qué evite o interfieran en las configuraciones de distintos usuarios o que puedan leer correos electrónicos, etc.

Cada usuario puede configurar su activo a su manera para el manejo adecuado del mismo ya que con su configuración ya sea de teclado, mouse, etc., será de mejor uso y no poseerá problemas en el manejo a futuro.

4.7.1 Personalizar a los usuarios.

Personalizar es un entorno establecido por el administrador o el usuario para dar soporte a distintos lenguajes, juegos de caracteres, estándares sobre fechas y horas, etc.

4.7.2 Tipos de cuentas de usuarios.

Existen tres tipos de cuentas de usuarios

- Estándar
- Administrador
- Invitado

4.7.3.1 Cuenta de usuario estándar

Esta cuenta "permite que una persona use la mayoría de las funciones del equipo, pero se requiere el permiso de un administrador si se intenta realizar cambios que afecten a los demás usuarios o a la seguridad del equipo.

Cuando se usa una cuenta estándar, se puede utilizar la mayoría de programas instalados en el equipo, pero no se puede instalar o desinstalar software ni hardware, eliminar archivos que son necesarios para que el equipo funcione, o cambiar opciones de configuración en el equipo que afecten a otros usuarios. Si usa una cuenta estándar es posible que algunos programas le soliciten que proporcione una contraseña de administrador antes que pueda ejecutar determinadas tareas."[42]

4.7.3.2 Cuenta de usuario para administrador

"Esta una cuenta de usuario es la que permite realizar cambios que afecten a otros usuarios. Los administradores pueden cambiar la configuración de seguridad, instalar software y hardware, y obtener acceso a todos los archivos en un equipo. Los administradores también pueden realizar cambios en otras cuentas de usuario.

Cuando configura Windows, se le pide que cree una cuenta de usuario, ésta cuenta es una cuenta de administrador que le permite configurar el equipo e instalar cualquier programa que desee usar. Cuando haya terminado de configurar el equipo, se recomienda que use una cuenta de usuario estándar para el trabajo diario. Es más seguro usar una cuenta de usuario estándar que usar una cuenta de administrador."[43]

4.7.3.3 Cuenta de usuario para invitado

"Una cuenta de invitado es una cuenta para los usuarios que no tienen una cuenta permanente en el equipo o dominio. Permite que las personas usen el equipo sin tener acceso a los archivos personales. Quienes usen la cuenta de invitado no pueden instalar

42 http://windows.microsoft.com/es-US/windows-vista/What-is-a-standard-user-account
43 http://windows.microsoft.com/es-ES/windows7/What-is-an-administrator-account

software o hardware, cambiar la configuración ni crear una contraseña, es necesario activar la cuenta de invitado antes de que pueda usarse."[44]

4.7.3 Cuentas de usuario en Italimentos

En Italimentos el jefe de sistemas es el único que puede crear, editar y eliminar las cuentas de usuario para cada persona que interactúe con una computadora en la empresa, pero cada usuario es responsable de su propia contraseña por políticas de la empresa pero no están descritas en un documento físico o de seguridad de la empresa. Para realizar cuentas nuevas estas tienen privilegios que pueden ser: usuarios finales, administradores, gerencia y servidores, la cual cada uno de ellos podrá realizar ciertas acciones sobre su estación de trabajo. Así mismo, para generar los nombres de las cuentas se realiza de tres formas: por nombre, por departamento o por cargo.

4.7.4.1 Privilegios de las cuentas de usuario

Se debe tener en cuenta que cualquier usuario con cualquier privilegio es vulnerable al contagio de virus informáticos, así como a la distribución del mismo por medio de la red local. Lo que se intenta en Italimentos al dar los privilegios es minimizar al máximo la infección y propagación de los virus por parte de los usuarios, actualizando antivirus y parchando los sistemas operativos de los equipos de la empresa. Con estos privilegios también se desea dar un acceso limitado a la información, pero a veces los usuarios guardan sus archivos en lugares de acceso público, siendo esto una debilidad en la seguridad de la información.

4.7.4.1.1 Nivel de usuario final o usuario invitado

En este nivel todos los usuarios con estos privilegios tienen acciones limitadas de los cuales se nombran a continuación:

- No pueden realizar modificaciones en las configuraciones propias de la computadora
- No pueden instalar programas ajenos a la empresa

44 http://windows.microsoft.com/es-MX/windows-vista/What-is-a-guest-account

- No puede realizar modificaciones en las configuraciones de programas instalados
- No pueden crear, eliminar o modificar cuentas de usuario
- No pueden acceder a modificar privilegios de usuarios
- Solo pueden acceder a aplicaciones remotas especificas a su cargo laboral

En este nivel los usuarios finales comparten información por medio de carpetas compartidas en la red local de la empresa, y para ello están definidos los siguientes usuarios:

- Asistente de gerencia
- Medico
- Gerente financiero
- Contador general
- Auxiliares contables
- Jefe cartera
- Recaudadores
- Auxiliares de cartera
- Tesorería
- Auxiliares de tesorería
- Jefe administrativo
- Coordinador administrativo
- Recepcionista

- Operadores administrativos
- Auxiliares de gestión humana
- Operarios de RRHH
- Coordinador de compras
- Bodeguero
- Operario de bodega

4.7.4.1.2 Nivel de usuario administrador

En este nivel de usuario, el administrador tiene todos los privilegios para realizar acciones tales como se nombra a continuación:

- Realizar modificaciones en las configuraciones propias de la computadora
- Realizar instalaciones de cualquier programa
- Realizar modificaciones en las configuraciones de programas instalados
- Crear, eliminar o modificar cuentas de usuario
- Asignar o eliminar privilegios a cuentas de usuario
- Pueden acceder a aplicaciones remotas especificas a su cargo laboral

En este nivel los usuarios administradores comparten información por medio de carpetas compartidas en la red local de la empresa, y para ello están definidos los siguientes usuarios:

- Coordinador de seguridad industrial
- Contador de costos
- Jefe de gestión humana

- Jefe de sistemas
- Auxiliar de soporte de sistemas

4.7.4.1.3 Nivel de gerencia o usuario estándar

En este nivel se otorga otros privilegios de acceso a información y aplicaciones; y se limita ciertos privilegios de administrador. Entre las acciones que puede realizar este usuario se nombran a continuación:

- Realizar modificaciones en las configuraciones propias de la computadora
- Realizar instalaciones de cualquier programa
- Realizar modificaciones en las configuraciones de programas instalados
- Crear, eliminar o modificar cuentas de usuario
- Asignar o eliminar privilegios a cuentas de usuario
- Pueden acceder a cualquier aplicación remota, previo aviso a jefe de sistemas para la instalación del programa a acceder: cámaras de seguridad, monitoreo de computadoras remotas, informes, etc.

En este nivel de usuario solo existe un grupo muy reducido, en el cual esta:

- Gerencia
- Jefe de compras

4.7.4.1.4 Nivel de servidores

En este nivel, solo pueden acceder los administradores de sistemas ya sea de forma local o remota a través de una red, permitiendo instalar aplicaciones de negocio de Italimentos para los usuarios finales. En esta cuenta el administrador puede ser:

- Realizar modificaciones en las configuraciones propias de la computadora

- Realizar instalaciones de cualquier programa
- Realizar modificaciones en las configuraciones de programas instalados
- Crear, eliminar o modificar cuentas de usuario
- Asignar o eliminar privilegios a cuentas de usuario
- Pueden acceder a aplicaciones remotas especificas a su cargo laboral
- Acceder a aplicaciones y bases de datos.

En este nivel se encuentran los servidores de la empresa Italimentos:

- Servidor de base de datos
- Servidor de internet proxy
- Terminal server
- Servidor de dominio
- Servidor de desarrollo
- Servidor de aplicaciones
- base de datos de respaldo

4.7.4.2 Estructura del nombre de cuentas de usuario

4.7.4.2.1 A nivel de nombre

Al crear una cuenta de usuario a nivel de nombre, se toma en cuenta la primera letra de su nombre, seguido del apellido. Por ejemplo.

cbaculima, mmuyulema, etc.

En el caso que existan más de dos personas con la misma letra en el nombre y tengan el mismo apellido, entonces se toma la primera letra del primer y segundo nombre, seguido del apellido. Por ejemplo.

Cmbaculima, mvmuyulema, etc.

Si existiera coincidencia para que se repita las dos iníciales y el mismo apellido, entonces se realizaría un nombre de cuenta de usuario a nivel de departamento o cargo; pero no se ha dado el caso en Italimentos.

4.7.4.2.2 A nivel de departamento

Al momento de crear el nombre de una cuenta a nivel de departamento, se pone el nombre del departamento seguido del número de la última computadora en producción de dicho departamento. Por ejemplo.

Cartera1, Cartera2, …, CarteraN

Todas estas cuentas, con sus responsables, sus características de cada PC, son registradas en un inventario para mayor control de las mismas.

4.7.4.2.3 A nivel de cargo laboral

Cuando se crea el nombre de usuario a nivel de cargo laboral, depende mucho del departamento, pero no en todos los casos se pone un nombre de cuenta de usuario a nivel de cargo laboral. Para asignar el nombre se necesita conocer el departamento y si existe más de un usuario en ese departamento se pone la palabra “Jefe_” seguido del departamento a su cargo. Por ejemplo.

Jeje_Ventas, Jefe_Cartera, Jefe_Produccion, etc.

Si existe una solo persona en el cargo, se asigna el nombre de la cuenta solo con su cargo laboral. Por ejemplo.

Secretaria, Auditor, Gerente, etc.

Para los servidores de la empresa, se toma en cuenta que función realiza cada uno y dependiendo de su uso se da su nombre. Por ejemplo.

Srv_Desarrollo, Srv_BBDD, Srv_Camaras, etc.

4.8 Almacenamiento de Contraseñas

Hablar de Almacenamiento de contraseñas, es hablar de un gestor de contraseñas ya que ellos se encargan de almacenar una gran cantidad de contraseñas seguras ya sea por alguna de aplicación que se encargue de realizar dicho trabajo.

La base de datos encargada de guardar las claves, estará cifrada mediante una clave única, de forma que para el usuario sea muy útil para su administración y establece el grado de confianza para escoger claves complejas sin miedo a no ser capaces de aprenderse solo una clave para acceder a las demás contraseñas.

4.8.1 Implementación

Una manera de las tantas maneras de gestionar las contraseñas es almacenarlas en páginas web que nos brinde éste servicio, con ello buscamos una mejor manera para acceder a ellas desde cualquier lugar con conexión a internet, por lo cual las claves dependerán mucho del nivel de confianza que pusimos a quien nos ofrece el servicio.

4.8.2 Seguridad

En la seguridad en el almacenamiento de contraseñas va a depender de varios parámetros que colocaremos a continuación:

- La robustez de la clave maestra.
- La seguridad del algoritmo de cifrado.
- La calidad del código fuente.
- La forma de almacenar la clave.

- La existencia de virus u otro tipo de malware45 en nuestro ordenador.

4.8.3 Open ID

Es una alternativa para el uso de gestores de contraseñas ya que es estándar de identificación digital descentralizada donde el usuario se identifica desde una página web a través de una URL 46 donde puede ser verificado por cualquier servidor.

Los usuarios no tienen que crearse una nueva cuenta de usuario para obtener acceso, para eso lo que se debe de hacer es de disponer de un identificador creado en un servidor que verifique OpenID llamado proveedor de identidad, por lo tanto la seguridad de una conexión OpenID depende de la confianza que tenga con el cliente, pero si no existe esa confianza, la autenticación no será adecuada para servicios como son de banco o transacciones de comercio, sin embargo el proveedor de identidad puede usar autenticación más confiable pudiendo ser usada para dichos fines.

4.8.4 Almacenamiento de contraseñas en Italimentos

En Italimentos no existe una política que defina un medio seguro de almacenamiento de contraseñas, sino que cada usuario se propone una contraseña y es responsable de la misma.

Los administradores de sistemas solo conocen las contraseñas de correo electrónico de cada usuario, puesto que primero se registra los datos del usuario en el servidor de correo y se imponen una contraseña, después se configura la aplicación de Microsoft Office Outlook [47]en la computadora del usuario dándole su correo y su contraseña de ingreso para enviar y recibir correo electrónicos. *La figura 4.8.4.1 muestra el asistente de configuración de Microsoft Office Outlook 2007.*

45 Malware: Programa malicioso.
46 URL: Uniform Resource Locator
[47] Microsoft Office Outlook: Navegador de correo electrónico

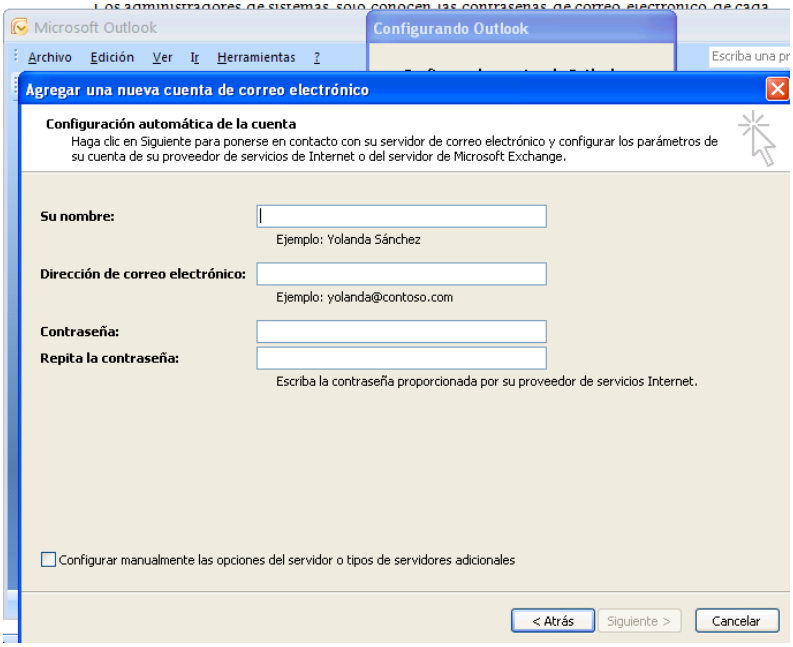


Figura 4.8.4.1. Asistente de configuración de Microsoft Office Outlook 2007

Las contraseñas de los servidores están guardados en un documento de texto, dentro de la computadora del jefe de sistemas, y solo pueden acceder tres personas a dicho documento: Jefe de sistemas, auxiliar de soporte de sistemas y jefe de desarrollo del nuevo sistema. Estas contraseñas de los servidores incluyen un cifrado obligatorio en el que constan: letras, números, mayúsculas, minúsculas y símbolos especiales.

CAPITULO 5

"Auditoría de la seguridad relacionada con el personal"

5.1 Uso de recursos informáticos

El usuario debe dar un uso adecuado a la información o recursos y servicios informáticos, utilizando cuentas de acceso, que únicamente le permiten realizar las actividades para las cuales fueron asignadas y evitando cualquier comportamiento que por acción u omisión conlleve a la violación de la privacidad, confidencialidad e integridad de la información o interrupción o disminución del desempeño de los servicios de información o funciones de otros usuarios.

El usuario al que se le ha asignado una cuenta de acceso es el único responsable por la misma. En consecuencia es responsable de toda actividad que genere a partir de la cuenta de acceso otorgada. La cuenta de acceso otorgada al usuario es propiedad de la empresa y es de carácter personal y es intransferible.

El usuario debe utilizar solamente las herramientas necesarias o autorizadas por el departamento de sistemas para la manipulación de la información y accesos a recursos y servicios informáticos. A través de un sistema se debe poder monitorear las estaciones de trabajo de la empresa, realizando así que el usuario evite el uso de recursos informáticos para fines privados o personales.

5.1.1 Uso de recursos informáticos en Italimentos

En Italimentos los recursos informáticos más usados son monitores, impresoras, CPU´s teclados y ratones; de las cuales más a menudo se cambian, por mal funcionamiento, los teclados, ratones y fuentes de poder de los CPU, discos duros de CPU. Al momento que se daña uno de estos recursos, el usuario responsable da a conocer al departamento de sistemas el fallo en uno de estos dispositivos permitiendo así, al jefe de sistemas o auxiliar de soporte de sistemas, poder realizar la respectiva reparación del dispositivo o el cambio del mismo.

Cuando no existen suficientes recursos para realizar los cambios con los dispositivos obsoletos, entonces los recursos rotan con los de otros departamentos hasta obtener otros nuevos. *La figura 5.1.1.1 muestra un set completo para un puesto de trabajo.*

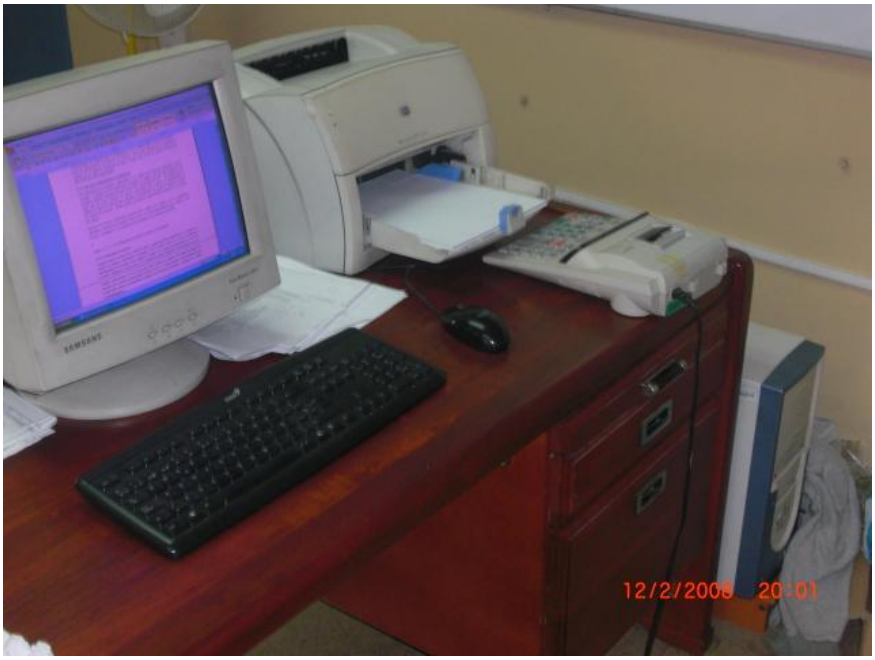


Figura 5.1.1.1. Set completo de un puesto de trabajo en Italimentos.

5.1.1.1 Rotación de recursos

Cuando dentro y fuera de la empresa rotan o ingresan nuevos empleados, se les asigna un puesto de trabajo, incluyendo su monitor, CPU, teclado, ratón y a veces una impresora dependiendo de su labor en la empresa. Cuando se le asigna su computadora se le da un formato completo a bajo nivel, se le instala su sistema operativo correspondiente con sus debidas aplicaciones y se le crea una nueva cuenta de usuario. El tiempo promedio de realizar las acciones anteriormente dichas es de cuatro horas aproximadamente, esto depende del CPU, puesto que existen computadoras antiguas que demoran en buscar e instalar los drivers correspondientes.

Esta aproximación se debe a que ingresan nuevas computadoras a producción y se dan de baja a las computadoras que no sirven o muchos problemas provocan. Al momento de realizar un movimiento de un equipo, el departamento de sistemas tiene un formato para dicho movimiento. *Véase Anexo C.1*.

5.1.1.2 Mantenimiento de recursos

Cuando se realiza los mantenimientos preventivos para impresoras, en su gran mayoría de impresoras matriciales, se las realiza cada mes permitiendo que continúe con el buen

uso de la misma. Estos mantenimientos de impresoras matriciales se las realizan individualmente para que no afecte demasiado a la productividad del empleado responsable de dicha impresora. El mantenimiento preventivo consiste en desarmar ciertos tornillos, quitarles restos de papel y basura, engrasar el rodillo y volver armar la impresora para que pueda volver a entrar a producción.

Cuando se realizan mantenimientos correctivos para las impresoras, el error de fallo de una impresora se comunica al jefe de sistemas o auxiliar de soporte de sistemas para ser reparada. Primero se toman acciones en el puesto de trabajo de la impresora y si es falla de software o configuración, la impresora se arregla en ese mismo rato. Cuando el error es de hardware la impresora es llevada al departamento de sistemas o al cuarto de servidores para poder desarmar y arreglar la misma.

El tiempo promedio de mantenimiento de una impresora matricial es de quince minutos dependiendo de la marca de la impresora y de cuan afectada este la misma. En la empresa Italimentos ubicada en el parque industrial existen las siguientes impresoras:

- 12 Epson matriciales
- 3 Xerox a láser + 1 de color
- 1 Canon a inyección de tinta
- 2 hp a laser

Cuando a una computadora se da un mantenimiento preventivo, se lo realiza cada seis meses individualmente para no afectar la productividad del usuario responsable de la misma. El mantenimiento preventivo consiste en abrir el case de la computadora y con un soplete sacar todo el polvo que se encuentre dentro de esta, después se verifica que las tarjetas y cables estén bien conectados para garantizar su buen funcionamiento, paso seguido se instala el case y entra de nuevo a producción en su puesto de trabajo.

Al momento que se da un mantenimiento correctivo a la computadora, el usuario notifica al jefe de sistemas o auxiliar de soporte de sistemas que existe un fallo de sistema, para ello se toman acciones, primero en el puesto de trabajo para verificar configuraciones o errores en la conexión de redes o tomas eléctricas; si no existe un

error en el puesto de trabajo entonces la computadora va al departamento de sistemas o cuarto de servidores para conocer si alguna pieza esta quemada o desconectada.

El tiempo de reparación de estos mantenimientos puede variar dependiendo de los fallos que existan. Un mantenimiento preventivo puede durar quince minutos aproximadamente, mientras que un mantenimiento correctivo puede tomar varios minutos u horas dependiendo del caso que se dé.

En la empresa de Italimentos ubicada en el parque industrial existen aproximadamente:

- 90 computadoras
- 7 servidores
- 9 laptops

Para el mantenimiento de servidores se las realiza igual que una computadora de escritorio, con la diferencia que estos mantenimientos se realizan en horas no laborables. *La figura 5.1.1.2.1 muestra el soplador utilizado para los mantenimientos de computadoras, servidores e impresoras.*

Figura 5.1.1.2.1. Soplador utilizado en mantenimientos.

5.1.1.3 Resultado de los hechos realizados en Italimentos

En Italimentos se realizó una encuesta, de la que se tomo una muestra de veinte empleados, logrando sacar conclusiones de que existe un 15% de movimientos de recursos informáticos entre distintos empleados, los cambios o movimientos realizados de los recursos informáticos se dan por nuevas características tecnológica. En Italimentos el departamento de sistemas y desarrollo del nuevo sistema de la empresa,

conocen los significados de los activos informáticos, y el 40% de los empleados de Italimentos desconoce de la dicha frase.

5.2 Funciones y obligaciones del personal

Las funciones y obligaciones de cada una de las personas con acceso a datos de carácter personal y privado, así como a los sistemas de información estarán claramente definidas y documentadas de acuerdo a lo establecido en un documento físico. El responsable de un fichero deberá adoptar medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de las funciones así como las consecuencias que pudiera ocurrir en caso de incumplimiento.

Debe existir una correcta concienciación y formación de los usuarios que tengan acceso a los datos personales o privados, haciéndolos conocedores de la importancia y seriedad de la normativa y formándolos sobre funciones, obligaciones y normas que se debe cumplir.

El personal se clasifica en dos categorías:

1.-Administradores del sistema: Son los encargados de administrar y mantener el entorno operativo de los ficheros. Tiene como función administrar el acceso a datos por parte de los usuarios.

2.- Usuarios del fichero: Se relaciona al personal que utiliza el sistema informáticos de acceso al fichero.

Además debe existir un responsable de seguridad del fichero cuyas funciones serán las de coordinar y controlar las medidas definidas en un documento, sirviendo.

5.2.1 Funciones y obligaciones del personal en Italimentos

En la empresa de Italimentos existe un reglamento que es general para todo el personal, en la que se incluyen responsabilidades para cada empleado mediante varios artículos que definen acciones que se deben realizar en el interior de la empresa. En este documento, que se da a cada empleado, no están descritas las funciones que debe

realizar en su departamento o puesto de trabajo, sino que existe un jefe de área o departamento que le explica cuales son los trabajos que se desea realizar y estos se deben cumplir. *La figura 5.2.1.1 muestra el reglamento interno de la empresa*

Figura 5.2.1.1. Reglamento interno de Italimentos

Este reglamento interno contiene varios artículos que deben ser cumplidos por los empleados, así mismo existen obligaciones y restricciones que se deben respetar.

5.2.1.1 Resultado de los hechos realizados en Italimentos

En Italimentos, con una encuesta realizada a veinte empleados, se llego a la conclusión de que el 62% de los usuarios tienen internet, de las cuales el 50% tienen acceso limitado a ciertas páginas web mediante un proxy con la finalidad que el empleado pueda cumplir las obligaciones de trabajo designado a realizar. Si se posee una laptop se puede ingresar a la red WIFI de la empresa mediante una contraseña que posee como caracteres letras, números y signos especiales, con la cual se tiene libre acceso a cualquier página web. El departamento de sistemas se encarga de configurar estas seguridades para el ingreso y restricciones de de páginas web para ciertos usuarios de Italimentos.

El 100% de los empleados tienen bien definidas sus funciones y obligaciones, aunque no poseen documentos que especifiquen las actividades que se deben realizar para cada empleado, pero poseen un reglamento interno que detalla a nivel general las funciones y obligaciones de todos los empleados.

5.3 Accesos de personal que tratan datos personales´

"Las empresas manejan un gran número de datos personales, necesarios para cumplir sus funciones. "Estos datos personales deben estar debidamente protegidos de acuerdo con las exigencias dadas por una política para protección de datos de carácter personal. Por ello, el acceso a los ficheros informáticos que contienen datos personales está limitado al personal autorizado según los casos y exige una contraseña.

Puede existir algún fichero con información a la que cualquier usuario pueda acceder, como un directorio de personas donde figuren sus nombres, apellidos, puesto de trabajo, teléfono e información de carácter público.[48]" La designación de una persona o departamento que administre datos personales, dependerá en gran medida del tamaño de la empresa u organización, así como de la cantidad de información de datos de carácter personal que trata y recibe dentro de la propia organización.

5.3.1 Accesos de personal que tratan datos personales en Italimentos

5.3.1.1 Compartición de recursos

En Italimentos los usuarios que comparten la computadora por turnos o trabajo de medio tiempo, usan la misma cuenta para ingresar a la sesión por lo que comparten toda la información que se encuentre en la computadora y pueden modificar, borrar o crear archivos dentro de la misma. Como la información se comparte por carpetas compartidas, los usuarios graban información en varias carpetas a las que pueden ingresar otros usuarios de otros departamentos. *La figura 5.3.1.1.1 muestra las carpetas compartidas en la red de Italimentos vista desde el usuario tesis en la computadora de vendedores*

48 http://www.coie.unican.es/includes/manualNormas.pdf

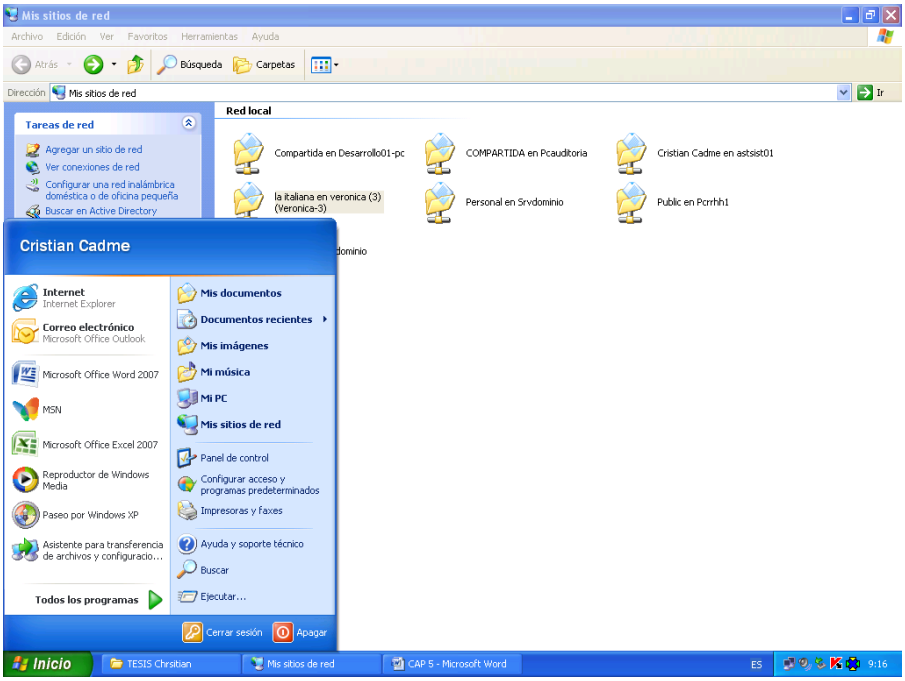


Figura 5.3.1.1.1. Carpetas compartidas de Italimentos

El departamento de sistemas tiene acceso a toda la información personal, puesto que ahí se encarga todo la administración del sistema. En el departamento de recursos humanos se maneja la información del personal de Italimentos tales como sueldos, datos personales, etc. Cierta información tales como cuentas del SRI, fotos, documentos de otros departamentos se pueden observar en las carpetas compartidas puesto que no existe un control en los departamentos para guardar de manera segura la información pública y privada.

Cuando el personal que comparte una computadora, se crea una contraseña para todos los usuarios, ya que no pueden estar pidiendo a una persona en especial que les dé ingresando cada vez que una sesión este cerrada.

5.3.1.2 Carpetas compartidas en Italimentos

Existen datos e información que se guarda en carpetas compartidas por parte de los usuarios pero no existe un debido control para almacenar la información en una carpeta a la que pueda acceder solo algún tipo de usuario. Los usuarios guardan la información en la carpeta compartida pero no tienen conocimiento de cuales otros usuarios pueden

ver, copiar, modificar o borrar la información. *La figura 5.3.1.2.1 muestra una carpeta compartida con información de documentos de SRI.*

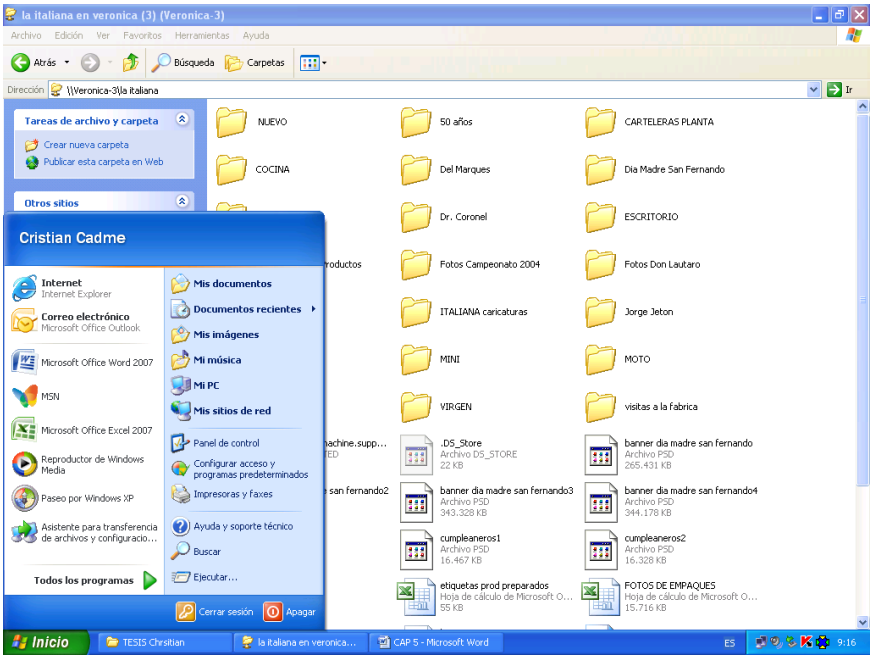


Figura 5.3.1.2.1. Documentos con acceso a usuarios

Existe también carpetas públicas a las que cualquier usuario puede ingresar, modificar o eliminar archivos. Una de estas carpetas es usada por el departamento de sistemas para mantenimientos ya que, desde la computadora del usuario, pueden ingresar para copiar e instalar aplicaciones, crear respaldos o respaldar información en las computadoras.

El acceso a varias carpetas compartidas se le impide el acceso a ciertos usuarios o ciertas veces pide nombre de usuario y contraseña. Ciertos archivos, con el fin de dar más de seguridad, se las guardan dentro de carpetas ocultas pero al configurar la computadora de un usuario para poder ver carpetas ocultas, la información se puede ver.

5.3.1.3 Mantenimiento de confidencialidad de Información en Italimentos

En Italimentos no ha existido un mantenimiento de confidencialidad de la información entre departamentos, ya que no existe un control o una capacitación para los usuarios sobre seguridad e importancia de la información para que así guarden su información en carpetas que solo puedan compartir con usuarios específicos.

En varias carpetas existen fotos antiguas sobre empleados, directivos y altos mandos de la empresa, así como declaraciones del SRI, documentos de vendedores, música, archivos de Excel y Word, etc. En la empresa cada usuario es responsable de la información que guarde y de la seguridad que le dé a la misma, puesto que ellos no conocen sobre quien tiene acceso a la información que almacenan.

5.3.1.4 Resultado de los hechos realizados en Italimentos.

En una encuesta realizada a veinte personas se llego a la conclusión que el 50% de los usuarios no cierra sus sesiones cuando van a estar ausentes en el puesto de trabajo, provocando una seguridad baja a nivel de usuarios y seguridad de la información que ellos manejan, pero el 95% guarda la información antes de su ausencia. Al momento de terminar las labores diarias el 50% de los usuarios deja prendida su computador provocando gastos de electricidad, posibles mantenimientos correctivos y de seguridad de la información que se maneja en el puesto de trabajo.

Entre los usuarios existe cerca del 50% que presta su contraseña o conoce la de otro usuario, provocando que se pueda ingresar a las cuentas de usuario y posible robo, modificación o eliminación de información. El 35% de ciertos usuarios utiliza la misma contraseña de su cuenta de usuario y para el ingreso a otras sesiones de correo electrónica personales con otros dominios, ya que las claves de email de Italimentos son dadas por el departamento de sistemas, siendo que el cerca del 40% utiliza como contraseñas caracteres como nombres de familiares, mascotas, etc. En lo que es servidores las contraseñas tienen como caracteres letras, números, símbolos especiales, mayúsculos y minúsculos. En la empresa el 10% de empleados comparte su computador con otros usuarios, para lo cual se debe compartir la contraseña de ingreso a la computadora, pero existen más personas que conocen otras claves, que los usuarios que comparten la PC.

Al momento de ausencia, por cualquier motivo en un puesto de trabajo, el 45% de las faltas es reemplazado por personal interno o el 5% es reemplazado por personal fuera de la empresa, siendo así que exista divulgación de contraseñas a otras personas ya que no se crea otras cuentas de usuario temporales para dichos usuarios nuevos. Para el

departamento de sistemas, por cuestiones de mantenimiento necesitan conocer las claves de ingreso a las cuentas de usuario, pero a veces no se da el caso por cuestiones de seguridad de información del usuario.

Para almacenar la información en distintas carpetas o carpetas compartidas en una red, el 50% de los usuarios guarda la información en carpetas compartidas, pero no saben para quien es visible dicha información que se guarda. El departamento de sistemas tiene acceso a cualquier tipo de información puesto que son los administradores del sistema de Italimentos. El 60% de los empleados han intentado acceder a un archivo pero se le a denegado el acceso, lo que limita acciones de lectura o escritura, pero en la red de Italimentos existe información que es pública o privada y se puede realizar cualquier tipo de acción sobre ellas; puesto que no se ha realizado un mantenimiento de privacidad de la información en la red. *La figura 5.3.1.4.1 muestra información compartida en la red de Italimentos.*

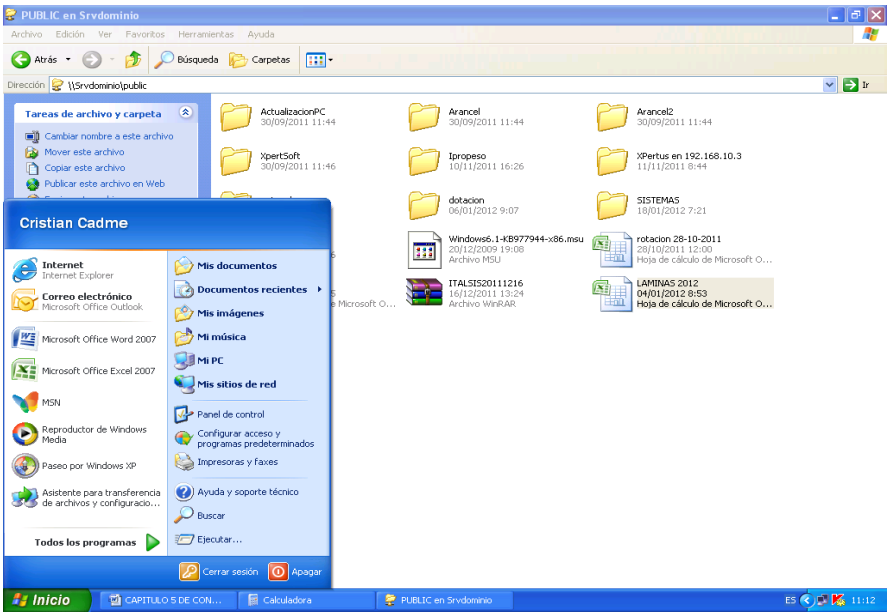


Figura 5.3.1.4.1. Información compartida en la red de Italimentos

De estos almacenamientos de información en carpetas compartidas, el 35% está confiado que la información que ellos almacenan no es visible para otros usuarios en la red de Italimentos y el 75% de estos usuarios piensan que la información que ellos manejan se encuentra segura en sus computadoras y que nadie puede acceder a sus datos.

5.4 Accesos de personal a soportes de datos e información

Debe existir una norma que regule las medidas de seguridad apropiadas para el acceso a soportes de datos e información, sea física o digital. Debe haber un control para acceder a soportes, sea solamente personal autorizado y otra persona que acompañe a realizar acciones con los soportes. Los ficheros de los soportes deben estar ubicados en lugares donde solo el personal autorizado tenga acceso, en la que el acceso a la información de terceros no autorizados requiera previa autorización del responsable interno en la empresa.

Los soportes que se ubiquen en ficheros deben quedar cerrados con llave, así mismo el mobiliario en el que se archiven soportes y documentos que contengan datos de carácter personal debe quedar bajo supervisión continua del responsable del tratamiento de esta información evitando o minimizando que exista alguna acción desfavorable para la empresa. Los listados, soportes, copias de seguridad a ser desechadas, deben ser destruidas totalmente puesto que con conocimiento técnico informático, la información puede ser recuperada y ser utilizada con propósitos de venta de información, fraude, etc.

5.4.1 Accesos a de personal a soportes de datos e información en Italimentos

Existe una área en la que se encuentra el departamento de sistemas y el departamento de cartera, haciendo vulnerable el acceso a copias de seguridad e información almacenada en computadoras vecinas, puesto que existen momentos en las que el departamento de sistemas a veces pasa vacio y regularmente con dispositivos como memorias USB, dispositivos móviles, CD’s o DVD’s, etc. En pocas ocasiones el departamento de sistemas y cartera permanece vacio, haciendo mayormente vulnerable el acceso a estos dispositivos o información dentro de alguna computadora, ya que se dejan abiertas sesiones en varias de estas computadoras. *La figura 5.4.1.1 muestra al departamento de sistemas junto con el departamento de cartera.*

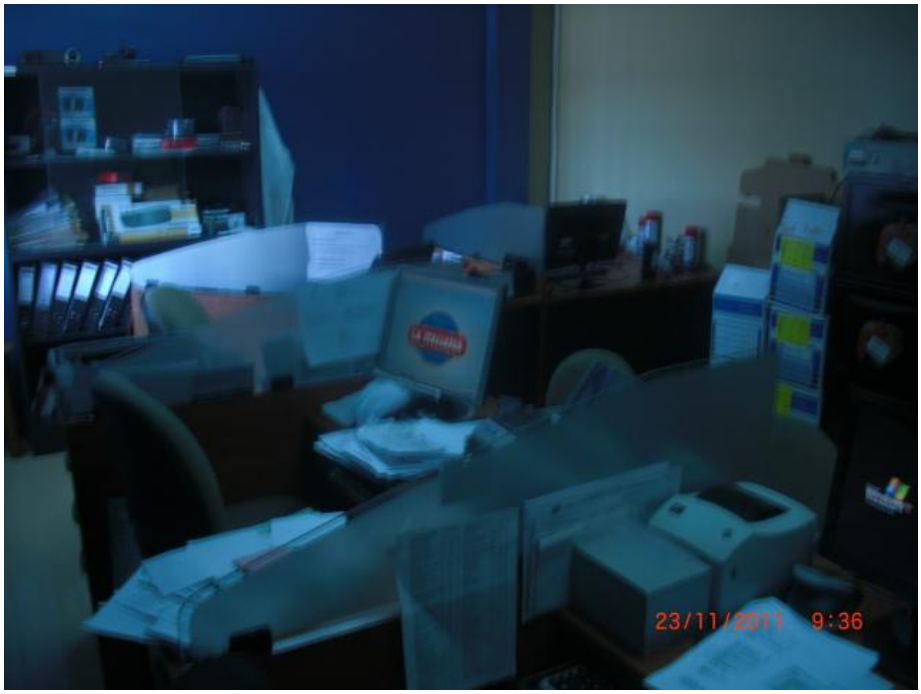


Figura 5.4.1.1. Departamento de sistemas y cartera

5.4.1.1 Guardado de información en Italimentos

En Italimentos ciertas computadoras permanecen con los puertos USB bloqueados para brindar seguridad, pero no existe un control regular para verificar que los puertos continúen bloqueados. Para deshabilitar puertos USB se realiza bloqueos, de los mismos, a nivel de software para poder solo conectar dispositivos como impresoras, ratones, etc; pero en ciertas computadoras no se podrá conectar dispositivos de almacenamiento.

Existe personal que pide al departamento de sistemas se le grabe en una unidad de almacenamiento cierta información para poder continuar con sus labores diarias, pero esta información se la llevan fuera de la empresa provocando una vulnerabilidad de seguridad y esta información se puede ser víctima de robo o pérdida, ya que al momento de una pérdida del dispositivo de almacenamiento esta información queda pública para terceras personas.

Así mismo en las palm de los vendedores, la información de los clientes se tiene que descargar diariamente puesto que se realizan actualizaciones diarias en el servidor. Esta

descarga de información es obligatoria ya que el software de las palm sincroniza la palm con el servidor, esta comunicación palm-servidor se la realiza por medio de una red GPRS[49] con proveedor de servicios la empresa de telefonía móvil Claro.

5.4.1.2 Seguridad de soportes de información

En Italimentos existen cámaras en varias áreas de la empresa y guardia de seguridad en la puerta de ingreso a Italimentos, pero en el interior del departamento de sistemas y cartera no existe una debida seguridad como cámaras de vigilancia o una persona encargada de la seguridad en el departamento de sistemas ni en el cuarto de servidores. *La figura 5.4.1.2.1 muestra el exterior del cuarto de servidores sin ninguna seguridad.*

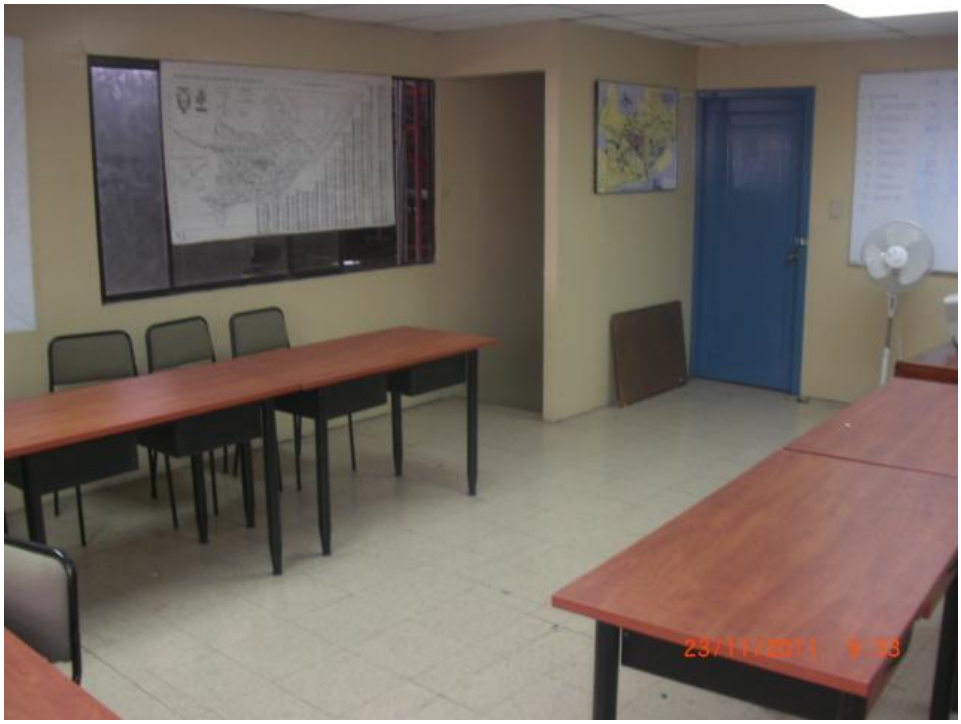


Figura 5.4.1.2.1. Exterior del cuarto de servidores

El acceso a los soportes de datos es limitado, ya que solo el personal de sistemas tiene acceso pero es vulnerable ya que no se tienen las debidas precauciones.

[49] GPRS: General Packet Radio Service

5.4.1.3 Resultado de los hechos realizados en Italimentos

En la encuesta realizada a veinte empleados de Italimentos, se llego a la conclusión que el 10% lleva información de la empresa hacia el exterior dispositivos de almacenamiento, dando un problema de seguridad crítico dependiendo de la información almacenada.

El 90% de los usuarios no utiliza en la empresa medios de almacenamiento USB para pasar información de un ordenador a otro; pero el departamento de sistemas usa estos dispositivos por cuestiones de mantenimiento.

Las USB de las computadoras están bloqueadas en algunas máquinas, permitiendo así dar una mejor seguridad de la información, pero no existe un mantenimiento para verificar que se tenga bloqueada las USB de las computadoras.

Cuando ha existido pérdida de archivos, el 50% de los usuarios ha logrado rescatar total o parcialmente sus archivos, con esto se llega a la conclusión que no existe respaldo para todos los usuarios sino para los usuarios más críticos que manejan información más crítica. Esta pérdida de información puede ser dada por apagones, accidentes o mala intención, de la cual el 45% de los usuarios alguna vez ha perdido algún archivo.

El 10% en las computadoras de los usuarios, se puede comprobar que existe información personal como fotos, videos, música, etc. para ello existe o existió la inserción de algún dispositivo para poder descargar los archivos en la PC.

En la red de Italimentos existe información personal y privada de la empresa como fotos que datan del año 2004. *La figura 5.4.1.3.1 muestra una carpeta compartida con información personal*

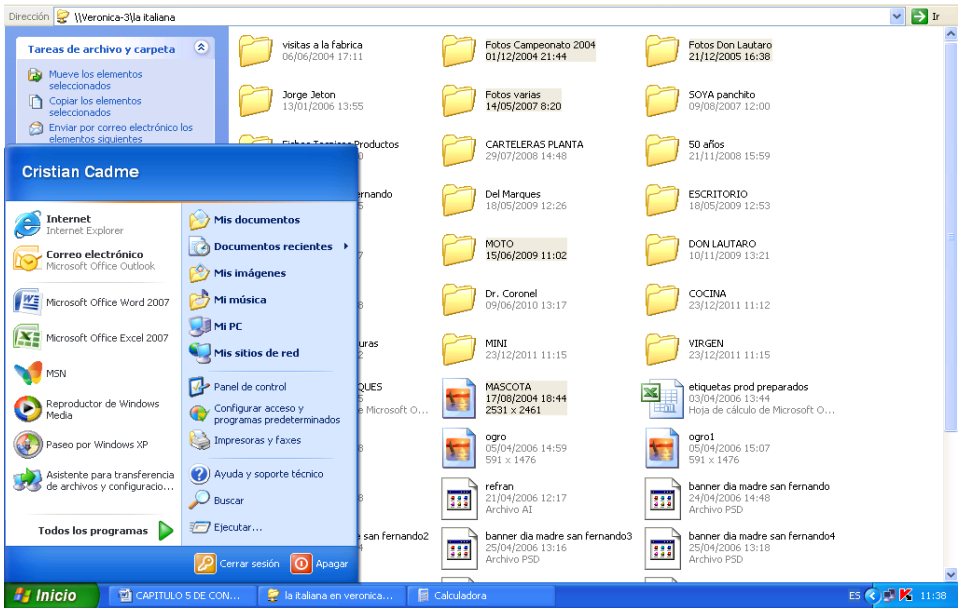


Figura 5.4.1.3.1. Información personal de fotos

De la muestra, de veinte personas, obtenida se conoce que el 20% de los usuarios necesita hacer uso de un dispositivo USB, para ello se habilitan los puertos USB de la computadora o piden al departamento de sistemas que se les dé guardando la información desde la computadora del jefe de sistemas. Para la instalación de aplicaciones el 35% ha instalado programas para mejorar el manejo de la información, esto se pudo haber realizado por la inserción de un dispositivo o mediante la red en la carpeta pública donde se encuentra aplicaciones que el departamento de sistemas necesita para mantenimientos.

5.5 Confidencialidad con todo el personal

Todo el personal de la empresa que intervenga en alguna fase de tratamiento de datos personales o que de cualquier modo tenga acceso a ellos, está obligado al secreto profesional respecto de dichos datos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones en la empresa. Este deber es de suma importancia en relación con los datos especialmente protegidos como salud, sueldo, afiliación, etc.

En este sentido, los datos personales solo deberán ser gestionados para los fines propios de la empresa y de acuerdo con los sistemas y `procedimientos en la misma. Como parte

de la confidencialidad del personal, esta la confidencialidad de la información para mantener el secreto profesional respecto a la información confidencial con la que se trata y así poder llevar un tratamiento adecuado de la información evitando que se pueda producir modificación, alteración, destrucción o desfase de los datos almacenados, responsabilizándose de cualquier actuación contraria a una norma dada por la empresa.

Así se puede reducir el uso de información confidencial a lo estrictamente necesario, estableciendo medios adecuados para evitar el acceso a los mismos por personas no autorizadas, ya que pueden destruir información confidencial o guardar información en soportes físicos.

5.5.1 Confidencialidad con todo el personal en Italimentos

Cada departamento posee y trata distinta información, siendo la más critica la información privada y personal sobre cada persona empleada dentro de la empresa. Existen medios por la cual se puede comunicar cierta información siendo las más usadas las carpetas compartidas en la red de Italimentos y por medio de correos electrónicos mediante la aplicación de Microsoft Office Outlook que están limitados a cargar archivos hasta de 6Mb de peso.

5.5.1.1 Información compartida en Italimentos

En Italimentos existe carpetas compartidas y en las que se puede acceder a información, actual o antigua, de algunos usuarios con carpetas compartidas siendo esta una debilidad puesto que esta información puede ser tratada para varios fines dañinos para la empresa. *La figura 5.5.1.1.1 muestra información antigua de la empresa vista desde un usuario final llamada tesis*

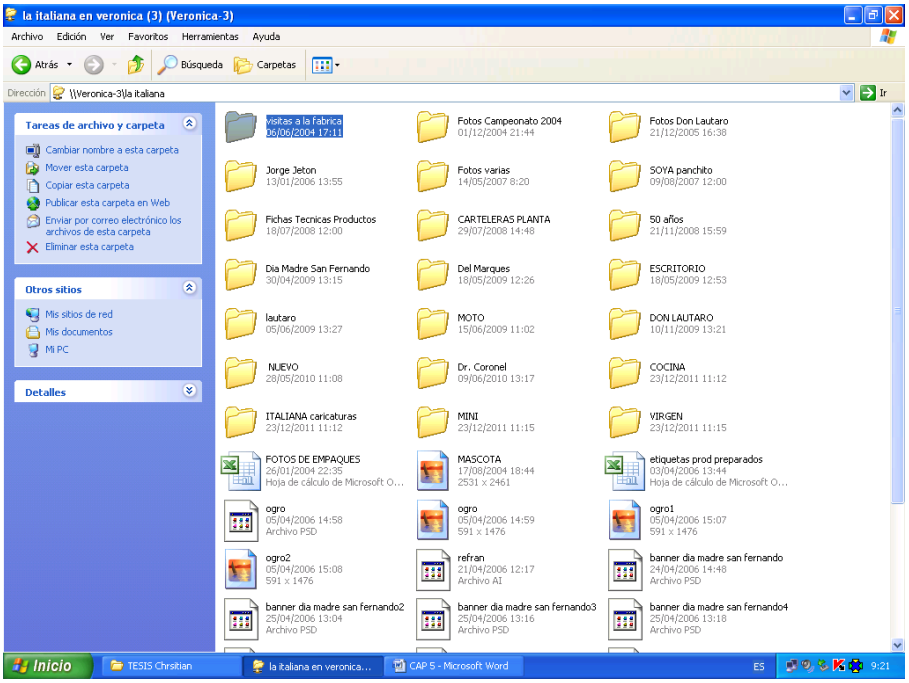


Figura 5.5.1.1.1 Información antigua de la empresa vista desde un usuario final llamada tesis

Esta información se puede observar al entrar a inicio- mis sitios de red en una computadora que está conectada a la red, y la información se puede copiar, alterar o borrar.

La figura 5.5.1.1.1 muestra información pública con documentos privados de la empresa de Italimentos

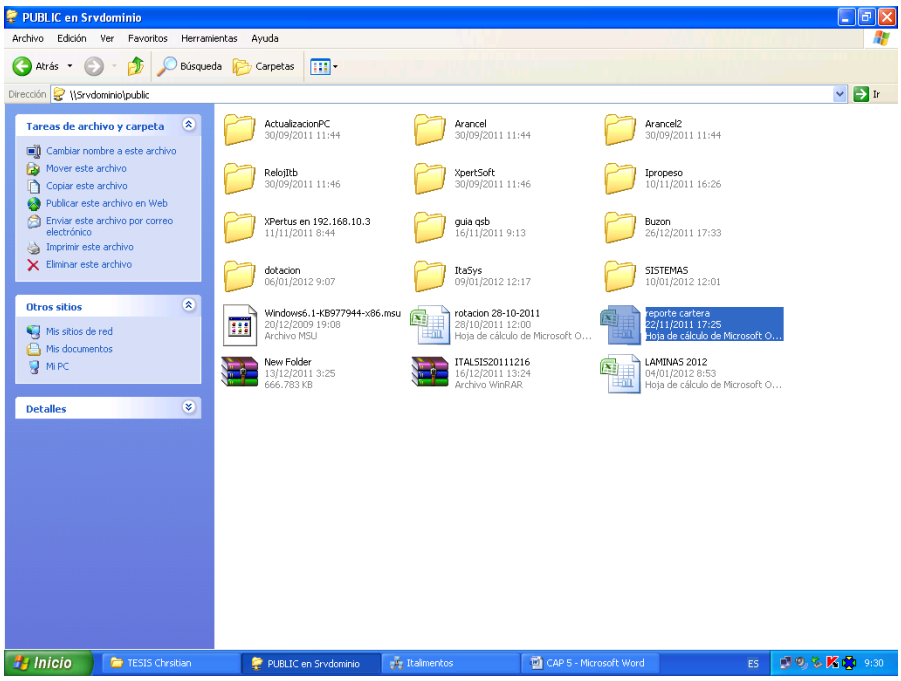


Figura 5.5.1.1.1. Información pública y privada

5.5.1.2 Mantenimiento de confidencialidad de información en carpetas compartidas

En Italimentos no se ha realizado un mantenimiento de confidencialidad de datos en la red de la empresa, puesto que los empleados guardan la información en sus carpetas compartidas, pero no conocen cuales otros usuarios podrán observar la información que se graba en cada una de ellas.

Desde la computadora de vendedores, se a ingresado a la cuenta de usuario tesis y se ha logrado observar que existe otros equipos a los que se puede acceder haciendo click en Inicio-Mis sitios de red- Toda la red-Red de Microsoft Windows-Italimentos. *La figura 5.5.1.2.1 muestra las computadoras conectadas dentro de la red de Windows de la empresa*

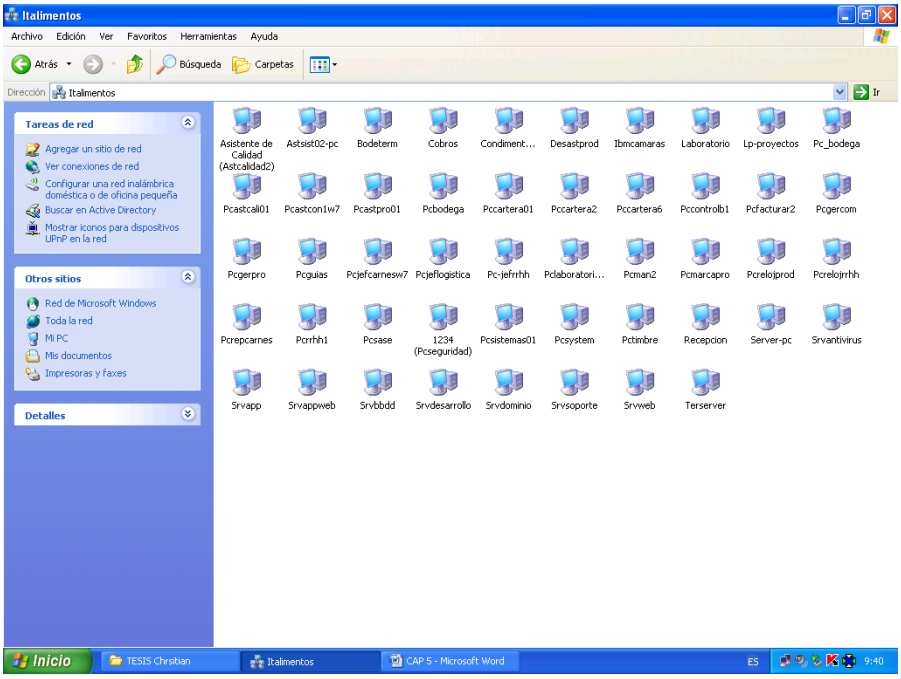


Figura 5.5.1.2.1. Computadoras conectadas en la red de Windows

La figura 5.5.1.2.2 muestra la computadora de Pcastcon1w7 ubicada en la siguiente dirección \\Pcastcon1w7\Respaldos

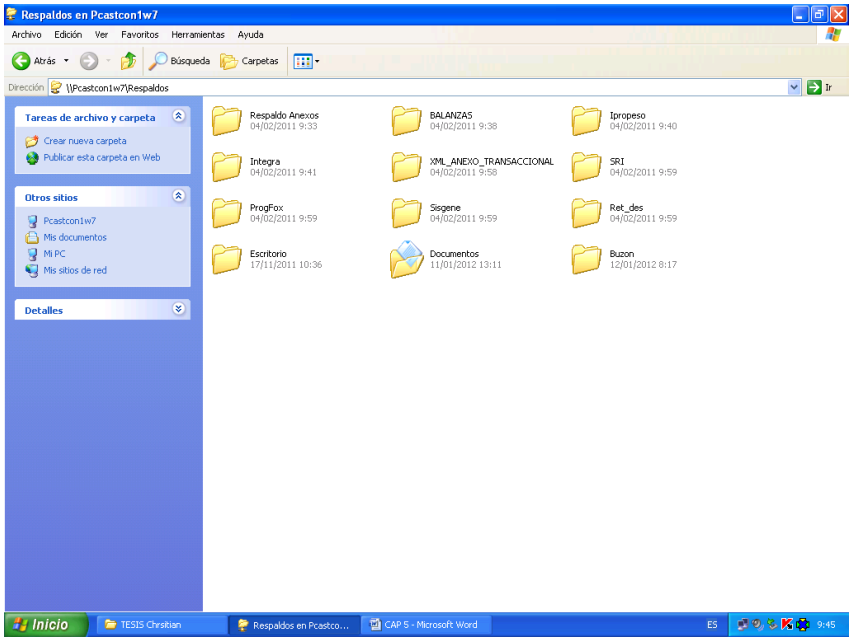


Figura 5.5.1.2.2. Información de Pcastcon1w7

Así mismo se tiene acceso a varios equipos que comparten carpetas compartidas con otros usuarios, esto lo realiza cada usuario responsable de su computadora ya que no posee un lugar seguro de almacenaje de información.

5.5.1.3 Encuesta sobre auditoría de seguridad relacionada con el personal

En la empresa de Italimentos se realizó una encuesta a con una muestra de veinte personas empleadas que tienen en su responsabilidad su propia computadora, para ellos se realizaron las siguientes sesenta y cuatro preguntas relacionadas con la seguridad relacionada con el personal. Para conocer más detalles sobre las actividades realizadas por los usuarios, se realizó un cuestionario individual para veinte empleados de la empresa. *Véase Anexo D.*

5.5.1.4 Resultado de hechos realizado en Italimentos

En la encuesta realizada a veinte empleados de Italimentos, se llego a la conclusión que el 50% de los usuarios clasifica la información, esta información se guarda en diferentes carpetas sean locales o compartidas en una red, pero desconocen si sus archivos están visibles para ellos mismos o para otros usuarios específicos En la red de Windows se puede ingresar a las computadoras de otros usuarios, algunas con acceso libre, otras con accesos denegados y otras mediante un registro de autenticidad de usuario y contraseña, para ello se hace vulnerable la información ya que el 32% de los usuarios comparte su contraseña con otros usuarios.

Cerca del 40% de los usuarios desconoce del término encriptación se archivos, lo que concluye que los usuarios no conocen como dar mayores seguridades a sus archivos digitales. Este término de encriptación de archivos lo tienen bien definido en el departamento de sistemas y el departamento de desarrollo del nuevo sistema de Italimentos.

Existe el 30% que utiliza distintos medios de envió de archivos por medio de cuentas de correo electrónico como Hotmail o Gmail, lo que se llega a la conclusión que poseen internet con libre acceso a diferentes páginas. Para el envío de correos electrónicos existe la aplicación Microsoft Office Outlook que es dada por el departamento de sistemas para no usar medios distintos por cuestiones de seguridad de la información.

En Italimentos no existe divulgación de información personal o privada en ninguno de los departamentos, concluyendo que no existe la curiosidad por entrar a otras computadoras con fines personales o comerciales. El departamento de sistemas tiene acceso a cualquier tipo de información puesto que son los administradores de toda el área de sistemas de Italimentos, pero existe ética ante la información que se pueda ver.

5.6 Comunicación de debilidades en materia de seguridad

Los usuarios deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad con relación a los sistemas y servicios. Se debe también comunicar estos asuntos a la directiva o directamente a su proveedor de servicios, tan pronto como sea posible. Se debe informar a los usuarios que bajo ninguna circunstancia se intente probar una supuesta debilidad ya que podrían ocasionar una catástrofe informática.

Los incidentes de seguridad deben ser comunicados a través de canales gerenciales apropiados tan pronto como sean posibles, estableciendo un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Estos procedimientos deben contemplar que cuando surja un incidente o violación a la seguridad, entonces el responsable de seguridad informática debe ser informado lo más pronto posible y con ello se tomara medidas y recursos necesarios para la investigación y resolución del incidente. Asimismo, se mantendrá al comité de seguridad al tanto de la ocurrencia de incidentes de seguridad.

El objetivo de comunicar debilidades es minimizar el daño producido por incidentes y anomalías en materia de seguridad, monitoreando dichos incidentes y aprender de los mismos. Se debe concientizar a todos los empleados y contratistas acerca de procedimientos de comunicación de los diferentes tipos de incidentes que podrían provocar un impacto en la seguridad de los activos de la organización. Para lograr abordar debidamente los incidentes podría ser necesario recolectar evidencia tan pronto sea posible una vez ocurrido el hecho.

5.6.1 Comunicación de debilidades en materia de seguridad en Italimentos

En Italimentos la comunicación del usuario de debilidades en su computadora hacia el departamento de sistemas se las puede realizar de tres maneras:

- Personal
- Vía telefónica
- Remota

Estas debilidades que se dan pueden ser de hardware o software y dependiendo del tipo de comunicación que se dé, entonces se toman varias medidas con los usuarios finales. Cuando existe algún problema, estos no se registran en un documento de gestión de incidencias, sino que la solución a las debilidades se las realiza en el momento que exista un problema informático.

5.6.1.1 Medio de comunicación personal de debilidades informáticas en Italimentos

Cuando existe un problema, en una computadora dentro de la empresa, entonces el usuario se dirige hacia el departamento de sistemas con los síntomas de su computadora o pidiendo que el jefe de sistemas o auxiliar de soporte de sistemas se dirija al puesto de trabajo para realizar los arreglos correspondientes, ya sean de software o hardware.

Si el problema se da con una palm de los vendedores, entonces el usuario de la palm se dirige al departamento de sistemas para comunicarle los errores que está provocando el dispositivo y en el mismo lugar se empieza a dar solución a dichos problemas hasta encontrar una solución.

5.6.1.2 Medio de comunicación vía telefónica de debilidades informáticas en Italimentos

Al existir un error en una computadora, fuera o dentro de la empresa, el usuario se comunica con el departamento de sistemas vía telefónica para comunicar los problemas que tiene. Cuando el problema es de software se intenta solucionar el error preguntándole e indicando pasos a seguir hasta encontrar una solución; si no se haya una solución entonces el jefe de sistemas o auxiliar de soporte de sistemas se dirige personalmente a solucionar el error. La mayor parte cuando se tiene que ir a solucionar,

de manera personal por alguien del departamento de sistemas, son problemas de hardware

Cuando se trata de problemas en una unidad palm, entonces el usuario llama al departamento de sistemas vía telefónica o por medio de un dispositivo móvil y le comenta el error que tiene, entonces por medio de preguntas y siguiendo pasos, sobre la palm, se intenta llegar a una solución. Si no se encuentra una solución entonces puede que existan problemas de hardware, sobre la red de datos GPRS o sobre el servidor.

5.6.1.3 Comunicación remota de debilidades informáticas sobre servidores de Italimentos

En el departamento de sistemas se tiene instalado en el sistema operativo, el visor de escritorios remotos y una aplicación llamada RadminView utilizados para poder acceder de manera remota a servidores o computadoras que se encuentran dentro o fuera de la empresa desde la computadora del jefe o auxiliar de soporte de sistemas. Cuando existe un problema en algún servidor o computadora se ingresa de manera remota al mismo, y se intenta arreglar remotamente; si no existe solución remotamente sea por problemas de red o hardware entonces un responsable en el departamento de sistemas se dirige al lugar donde está ubicado el servidor del problema.

Estos accesos remotos pueden realizarse a servidores y ciertas computadoras de escritorio pertenecientes a Italimentos, donde las computadoras más críticos y que más causen problemas tales como Marcación, Servidor de base de datos, servidor de cámaras, y otros usuarios críticos sean observadas como recursos importantes en la empresa.

5.6.1.4 Manuales de reparación

Al momento que existe un error de cualquier tipo no se tiene manuales de reparación que indiquen como resolver un problema en especial, sino que se lo realiza mediante la experiencia y conocimiento del jefe y auxiliar de soportes de sistemas. En la red existe compartida una carpeta que es usada por el departamento de sistemas para realizar los mantenimientos, ya que cuando se encuentran realizando un mantenimiento en un puesto de trabajo remoto al departamento de sistemas, se obtienen las herramientas

necesarias para realizar las debidas soluciones a la computadora en mantenimiento preventivo o correctivo. *La figura 5.6.1.4.1 muestra la carpeta de sistemas con aplicaciones útiles para usuarios finales y otros archivos más*

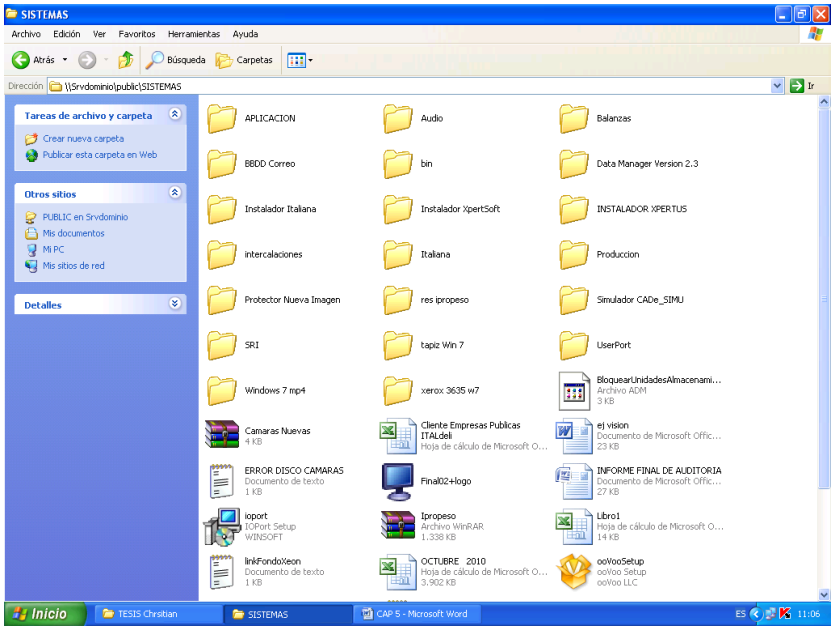


Figura 5.6.1.4.1. Aplicaciones para usuarios finales y otros documentos digitales

5.6.1.5 Gestión de Incidencias

Al momento que se ha comunicado al departamento de sistemas un problema informático, no se tiene un documento físico o digital que indique si el problema ya a pasado anteriormente o es un problema nuevo, así como las soluciones que se han dado a dichos problemas. El error más crítico que se puede dar en Italimentos es que colapse el servidor de base de datos ya que todos los usuarios se conectan con la información dentro de la misma. Durante todo el tiempo se ha dado problemas en servidores y computadoras pero no se tiene un documento con la gestión de incidencias de problemas informáticos

5.6.1.6 Resultado de hechos realizados en Italimentos

En la encuesta realizada a veinte empleados de Italimentos se concluyó que el 35% comunica debilidades de seguridad al departamento de sistemas, sean alertas de antivirus, firewall, etc. El departamento de desarrollo del nuevo sistema de Italimentos,

comunica debilidades de seguridad informática cuando el sistema colapsa y queda sin servicio. Al momento de salir advertencias de seguridad en la computadora de un usuario el 55% cierra dichas advertencias y continúan sus labores; pero cuando existe un error, hardware o software que no permite laborar normalmente, entonces el usuario se comunica con el departamento de sistemas para buscar la solución más óptima. *La figura 5.6.1.6.1 muestra una notificación de antivirus de des actualización.*

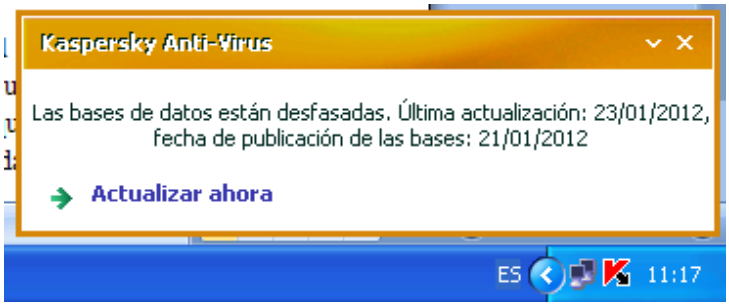


Figura 5.6.1.6.1. Notificación de antivirus

Cuando se provocan nuevas debilidades, el 30% de los usuarios recibe capacitación para mejorar el manejo de aplicaciones con el objetivo de evitar que vayan apareciendo nuevas debilidades informáticas.

CAPITULO 6

"Auditoría de la seguridad física y el entorno"

6.1 Acceso físico a copias de seguridad

La seguridad física es uno de los aspectos más importantes al momento de realizar un diseño de un sistema informático, hay que tener en cuenta algunos aspectos importantes como la detección de un atacante interno a la empresa que intenta acceder físicamente en áreas donde se encuentra datos e información importante, tales como copias de seguridad. Así, entonces la seguridad física a las copias de seguridad consiste en aplicar barreras físicas y procedimientos de control para la prevención ante amenazas a los recursos e información confidencial. En este tema los controles y mecanismos de seguridad dentro y alrededor del almacenamiento de copias de seguridad, deben tener implementadas seguridades para proteger hardware y medios de almacenamiento de datos.

La seguridad de los datos implica a la seguridad de la información, tanto la que esta almacenada como la que se transmite a otros equipos, para ello primero se debe proteger el hardware ya que con eso protegemos la información que se almacena o comunica a través y dentro de la misma. Hay que tener en cuenta que la seguridad de las copias de seguridad hay que protegerlas igual como al sistema propio de la empresa, en la que un error muy habitual es dejar los respaldos muy cerca al departamento de sistemas por comodidad cuando se necesita realizar las restauraciones de archivos o sistema.

Al momento de perder todas las copias de seguridad en los DVD's, en casos de incendio, robo, etc., no se tiene manera alguna de recuperar la información para volver a comenzar los servicios en el sistema. Para ello resulta recomendable guardar las copias de seguridad en una zona alejada de la sala de operaciones de sistemas. Los equipos o dispositivos que puedan tener información de nuestro sistema debería estar situado el lugar con acceso restringido para así prevenir que terceras personas recojan información y la pueda usar para otros fines ajenos a la empresa.

6.1.1 Acceso físico a copias de seguridad en Italimentos

En Italimentos las copias de seguridad de usuarios críticos se las realiza con la aplicación FBackup y se almacenan en los discos duros de los servidores con acceso restringido a los usuarios por carpeta. El área de sistemas está conformado por dos personas del departamento de sistemas y tres personas del departamento de cartera, lo que hace vulnerable al acceso físico a las copias de seguridad u otros recursos cuando no existe ninguna persona del departamento de sistemas. *La figura 6.1.1.1 muestra el departamento de sistemas junto con el departamento de cartera.*

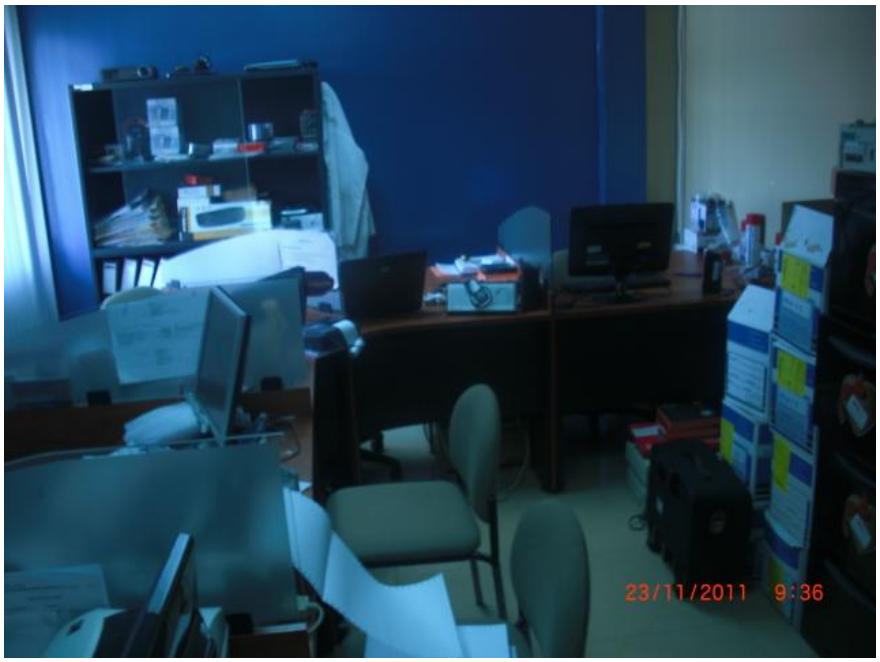


Figura 6.1.1.1. Departamento de sistemas y cartera

Las copias de seguridad de la base de datos se las guardan en el mismo servidor mediante la aplicación SQLServer y a esas copias solo tiene acceso del personal de sistemas y personas que deseen realizar consultas sobre algún tema en común. Todas estas copias de seguridad son grabadas en DVD's de manera incremental y guardadas en el departamento de sistemas y el mismo disco duro del servidor como un medio de seguridad

6.2 Almacenamiento de la información

6.2.1 Dispositivos de almacenamiento de la información

"Los dispositivos o unidades de almacenamiento son componentes que leen o escriben datos en medios o soportes de almacenamiento y juntos conforman el almacenamiento secundario de la computadora."[50] La información que se maneja en cualquier empresa se guarda en dispositivos tales como discos duros de las propias computadoras, servidores, storages, USB, CD, DVD, etc. Para los cuales se dividen en tres categorías:

6.2.1.1Almacenamiento óptico

El almacenamiento óptico es un método de almacenamiento de la información que consiste en la lectura y escritura a través de haces de luz que interpretan refracciones que son provocadas por su propia emisión. Estos soportes de almacenamiento pueden ser CD, HD DVD, etc.

6.2.1.2 Almacenamiento magnético

Los archivos que se utilizan a diario en el trabajo son secuencias de datos digitales en forma de unos y ceros. Estos datos se escriben y leen en una capa magnética muy delgada en el interior de discos duros, casetes, etc.; de manera que cuando medio de lectura pasa por una serie de bits, esta puede recrear imágenes, música, video, etc.

6.2.1.3 Almacenamiento electrónico

Esta tecnología también es conocida como memorias de estado sólido porque no tienen partes móviles sino que son circuitos cerrados que no necesitan desarmarse para leer grabar o leer información. Estos dispositivos pueden ser encontrados desde los pen drives hasta tarjetas de memoria de cámaras digitales.

Estos dispositivos almacenan cargas eléctricas, las cuales definen unos y ceros y pueden mantener almacenado un dato de manera temporal o a largo plazo dependiendo de la tecnología que se use. La ventaja es que no hay partes en movimiento así que no genera calor ni fricción, además de la alta velocidad, inmunidad a los campos magnéticos, temperatura y humedad, etc.

50 http://michelleinformate.blogspot.com/?zx=4e0987608e158b18

6.2.2 Almacenamiento de la información en Italimentos

La información de los usuarios críticos se guarda en unidades de red en una o varios dominios, haciendo vulnerable el acceso a la misma, pero estos accesos están limitados ya que existen ciertas carpetas compartidas en la red a la cual no se puede tener acceso, ya sea por privilegios, o no encuentre encendido un computador en especial El acceso al departamento de sistemas es limitado, ya que solo empleados de la empresa pueden acceder por cuestiones laborales. *La figura 6.2.2.1 muestra la vitrina en la cual se almacenan las copias de seguridad.*

Figura 6.2.2.1. Vitrina de almacenamiento de copias de seguridad

La información que se almacena en el cuarto de servidores es restringida y solo puede tener acceso físico el jefe del departamento de sistemas, el auxiliar de soporte de sistemas y ciertas personas del departamento de desarrollo del nuevo sistema de Italimentos y el departamento de mantenimiento. Estos accesos de otras personas se hacen por cuestiones de mantenimiento y dar soluciones a problemas nuevos y complicados en los servidores; hasta el momento no se han reportado problemas de robos de copias de seguridad o información privada almacenada en algún servidor de la

empresa. *La figura 6.2.2.2 muestra el rack de servidores, en los cuales se almacena la información de todo Italimentos*

Figura 6.2.2.2. Rack de servidores de Italimentos

6.3 Accesos de personal a cuarto de servidores

6.3.1 Acceso físico a cuarto de servidores

Los accesos de personal no autorizado al cuarto de servidores hace conocer la necesidad de garantizar la seguridad global de la red y los sistemas conectados a los servidores, en la que el nivel de seguridad física depende mucho del entorno en el que se encuentren puntos estratégicos para proteger el acceso no autorizado al cuarto de servidores. Mientras que parte de los equipos de la empresa estarán bien protegidos, otros tendrán accesos menos limitados; pero es importante extremar precauciones ya que lo más fácil para un atacante es ser discreto y atacar a cualquiera de estos equipos y luego lanzar un ataque a toda la red, sea realizando cualquier acción en los servidores para dejar sin servicio a toda una red.

Este cuarto de servidores debe tener características especiales en cuanto a seguridad y a otras áreas de la empresa. Se debe tener un acceso suficientemente seguro mediante

tarjetas de identificación o medios electrónicos para garantizar que a los servidores solo pueda entrar y realizar acciones solo el personal autorizado. Se debe contar un suministro de energía asegurado, para lo cual se toman medidas en la seguridad física del edificio, así mismo las conexiones a la red debe estar protegidas contra amenazas ambientales o accidentales para evitar catástrofes informáticas en toda la empresa.

6.3.1.1 Prevención

Existen métodos para poder prevenir accesos no autorizados al cuarto de servidores que van desde analizadores de retinas hasta videocámaras, así como la seguridad física de puertas blindadas. Mediante un método de acceso a los servidores se podrá tener un mejor control sobre la hora que ingresaron, salieron, las acciones que se realizaron, que personas entraron y los resultados se obtuvieron. Para prevenir hay normas elementales como cerrar la puerta con llave al salir, apagar la luz y constatar que todo esté en orden con las sesiones cerradas y monitores apagados, etc.

Se trata de buscar un sistema sencillo para implementar y que sea de gran eficacia y eficiencia en una empresa con el fin de administrar accesos a los servidores y mejorar la seguridad de la información que se encuentra dentro de la misma.

6.3.1.2 Detección

Cuando la prevención resulta difícil, entonces es mejor que un ataque sea detectado cuanto antes para evitar o minimizar sus efectos, pero para detectar problemas intervienen medios técnicos como cámaras de seguridad o alarmas ya que estos indican una vez que se está o quiere realizar un ataque hacia el cuarto de servidores. Se tiene que detectar la presencia de un sospechoso que no tiene autorización para así poder avisar a un administrador o responsable de alguna área para dar aviso a seguridad e inmediatamente intervenir si es necesario

6.3.2 Acceso de personal a cuarto de servidores

Al cuarto de servidores solo tienen acceso el personal de sistemas, pero cuando ocurre algún problema crítico en la base de datos entonces se incorpora el jefe del departamento

de desarrollo del nuevo sistema de la empresa para así dar una mejor y rápida solución a los problemas que se den en la base de datos u otro cualquier servidor.

Cuando se realizan mantenimientos o instalaciones eléctricas, cableado, etc.; el personal de mantenimiento de la empresa permanece, en algunas ocasiones, sin supervisión del departamento de sistemas en el cuarto de servidores, haciendo vulnerable a la información que se guarde en los servidores, pero no se ha dado ningún problema hasta ahora sobre el robo o daño de información. *La figura 6.3.2.1 muestra personal de mantenimiento de la empresa en el cuarto de servidores de Italimentos*

Figura 6.3.2.1. Personal de mantenimiento en cuarto de servidores

Cuando existen mantenimientos de limpieza, entonces alguna persona del departamento de sistemas se queda en el cuarto de servidores hasta que la limpieza concluya. En varios casos existe personal de otros departamentos que ingresa al departamento para realizar consultas sobre algún servidor, sea el caso de videos de seguridad, errores en alguna cuenta de usuario, instalaciones eléctricas y cableadas de red, etc. La figura 6.3.2.2 muestra el cableado sobre el techo del cuarto de servidores

Figura 6.3.3.2. Cableado sobre techo de cuarto de servidores

El exterior del cuarto de servidores no consta de las debidas seguridades, ya que existen varios lugares de acceso tales como una puerta ubicada en la sala de reunión de los vendedores, y ventanas que dan hacia el techo del segundo piso por el cual regularmente pasa personal de mantenimiento. *La figura 6.3.3.4 muestra el exterior del cuarto de servidores*

Figura 6.3.3.4. Exterior del cuarto de servidores

6.4 Estructura física del ambiente informático

6.4.1 Cuarto de servidores

Se debe tener en cuenta el entorno, localización y consideraciones para poner uno o más servidores, así como de los equipos de soporte como armarios y racks para contener las máquinas y dispositivos de red, esto incluye que debe existir una potencial seguridad puesto a la criticidad de los equipos con los que se trabaja. Para ello el cuarto de servidores debe estar aislado de accesos no autorizados y con un correcto ambiente físico para evitar que sucedan accidentes dentro del mismo. Al ubicar un servidor en un área con las debidas seguridades ambientales y se tenga bien identificados los riesgos, entonces se estará seguro que un supuesto intruso intente realizar acciones físicas en el cuarto de servidores. Para ello se debe tener en cuenta varias características

6.4.1.1 Local físico

Es importante que el personal de sistemas adapte los servidores al espacio disponible para poder acceder a ellos de manera segura, el local debe constar de seguridad e instalaciones eléctricas

6.4.1.2 Espacio y movilidad

Se considera características en el espacio como la altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos para mantenimientos o reparaciones, etc.

6.4.1.3 Iluminación

La iluminación debe ser apropiada para evitar reflejos en las pantallas del servidor, y para ello los servidores no deben estar expuestos directamente al sol para prevenir la corrosión de dispositivos internos.

6.4.1.4 Seguridad física del local

Se debe tener en consideración que puede existir catástrofes, para ello los materiales de construcción y recursos deben ser incombustibles para evitar amenazas de incendio. Se debe estudiar la protección contra inundaciones y otros peligros físicos que pueden afectar a la instalación .

6.4.1.5 Suministro eléctrico

En cualquier área se debe contar con los toma corrientes y puntos de red necesarios para cada equipo, sobre todo en áreas de soporte donde sean muy necesarios.

6.4.2 Departamento de sistemas

El departamento de sistemas debe estar ubicado en una zona acorde a las necesidades ya que no puede estar ubicado junto con otro departamento que distraiga sus actividades. Para ello se deben tomar en cuenta varios factores como son el tamaño de la empresa, en cuantas secciones se divide el área y las necesidades en cuanto a espacio, ruido, aire acondicionado, iluminación, etc. Para algunas de las necesidades generales en el departamento de sistemas se deben tomar en cuenta varias características como local físico, espacio y movilidad, iluminación, tratamiento acústico, seguridad física del local y suministro eléctrico.

6.4.2.1 Local físico

Es importante que el personal de sistemas se adapte, al espacio, accesibilidad, seguridad e instalaciones eléctricas; para así poder dar un correcto soporte, reparaciones y almacenamiento de repuestos para los mantenimientos.

6.4.2.2 Espacio y movilidad

Se considera características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos para mantenimientos o reparaciones, etc.

6.4.2.3 Iluminación

La iluminación debe ser la apropiada para evitar reflejos en las pantallas y para evitar que la luz caiga directamente sobre los equipos.

6.4.2.4 Tratamiento acústico

Los equipos ruidosos como impresoras, equipos de aire acondicionados o equipos sujetos a grandes vibraciones, deben estar ubicadas en zonas donde el ruido se encuentre amortiguado.

6.4.2.5 Seguridad física del local

Se debe tener en consideración que puede existir catástrofes, para ello los materiales de construcción y recursos deben ser incombustibles para evitar amenazas de incendio. Se debe estudiar la protección contra inundaciones y otros peligros físicos que pueden afectar a la instalación .

6.4.2.6 Suministro eléctrico

En cualquier área se debe contar con las toma corrientes y puntos de red necesarios para cada equipo, sobre todo en áreas de soporte donde sean muy necesarios.

6.4.3 Estructura física del ambiente informático en Italimentos

6.4.3.1 Estructura física del departamento de sistemas

El departamento de sistemas de Italimentos se encuentra compartiendo un área con el departamento de cartera, puesto que la empresa está limitada para extenderse físicamente. En esta área, ocupada por los dos departamentos, no existe un área para poder realizar mantenimientos a computadoras de otros usuarios, sino que un responsable tiene que ir al cuarto de servidores para realizar los respectivos mantenimientos a recursos informáticos de la empresa. *La figura 6.4.3.1.1 muestra el departamento de cartera y sistemas*

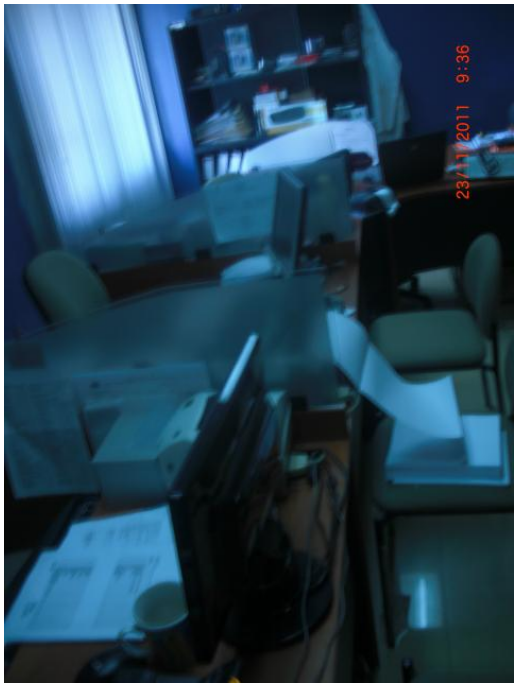


Figura 6.4.3.1.1. Departamento de sistemas y cartera

El departamento de sistemas necesita un área tranquila, sin ruidos que causan las impresoras del departamento de cartera y un espacio donde se puedan realizar las diferentes actividades de mantenimiento de computadoras, impresoras y otros recursos de la empresa.

6.4.3.2 Estructura física del cuarto de servidores

El cuarto de servidores se encuentra distribuido de mala manera, ocasionando así que se pierda espacio físico que puede ser utilizado por el mismo departamento de sistemas. El espacio del cuarto de servidores debe estar ubicado en un área limitada junto con los demás recursos como el aire acondicionado, rack de switches, rack de servidores y ups; Ya que el cuarto de servidores es muy amplio para realizar otras tareas.

En el cuarto existen varias aberturas que provocan cierto tipo de vulnerabilidad en la seguridad física de los servidores, ya que por esos medios puede existir mayor presencia de polvo, intrusión de roedores y otros animales que provocarían el daño de ciertos recursos y partes del ambiente informático. *La figura 6.4.3.2.1, 6.4.3.2.2 y 6.4.3.2.3 muestran varias aberturas en el cuarto de servidores*

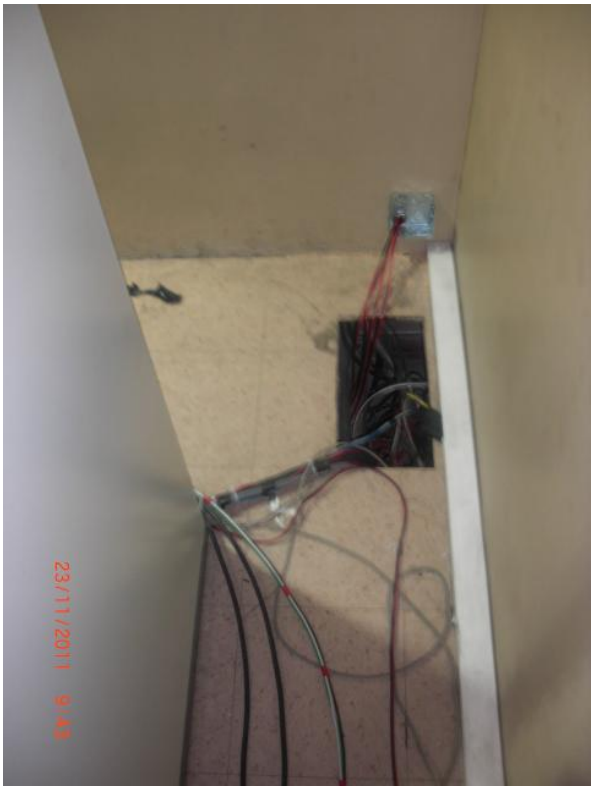


Figura 6.4.3.2.1. Abertura cerca del rack de switches

Figura 6.4.3.2.2. Abertura cerca de UPS

Figura 6.4.3.2.3. Abertura en el exterior del cuarto de servidores

6.5 Factores ambientales del entorno informático

Existen medidas que se deben tomar ante desastres y para ello se debe tener las seguridades correctas para prevenir o minimizar los costos en caso que ocurra algún accidente dentro de la estructura del edificio. Entre las principales amenazas ambientales se tiene por ejemplo desastres naturales, incendios accidentales, tormentas e inundaciones.

6.5.1 Peligros importantes

Aquí se puede analizar sobre los peligros más importantes que puede ocurrir en un centro de procesamiento de datos; con el objetivo de mantener una serie de acciones eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos:

6.5.1.1 Incendios

Los incendios pueden ser causados por el uso no adecuado de combustibles, instalaciones eléctricas defectuosas o el uso inadecuado de almacenamiento y traslado de sustancias peligrosas. Este tipo de amenazas son una de las más peligrosas contra la seguridad de una computadora, ya que puede destruir fácilmente archivos de información y programas. Algunos sistemas anti fuego causan casi el mismo daño que el propio fuego, ya que afectan a los elementos electrónicos pero existen métodos, como el dióxido de carbono, que es una alternativa del agua pero resulta peligroso para los propios empleados si quedan atrapados en el departamento de sistemas o cuarto de servidores.

6.5.1.2 Inundaciones

Se define una inundación cuando existe un exceso de agua en una superficie ya sea por terrenos planos o falta de drenaje natural o artificial. Una causa de inundación también puede ser provocada por la necesidad de apagar un incendio en un piso superior o por una cañería dañada o en mal estado que este cerca del departamento de sistemas o cuarto de servidores.

6.5.1.3 Condiciones climatológicas

Frecuentemente se recibe por anticipado avisos de tormentas, tempestades, tifones, etc. pero las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad con la que pueda ocurrir. La frecuencia y severidad con la que sucedan, deben ser tenidas en cuenta al momento de decidir la construcción de un edificio o un área nueva sobre un edificio ya realizado.

La comprobación de informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite tomar precauciones adicionales, tales como la retirada de objetos móviles, provisión de calor, iluminación de emergencia, etc.

En muy poca frecuencia los fenómenos sísmicos, como terremotos, son poco predecibles y suelen causar la destrucción de un edificio y hasta la pérdida de vidas humanas. El problema de este fenómeno es que en la actualidad están sucediendo muy a menudo y en

lugares donde antes no se daba y los daños a la información o recursos informáticos suele ser crítico.

6.5.1.4 Señales de radar

Cuando existen señales de radar, sobre el funcionamiento de una computadora ha sido estudiada durante años. Los resultados de las investigaciones revelan que señales muy fuertes de radar pueden interferir en el procesamiento electrónico de la información pero si la señal que alcanza es de cinco voltios por metro o mayor.

Estos problemas pueden inferir si la antena fuera visible desde una ventana del centro de procesamiento de datos, y si estuviera apuntando directamente hacia dicha ventana.

6.5.1.5 Instalaciones eléctricas

"Al trabajar con computadoras implica trabajar con electricidad, por lo tanto esta es una de las principales áreas a considerar en la seguridad física. A medida que los sistemas se vuelven más complejos, se hace más necesaria la presencia de un especialista para evaluar riesgos y aplicar soluciones que vayan de acuerdo con un estándar empresarial de seguridad.

6.5.1.5.1 Picos y ruidos electromagnéticos

Las subidas y caídas de tensión en la electricidad no son problemas que tiene que enfrentar los usuarios, sino que también está el tema del ruido que interfiere en el funcionamiento de componentes electrónicos.

6.5.1.5.2 Cableado

Los cables utilizados para construir van del cable telefónico normal, hasta el cable coaxial de fibra óptica, en la que algunos edificios ya se construyen con los cables instalados para evitar pérdidas de tiempo, y en futuro, minimizar cortes, rozaduras u otro daño accidental.

La mayor parte de las empresas, estos problemas entran dentro de la categoría de daños naturales, pero también se puede ver como un medio de ataque a la red si el objetivo es únicamente para parar servicios. Por medio del cable de red, intrusos con suficientes conocimientos pueden intentar acceder a los datos realizando:

- Desvíos en una conexión no autorizada en la red y capturando los datos que se transportan
- Haciendo una escucha sin establecer una conexión, en la que los datos se pueden seguir y estar comprometidos para varias acciones.

6.5.1.5.2.1 Interferencia sobre el cableado

Estas acciones pueden ser generadas por cables de alimentación de maquinaria pesada o por equipos de radio microondas, pero los cables de fibra óptica no sufren el problema de alteración de campos magnéticos como lo sufren los cables metálicos o de cobre.

6.5.1.5.2.2 Corte de cables

Los cables se pueden cortar **p**or accidente o por daño, los cables normales con el uso se pueden dañar e impedir que el flujo de datos circule por el mismo.

6.5.1.5.2.3 Daños en el cable

Los cables se pueden dañar por el paso del tiempo o por lo que se da un mal uso, ya que los cables preservan la integridad de los datos transmitidos y esta debe realizar que las comunicaciones deben ser fiables.

6.5.1.5.3 Cableado de alto nivel de seguridad

El objetivo de estos cableados es de impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable que consta de un sistema de tubos, herméticamente cerrados, por el cual atraviesa aire a presión y el cable. A lo largo del tubo existen sensores que están conectados a una computadora el cual detecta alguna variación en la presión, dando así la idea que existe algún cable o tubo roto.

6.5.1.5.4 Picos de placas extraíbles

Todos los cables de alimentación, comunicaciones, interconexión de equipos, etc.; pueden ser alojados en el espacio debajo de piso o placas extraíbles para mejorar un mantenimiento y poder separar de mejor manera los distintos cables.

6.5.1.5.5 Sistema de aire condicionado

Se debe estar provisto de calefacción, ventilación y aire condicionado separado, que se dedique al cuarto de servidores y equipos de proceso de datos, teniendo en cuenta que los equipos de aire condicionados son una causa potencial de incendios e inundaciones ya que es recomendable instalar redes de protección en todo el sistema de cañería interior y al exterior, detectores y extinguidores de incendio, monitores, alarmas efectivas y climatizadores.

6.5.1.5.6 Emisiones electromagnéticas

Desde hace mucho se sospecha que las emisiones de baja frecuencia de algunos periféricos son dañinas para el ser humano ya que causan radiación, pero según recomendaciones científicas estas emisiones se pueden minimizar con filtros adecuados al rango de las radio frecuencias.

Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar el envejecimiento, ya que estas emisiones también afectan a medios de trasmisión de datos."[51]

6.5.2 Factores ambientales en Italimentos

En Italimentos se tiene accesorios de seguridad tales como un extintor de fuego, detectores de humo, esto se basa en la protección industrial, ya que la puerta es de madera, las paredes son, en su mayoría, de madera y cemento lo que da estabilidad a la estructura cuando suceda alguna catástrofe.

Sobre el techo del cuarto de servidores se tiene una esponja y fibra de vidrio para intentar repeler el calor y así no forzar mucho los ventiladores de los servidores, pero se tiene el peligro de un incendio ya que la esponja es muy fácil de prender y la expansión de fuego es muy rápida. *La figura 6.5.2.1 muestra el techo del cuarto de servidores con la esponja expandida*

51 http://www.segu-info.com.ar/fisica/instalacioneselectricas.htm

Figura 6.5.2.1. Techo del cuarto de servidores

En la empresa no ha existido ninguna catástrofe ambiental ya que se tienen sumos cuidados de prevención, cuando existe descargas eléctricas por rayos, las propias computadoras tienen estabilizadores de voltaje internos los cuales previenen que se quemen computadoras, así mismo existe un UPS para todas las computadoras de Italimentos, permitiendo así continuar con las labores de los empleados. *La figura 6.5.2.2 muestra el UPS a la que se conectan todas las computadoras de Italimentos.*

Figura 6.5.2.2. UPS de Italimentos

6.6 Medidas de protección del ambiente informático

Cuando se habla de medidas de protección de un área informática, se tiende a hablar de tecnología nueva, nuevas aplicaciones, nuevos dispositivos, etc.; para lo cual se deben tomar y elaborar planes para que la información sea más consistente. Dependiendo del tipo de información se debe considerar que la información:

- Esta almacenada y procesada en computadoras
- Puede ser confidencial para algunas personas
- Puede ser mal utilizada y divulgada
- Puede estar sujeta a robos, sabotajes o fraudes

Para todo ello se debe dar las seguridades para garantizar que la información está segura en el sector informático. Con las medidas que se tengan se debe evitar o minimizar que la información privada o confidencial salga de la empresa con otros fines ajenos a la empresa.

6.6.1 Medidas de protección del ambiente informático en Italimentos

En el departamento de sistemas se toman medidas de seguridad ante catástrofes informáticas realizando copias de seguridad de la información de usuarios críticos, copias de seguridad de la base de datos para así salvar la información cuando se dé un error en la información de la empresa. También se toman medidas de seguridad a nivel de la red usando como antivirus la aplicación Kaspersky y configurado para realizar actualizaciones por medio de la red mediante la unidad K. *La figura 6.6.1.1 muestra la unidad de descarga de actualización del antivirus*

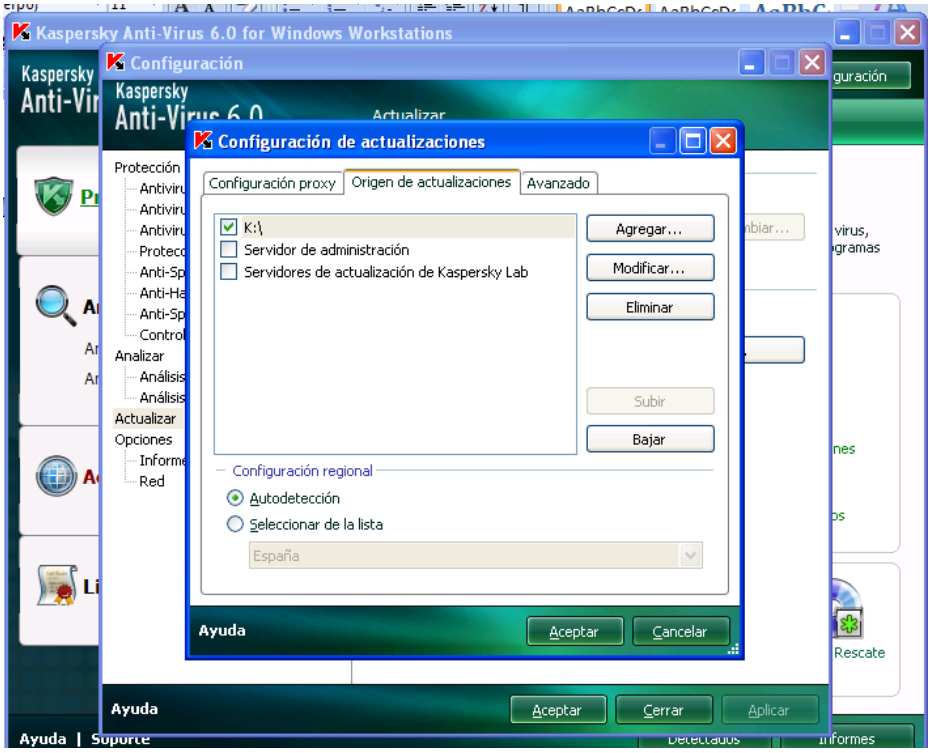


Figura 6.6.1.1. Zona de descarga de actualizaciones de anti virus

En Italimentos no se han realizado simulacros como capacitación a riesgos tales sean incendio, inundaciones, robo, etc.; provocando así una falla en la seguridad de la información y del personal ya que realizando estos simulacros se lograría minimizar o prevenir catástrofes informáticas y del personal. *La figura 6.6.1.2 muestra el extintor ubicado cerca del departamento de sistemas.*

Figura 6.6.1.2. Extintor ubicado cerca del departamento de sistemas

6.7 Protección a riesgos identificados

6.7.1 Controles de acceso

El control de acceso no solo requiere una capacidad de identificar, sino hay que asociarla a la apertura o cerramiento de puertas, para así permitir o negar acceso mediante restricciones de tiempo, área o sector de una empresa con el fin de evitar:

- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos.

Hay que tener en cuenta que para provocar un accidente, basta solo con recurrir a cerrar una puerta con llave o cortar la electricidad en ciertas áreas para y con eso dejar sin servicio a ciertos empleados hasta que se logre recuperar el sistema.

6.7.1.1 Robo

Los equipos informáticos son posesiones valiosas de las empresas y están expuestas a varios peligros, así mismo como las piezas y repuestos e incluso el dinero. Es frecuente que los usuarios usen la computadora para realizar trabajos privados o de la empresa para evitar robar tiempo de máquina. La información que se maneje, importante o confidencial, puede ser copiada fácilmente y para ello las empresas realizan inversiones en programas y archivos de información con el fin de dar mayor seguridad a la información. Así, que el software es muy fácilmente sustraible y las cintas y discos son fácilmente copiables sin dejar ningún rastro.

6.7.1.2 Fraude

Con el pasar de los tiempos, millones de dólares son sustraídos de empresas y en muchas de las veces las computadoras han sido utilizadas para tales fines, pero debido a las partes implicadas como empresas, compañías, fábricas, etc.; se debe tener ganancias y no pérdidas, para ello se deben tomar medidas adecuadas en la seguridad de la información para evitar tales gastos económicos y de reputación.

6.7.1.3 Sabotaje

Existen empresas que han intentado implementar programas de seguridad de información a alto nivel, pero han encontrado que la protección contra el saboteador es uno de los retos más duros, ya que este puede ser un empleado o sujeto ajeno a la empresa. Este saboteador puede utilizar imanes, quitar protecciones de seguridad o entrar a una habitación llena de recursos e información y destruirla . Mediante una correcta medida de seguridad se puede evitar que saboteadores destruyan equipos, información, dispositivos intencionalmente.

6.7.2 Métodos de protección a riesgos identificados

6.7.2.1 Guardias de seguridad

Los guardias de seguridad se encargan del control de acceso de todas las personas al edificio y este servicio se debe realizar en lugares estratégicos y críticos para cumplir con objetivos y así controlar el acceso de personal a diferentes áreas de la empresa. Se

debe verificar el uso de credenciales de identificación para el acceso a puntos importantes para así efectuar un control eficaz del ingreso y egreso del personal.

En el caso que una persona se identifica por algún recurso que posee, para ingresar o egresar de la empresa como una computadora, USB, DVD, etc.; entonces este usuario debe tener una credencial y se debe almacenar en una base de datos para su posterior seguimiento. Estas credenciales pueden ser clasificadas por:

- Normal: Para empleados de la empresa
- Temporal: Para personal recién ingresado
- Contratistas: Personas ajenas a la empresa que ingresa para dar un servicio
- Visitas.

6.7.2.2 Detectores de metales

El detector de metales es un elemento útil para la revisión de personas, dando ventajas para evitar el ingreso a lugares donde no se puede ingresar con dispositivos de almacenamiento, CD o DVD, etc.; ya que la sensibilidad del detector es regulable y permite un volumen metálico mínimo, al cual se activara una alarma.

6.7.2.3 Sistemas biométricos

La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas que pueden ser almacenadas en una base de datos. Mediante este sistema se evita la necesidad de poseer una tarjeta de identificación y realizar mantenimientos o ingreso a lugares privados solo de personas especificas. Existen diferentes sistemas biométricos como:

- Emisión de calor: Mide el calor del cuerpo la forma de la persona
- Huella digital: Basado en el principio que no existen 2 huellas dactilares iguales
- Verificación de voz: Decir una frase clave y comparación de cuerdas bucales

- Verificación de patrones oculares: Basados en patrones de iris y retina.

6.7.2.4 Verificación automática de firmas

Tiene que ver con la firma de exactitud de la persona dueña de la misma en la que el patrón de, puntos y líneas, contiene información exacta sobre la manera en que la escritura es ejecutada y es un equipamiento de bajo costo y robusto.

6.7.2.5 Seguridad con animales

Se trata de que la seguridad, de soporte de datos o recursos informáticos, que contengan información importante esté al alcance de animales, ya sean estos roedores, moscos u otros animales, para evitar que provoquen algún daño a los equipos de cómputo.

6.7.2.6 Protección electrónica

Con estas medidas se puede detectar un robo, intrusión, asalto e incendios mediante sensores conectados a alarmas centrales para así tomar medidas adecuadas de emergencias. Existen varios tipos de protección electrónica como:

- **Barreras infrarrojas:** Transmiten y reciben luces infrarrojas entre sensores invisibles al ojo humano, se activa una alarma cuando se bloquea esta transmisión.

- **Detector ultrasónico:** Crea un campo de ondas para detectar cualquier movimiento dentro de un espacio, al detectar movimiento se activara una alarma.

- **Detectores pasivos sin alimentación:** Son elementos que se conectan a una central que recibe información como: detectar aberturas, roturas de vidrio o vibraciones

- **Sonorización y dispositivos luminosos:** Son dispositivos que transmiten señal sonora o luminosa con el fin de que sean vistos u oídos por el personal.

- **Circuitos cerrados de televisión:** Permiten el control de todo lo que sucede en la empresa por medio de cámaras estratégicamente colocadas.

- **Edificios inteligentes:** Propone la integración de todos los sistemas inteligentes dentro del edificio como: teléfono, comunicaciones por computadora, seguridad, control de subsistemas de gas, calefacción, ventilación, etc.

6.7.3 Protección a riesgos identificados en Italimentos

6.7.3.1 Control de accesos

En Italimentos existe una área de seguridad para el ingreso y salida del personal en el cual, las personas que trabajan en la empresa marcan su hora de llegada en la garita y en el segundo piso y las personas que no trabajan dentro de la empresa dejan la cedula al guardia de ingreso a la compañía para registrar en un formulario la hora de entrada y salida. El guardia de seguridad de la empresa realiza las respectivas revisiones para evitar el hurto de activos, ya que al momento de sacar algún recurso se necesita un formulario de salida para poder realizar mantenimientos fuera de la empresa o movimientos con otros equipos. *La figura 6.7.3.1.1 y 6.7.3.1.2 muestra el área de seguridad para ingreso y salida de Italimentos*

Figura 6.7.3.1.1. Área de seguridad de ingreso y salida

Figura 6.7.3.1.2. Área de seguridad de ingreso y salida

Para la información que se lleve en memorias USB o por algún tipo de dispositivo de almacenamiento, no se realiza ningún tipo de vigilancia por parte del guardia de seguridad, ya que la información puede salir de manera muy fácil. El ingreso de vehículos es solo para el personal ejecutivo y personas con permisos especiales, en el cual no se realiza revisiones para controlar el robo de recursos de la empresa. *La figura 6.7.3.1.3 muestra el parqueadero de Italimentos*

Figura 6.7.3.1.3. Estacionamiento de Italimentos

La empresa Italimentos tiene cámaras de seguridad en varios puntos estratégicos para la seguridad del personal con el fin de tener evidencia física cuando exista algún inconveniente dentro de la compañía. Para el ingreso al departamento de sistemas no se posee una cámara que muestre el interior del mismo, pero existen cámaras que ayudan a conocer quienes transitan por los pasillos así como la fecha y la hora en la cual pasaron por un sector específico.

Así mismo, no existen cámaras de seguridad en las afueras del cuarto de servidores para controlar quienes pueden haber forzado o intentado ingresar al mismo, pero existe una cámara en el interior del cuarto que se enciende cuando detecta movimiento y graba la información en el disco duro del servidor de cámaras. Al momento que existe algún problema interno, se recurren a las cámaras de seguridad en el cual ingresa algún responsable del departamento de sistemas y personal autorizado a ingresar para conocer y estudiar el caso para lograr una solución al problema dado.

En el cual solo existe una cámara de seguridad para controlar el acceso al cuarto de servidores y no existe alguna cámara `para controlar el acceso al departamento de sistemas. Cuando existen problemas en las cámaras de seguridad, se notifica al departamento de mantenimiento para realizar los respectivos cambios o arreglos y así mejorar la seguridad al interior de la empresa.

6.7.3.2 Acciones hostiles

En Italimentos no se ha dado el caso que exista robo de información o recursos informáticos, pero varias personas guardan información en dispositivos de almacenamiento y con ello se trasladan a varias partes provocando que la seguridad de la información se vea limitada. Para prevenir este tipo de acciones hostiles el cuarto de servidores permanece cerrado con llave y los servidores cerrados las sesiones y con claves de ingreso que solo conoce el personal de sistemas.

En la empresa se toman medidas de seguridad para evitar que la información salga de la misma, para ello se realizan bloqueos de varios puertos USB de las computadoras de los usuarios para evitar el ingreso de memorias de almacenamiento, pero ello no se da en

todas las computadoras y con ello existe la posibilidad de que se lleve información al exterior.

CAPITULO 7

"Auditoría del acceso"

7.1 Personal autorizado a conceder, alterar o anular accesos sobre datos y recursos

El objetivo de este tema, es el de proteger la información de la base de datos contra accesos no autorizados llamado también como privacidad de los datos, en el cual se incluye aspectos importantes como:

- Aspectos legales, sociales y éticos
- Políticas empresariales y manejo de información pública y privada
- Controles de tipo físico y acceso a las instalaciones
- identificación de usuarios
- Controles de los sistemas operativos

Para tener controlada la seguridad de la información de los datos, existen varios usuarios con sus respectivos privilegios tales como:

- DBA: perite todas las operaciones, conceder privilegios y establecer usuarios
- Usuario con privilegios de crear, borrar y modificar objetos
- Usuario con derecho a consultar y actualizar objetos.

Mediante un subsistema de la base de datos, se asegura y garantiza el acceso no autorizado por medio de identificación de los usuarios para que puedan tener acceso por un solo terminal, teniendo en cuenta que se debe tener técnicas de cifrado y un medio de comunicación segura entre la base de datos y el usuario final.

El problema de la seguridad de los datos consiste en que sean usados con fines previstos y para ello se utilizan mecanismos de protección. Los sistemas operativos proveen ciertos mecanismos de protección y con ello realizar políticas de seguridad que definan que hay que hacer y cómo hacerlo.

Al momento de tener una base de datos, implica que se debe implementar seguridades en componentes de la red y el administrador debe garantizar la seguridad de los recursos de la red, evitando accesos no autorizados y daños accidentales o deliberados. Para ello se deben otorgar permisos y derechos a los recursos de la red para poder competir la información de manera protegida mediante una contraseña. *La figura 7.1.1. Muestra los privilegios que se puede otorgar al usuario*

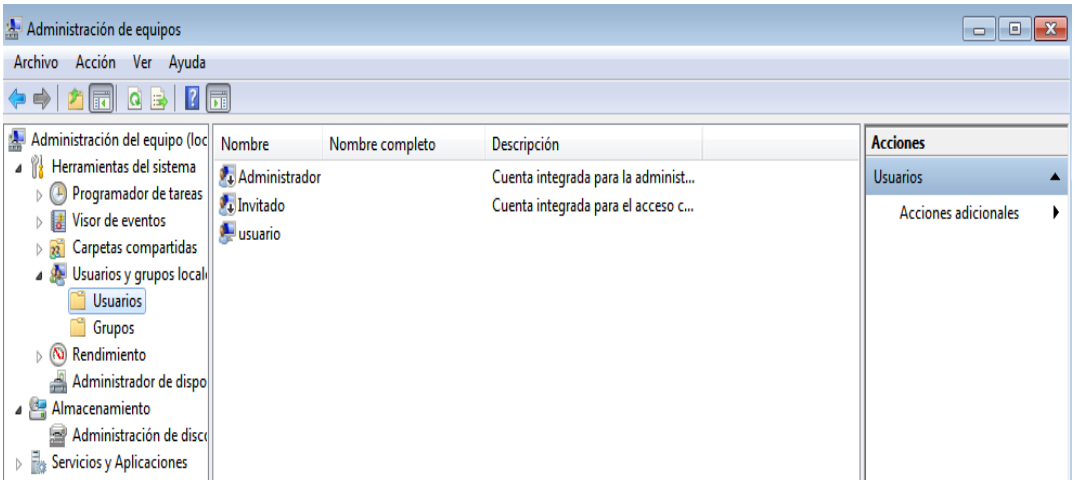


Figura 7.1.1. Tipos de privilegios para cuentas de usuarios

La seguridad basada en personal con ciertos privilegios, implica el control de ciertos usuarios que deben escribir una contraseña para entrar en la red y con ello asignar o denegar el acceso a recursos compartidos entre computadoras o en una base de datos.

7.1.1 Personal autorizado a conceder, alterar o anular accesos sobre datos y recursos en Italimentos

En Italimentos el responsable de los archivos digitales, es el único con privilegios de conceder, alterar o anular el acceso a la información contenida dentro del mismo. El usuario crea su archivo y lo almacena en una carpeta privada o en una carpeta compartida con otros usuarios específicos y el departamento de sistemas es el encargado de realizar las configuraciones para poder compartir la información y dar los privilegios a los respectivos usuarios. El departamento de sistemas se encarga de dar privilegios a los diferentes tipos de usuarios y de la modificación de los mismos, con el fin de

salvaguardar los archivos digitales y la información contenida en la misma. *La figura 7.1.1.1 muestra las carpetas compartidas en la red de Italimentos para usuarios.*

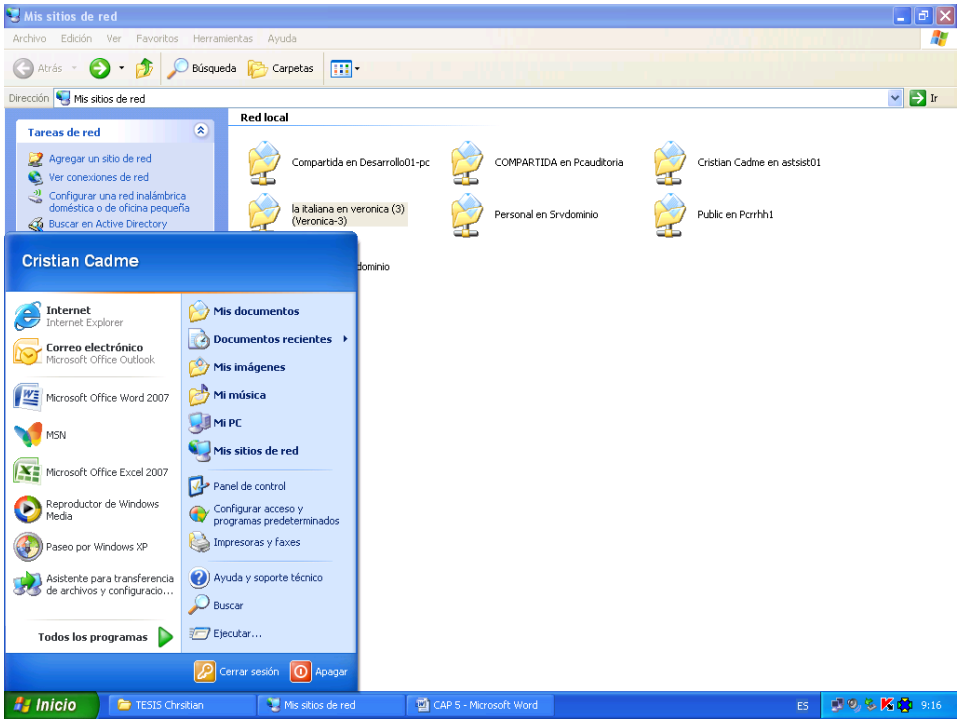


Figura 7.1.1.1. Carpetas compartidas en Italimentos para usuarios

Para el acceso a los servidores, el personal del departamento de sistemas y parte del departamento de desarrollo del nuevo sistema de Italimentos, son los únicos autorizados de ingresar al cuarto de servidores para realizar configuraciones en los sistemas de los servidores. El departamento de sistemas se encarga de la seguridad de la información de Italimentos en los servidores y de la modificación de la misma, ya que existen privilegios para los usuarios para el acceso a la información de los servidores.

7.2 Número máximo de intentos de conexión

Existen muchos administradores de red que necesitan conectarse de manera remota a los servidores, pero suele existir cierta vulnerabilidad cuando un puerto se va a abrir, por lo que se tendría que configurar una VPN o limitar las conexiones de ese puerto y número de intento de conexión.

La mayoría de los servicios que requieren un inicio de sesión determinado necesitan un número de intentos permitidos de entrada consecutivos no válidos, pero ahora en los sistemas operativos y herramientas actuales ya hay como configurar o limitar el acceso no autorizado de manera temporal o permanente. Estas técnicas se implementaros para impedir que los hackers decodifiquen las contraseñas mediante la introducción de caracteres aleatorias de forma continua. *La figura 7.2.1 muestra la configuración de un usuario en Windows 7.*

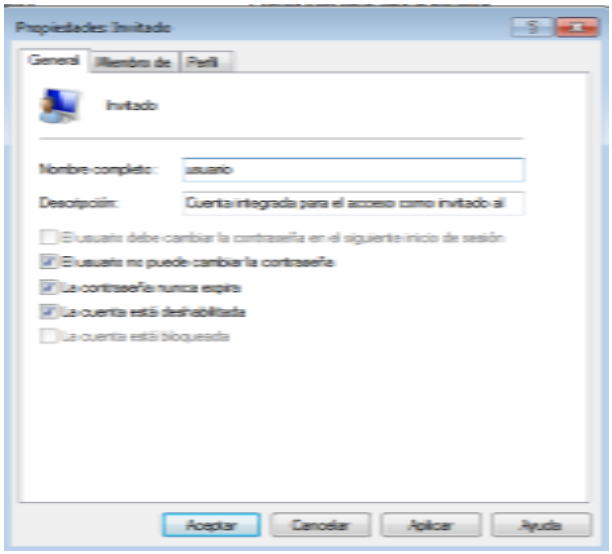


Figura 7.2.1. Configuración de la cuenta usuario en Windows 7

Las configuraciones que se realicen para evitar el número de intentos fallidos de conexión, determinará el que el sistema pueda bloquearse antes de realizar otro ingreso erróneo en la clave. Cuando una cuenta esta bloqueada, no se podrá utilizar hasta que sea restablecida por un administrador o hasta que caduque el tiempo de la duración del bloqueo.

7.2.1 Número máximo de intentos de conexión en Italimentos

En la empresa de Italimentos se tiene un número máximo de intentos de ingreso a las sesiones de Windows con un máximo de cinco oportunidades para poder ingresar bien su usuario y contraseña en los usuarios finales. Hasta el momento no se ha dado ningún

caso de bloqueo de cuentas por intentos fallidos de conexión en la empresa ya que cada usuario conoce su cuenta y su contraseña de acceso al sistema.

En los servidores, que dan los diferentes servicios a los usuarios, se tiene como máximo tres intentos de conexión e ingreso al sistema ya que poseen información crítica dentro de los mismos y su acceso está limitado solo al departamento de sistemas. Como solo el departamento de sistemas tiene los nombres de las cuentas y las contraseñas de los servidores, no se ha dado ningún tipo de intentos fallidos de acceso a algún servidor por terceras personas, sea de manera local o remota. En la empresa ha existido un cierto número de intentos fallidos pero se dan por causas accidentales de escritura en el teclado, ya que esto no causaría un tipo grave de problema en Italimentos a no ser que sea por causas de hardware.

Para el ingreso a cuentas de correo electrónico, no existe un debido control en el número máximo de intentos de conexión, ya que el usuario puede intentar ingresar a la fuerza hasta conseguir la clave de acceso a una cuenta de correo. El usuario no es difícil de encontrar ya que el correo electrónico tiene una estructura para todos los usuarios y mediante este correo se puede intentar ingresar a otro correo electrónico sin estar limitado en los intentos fallidos de ingreso al correo. La estructura usada para correos electrónicos consiste en utilizar el primer nombre, con el símbolo especial guion bajo, seguido del apellido del usuario y el dominio [52] @laitaliana.com.ec. Ejemplo. juan_perez@laitaliana.com.ec

Para el número de intentos máximos de conexión de los vendedores a sus Palm, se los realiza localmente, es decir, desde Italimentos el servidor de la base de datos actualiza las rutas que van a ser trabajadas por los vendedores de la fábrica.

7.3 Descarga de información

Cualquier empresa que tenga empleados, departamentos, sucursales y demás dentro de la organización, requiere de una infraestructura tecnológica para llevar a cabo sus obligaciones y mejorar la comunicación, lo que hace que las redes de comunicación sean

[52] Dominio: Nombre que identifica una dirección

parte vital ya que son las que interconectan y permiten la comunicación de empleados y departamentos. Los administradores de estas redes deben proveer de servicios e información a los usuarios de manera segura, otorgando privilegios y contraseñas seguras de acceso a la red de la empresa.

Al momento de aumentar el número de empleados, equipos, servidores y demás, a los administradores de la red se complica hacer un seguimiento continuo a cada usuario y a la información que viaja través de la misma. Como los equipos se conectan a una base de datos y comparten carpetas con otros usuarios, se debe proveer de la información suficiente realizando mantenimientos de privacidad de información y usando protocolos de conexión segura tales como sshell[53] o https[54].

Así mismo, se debe proveer a ciertos usuarios el acceso a internet pero a la vez limitando el acceso a varias páginas con el objetivo de no distraer al usuario y que cumpla sus funciones en la empresa. Al momento que se desee descargar archivos digitales, este primero debe pasar por un escaneo un firewall seguido de un escaneo de un antivirus para así garantizar que no exista código maligno que pueda dañar el equipo y no se pueda propagar por la red interna infectando más equipos e incluso los servidores.

Cuando se realiza conexiones externas, existe la probabilidad para accesos no autorizados a la información de la empresa para ello se debe tener técnicas de autenticación tales como criptografía, protocolos de pregunta/respuesta, líneas dedicadas, etc. con el objetivo de prevenir estas intrusiones no deseadas.

7.3.1 Descarga de información en Italimentos

En Italimentos la información se puede descargar por la red LAN[55] de la empresa ya que existen carpetas compartidas con archivos digitales que llevan información de varios departamentos, estos archivos pueden ser descargados por varios usuarios que pueden guardar la información en dispositivos de almacenamiento y ser trasladados a varias partes de la empresa o hacia el exterior. En Italimentos las mayor parte de las

[53] Sshell: Protocolo Secure Shell
[54] Https: Hiper Text Transfer Protocol Secure
[55] LAN: Local Area Network

computadoras tienen bloqueado los puertos USB para evitar que memorias USB contaminadas con virus entren en la red de Italimentos y se propaguen o para evitar el robo o traslado de información con fines de lucro. *La figura 7.3.1.1 muestra carpetas compartidas en Italimentos.*

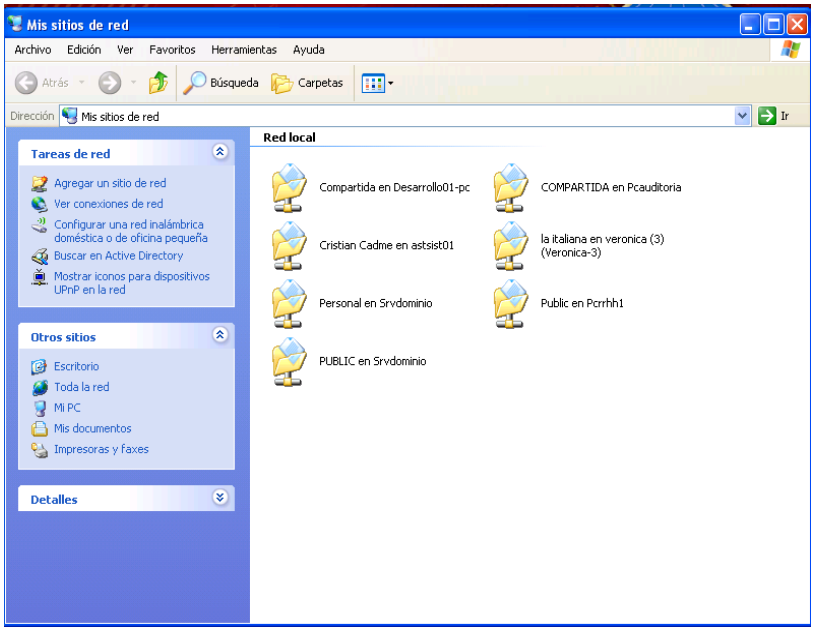


Figura 7.3.1.1. Carpetas compartidas en Italimentos

Mediante la red WAN[56] que tiene la empresa con otros locales comerciales, tales como Italdelis, existe información que se puede descargar de manera remota, pero cierta información es privada y solo un grupo selecto de usuarios puede tener ingreso a la información para realizar acciones sobre la misma, pero existe también información pública, ya que los usuario graban esta información para compartir con ciertos departamentos específicos o con todos los departamentos.

La descarga de información de internet está limitada en las computadoras que se conectan a la red local de Italimentos ya que el acceso a ciertas páginas web está restringida por un proxy, pero ciertos usuarios tienen mayor libertad de acceso a otras páginas por la información que se tiene que conocer u otras acciones que se tenga que realizar tales como descarga de archivos, imágenes, etc.

[56] WAN: Wide Area Network

Las computadoras que tengan un adaptador wireless[57] pueden conectarse a la red inalámbrica de la empresa con acceso a todas las páginas que se desee ingresar ya que si se tiene restricciones configuradas en el routers inalámbrico. La única restricción que existe al momento de conectarse a la red inalámbrica es la contraseña de conexión que tiene como caracteres letras, números y símbolos especiales. *La figura 7.3.1.3 muestra la red wifi de la empresa*

Figura 7.3.1.3. Red Wi-Fi Italimentos

Los vendedores descargan información a sus palm, con el objetivo de actualizar sus clientes, productos y rutas que se tiene que realizar en el día, esta información se la realiza mediante la empresa de telecomunicaciones claro, la cual se encarga de dar el servicio de conexión a la base de datos de Italimentos y así poder descargar la información necesaria. Esta información se la descarga diariamente ya que cada día se necesita realizar una ruta específica para vender los productos de Italimentos.

7.4 Conexiones entre empresas y redes públicas o privadas

En Ecuador existen miles de conexiones de banda ancha, lo que quiere decir que muchas de estas redes se conectan a internet por estos accesos y ahora es muy necesario ser consientes de la necesidad de fortalecer la seguridad de los sistemas actuales para mantener la integridad de la información, para ello se necesita conocer:

[57] Wireless: Medio de comunicación inalámbrica

- Infraestructura de la empresa, interconexión de dispositivos y direcciones IP.
- Claves por defecto o modificados de routers y firewalls.
- Configuración de routers y puentes.
- Configuración del wireless en computadoras portátiles.
- Firewall instalado.
- Copias de seguridad realizadas.
- Permisos de acceso a la información otorgados.
- Antivirus y actualización.

Existen varias formas de conectar este tipo de redes, para ello se utilizan varios elementos fundamentales tales como: servidores, estaciones de trabajo, tarjetas de red y cables. A estos elementos se le suman elementos propios de cada uno como el tipo de cableado, manuales y software de red, instalación y mantenimiento. Estas conexiones pueden ser por varios medios tales como cables UTP, fibra óptica, medios inalámbricos, etc. *La figura 7.4.1 muestra los distintos medios de comunicación informáticos*

Figura 7.4.1. Medios de comunicación informática [58]

[58] http://majandratv.blogspot.com/

Dependiendo de la topología que se maneje en una empresa y de los dispositivos conectados a la misma, se debe tener en cuenta ciertas características de la red como velocidad de transmisión de datos y confiabilidad de la conexión. Para ello se pueden ver ciertas topologías utilizadas por empresas como: bus, estrella, malla, etc. *Véase capitulo 2 sección 2.12.*

7.4.1 Conexiones entre empresas y redes públicas o privadas en Italimentos

La empresa de Italimentos tiene una red LAN interna a la que se conectan todos los usuarios para cumplir con sus labores diarias, esta red LAN es centralizada ya que los usuarios se conectan a un servidor de base de datos central mediante cable UTP[59] categoría cinco conectado a varios switch capa dos. La conexión entre los switch en la empresa se los realiza por cable de fibra óptica para optimizar la transferencia de datos. *La figura 7.4.1.1 muestra la estructura de los switch dentro de la fábrica de Italimentos*

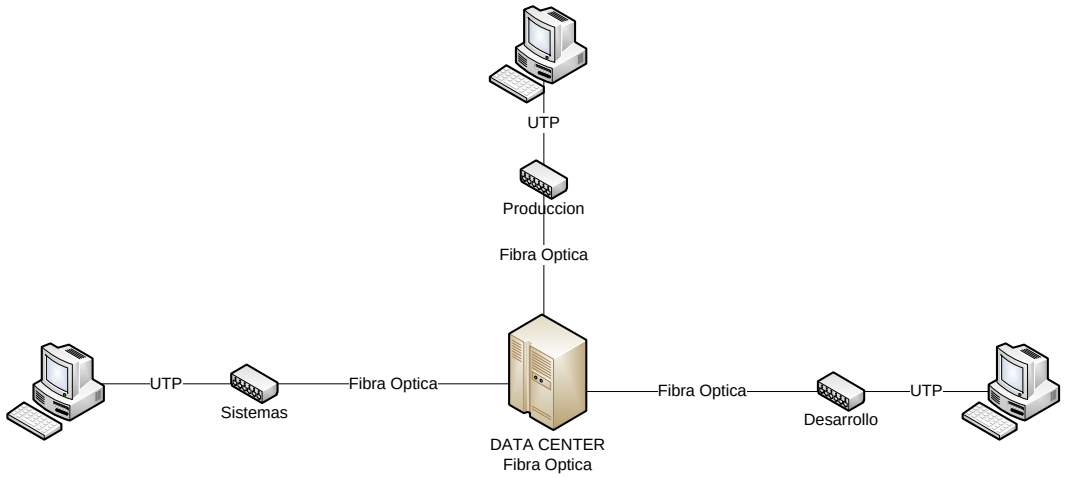


Figura 7.4.1.1. Estructura de los switch dentro de la fábrica de Italimentos

Todos los locales comerciales, pertenecientes a Italimentos, se conectan a los servidores ubicado en el sector del parque industrial para que la información este centralizada y sea más fácil el tratamiento y el mantenimiento del mismo. Italimentos está conectado mediante una red WAN con otros locales comerciales mediante un proveedor de

[59] UTP: Unshielded Twisted Pair

servicios de internet llamado Puntonet, el cual se encarga de la comunicación de estos locales comerciales, tales como son:

- Italdeli solano
- Italdeli Fátima
- Italdeli San Sebastián
- Italdeli Costo
- Italdeli Quito
- Próximamente Italdeli Granja 16/03/2012

La figura 7.4.1.2 muestra un diagrama didáctico de las conexiones de Italimentos

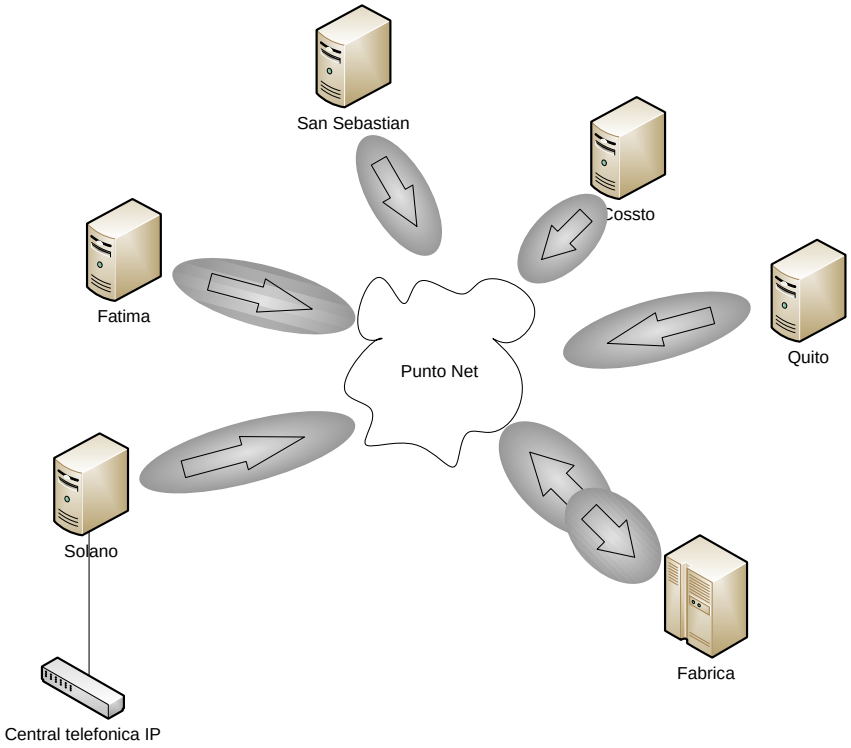


Figura 7.4.1.2. Estructura didáctica de conexiones de Italimentos

En esta red no se ha dado problemas de inseguridad de la información, ya que los datos se guardan en un solo servidor de base de datos y existen los respaldos de la información.

Los vendedores que tienen Palm para realizar pedidos se conectan a la base de datos para descargar actualizaciones sobre rutas de visita, clientes y productos; para esta conexión se realiza mediante el proveedor de servicios de claro, ya que el pedido se realiza de manera inmediata y la base de datos se actualiza con dicho pedido. En ciertos casos se ha dado que al momento de realizar varios pedidos por parte de varios vendedores simultáneamente, han existido errores sobre códigos provocando que exista confusión al momento de despachar el pedido.

7.5 Eventos realizados por otros usuarios

En los sistemas operativos se viene incorporado eventos que se registran automáticamente, para ello se debe hacer uso del viso de sucesos. *La figura 7.5.1 muestra el visor de sucesos de Windows 7.*

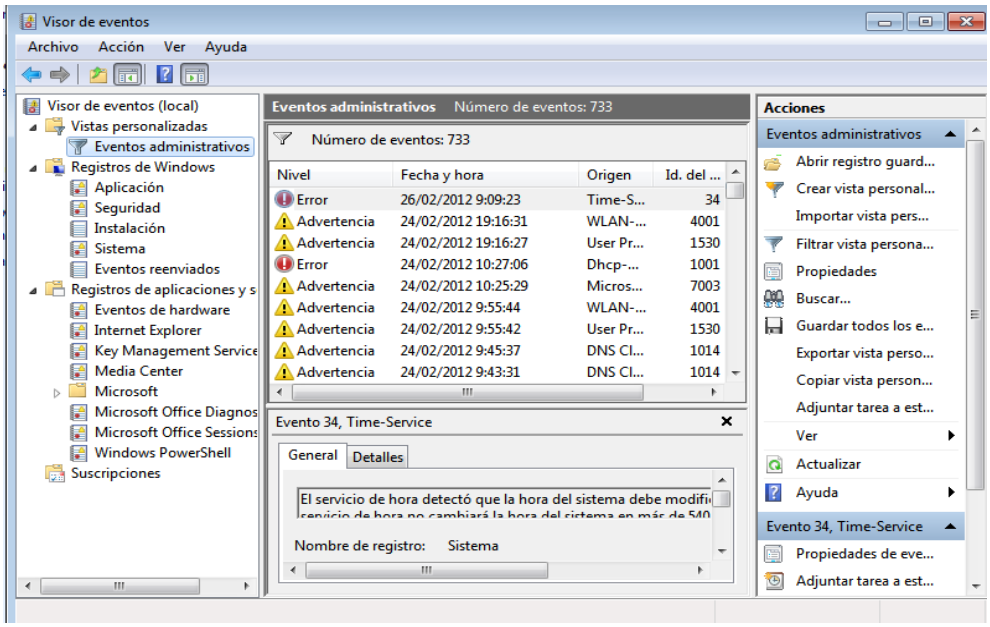


Figura 7.5.1. Visor de sucesos de Windows 7

El registro de seguridad guarda todos los eventos como intentos válidos y no válidos de inicio de sesión, así como varios eventos que se relacionan con el uso de recursos como crear, abrir o eliminar archivos con el fin de obtener un detallado visor de eventos que se realizó en el equipo. El profundo análisis de los eventos, permitirá encontrar muchas actividades sospechosas en el sistema y el usuario responsable de tal actividad.

Existen también varias aplicaciones que permiten registrar actividades que se realicen sobre un equipo, facilitando así una mejor gestión sobre las actividades que realice el usuario mediante el uso de filtros de ordenamiento para realizar acciones determinadas en un contenido en particular. Los sistemas de registro de eventos administrar, registrar, consultar, suscribirse y administrar metadatos en tiempo real, si se detiene este servicio podría ponerse en peligro la seguridad y confiabilidad del sistema.

7.5.1 Eventos realizados por otros usuarios en Italimentos

En Italimentos, cada computadora tiene un log de registro de eventos que se realiza en la computadora, este log de registros es propio del sistema operativo de Microsoft Windows y aparte no existe aplicaciones extras para registrar acciones realizadas en la computadora del usuario de Italimentos.

Cuando existe algún problema en un equipo informático y no se conoce que pasó, se suele revisar el log de registro de eventos para así dar solución de hardware o software en ese momento para que el equipo pueda entrar a producción lo más pronto posible. En Italimentos no existe un registro o historial de eventos o gestión de incidentes cuando existe un problema en alguna computadora o servidor ya que no se poseen las herramientas adecuadas para administrar los mismos. *La figura 7.5.1.1 muestra el visor de sucesos de computadora de vendedores.*

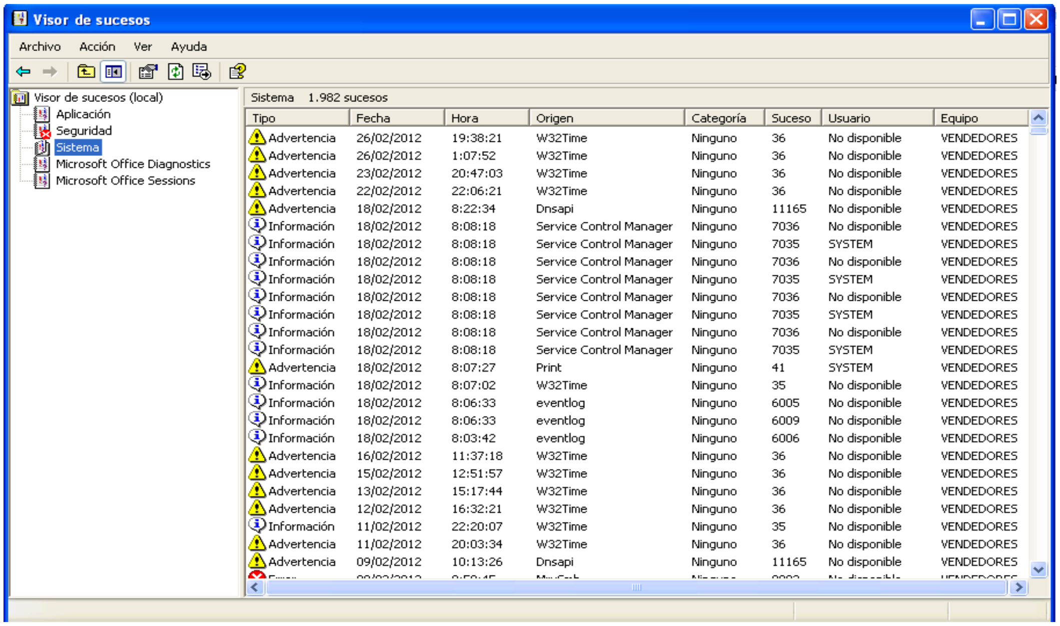


Figura 7.5.1.1. Visor de sucesos de computadora de vendedores

Para terceras personas que remplazan a un usuario de la empresa, no existe un control de eventos que se realiza en un equipo, ya que se conocen contraseñas de acceso al computador y se realizan otras actividades que con el tiempo pueden causar algún tipo de problema de información, si el error es crítico se suele revisar log de registro para conocer las actividades realizadas en el equipo informático y así poder dar una solución al problema.

7.6 Responsabilidad del personal ante contraseñas y equipos

Aquí se debe recoger las principales funciones y obligaciones del personal que accede a los datos de los ficheros, ya que deben definirse y recogerse los tipos de acceso y los permisos de cada usuario. Las claves de seguridad son el método principal que se utiliza para verificar la identidad de un usuario, el cual debe tener una contraseña segura, cambiarla cada cierto tiempo y la no divulgación de la misma con el objetivo de evitar intrusiones y posibles ingresos a la información dentro de un equipo informático.

En una empresa cada usuario, que interactúa con un equipo informático es responsable de la seguridad de la información que se encuentre dentro de la misma, aunque intervienen otros medios como la seguridad de la red, servidores, etc. Las contraseñas

son personales y privadas, pero la complejidad de la contraseña se debe realizar de manera balanceada entre seguridad y comodidad para evitar que terceras personas tengan acceso a ciertos recursos.

El compromiso de mantener las contraseñas personales y grupales en secreto es cuestión de seguridad en la información ya que la divulgación puede causar ciertos problemas a futuro, para ello se deben tomar contraseñas provisionales en caso de pérdida de la misma. Una causa grave es la distribución de claves por internet, mails o papeles siendo así que pueden participar terceros y provocar desastres en una empresa, para eso se debe cambiar regularmente contraseñas como compromiso con el sistema y la seguridad de la información que se utiliza.

Los usuarios deben imponerse sus contraseñas ya que al momento de imponerle la clave, esta es más fácil de olvidar y el usuario debe ser capaz de poder cambiar la contraseña por una de seguridad igual o mejor a la previa. El administrador del sistema debe tener un registro histórico y seguro de las contraseñas ya que con el tiempo se puede volver a utilizar la misma, así mismo estas contraseñas deben estar muy bien cifradas para eliminar o minimizar así el adivinar la clave.

7.6.1 Responsabilidad del personal ante contraseñas y equipos en Italimentos

En la empresa el usuario es responsable de su contraseña y de la divulgación de la misma, sea para el inicio de sesión en un equipo informático o para acceder una cuenta de correo electrónico, ya que el usuario se propone su propia seguridad en la clave. Para el acceso a servidores las contraseñas de inicio de sesión tienen seguridad alta, ya que son sistemas críticos para la empresa y estas contraseñas tienen como caracteres letras, números y símbolos especiales y solo el departamento de sistemas conoce las claves de acceso a los servidores.

Las contraseñas de acceso a los correos electrónicos están configuradas en el servidor proxy con sistema operativo Centos y administrado personalmente para el servidor y próximo al usuario final que desee dicha cuenta de correo. El dominio utilizado para los correos electrónicos es "@laitaliana.com.ec" el cual se configura en el servidor de correo

y en el equipo del usuario mediante la aplicación Microsoft Office Outlook para poder enviar y recibir correos electrónicos.

Para computadoras que utilicen dos o más usuarios, se conoce la contraseña utilizada ya que se utiliza la misma cuenta para acceder a los datos y archivos digitales que se encuentra en la misma, pero no se ha dado casos de acciones dañinas en este tipo de uso de los equipos informáticos.

7.7 Seguridad ante el trabajo remoto

Las nuevas tecnologías han puesto a las empresas a pensar en un esquema de trabajo remoto para seguir operando ya sea desde VPN o escritorios remotos, en el que influyen también aspectos de infraestructura en el que actúan varias cuestiones que afectar al trabajo remoto.

7.7.1 Electricidad

La electricidad es muy importante ya que se tienen equipos electrónicos que son usados para realizar los trabajos remotos. Esto puede afectar definitivamente al trabajador ya que corre el riesgo de quedar sin internet y sin baterías en una laptop y que tienen un periodo finito de carga.

7.7.2 Distracciones

El trabajo remoto puede verse afectado por distracciones que están a la orden del día, como mantenimientos de rutina mientras se trabaja con un equipo remoto, llamadas por teléfono y demás, para ello se debe ver personal que se encargue o ayude a las labores, ya sea de trabajo remoto o demás actividades dentro de una área de trabajo.

7.7.3 Espacio adecuado

Se debe tener un buen espacio para poder trabajar remotamente las horas contratadas, con una correcta iluminación, evitando ser parte de distracciones.

7.7.4 Internet

Para trabajar remotamente se necesita de internet y a veces resulta irresistible navegar un rato por internet provocando distracciones al personal, esto se puede evitar mediante un proxy en la red que restringa el acceso a varias páginas.

7.7.5 Experiencia remota

Aquí depende mucho del esquema tecnológico que se tenga, pero en varias ocasiones es necesario y útil tener una extensión de teléfono para soporte a usuarios..

Es importante tener una política móvil que tome en cuenta los riesgos que implica trabajar con herramientas informáticas móviles, ya que el equipamiento transporta información importante, critica o sensible de la empresa. Estos accesos se realizan través de redes públicas, utilizando herramientas informáticas móviles, previo a esto debe existir un medio de autenticación para poder ingresar a la red privada de la empresa.

7.7.6 Seguridad ante el trabajo remoto en Italimentos

En la empresa el departamento de sistemas tiene acceso a varios equipos, centrales telefónicas IP y servidores que se encuentran dentro y fuera de la empresa, estos accesos remotos se los realiza con la aplicación propia de Windows llamada escritorio remoto o una aplicación llamada VNC[60] para controlar aplicaciones y realizar acciones de manera remota. Cuando existe un error en un equipo remoto y no se puede solucionar, entonces, algún responsable del departamento de sistemas va de manera física a revisar el equipo informático y dar solución al mismo. *La figura 7.7.6.1 muestra la aplicación VNC para escritorios remotos*

[60] VNC: Aplicaion para escritorio remoto Virtual Network Computing

Figura 7.7.6.1. Aplicación VNC[61]

Cuando se instala un nuevo usuario crítico o un servidor, se habilita la opción para realizar escritorios remotos para así poder dar atención al usuario cuando este lo requiera en cuestiones de software y configuraciones.

Últimamente se instaló una central telefónica IP marca Alcatel en Italdeli Solano, en la cual el jefe de sistemas administra de manera remota, dando así un número de extensión a cada departamento o puesto de trabajo en los locales comerciales pertenecientes a Italimentos, con la finalidad de mantener comunicado a todos ellos. También se está realizando una guía telefónica de Italimentos, con la finalidad de conocer las extensiones que se está utilizando y poder gestionar los mismos de una mejor manera.

7.8 Técnicas de identificación y autenticación

La identificación y autenticación es lo más importante en lo que a seguridad informática se refiere, en el cual se previene el ingreso de personas no autorizadas, controlando así el acceso y seguimiento de usuarios. Para ello se denominan dos términos:

- Identificación: Cundo el usuario se da a conocer en el sistema

[61] http://vnc-scan-enterprise-console.softonic.com/descargar

- Autenticación> Verificación que realiza el sistema sobre la identificación

Existen 4 tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales son nombradas:

- Solo la persona conoce: Clave secreta, clave criptográfica, pin, etc.
- Algo que la persona posee: tarjeta magnética
- Identifica únicamente a una persona: huella digital, biometría, etc.
- Solo el individuo lo puede realizar: Patrones de escritura.

Todas estas técnicas pueden ser usadas dependiendo de la criticidad del asunto, permitiendo así tener una mejor seguridad. Se debe tener en cuenta que las claves pueden ser olvidadas o que las tarjetas o dispositivos se pierdan, mientras que los controles biométricos serian los más apropiados para administrar pero en estos dispositivos se invierte una cantidad económica más grande.

7.8.1 Técnicas de identificación y autenticación en Italimentos

Existen varias técnicas de autenticación en Italimentos de las cuales la principal es por medio telefónico, en el cual se llama al departamento de sistemas para algún servicio técnico, ya sea por teléfono, medios remotos o de manera personal en el cual el jefe de sistemas ya reconoce con quien habla y en que área se encuentra el usuario, pero no existe un identificador de llamadas para estar asegurado que se llama de un lugar en especifico. Este método de identificación y autenticación no ha provocado problemas de seguridad hasta el momento ya que el departamento de sistemas ya conoce a la mayoría del personal de Italimentos y las acciones que deben tomar al momento de dar servicio informático los usuarios.

Cuando existe un empleado, dependiendo del cargo, se le asigna una computadora con una cuenta de usuario otorgada por el departamento de sistemas, para esa manera ya conocer al nuevo usuario y con ello poder otorgar servicios técnicos que sean requeridos, a futuro, por el nuevo usuario del equipo informático.

Otro tipo de método de identificación y autenticación es de manera personal, ya que el usuario se hace presente físicamente para pedir ayuda sobre algún tema informático. Con este medio se puede reconocer de forma física al usuario y así poder ofrecer las respectivas soluciones a los problemas que estén por resolver.

7.9 Registro y revisión de eventos realizados por terceros

Cuando exista la necesidad de otorgar accesos a terceras personas a información de una empresa, el responsable de seguridad informática y el propietario de la información que se trae, deben llevar a cabo una documentación o un registro de eventos en el visor de sucesos del equipo para así poder conocer que acciones se realizaron.

En todos los accesos por terceras personas, sean por contrato, mantenimientos, remplazos laborales y demás, se debe chequear al inicio y final los sucesos ocurridos ya que pueden ocurrir errores y provocar fallos a futuro. Estos errores debe ser revisados regularmente par poder tomar las medidas adecuadas, ya que cuando vuelva a ocurrir una incidencia, poder minimizar tiempos de reparación.

En las aéreas criticas sería muy importante dar seguimiento a las actividades que se van realizando ya que pueden provocar fallos en los servicios, para ello se implementan controles para definir las condiciones para una conexión o acceso.

El acceso a cierta información y aplicaciones debe estar limitado para así controlar las funciones del sistema, garantizando así que las salidas de los sistemas de la aplicación, contenga la información pertinente a la salida. Para ello también se debe contener un registro de entrada y salida de la persona que va a interactuar con un sistema o equipo informático y monitorear las actividades realizadas por la misma.

7.9.1 Registro y revisión de eventos realizados por terceros en Italimentos

En Italimentos no suele suceder mucho el remplazo de personal por terceras personas o ajenas a la empresa, pero se tiene un log de registro de acciones realizadas en el equipo informático con el cual se puede obtener la información necesaria para problemas que puedan ocurrir en dicho equipo. Con el registro de eventos realizados un una computadora no se puede revisar si ha existido la copia de información a un dispositivo

de almacenamiento, provocando así un tema grave de seguridad de la información, pero la mayoría de las computadoras tienen bloqueados los puertos USB con la finalidad de evitar la copia de información a dispositivos de almacenamiento. *La figura 7.9.1.1 muestra puertos USB habilitados en computadora de vendedores.*

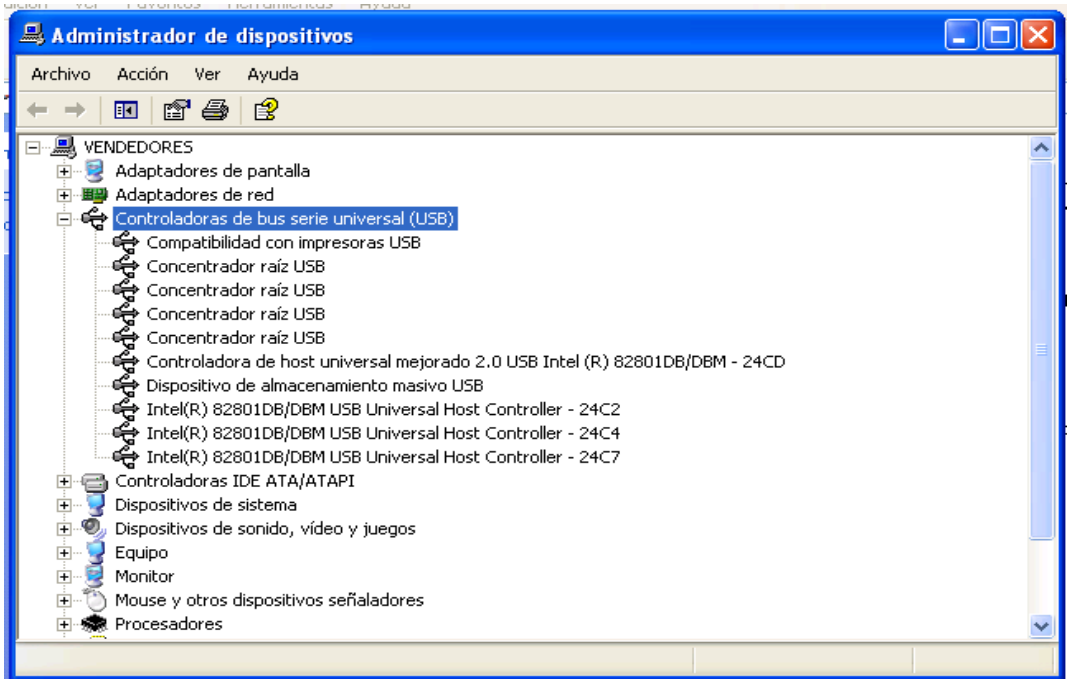


Figura 7.9.1.1. Puertos USB habilitados en computadora de vendedores

La figura 7.9.1.2 muestra una memoria flash insertada en computadora de vendedores

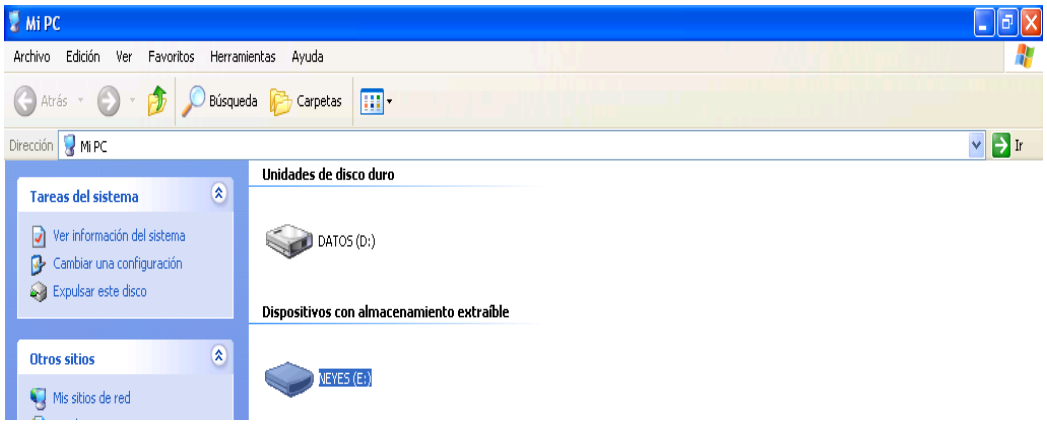


Figura 7.9.1.2. Flash insertada en computadora de vendedores

Las palm de los vendedores puede ser utilizada por terceras personas, en la cual no existe un registro de eventos para poder dar soluciones técnicas cuando exista un problema en el mismo, provocando así un serio problema al momento de dar mantenimientos. A menudo suelen suceder problemas con las palm a las cuales se da las respectivas soluciones para que puedan entrar a producción lo más pronto posible.

CAPITULO 8

"Estrategia de la solución"

8.1 Recomendaciones de la auditoría de políticas de seguridad

8.1.1 Alcance

Este manual de políticas de seguridad es elaborado de acuerdo al análisis exhaustivo de los riesgos y de vulnerabilidades en la compañía Italimentos Cía. Ltda. Por consiguiente el alcance de estas políticas, se encuentra a la espera de que cumplan a la medida toda la empresa y en especial el departamento de sistemas.

8.1.2 Objetivos

Los objetivos de una auditoría de seguridad con políticas claramente establecidas y bien elaboradas son inmediatos, ya que Italimentos trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- "Aumento de la productividad de la compañía.
- Aumento de la motivación del personal al cumplir con su trabajo.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales entre el personal.
- Ayuda a formar equipos confiables.
- Mejora del ambiente laboral para los recursos humanos."[62]

8.1.3 Introducción

La seguridad informática ha sido en los últimos tiempos de suma importancia, debido a las nuevas plataformas tecnológicas disponibles que existen la actualidad. El Internet y las redes LAN son herramientas claves para cualquier daño físico o lógico en un ambiente informático, ha abierto nuevas ideas a las empresas para mejorar su productividad y poder investigar más allá de lo que puede llegar una empresa en el ámbito de Seguridad, lo cual lógicamente ha traído consigo, la aparición de nuevas

62 http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml

amenazas para los sistemas de información. Estos riesgos que se enfrentan cada día han llevado a que se desarrolle un documento de sugerencias para el uso adecuado de estos riesgos tecnológicos en lo cual las recomendaciones van hacer de mayor provecho para el futuro de la empresa, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa de Italimentos.

8.1.4 Análisis de las razones que fortalecen la aplicación de las políticas de seguridad informática.

En la actualidad la mayoría de organizaciones enfatizan sus esfuerzos para definir posibles políticas de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas empresas alcanzan el éxito ya que el problema principal es de convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

A la vez otro problema viene a ser el departamento de sistemas ya que la falta de estrategia al momento de la adquisición del material informático por parte del administradores de sistemas o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como el mal gasto de dinero en adquisiciones que no valen la pena.

Esta problemática ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos, que en muchos casos comprometen información de suma importancia para la compañía. "Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean acogidas, deben aplicar las estrategias o recomendaciones para que se cumplan con mayor facilidad su misión y visión, con el propósito de que quienes toman las decisiones reconozcan su importancia e incidencias en las utilidades de la empresa.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la empresa, con ello estamos confiados en responder a intereses y necesidades empresariales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y adquisición del material para compromisos adquiridos con la empresa."[63]

8.1.5 Responsabilidades

Es responsabilidad del jefe del departamento de sistemas, desarrollar, someter a revisión y divulgar los Procedimientos de Seguridad en adición a los demás medios de difusión tecnológica como es la intranet, email, sitio web oficial, revistas internas. Así mismo, es responsabilidad del supervisor inmediato capacitar a sus empleados en lo relacionado con las recomendaciones de Seguridad que colocaremos posteriormente.

8.1.6 Definición de políticas de seguridad informática

En esta parte del capítulo el documento se presenta una propuesta de políticas de seguridad, como un recurso para eliminar los posibles riesgos a los que puede estar propensa la compañía Italimentos. Para ello se realizará unas políticas que deben ser acatadas por cualquier personal de la empresa.

8.1.7 Disposiciones generales

8.1.7.1 Medidas, controles, procedimientos, normas y estándares de seguridad.

El presente documento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la compañía Italimentos. Para mayor comprensión se tomará en cuenta los siguientes cargos que se entenderá por:

8.1.7.2 Comité

Al equipo integrado por la alta gerencia, gerencias por departamentos, los jefes de área y el personal administrativo convocado para fines específicos como:

- Adquisiciones de hardware y software.

63 http://www.univalle.edu/publicaciones/journal/journal18/pagina17.htm

- Establecimiento de estándares de la compañía tanto de hardware como de software.

- Establecimiento de la arquitectura tecnológica del personal.

8.1.7.3 Administración de informática

Está integrada por la gerencia y jefes de área, las cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.

- Elaborar y efectuar seguimiento del plan maestro de informática.

- Definir estrategias y objetivos a corto, mediano y largo plazo.

- Mantener la arquitectura tecnológica.

- Controlar la calidad del servicio brindado.

- Mantener el inventario actualizado de los recursos informáticos.

- Velar por el cumplimiento de las políticas y procedimientos establecidos.

Para la realización de este documento, se entiende por políticas en informática, al conjunto de reglas obligatorias, que deben observar los jefes de sistemas responsables del hardware y software existente en Italimentos, siendo responsabilidad de la administración del sistema, vigilar su estricto reglamento en el ámbito de las políticas de seguridad para que sea tomando las medidas preventivas y correctivas en su debido tiempo.

Estas normas inciden en la adquisición y el uso de los bienes y servicios informáticos, las cuales se deberán de cumplir, por aquellos problemas que intervengan directa o indirectamente en ello.

La jerarquía mayor de los sistemas informáticos de Italimentos es la gerencia, y el organismo competente para la aplicación de este documento es el comité.

Las políticas que se expondrán, son de observancia para el uso debido de las contraseñas informáticas, en Italimentos, cuyo incumplimiento generará problemas en responsabilidad administrativa; teniendo en cuenta lo que puede ocasionar en los departamentos administrativos de sistemas de toda la compañía.

Italimentos deberá contar con un jefe o responsable, en el que recaiga la administración de los bienes y servicios, que vigilará la correcta aplicación de los documentos establecidos por el comité y demás disposiciones aplicables.

Aquí colocamos algunas disposiciones generales para el buen manejo de las medidas, controles, procedimientos, normas y estándares de seguridad que se deben de emprender con suma importancia para la empresa de Italimentos.

Italimentos deberá contar con un jefe o responsable, en el que recaiga la administración de los bienes y servicios, que vigilará la correcta aplicación de los ordenamientos establecidos por el comité y demás disposiciones aplicables.

Con esto ya colocaremos las sugerencias que se deben de aplicar en el capítulo tres como una norma que les ayudará para el proceso informático y organizacional de Italimentos.

8.1.8 Privilegios del personal

- "Sugerimos que todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

- Ningún usuario recibirá un identificador de acceso a la red de comunicaciones, recursos informáticos o aplicaciones hasta que no acepte formalmente la política de seguridad vigente.

- Todos los usuarios tendrán acceso autorizado únicamente a aquellos datos y

recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

- Tengan presente que los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

- Proteger en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso cualquiera que sea el soporte en que se encuentren contenidos los datos.

- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

- Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo o carpetas compartidas de la red y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad de ser divulgados.

- Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas." [64]

64 http://mgeseguridadinformatica.wordpress.com/paguina2/

8.1.9 Contraseñas

- "Sugerimos que el usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.

- No deben usarse contraseñas que sean idénticas o similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores. "[65]

- "Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

- Está prohibido el uso de contraseñas en grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

- Las contraseñas iníciales sean emitidas a un nuevo usuario cuando sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a tres el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema.

- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la

65 http://www.ilustrados.com/tema/4923/Politicas-Procedimientos-seguridad-Informacion.html

pantalla y suspender la sesión. El periodo recomendado de tiempo es de quince minutos. El re-establecimiento de la sesión requiere que el usuario se autentique mediante su contraseña o tarjeta inteligente.

- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran como atentatoria de las políticas de la Compañía, teniendo en cuenta su respectiva sanción."[66]

- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos y numéricos para los usuarios.

- La longitud mínima de las contraseñas será igual o superior a once caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales para los servidores.

- Las contraseñas para usuarios se configurarán para un corto período de tiempo, una vez expirado dicho período, se desactivarán de los sistemas para una nueva configuración de la contraseña para usuarios y servidores.

- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

- Si un usuario tiene sospechas de que su acceso autorizado ya sea por un identificador de usuario y contraseña está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración del sistema.

- "La contraseña no debe hacer referencia a ningún concepto, objeto o idea

66 http://www.sabetodo.com/contenidos/EplpVplEZlTOfazBIB.php

reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada treinta días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos."[67]

8.1.10 Cifrado de la información

"Hoy en día la información fuera de nuestra empresa puede ser tanta o más que la disponible en nuestra empresa. Por eso poco a poco tenemos que ir adaptando el trabajo con este tipo de información de forma distinta a como lo venimos haciendo. El cifrado de información es una tarea pendiente en pequeñas y medianas empresas.

No se trata sólo de dispositivos portátiles que puedan tener nuestros trabajadores en movilidad, ya sean portátiles, teléfonos móviles o simplemente memorias USB que pueden extraviarse en un momento dado, dejando expuestos datos o ficheros de clientes que pueden caer en manos inadecuadas. No sólo se trata del perjuicio por la pérdida de información sino también el descrédito de nuestra empresa.

Imaginaros un empleado que olvida su móvil en una visita a un cliente, donde se da cuenta que se lo ha olvidado y pasa a recuperarlo lo antes posible. No ha habido ninguna pérdida, pero imaginad que al cliente le da por investigar que tiene este teléfono de

67 http://mgeseguridadinformatica.wordpress.com/paguina2/

especial, y accede a nuestro CRM[68] o a ficheros de clientes de la competencia.

No estamos hablando de un par de archivos, sino que hoy en día un dispositivo móvil puede contener todos los detalles relativos a nuestra empresa, clientes, situaciones financieras, datos personales, etc. Son cuestiones que no dejaríamos en una nota adhesiva en nuestra empresa y tampoco podemos hacer lo mismo con nuestros soportes informáticos para la información.

Por eso y como medida preventiva para evitar o intentar dificultar la fuga de información en las empresas es necesario implantar sistemas de cifrados de datos. Si no para todas las carpetas de información, si para las que contengan información más sensible. Ya sea a nivel de hardware o de software existen soluciones adecuadas para el mundo de la pyme cuya adopción es más que recomendable.

Por la misma razón que tenemos distintos perfiles de acceso a la información en las empresas, carpetas con contraseñas, etc. debemos buscar que si se rompen estas medidas básicas de seguridad no puedan acceder a la información a través del cifrado de la misma. Muchas empresas no se plantean estos aspectos, luego cuando pasa algo no sirve lamentarse."[69]

8.1.10.1 Sugerencia

Sugerimos que para la realización del cifrado de información se utilice el software Truecrypt. *La figura 8.1.10.1.1 muestra la interfaz de instalación de la aplicación Truecrypt.*

68 CRM: Gestión de relaciones con clientes
69 http://www.tecnologiapyme.com/hardware/el-cifrado-de-informacion-es-una-tarea-pendiente-en-la-pyme

Figura 8.1.10.1.1 Interfaz de la instalación del TRUECRYPT

"Es un software para el cifrado de los datos ya que Proteger los datos sensibles que contienen los ordenadores y sistemas de almacenamiento de nuestra empresa debería ser algo prioritario en cualquier compañía, ya sea por nuestro interés ya por que nos obliga la ley a ello. Hemos hablado de soluciones de hardware que incorporan el cifrado de datos, pero tenemos alternativas en el lado del software capaces de proteger el contenido de cualquier tipo de disco o memoria "normal". Vamos a hablar en concreto de TrueCrypt, una aplicación multiplataforma, gratuita y de código abierto que permite cifrar casi cualquier tipo de medio de almacenamiento.

Protege el contenido utilizando diferentes algoritmos entre los que podemos elegir, es bastante sencillo de utilizar y el resultado final es una ubicación protegida a la que tendremos que acceder mediante una contraseña, sin la cual todo el contenido de la misma permanece cifrado.

Es un software con multitud de opciones, y conocerlo a fondo tiene su virtud. Sin embargo las operaciones básicas son más bien sencillas, aunque conviene leer detenidamente las instrucciones si no queremos llevarnos alguna sorpresa. Entre sus características principales destacaría las siguientes.

- Se pueden crear volúmenes virtuales cifrados, en esencia un disco virtual en el que todo lo que coloquemos quedará automáticamente protegido.

- Es capaz de proteger al completo particiones, discos, y unidades de almacenamiento externas, incluso aquellas en las que Windows esté instalado, en cuyo caso pide una contraseña antes de arrancar el disco.

- El cifrado se realiza en tiempo real y de forma automática, basta con colocar el archivo en el volumen protegido.

- Como salvaguarda frente a intrusiones, los volúmenes pueden quedar ocultos e imposibles de diferencia de otro tipo de datos.

La figura 8.1.10.1.2 muestra la interfaz de elección del tipo de volumen.

Figura 8.1.10.1.2. Interfaz de tipo de Volumen que tiene el TrueCrypt

¿Es mejor solución que los discos cifrados por hardware? Pues depende del uso que le vayamos a dar. Si pensamos proteger unidades de disco fijas o externas que únicamente vayamos a utilizar en nuestro equipo es una alternativa más económica, aunque tenemos que utilizar y configurar el software. Si hablamos de una memoria flash USB que vamos a ir enchufando a distintos equipos podemos tener algún que otro problema, tal y como señalaba nuestro lector Metagrama en los comentarios de una entrada anterior.

Hecha esta apreciación, decir que es un programa realmente útil, ya que es mucha la información que necesitamos proteger en las empresas, y en algunos casos estamos

incluso obligados a ello por la Ley de protección de los datos versiones para Windows, Linux y Mac OS X, gratuito y relativamente sencillo de configurar, es una de las mejores soluciones de este tipo que nos podemos agenciar."[70]

8.2 Recomendaciones de la auditoría de gestión de activos.

8.2.1 Alcance

Este manual de gestión de activos es elaborado de acuerdo al análisis realizado día a día en la empresa de Italimentos. Por consiguiente el alcance de ésta auditoría en gestión, se encuentra a la espera de que cumplan a la medida toda la empresa y en especial el departamento de sistemas.

8.2.2 Objetivos

Los objetivos de una auditoría de gestión de activos en la empresa de Italimentos son dos, que son de suma importancia para la producción de la compañía y esto se lo resume en:

- Da visibilidad al coste y beneficio asociado con dar el servicio apropiado y acordado.
- Minimizar el coste de la vida del activo incluyendo la exportación del producto, mantenimiento y la eliminación del activo que posee en la empresa.

8.2.3 Introducción

Para una correcta administración de activos, generalmente intervienen las siguientes áreas:

1. Descripción del activo en el sistema
2. Definición del estándar de servicio
3. Rendimiento actual del activo
4. Acciones planificadas

70 http://www.tecnologiapyme.com/software/truecrypt-software-para-el-cifrado-de-datos

5. Costes
6. Beneficios
7. Mejoras potenciales

8.2.3.1 Descripción del activo en el sistema

Aquí se describe problemas con el objetivo de reducir y explicar que activos se encuentran en uso para solucionar problemas definidos. Se explica porque existen activos y que pasaría si no existieran, para ello se debe identificar las dependencias ende los diferentes activos.

8.2.3.2 Definición del estándar de servicio

Aquí se define el rendimiento que deben tener los activos y bajo qué condiciones, así como un estándar de servicio para los diferentes activos del sistema, de tal manera que el sistema debe funcionar de manera eficiente.

Generalmente consta de dos partes: las especificaciones del rendimiento y el nivel de condiciones. El nivel de condición debe tener en cuenta las consecuencias de un fallo, la posibilidad de un fallo de un activo y la velocidad a la que este puede ocurrir. Es importante entender qué función debe cumplir cada activo, y que mínimo de condiciones es considerado como aceptable.

8.2.3.3 Rendimiento actual del activo

"Se debe definir en qué condiciones se encuentran los activos actualmente. Para ello debe elaborarse un inventario de todos los activos con identificadores únicos y que además incluya información como propietario del activo, edad, tiempo de vida estimado, etc.

Este paso es importante para conocer el estado en el que se encuentran los activos en la actualidad.

8.2.3.4 Acciones planificadas y gestión del ciclo de vida

Mediante acciones a corto plazo es necesario conocer entre el punto donde nos encontramos y el punto en donde queremos estar. Si se tiene ya un estándar de servicio definido, está ya permite realizar acciones a un menor coste posible, creando un enfoque innovador en el método para cumplir el estándar designado. Con esto se podrán tomar qué acciones mantendrán los activos sobre la condición mínima establecida y con qué capacidad desarrollara su función en el mejor modo posible.

8.2.3.5 Costes

Hay que conocer cuáles son los costes a corto, medio y largo plazo para el sistema de activos. Se debe realizar una planificación de costes para la explotación, mantenimiento, reparación y reemplazo de los activos para mantener el servicio. En este paso se necesita revisar y actualizar anualmente para poder tener en cuenta dotaciones económicas. Después de este periodo, se debe planificar grandes gastos previstos a medio plazo, y permitir disponer de suficiente tiempo para realizar una tasación en profundidad del coste de activos.

Es necesario conocer el coste de las acciones planificadas, así como la gestión y gastos indirectos relacionados con activos en especial. Es también importante desarrollar esfuerzos necesarios que permitan optimizar el servicio.

8.2.3.6 Beneficios

Todos los activos deben ofrecer una serie de beneficios que puedan ser medidos, pero lo más habitual es transformar el servicio en una cifra económica. Otros beneficios son más difíciles de medir como puede ser de tipo social o medio ambiental, aunque es importante dejan un registro de ellos. Todo esto influye a demostrar que el plan de gestión de activos es beneficioso para la empresa y que el gasto que se genera está justificado por el beneficio de la empresa.

8.2.3.7 Mejoras

Estas mejoras representan cambios en los estándares de los servicios y son gestionadas como proyectos completos, permitiendo gestionar los gastos, comparar diferentes opciones para así seleccionar la mejor opción."[71]

8.2.4 Beneficios de la gestión de activos de Italimentos.

Todos los activos deben brindar una serie de beneficios que pueden ser accesibles o específicamente explicados ya sea manualmente en la empresa, por tal motivo lo más interesante es que se debe de transformar el estándar de servicio en una cifra económica para ver cómo ha crecido la producción de la empresa, otro beneficio también es generan gastos innecesarios por la justificación que se obtiene en cada activo esto es beneficioso para la empresa por el gasto justificado que se realiza a cada activo adquirido.

8.2.5 Responsabilidades

Es responsabilidad del jefe del departamento de sistemas y del departamento de compras, desarrollar, someter a revisión y divulgar al departamento de compras para su respectiva adquisición del activo ya sea por medio de email o por escrito. Así mismo, es responsabilidad del supervisor inmediato capacitar a sus empleados en el manejo adecuado del activo para su respectiva configuración y soporte del mismo.

8.2.6 Definición de gestión de activos

Es planificar tácticamente para la realización de una gestión de la infraestructura y activos de la empresa en Italimentos, con la finalidad de cumplir un estándar de servicio al momento de cubrir un activo y como se encuentran relacionados entre sí, obligando a la alta gerencia a determinar un nivel de servicio apropiado para todos los trabajadores que poseen activos.

8.2.7 Disposiciones generales

El presente documento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la compañía Italimentos. Para mayor comprensión

71 http://es.wikipedia.org/wiki/Plan_de_gesti%C3%B3n_de_activos

se tomará en cuenta los siguientes cargos de los que serán imprescindibles en el momento de gestionar un activo:

8.2.7.1 Administración de informática

Está integrada por el Jefe de departamento de Sistemas, el cual es el responsable de:

- Velar por el funcionamiento de la tecnología informática que se utilice en los diferentes activos.
- Elaborar y efectuar seguimiento del activo informático.
- Buscar soluciones que a la larga faciliten en la producción de la empresa.
- Buscar soluciones del activo innecesario en la empresa.
- Realizar el pedido del activo necesario para la empresa.
- Dar a conocer las características de los activos a ser adquiridos.

Estas normas inciden en la adquisición y el uso de los bienes y servicios Informáticos, las cuales se deberán de cumplir, por aquellos problemas que intervengan directa o indirectamente el activo.

8.2.7.2 Inventario de soportes y actualizaciones.

En el análisis que realizamos en Italimentos, vimos la necesidad de implementar las siguientes sugerencias que a la larga será de mucha importancia para realizar un inventario de soportes y actualizaciones sin ningún inconveniente:

Cada soporte informático será identificado mediante un código único. Este identificador será representado gráficamente mediante un código de barras para facilitar su control y lectura, siempre que sea físicamente posible, la etiqueta estará firmada y sellada.

En cada soporte físico inventariado queda adherida en el activo una etiqueta con el código de barras, etiqueta con características físicas tales que no resulte posible despegarla sin que se produzca su destrucción, con el fin de que no pueda ser suplantado el soporte físico original por otro de similares características.

El inventario de soportes informáticos debe de ser detallada la fecha de adquisición, proveedor, características del elemento, destino que se le da, estado en que se encuentra

activo o desechado, en caso de ser desechado se adjuntará la fecha y causa. Así mismo ha de constar la valoración que le ha otorgado el responsable de seguridad de ficheros y sistemas.

8.2.7.3 Registro y actualización de entrada y salida de información

- "Sugerimos que la información de la compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la gerencia de informática.
- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.
- Siempre que sea posible, deba eliminarse información confidencial de de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la compañía.
- No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo o se va a imprimir información confidencial de la compañía.
- El personal que utiliza un computador portátil que contenga información confidencial de la compañía, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada."[72]
- Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifradas. Para tal fin debe utilizarse Outlook Express u otros productos previamente aprobados por la gerencia de informática.
- Los empleados y gerentes por departamentos de la compañía no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a

72 http://www.sabetodo.com/contenidos/EplpVplEZlTOfazBIB.php

otros para que lo hagan. La compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

- El uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.
- Tomar en cuenta que cierta información que está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la compañía, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la compañía sin la debida aprobación
- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

8.2.8 Medidas a utilizar cuando un soporte vaya ser desechado o reutilizado

El Responsable de Seguridad de ficheros y sistemas debe de crear en los locales o cuartos protegidos una zona destinada a soportes de almacenamiento desechado.

Transcurrido el plazo de tres meses y tras asegurarse el responsable de la destrucción de los datos, el soporte debe salir de las instalaciones de seguridad y ser dado de baja del inventario de soportes físicos de almacenamiento. Para ello se adoptarán las siguientes medidas adecuadas como sugerencias cuando un soporte va ser desechado o reutilizado, en función de los datos que contenga y el tipo de soporte ya sea magnético o papel, que no estaría incluido en el presente procedimiento, aunque puede proceder su destrucción.

- Sugerimos que en los soportes, servidores y portátiles se debe de realizar un borrado completo cuando va ser desechado, sobre grabando en algún backup cifrando la información importante para que el contenido anterior no resulte accesible ni con mecanismos o dispositivos sofisticados.

- Los soportes que no forman parte de un equipo o son extraíbles, se pueden desmagnetizar si se trata de soportes magnéticos e incinerar, triturar o destruir en cualquier caso.
- Si los soportes son ópticos y no regrabables se puede triturar en equipos adecuados, o destruir.
- Si se entregan a una entidad para mantenimiento, y no ha sido posible borrarlos, o bien se intenta la recuperación o es para su destrucción y en especial si no existe un contrato se debe de exigir clausulas de confidencialidad, y en su destrucción la confirmación escrita.
- Hasta que proceda al tratamiento respectivo, borrado o destrucción, los soportes deben de estar protegidos frente al acceso no autorizado.
- Se deberá dar de baja en el inventario, anotando el método utilizado incinerado y entregando a departamento de sistemas para su respectiva revisión.

8.2.9 Almacenamiento de contraseñas

- "Sugerimos que el usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.
- No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- Las contraseñas iníciales emitidas a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a tres el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.
- Para el acceso remoto a los recursos informáticos de la compañía, la combinación del ID[73] de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas o tarjetas inteligentes.
- Si no ha existido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de quince minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad.
- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la compañía.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos."[74]

[73] ID: Identificador Unico
74 http://www.ilustrados.com/tema/4923/Politicas-Procedimientos-seguridad-Informacion.html

8.2.10 Lugar de almacenamiento de contraseñas

- Sugerimos que toda bitácora ó logs y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría.
- Todo archivo importante deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas y ser almacenados en aplicaciones como KeePass[75] ó Last Pass[76] que son Open Source[77].
- Los servidores de red y los equipos de comunicación como routers, deben estar ubicados en locales apropiados, protegidos contra daños y robo.
- Se debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso por ejemplo, tarjetas de proximidad.

8.2.11 Etiquetado de activos

- Sugerimos que realicen un inventario ya sea en papel o por vía mail donde permitan identificar, realizar seguimientos, asegurar y recuperar sus equipos de forma más fácil, sencilla y accesible.
- La forma más sencilla de realizar un seguimiento de los activos de hardware es etiquetarlos físicamente durante la adquisición del producto para su nombramiento como activo, la etiqueta será de código de barras identificadas con una serie de números alfanuméricos de diez caracteres para procesarla con el nombre del dueño
- Se realice informes sobre los activos cada mes ya que ayudan a integrar nuevos activos en los sistemas de administración de activos existentes.

[75] KeePass: Aplicación para almacenamiento de contraseñas
[76] LastPass: Aplicación para almacenamiento de contraseñas
[77] Open Source: Software Gratuito.

- Se deberá enviar un informe por mail cada día, cada semana o cada mes del seguimiento de todos los activos que se enviaron en el plazo anterior y de los que van a ser adquiridos por el departamento de sistemas.

8.2.12 Cuentas de usuario

- "Sugerimos que cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
- No debe concederse una cuenta a personas que no sean empleados de Italimentos Cía. Ltda., a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de treinta días.
- Los privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo. Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas o tarjetas inteligentes.
- Se prohíbe el uso de cuentas anónimas o de invitado y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.
- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de treinta días.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

- Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo."[78]

8.3 Recomendaciones de la auditoría de seguridad relacionada con el personal.

8.3.1 Alcance

Este manual de Seguridad relacionada con el personal es elaborado de acuerdo al análisis arduo realizado día a día en la empresa de Italimentos Cía. Ltda., y con las entrevistas que se compartió al personal que ayudaron para que se realice efectivamente este tema. Por consiguiente el alcance de ésta auditoría en seguridad, se encuentra a la espera de que cumplan a la medida toda la empresa y en especial el departamento de sistemas para que no se produzca graves problemas posteriormente.

8.3.2 Objetivos

Los objetivos de una auditoría de seguridad relacionada con el personal en la empresa de Italimentos son de suma importancia para que la empresa no tenga problemas en el acceso de personal a datos o información de suma importancia y esto se lo resume en:

- Definir sugerencias que permitan a la empresa de Italimentos hacer el mejor uso posible de los recursos informáticos, para promover los objetivos de la empresa en un ambiente seguro y claro.
- Entender el adecuado uso de recursos informáticos, para que cada personal en su puesto de trabajo revise el funcionamiento del activo, y su compromiso a la no divulgación de datos o información imprescindible de la empresa.
- Garantizar la seguridad, rendimientos y privacidad de los sistemas y máquinas de la empresa como también la de las Italdelis.

8.3.3 Introducción

Los riesgos y las amenazas representan los tipos de acciones donde tienden a ser dañinos con cualquier tipo de información, mientras que la vulnerabilidad conocida también como falencias o brechas representan el grado de exposición a las amenazas

78 http://www.sabetodo.com/contenidos/EplpVplEZlTOfazBIB.php

en un contexto particular o interno de la empresa, la contramedida representa todas las acciones que se implantan para prevenir la amenaza. También debe implementarse no sólo soluciones técnicas cuando se habla de la contramedida, sino que también reflejen la capacitación y la toma de soluciones por parte del usuario además de sus funciones y responsabilidades que se le dan a cada empleado en su puesto de trabajo.

Para que un sistema sea seguro, se debe como primer paso identificar las posibles amenazas y por lo tanto tener una toma de solución adecuada para dicha vulnerabilidad, en donde el objetivo primordial de este informe es de generar sugerencias que se apliquen en la empresa de Italimentos con el fin de categorizar sus errores y dar ideas para el posible arreglo de los problemas suscitados para la reducción de riesgos de intrusos.

8.3.4 Beneficios de la seguridad relacionada con el personal de Italimentos.

Los beneficios para este tipo de seguridad son los más importantes y esenciales en Italimentos ya que ayudan a mantener la ventaja competitiva en el ámbito de embutidos no solo a nivel local sino nacionalmente por ello su rentabilidad va ser respuesta de todo lo planeado en los objetivos de la empresa viendo al personal con remuneraciones constantes pero con la ayuda en el respeto de las leyes y reglamentos que se rigen en la fábrica, y lo más importante previniendo la divulgación de información confidencial que se dan internamente en sus puestos de trabajo, protegiendo los datos y resguardando las políticas de la empresa.

8.3.5 Responsabilidades

Es responsabilidad del todo el personal de Italimentos Cía. Ltda., hacer que se respeten las seguridades de la empresa con el fin de que se cumplan todas las sugerencias que ponemos a continuación y aplicar todo lo que sea necesario para que la empresa surja a nivel nacional como se lo establece en su visión.

8.3.6 Definición de seguridad relacionada con el personal

Como definición es establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la compañía de Italimentos. Esa

información asegura un nivel de protección adecuado donde clasifica las necesidades, prioridades previstas para su tratamiento adecuado y las sugerencias que se aplicaran para la seguridad relacionada con el personal.

8.3.7 Disposiciones generales

El presente documento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la compañía Italimentos Cía. Ltda. Para mayor comprensión se tomará en cuenta los siguientes cargos de los que serán imprescindibles en el momento de gestionar un activo y poner en práctica la seguridad que se realizará en este capítulo.

8.3.7.1 Gerentes

Por lo general los ejecutivos o los jefes de departamentos son responsables de la gestión y protección de la información. Pueden tomar todas las decisiones necesarias relativas a la información bajo su control con el fin de mantener su integridad y su confidencialidad.

8.3.7.1.1 Administración de informática

Los administradores de activos son generalmente miembros del departamento de seguridad de la información donde administran el sistema y operan el control de accesos a los datos, mantienen la gestión de los sistemas procesando información y monitoreando el mismo.

8.3.7.1.2 Usuarios

Son miembros del personal de la empresa o terceros que tienen acceso y utiliza los datos de la compañía únicamente con fines de negocio o según lo dispuesto por la empresa. Pide al administrador del sistema el permiso de acceso a la información.

8.3.7.2 Uso de recursos informáticos.

En el análisis que realizamos en Italimentos. Cía. Ltda., vimos la necesidad de implementar las siguientes sugerencias que a la larga será de mucha importancia para realizar un uso de recursos informáticos sin ningún inconveniente, en donde colocamos a continuación para su respectivo cumplimiento:

- Sugerimos que el almacenamiento de la información requerida para el desarrollo de las actividades laborales en los equipos y sistemas de información que son suministrados por Italimentos para este fin, eviten tener dicha información en otros equipos sino en dispositivos como flash o CD que rote solo internamente.
- Evitar utilizar, recibir, mantener o copiar información o sistemas de información, que estén protegidos por leyes de derechos de autor, así como la distribución ó instalación de software pirata u otros productos que no estén licenciados por Italimentos, incluidos fotografías de revistas, libros, música u otras fuentes.
- "Evitar tanto en su equipo de cómputo como en las que estén a su alcance que se almacene material con contenido pornográfico u ofensivo en los equipos asignados por la empresa.
- Apoyarse para la Instalación de software libre en los lineamientos definidos por la empresa, evitando utilizar software diferente al establecido por Italimentos para el desarrollo de las actividades. En caso de requerir software adicional deberá hacer la solicitud por escrito. La responsabilidad sobre el software no autorizado en los equipos asignados es de la persona sobre la cual recae la asignación del equipo.
- No introducir intencionalmente programas “maliciosos” ó virus dentro de la red de datos y comunicaciones de la empresa, ni acceder o forzar accesos a información sobre la cual no se tengan los permisos y autorizaciones adecuadas.
- Que el escaneo de puertos ó el análisis de tráfico y vulnerabilidades de la red con el propósito de evaluar vulnerabilidades de seguridad, sólo se considera adecuado cuando se lleve a cabo por parte de los encargados de la seguridad de la información en Italimentos, u otras personas con una autorización previa.
- Evitar realizar ataques para aprovechar vulnerabilidades identificadas en los servicios brindados por la compañía o sobre la infraestructura de servicios de Italimentos con la finalidad de interrumpir, interferir, deshabilitar y en general cualquier aspecto que afecte la prestación de los servicios de Italimentos Cía. Ltda., o para propósitos que vayan en contra las personas, instituciones o deriven en incumplimiento de las políticas que se rigen en la fábrica.

- Evitar que se ejecute cualquier forma de monitoreo de red, con la finalidad de interceptar datos ó mensajes que viajan por las redes de comunicación de la compañía.
- Evitar que se adicionen equipos de cómputo o dispositivos a la red de datos que no hayan sido autorizados por la compañía.
- No enviar mensajes de correo no solicitados, incluyendo material publicitario enviado por correo o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado dicho material como el correo Spam, correos electrónicos masivos, no solicitados o no autorizados.
- No generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
- El uso de los servicios de telefonía debe ser orientado al cumplimiento de los objetivos internos y del cargo para el cual fue contratado y evitar otros usos sin las debidas autorizaciones.
- La utilización de los privilegios en los sistemas de información debe ser realizada para el cumplimiento de su labor por lo cual evitar el obtener información de usuarios que pueda considerarse violatoria de los derechos de intimidad.
- Evitar realizar cambios no autorizados, e ir en contra de las funcionalidades para los cuales los sistemas de información están definidos que impacten la confidencialidad, integridad y disponibilidad de la información y los medios de procesamiento."[79]

8.3.7.3 Funciones y obligaciones del personal.

Gerente

- Comprende los principales riesgos relacionados con los usos internos de un tipo específico de información.
- Determina el porcentaje de sensibilidad en nivel de criticidad de la información teniendo en cuenta su clasificación ya sea privada, confidencial o pública.

79 http://www.univalle.edu.co/politicainformatica/Pol_URI.html

- Especifica los métodos de control adicional requerido para proteger esta información.
- Suscribe las peticiones de los usuarios para acceder a la información.
- Revisa el acceso de los usuarios de la empresa la lista de control para determinar si retirarle privilegios y también poder ingresar nuevos usuarios.

Administrador

- Guarda físicamente la información.
- Realiza manuales de usuario para la elaboración y monitorización de la información.
- Mantiene la confidencialidad de la información del equipo de acceso.
- Instala mecanismos de seguridad en los activos informáticos.
- Realiza copias de respaldo regularmente y restaura datos de copias de seguridad cuando sean necesarias.

Usuario

- No utilizar los sistemas o información sin autorización.
- Utiliza equipos de acceso de seguridad proporcionada por el administrador.
- Cumple con los controles establecidos por el departamento de sistemas.
- Informe de errores de la información y anomalías del sistema por parte del administrador.
- Informe de las vulnerabilidades de la información y violaciones al departamento de seguridad de información.

8.3.8 Accesos de personal que tratan datos personales

- Sugerimos recoger y tratar datos personales solo del personal de la empresa para finalidades legítimas y definidas, y hacerlo cumpliendo determinadas obligaciones formales.
- Captar los datos mediante procedimientos que garantice que se ha informado adecuadamente al personal de la empresa cuyos datos se trate de aspectos

importantes y principales de tratamiento sobre sus derechos y obligaciones que ejerzan.

- Mantener los datos debidamente actualizados y cancelarlos cuando ya no sean necesarios o no estén trabajando en la empresa.
- Implantar medidas que garanticen la seguridad de los datos en sus dimensiones de confidencialidad donde el personal no autorizado de la empresa puedan alterar de manera ya sea accidental o por su propia cuenta para beneficio propio o de terceros.
- Implantar medidas donde la disponibilidad también es importante cuando hablamos de catástrofes ya sea incendio y el método de recuperación de datos es lo más importante o los sistemas que los soportan.
- Elaborar un documento de seguridad para el cumplimiento del personal que describa medidas exigidas por la empresa de Italimentos. Cía. Ltda., tales como la respuesta ante incidentes de seguridad los deberes de los empleados o el control de salidas y entradas de datos.
- Registrar y mantener actualizados los ficheros de datos en el registro que posean para la protección de datos personales en la empresa de Italimentos.
- Adoptar una correcta política en relación con las posibles sesiones a los activos de información por parte de personal que no sea de la empresa.
- Que al momento de contratar a personal por enfermedades o cualquier motivo no previsto se realice una sesión para que pueda acceder a los datos y trabajar sin que sepa de contraseñas de sesiones de personal titular del activo.
- Que al momento de querer realizar envío de datos por medio de navegadores de correos se dé información de aviso del mismo y se realice la transferencia de datos personales fuera del espacio donde trabaja por parte del departamento de sistemas.
- Realizar periódicamente la comprobación de los procedimientos que se realicen para la seguridad de los datos.

8.3.9 Accesos de personal a soporte de datos e información.

- Sugerimos dar a conocer al personal las áreas protegidas sólo si es necesario para el desarrollo de sus funciones en la empresa con el fin de que no ingresar a lugares donde se guarden los soportes de información.
- Tener bajo candado y alejado del personal de la empresa los soportes de información.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión del gerente del departamento al que está trabajando.
- Bloquear físicamente e inspeccionar periódicamente las áreas protegidas en donde se guardan la información de la empresa.
- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas.
- Se realizará un registro ya sea en papel de todos los accesos de personas ajenas a la información requerida autorizadas por la gerencia.
- Impedir el ingreso de equipos de computación externos, móviles, cámaras fotográficas, de video, audio o cualquier dispositivo de equipamiento que registre información sin autorización.
- Disponer de un Backup de sus datos alejados del personal ajeno a la información, esto lo realizará el departamento de sistemas.
- Conservar una copia de cada mes, al menos durante un año conservando la información de cierta antigüedad.
- Para poder obtener la información guardada en los soportes comunicar al departamento de sistemas para la revisión de la información y entrega del mismo.

8.3.10 Confidencialidad con todo el personal.

En el tema como lo es la confidencialidad con todo el personal hace referencia a todos los documentos, información y material divulgado por cualquiera de las partes ya sea por escrito, verbalmente o por cualquier activo informático en cuanto a las medidas que

se debe de tomar en cuenta para que las condiciones de que se den para el personal se acaten llegando al acuerdo necesario para que la empresa no tenga problemas a futuro.

Para ello colocamos algunas clausulas de confidencialidad para que el personal acaten esta disposición, y la empresa de Italimentos no tenga problemas de divulgación de información.

- Sugerimos que toda la información o datos que se describen en la empresa ya sea en activos informáticos como papeles, cualquiera que sea su forma, está sujeto a las disposiciones del presente documento o convenio con el personal de la empresa donde se establece el carácter confidencial y la fecha de divulgación se indica claramente o que, cuando se reveló verbalmente, su carácter confidencial, se confirma por escrito dentro de los treinta días siguientes de la divulgación.
- La persona siempre y cuando sea autorizado para hacerlo, deberá remitir al departamento de sistemas la información procesada para que pueda salir de las instalaciones de la empresa.
- Toda la información divulgada por el personal y todas las copias hechas por parte del departamento de sistemas seguirá siendo propiedad de la parte reveladora y deben ser devueltos previo a la revisión por parte del departamento de sistemas.
- Toda información interna de la empresa estará protegido, confidencialmente y manejada por la parte que recibe la información con el mismo cuidado y protección dada a su propia información.
- Solo puede ser utilizada, reproducida o divulgada internamente por personal de la parte receptora, debidamente autorizados por parte del departamento de sistemas.
- Todo el personal de la empresa que tiene en uso de un activo informático no realice trabajos fuera de la empresa ni lleve información procesada por dicha entidad.

- El empleado no debe utilizar de una manera perjudicial para el empleador la información confidencial a la que él o ella tiene acceso a través del desempeño de sus funciones o debido a su posición en la organización.
- El empleado se comprometa a proteger a todas las herramientas de identificación que se le dará como por ejemplo las contraseñas.
- El empleado debe entender que revelar su identificador o ID del usuario está prohibido en el cual donde se cambie por error su contraseña será avisado de urgencia al departamento de sistemas para su nueva configuración.
- Los empleados de la empresa deberán saber que los procesos industriales, programas de software y otras propiedades intelectuales, así como información de los negocios de la compañía y sus socios son activos de gran valor que son especiales e insustituibles para la empresa.
- Que todo el personal debe de saber que para el acceso a la información privilegiada es necesario para el empleado como funciones a comprometerse a no divulgar la información o parte de la información a nadie durante el tiempo que este en la empresa.
- Que los empleados no se usen secretos de la compañía en la parte de lo que es la producción y comercio a beneficio propio o al de cualquier persona, excepto cuando la información ya ha entrado en el dominio público, siempre y cuando el empleado no era el mismo responsable de hacer llegar la información

8.3.11 Comunicación de debilidades en materia de seguridad

- Sugerimos que los incidentes relativos a la seguridad deben de comunicarse a través de canales gerenciales como son el teléfono, celular, etc., tan pronto como sea posible.
- Se debe establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta a incidentes, que establezca la acción que ha de emprenderse al recibir un informe sobre incidentes
- Todos los empleados de Italimentos deben de estar al corriente del procedimiento de comunicación de incidentes de seguridad, y deben de informar de los

mismos tan pronto como sea posible al administrador de seguridad de información de la empresa.

- Deberán implementarse adecuados procesos de Feedback para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados y resueltos los mismos.
- Deberán realizar capacitaciones cada dos meses de incidentes que se pueden producir a los activos informáticos exponiendo los temas los responsables del mantenimiento de sistemas y personal del departamento de sistemas.
- Estos incidentes pueden ser utilizados durante la capacitación a fin de crear conciencia con el personal de Italimentos de la seguridad de usuario como ejemplos de lo que puede ocurrir, de cómo responder a dichos incidentes y cómo evitarlos a futuro.
- Los usuarios de servicios de información deben advertir, registrar y comunicar las debilidades supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios.
- Deberán comunicar estos asuntos al departamento de sistemas tan pronto como sea posible.
- Se deben informar a los usuarios que ellos no deben, bajo ninguna circunstancia, intentar probar una supuesta debilidad, esto se lleva a cabo para su propia protección, debido a que el intentar probar debilidades puede ser interpretado como un potencial mal manejo del sistema.
- Deben advertirse y registrarse los síntomas del problema y los mensajes que aparecen en la pantalla.
- La computadora debe ser aislada, si es posible y debe detenerse el uso de la misma y contactarse con el personal responsable para el respectivo mantenimiento.
- En el momento del mantenimiento debe ser desconectado de las redes de la organización antes de ser activado nuevamente.
- El dispositivo Flash Memory no deben de transferirse a otras computadoras con la información del ordenador que está en mantenimiento.

- Los usuarios no deben de quitar el software que supuestamente tiene la anomalía, a menos que este autorizado por el departamento de sistemas a realizarlo.
- La recuperación debe ser realizada por el personal adecuadamente capacitado y experimentado.
- Deben de implementar mecanismos que permitan cuantifica y monitorear los tipos, volúmenes y costos de los incidentes y anomalías recurrentes o de alto impacto, esto puede señalar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño, costo de casos futuros.
- Estos procesos deben garantizar un trato imparcial y correcto hacia los empleados sospechosos de haber cometido violaciones graves o persistentes a la seguridad.

8.4 Recomendaciones de la auditoría de seguridad física y del entorno.

8.4.1 Alcance

Este documento donde se transcribirá las sugerencias para este capítulo de Seguridad Física y del entorno es elaborado de acuerdo al análisis realizado en la empresa de Italimentos, y con la ayuda del departamento de sistemas pudimos observar cómo se encuentra la empresa en lo que se le denomina seguridad informática y más en la parte del entorno físico en la que está situada los activos informáticos. Por consiguiente el alcance de ésta auditoría en seguridad, se encuentra a la espera de que se cumplan las sugerencias en la empresa y en especial el departamento de sistemas para que no se produzca graves problemas posteriormente.

8.4.2 Objetivos

Los objetivos de una auditoría de seguridad física y del entorno en la empresa de Italimentos son de suma importancia ya que el acceso no permitido a lugares restringidos van a ser muy perjudiciales en el momento de la divulgación de información imprescindible para la producción y esto se lo resume en:

- Evitar el acceso físico no permitido, el daño o la divulgación de la información emitida por los departamentos y de toda la empresa de Italimentos.

- Garantizar la seguridad, rendimientos y privacidad de los sistemas y máquinas de la empresa.
- Evitar la pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la compañía.

8.4.3 Introducción

Es muy importante darnos cuenta que por más que la empresa sea la más segura desde un punto de vista de ataques ya sea internos como externos, la seguridad será nula si no se ha previsto como combatir contra ataques ambientales como son los incendios, terremotos, etc.

La seguridad física es uno de los aspectos olvidados a la hora del diseño informático, si bien algunos de los aspectos que se verán a continuación son estudios que se realizaron en la compañía donde se visualizo ciertas falencias en el área de seguridad de la empresa de Italimentos y se sugiere para combatir con las vulnerabilidades que se aplican para no tener problemas en posteriores ocasiones.

8.4.4 Beneficios de la seguridad relacionada con el personal de Italimentos.

Los beneficios para este tipo de seguridad es la confidencialidad de los datos, ya que toda la información relacionada con la empresa debe de restringirse para el acceso de personal externo y la no divulgación del personal interno de la compañía dando confianza y veracidad de los productos, consiguiendo con ello ser a nivel local los primeros pioneros en tener la certificación BPM[80] que ayudan a la producción de la empresa ya sea por sus ventas y compras de embutidos hacia otras ciudades y localmente.

8.4.5 Responsabilidades

Es responsabilidad del todo el personal de Italimentos, hacer que se respeten las seguridades de la empresa con el fin de que se cumplan todas las sugerencias que ponemos a continuación y aplicar todo lo que sea necesario para que la empresa surja a nivel local como se lo establece en su visión.

[80] BPM: Buenas Prácticas de Manufactura.

8.4.6 Definición de seguridad física y del entorno.

Evaluar y controlar permanentemente los lugares de alto riesgo informático de la empresa de Italimentos como base para comenzar a integrar la seguridad como una función específica dentro de la compañía.

También ver los mecanismos de prevención y detención de riesgos donde involucren la parte informática de la empresa teniendo en cuenta que sin éstos activos la producción de la empresa esta propensa a pérdidas continuas de dinero.

8.4.7 Disposiciones generales

El presente documento tiene por objeto contribuir de forma específica al desarrollo informático en la parte de seguridad física y del entorno de la empresa Italimentos.

Con ello buscamos mantener la información segura ante los futuros riesgos en los que se puede establecer sino llevamos una buena seguridad en cada departamento, con ello todo el personal de la empresa está en la obligación de cuidar los activos informáticos y cualquier anomalía hacerlos llegar de manera rápida y eficiente al personal encargado del departamento de sistemas, con ello buscamos ayudar con sugerencias donde a continuación se colocará para un buen rendimiento y después no exista pérdidas en la información de la compañía.

8.4.8 Acceso físico a copias de seguridad.

En el análisis que se realizó en Italimentos, se analizó la necesidad de implementar varias sugerencias que a la larga serán de mucha importancia para los posibles robos, incidentes informáticos con eso llevamos a que tengan una empresa segura y personal responsable de sus activos informáticos.

- Sugerimos que los equipos se deberán ubicar en lugares seguros de tal modo que se minimice el acceso innecesario a las áreas de trabajo.
- Los servicios que manejan información o datos sensibles deberán estar ubicados en CD o algún dispositivo de almacenamiento de forma que reduzca el riesgo

de visualización del personal no autorizados durante su uso y los sitios de almacenamiento se deberán asegurar para evitar el acceso no permitido.

- Los elementos que se requiere de mayor seguridad por el nivel de información que se procesó, deberán estar aislados para reducir el nivel general de protección requerida de los demás departamentos.
- Se deberá aplicar protección contra rayos a la edificación de los servidores que tengan los respaldos y adaptar filtros protectores a las fuentes de energías entrantes y a las líneas de comunicación.
- Los equipos de procesamiento de la información confidencial de la empresa deberá estar protegido en la edificación donde están el personal de desarrollo para minimizar el riesgo de fuga de información debido al filtrado del personal interno de la compañía.
- Se hará llegar por medio del jefe de su departamento la solicitud para cualquier información que requiera, y esté respaldada donde se transcribirá el porqué de su adquisición.
- Se deberá estar registrados la fecha, la hora de entrega de documentos, para cualquier personal interno que desee cualquier tipo de respaldo en donde posea información confidencial, caso contrario no se le entregará ningún tipo de documento y se le avisará al Gerente de su departamento.

8.4.9 Almacenamiento de la información.

- Sugerimos que definan el nivel necesario de respaldo para la información de respaldo esto quiere decir que definan si es confidencial, privada, pública.
- Se debería hacer registros encriptados para respaldar y generar procedimientos documentados de su restauración de la información.
- Los respaldos se almacenaran en un sitio lejano, a una distancia suficiente para escapar de cualquier riesgo debido a desastres en la sede principal de la empresa.
- La información almacenada o respaldada se le deberá dar el grado apropiado de protección física y ambiental consistentes en las funciones y obligaciones que poseen para el personal de la empresa.

- Es conveniente probar con regularidad por lo menos cada dos meses los medios de respaldos para garantizar el desempeño del dispositivo y evitar emergencias posteriores.
- Los procedimientos de restauración se debería verificar y probar con regularidad para garantizar su eficiencia en el tiempo designado para su respectiva recuperación.
- Los datos almacenados se deberán encriptar para proteger de la confidencialidad por parte del personal de la empresa.

8.4.10 Acceso de personal a sala de servidores.

Sugerimos que para el ingreso al cuarto de servidores se haga por medio del personal de sistemas donde se almacenará los datos de la persona que ingresa en un sistema biométrico. Ahí se procesará la entrada y salida del personal donde se verificará quien ingreso al cuarto de servidores y sus posibles causas de algún colapso informático.

8.4.11 Estructura física del ambiente informático.

En este tema la sugerencia se realizará para el cuarto de servidores y el departamento de sistemas donde en la actualidad trabajan iguales con el departamento de cartera por falta de espacio de la empresa donde buscamos la mejor opción y transcribimos lo siguiente:

Se realizará la división del cuarto de servidores donde el espacio restante se remodelará para el departamento de sistemas con la finalidad que estén pendientes por cualquier vulnerabilidad que se presente, con ello los servidores estarán en otro cuarto con ventilación y todos los requerimientos necesarios para que no se produzca riesgos que ocasionen colapsos en la producción de la empresa.

8.4.12 Factores ambientales del ambiente informático.

8.4.12.1 Incendio

- Sugerimos que el área en donde se encuentren las computadoras debe estar en un local que no sea combustible o inflamable.

- El local no debe estar encima, debajo o adyacente a las áreas donde almacenen materiales inflamables o cualquier sustancia donde se puede producir fuego.
- Las paredes deben de hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe de construirse un falso piso que estará instalado sobre el piso real con materiales incombustibles y resistentes al fuego.
- No se permitirá fumar en ninguna área de la fábrica.
- El piso y el techo en el cuarto de servidores y almacenamiento de los dispositivos deben de ser impermeables.
- Tener dos niveles de estuco sobre el techo del cuarto de servidores para detener el calor y procurar que no se sobrecaliente el ambiente del centro de procesamiento de datos.

6.8.12.2 Inundaciones

A las sugerencias expuestas por incendios lo único que se necesita para las inundaciones es que construyan un techo impermeable para evitar el paso del agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

8.4.12.3 Instalaciones eléctricas

Para las sugerencias a este tema se tomará en cuenta dos tipos de instalaciones que son muy importantes donde exponemos a continuación:

8.4.12.3.1 Instalaciones de cableado

Sugerimos que tengan presentes el personal de sistemas los riesgos que interfieren en el cableado, dando así los principales problemas que se dan por medio de dichos materiales como son la interferencia de campos magnéticos, corte del cable producido accidentalmente o intencionalmente y daños del propio cable por factores ambientales como son el alejarse del agua o gas con ello hablar con el personal de mantenimiento eléctrico para el cambio respectivo y su aprobación para el uso del mismo.

8.4.12.3.2 Instalaciones de picos y ruidos electromagnéticos

Para este tipo de instalación sugerimos que se debe de tener especial cuidado de los picos y ruidos electromagnéticos donde se debe de tener un regulador de voltaje general donde se genere para todos los departamentos dando energía necesaria para no perder la producción de la empresa, y con ello ponerse de acuerdo con el departamento de mantenimiento donde realicen la revisión semanal de los UPS y dichos reguladores para no tener posteriores problemas en la baja de equipos informáticos para ello se recomienda que los UPS estén dentro del rack para no ser desactivados por ningún usuario o intruso mal intencionado.

8.4.12.4 Terremoto

La sugerencia principal que colocamos para este tipo de riesgo ambiental es de que toda información sea confidencial o privada debe de estar respaldada por cualquier dispositivo de almacenamiento donde se realizará su copia respectiva y se colocará fuera de espacio principal de la empresa para este caso recomendamos que sea en el departamento de desarrollo.

8.4.13 Medidas de protección del ambiente informático.

Se sugiere al jefe de sistemas realizará un evento con el permiso de la gerencia para realizar un simulacro donde observaran, vivirán, palparan el momento previo a destrucciones de riesgos ambientales para buscar medidas hacia los recursos informáticos, donde se dictaran este simulacro el personal del cuerpo de bomberos de la ciudad de Cuenca con el fin de saber las principales etapas de un simulacro donde intervienen las siguientes medidas a tomar en la empresa:

8.4.13.1 Planeación

En ésta medida de ejercicio de evacuación se deberá tomar en cuenta todo lo que se refiere a los materiales y recursos informáticos donde se verán en la obligación de cuidarlos por el beneficio de la producción de la empresa donde se recomienda:

- Sonidos especiales.
- Suspensión de energía eléctrica.
- Uso de pañuelos mojados.

- Fuego real en una zona segura o fuera del edificio.
- Traslado de ambulancia.
- Simulación de heridos.
- Desplazamiento de personas por escaleras con ojos vendados.
- Fingimiento de pánico o desmayo.
- Apoyo a minusválidos.

8.4.13.2 Preparación

En este caso los brigadistas deben de conocer el establecimiento donde deberán saber las funciones del personal y ellos buscar a las personas más fuertes e inteligentes de la empresa para enseñarlos a como poder rescatar a compañeros sobre riesgos ambientales que se puede dar en cualquier compañía y saber cómo salir de dicha incidencia ilesos.

8.4.13.3 Ejecución

Para este tipo de medida se buscará ejecutar los siguientes puntos:

- Aplicación de lineamientos, procedimientos y normas establecidas.
- Consecución de los objetivos del ejercicio.
- Solución de los problemas imprevistos derivados de la emergencia simulada.
- Actuación oportuna y eficiente.
- Empleo adecuado de los recursos existentes y medios asignados.
- Aviso a los ocupantes del inmueble.
- Selección de un mecanismo de alerta claramente identificable para evitar confusión.
- Proporcionar material impreso a los visitantes, para informarlos sobre las acciones a seguir.

Donde se realizará en el siguiente tiempo:

- Zona de alto riesgo: uno cada mes.
- Zona de riesgo medio: uno cada tres meses.
- Zona de bajo riesgo: uno cada seis meses

8.4.13.4 Evaluación

En esta etapa se evaluará el tiempo que tomó hacer el simulacro y las respectivas observaciones que se dieron ante dicho evento no olvidarse que no necesariamente es mejor un simulacro que toma menos tiempo sino aquel que resuelve los efectos de una emergencia o desastre y protege a la población susceptible de ser afectada.

8.4.14 Protección a riesgos identificados.

Para los riesgos identificados en la empresa de Italimentos se dividió en dos incidencias importantes que se realiza en la compañía y su respectivo cuidado que se aplicará por la seguridad contratada por RRHH de la empresa, estas dos incidencias son:

8.4.14.1 Control de acceso

Para este tipo de control se sugiere dos tipos de seguridades en la que estará pendiente el personal contratado para el ingreso y egreso de cualquier individuo a los interiores de la empresa y estos son:

8.4.14.1.1 Guardias de seguridad

- Sugerimos que el personal contratado solicitará completar un formulario de datos personales, motivos de la visita, hora de ingreso y egreso, etc.
- El uso de la identificación será el motivo principal para que ingrese y con ello hacerle su respectivo chequeo para luego proceder a enviarle a los distintos sectores de la empresa.
- Al finalizar su visita se realizará lo mismo que se hizo para el ingreso y su devolución de su identificador personal para su egreso.
- Estará instalado las cámaras de seguridad en espacios estratégicos para alguna anomalía por parte del personal de seguridad.

8.4.14.2 Acciones hostiles

Para este tipo de acciones se vieron los más importantes que se pueden dar en la empresa de Italimentos en la parte de activos informáticos estos son:

8.4.14.2.1 Robo

- Se sugiere que todas las copias de seguridad estén en una caja fuerte con clave donde el único que debe de saber la contraseña es el jefe del departamento de sistemas con ello evitaremos el hurto de información almacenada en algún dispositivo por parte del personal interno que trabaja en la empresa.
- El guardia debe de estar en la obligación que cuando sale un activo informático debe de realizar el llamado al personal de sistemas para la aprobación de su salida caso contrario no saldrá ningún dispositivo interno de la empresa.

8.4.14.2.2 Fraude

Se sugiere que el jefe de sistemas intente detectar a personas que estén en un cargo y el mismo intente realizar un intento de fraude ya sea por la información o recurso cambiado, donde será avisado a la gerencia para su respectiva sanción por la falta de integridad de los datos observados que produzcan pérdidas en la producción de la empresa y en la imagen de la misma.

8.4.14.2.3 Sabotaje

Sugerimos que el personal de sistemas tengan cuidado en que las redes estén completamente seguras, que los canales de comunicación estén en buen estado y que se comprometan a las normas que se dieron en la parte de confidencialidad de los datos, cuidados de los activos y recursos informáticos para que no se paralice la producción de la empresa y peor dar de baja al personal por consecuencias de una información que se divulgó accidentalmente o intencionalmente.

8.5 Recomendaciones de la auditoría del acceso.

8.5.1 Alcance

Este documento donde se transcribirá las sugerencias para este capítulo del acceso es elaborado de acuerdo al análisis realizado en la empresa de Italimentos, y con la ayuda del departamento de sistemas pudimos observar cómo se encuentra la empresa en lo que se le denomina acceso a los datos y recursos, pero en la parte responsable del cambio de

información de la base de datos y aplicaciones en la que está situada los activos informáticos. Por consiguiente el alcance de ésta auditoría en seguridad, se encuentra a la espera de que se cumplan las sugerencias en la empresa y en especial el departamento de sistemas para control de ingreso de personas externas a la empresa.

8.5.2 Objetivos

Los objetivos de una auditoría del acceso en la empresa de Italimentos tienen como objetivos:

- Saber que personal es el encargado de conceder, alterar o anular el acceso de los datos y recursos con el fin del buen manejo de la aplicación y uso de los mismos.
- Conocer el número máximo de intentos de conexión de los usuarios para ingresar al sistema de la empresa con el fin de analizar si terceras personas quieren acceder de forma excesiva.
- Tener en cuenta el manejo de una buena descarga de información con el fin de que no se de los ataques de personas maliciosas denominadas hackers.
- Mantener la seguridad de las configuraciones de accesos remotos e información.

8.5.3 Introducción

Es importante que la empresa y el personal de Italimentos debe tener una fuente principal de información que se brinda en los negocios y más en la producción de la compañía, donde el responsable de la confidencialidad de la información brinde seguridad ante el personal interno como también externo de la compañía, configurando sus aplicaciones y especialmente supervisando diariamente la red que poseen para el robo de la información por parte de personal que ingresa a las redes.

Esto conlleva mucho tiempo, donde las vulnerabilidades es tema de todos los días, dependiendo de la seguridad que posee la empresa emprenderá nuevos resultados para los riesgos, donde sean resueltos sin novedades y poniendo a consideraciones nuevos

tutoriales o manuales para la solución de posibles incidentes que pueden suceder en el ámbito administrativo de la empresa.

8.5.4 Beneficios de la seguridad relacionada con el personal de Italimentos.

Siempre se busca medidas claras para la solución de incidentes donde la producción no se involucre ante los riesgos propinados por personas extrañas, encontrando así el manejo adecuado y sobre todo la solución de dichos incidentes que se producen por el mal manejo de la seguridad, dando así un objetivo principal para el beneficio de este capítulo, evitando la paralización de la producción y pérdidas económicas en la fábrica.

8.5.5 Responsabilidades

Es responsabilidad del todo el personal de Italimentos Cía. Ltda., pero en especial en el departamento de sistemas para realizar medidas de seguridad empresariales, con el fin de que se cumplan todas las sugerencias que se den al departamento, para realizar los cuidados necesarios para las incidencias y verificar que el personal este atento a las vulnerabilidades que están acechando en las compañías y en especial en Italimentos.

8.5.6 Definición de seguridad del acceso.

Es uno de los elementos más importantes dentro de la organización ya que debe ser administrada según los criterios establecidos por los administradores y supervisores de sistemas, evitando que los empleados de Italimentos y los que no pertenecen a la compañía puedan acceder a la información sin la respectiva autorización con el fin de reducir los limites de vulnerabilidad a los que están expuestos y especialmente a la integración de los datos.

8.5.7 Disposiciones generales

Para realizar las sugerencias de este capítulo lo más importante es que el personal de sistemas realice todas las recomendaciones que planteamos en los anteriores capítulos de la tesis con el fin de impedir todos los posibles riesgos que están acechando en todas las empresas del país, motivo en el cual, se debe tener cuidado ante el personal externo de la empresa, para posibles accesos a información confidencial donde su robo es motivo de pérdidas de producción e incluso de credibilidad de la compañía.

8.5.8 Personal autorizado a conceder, alterar o anular acceso sobre datos y recursos

Sugerimos que el personal del departamento de sistemas se debe poner de acuerdo con otros departamentos que manejan información critica en Italimentos para designar a una persona responsable de conceder, alterar o anular el acceso sobre los datos o recursos de cada departamento, donde él será la persona indicada para los cambios efectuados a los recursos de información.

8.5.9 Número máximo de intentos de conexión.

Sugerimos que el número de intentos de conexión deben de estar configurados para tres a cinco intentos en todos los recursos informáticos de la empresa donde el usuario al colocar mal la clave de conexión salga un mensaje de error y después de los cinco intentos se bloquee el programa donde el mensaje llegue al departamento de sistemas para la debida observación del mensaje siendo ellos las personas que configuren nuevamente el ingreso del usuario.

8.5.10 Descarga de información.

- Sugerimos que las descargas de información pasen por un antivirus para detectar código maliciosos donde puede afectar al activo informático de la empresa.

- Tener restringido las descargas de páginas que no son de interés de la fábrica por medio de un proxy para la configuración del mismo.

- Tener configurado el ancho de banda para cada usuario donde la descarga no puede ser más de 10 Mb.

- Descargar únicamente programas que se necesiten para beneficio de la empresa y solo el departamento de sistemas deberá realizarlos.

- Comprobar si el programa a descargar es gratuito o privado, con el objetivo de conocer cual aplicación es la más acoplable a las acciones que se quieran dar.

- Asegurar que el recurso o equipo cumple con los requisitos del programa.

- Clasificar las aplicaciones o información descargada, para ubicar de manera más fácil al utilizar una de ellas.

- Colocar en una carpeta específica exclusivamente las descargas, para gestionar de mejor manera los archivos.

- Utilizar un gestor de descargas, tales como ares, limewire, emule, etc.

8.5.11 Conexión entre empresa y redes públicas o privadas.

- Sugerimos que se instale un sistema de detección de intrusos basados en red denominado Snort.

- Realizar una topología física y lógica de la red de la empresa de Italimentos.

- Análisis de control de puertos ya sea por máquina local como también en la administración de red.

- Como medida de ataques externos configurar los firewall personales.

- Realizar un escaneo de puertos, aplicaciones con el sistema Nmap.

- Protección mediante filtrado de puertos y conexiones hacia y desde el exterior de una red privada con cortafuegos y proxy perimetrales.

- Controlar el estado de conexiones.

- Editar configuraciones y contraseñas por defecto en el sistema para mejorar la seguridad.

- Reducir el alcance de la señal wireless, ubicando el router inalámbrico a una posición para que el radio de la señal no vaya demasiado hacia el exterior de la empresa.

- No configurar la red Wi-Fi como oculta, sino como visible con seguridad WEP de 128 bits en la contraseña, para mayor seguridad.

- Actualizar el sistema operativo con parches de seguridad menos con actualizaciones automáticas de internet, ya que varios sistemas operativos no tienen licencias originales.

- Deshabilitar el interfaz Wi-Fi cuando no sea utilizado.

- Evite conectarse a redes Wi-Fi inseguras, como por ejemplo redes públicas abiertas o basadas en WEP.

8.5.12 Eventos realizados por otros usuarios y terceros.

Para estos capítulos que se manejan similares con terceras personas los eventos deben de ser manejados con mucho cuidado ya que cualquier manipulación puede establecer un daño a la producción y en especial a la identidad de la empresa, con esto pongo a consideración algunas sugerencias para evitar el uso indebido de la información:

- Sugerimos conectar a ninguno de los recursos, ni equipos de comunicaciones como son el modem que faciliten la salida de la información de la empresa.

- No obtener información de datos o acceso a la información que no le han sido asignados por el departamento de sistemas.

- No acceder a sitios o áreas restringidas de los sistemas de información o de la red de la empresa.

- No reconfigurar o falsear los registros de log de los sistemas de información.

- No descifrar claves en las sesiones de los usuarios que no son del departamento al que esté laborando y cualquier otro elemento de seguridad donde intervienen los sistemas de información.

- No instalar ni ejecutar programas que puedan interferir sobre el trabajo de otros usuarios, donde alteren el trabajo diario que poseen información confidencial en cada uno de los departamentos.

- El departamento de sistemas se verá en la obligación de ayudar a personas que solicitaron el remplazo respectivo con la revisión de la máquina que será imprescindible para el uso diario y personal del que esté a cargo del recurso informático.

- Inhabilitar los puertos USB para memorias Flash del recurso que tiene a la persona que va a remplazar en cualquier departamento de la empresa.[81]

8.5.13 Responsabilidad personal ante contraseñas y equipos.

En este capítulo las responsabilidades recogen varios procedimientos de seguridad de acceso tanto físico como lógico, donde se indicaron en los capítulos anteriores y colocamos a breve rasgos los siguientes puntos a tomar en cuenta:

- Sugerimos que tomen en cuenta los procedimientos y normas de acceso al sistema informático como son la asignación, distribución, almacenamiento y cambio de contraseñas de acceso al sistema y equipos.

- Los procedimientos, normas y medidas de seguridad lógica y física adoptadas en el capitulo tres para la defensa ante ataques externos e internos donde son adaptadas para robos de información esencial de la empresa se deben de tomar a consideración y aplicarlas como se les recomendó en dicho capítulo dado que ahí se indica sobre como tener las contraseñas y su cuidado específico.

- Se tomará en cuenta el reglamento de la empresa si no realizan el cuidado específico de cada recurso donde el gerente se verá obligado a tomar medidas sobre el asunto con cada uno que falte ante éste activo informático.

8.5.14 Seguridad ante trabajo remoto.

Sugerimos que en lo posible todo trabajo realizado en la empresa se debe de culminar en la fábrica por tal motivo no existe escusa para acabar sus labores en los hogares dado que la información que poseen la empresa es de carácter confidencial donde cualquier personal de sistemas que desee sacar información será anunciado al gerente de la

[81] www.dspace.espol.edu.ec/.../04-Capitulo3-...

empresa para su respectiva autorización de la salida, en caso de pérdida el gerente será la persona indicada para su respectiva sanción.

- El personal de sistemas implementará un sistema remoto para todas las sucursales locales de Italdelis donde se realizará el mantenimiento manual de las mismas.

- El personal de sistemas ayudará remotamente a cualquier usuario que necesite ayuda para configuraciones de contraseñas del activo.

- Este sistema será de ayuda remota donde todo será manejado desde el administrador del sistema.

- El sistema será utilizado mediante la autenticación del personal al ingresar el sistema.

- Antes de aplicar cualquier manipulación remotamente el personal solicitante debe indicarle que es la persona dueña del activo para su debida ayuda.

8.5.15 Técnicas de identificación y autenticación.

- Sugerimos establecer un número máximo de tres intentos de ingreso a la sesión de Windows.

- Debe bloquearse tras tres intentos fallidos al introducir sus datos.

- No utilizar secuencias ni caracteres repetidos.

- No utilizar el nombre de inicio de sesión.

- No utilizar palabras del diccionario de ningún idioma.

- Utilizar varias contraseñas para distintos entornos.

- Evitar la opción de contraseña en blanco.

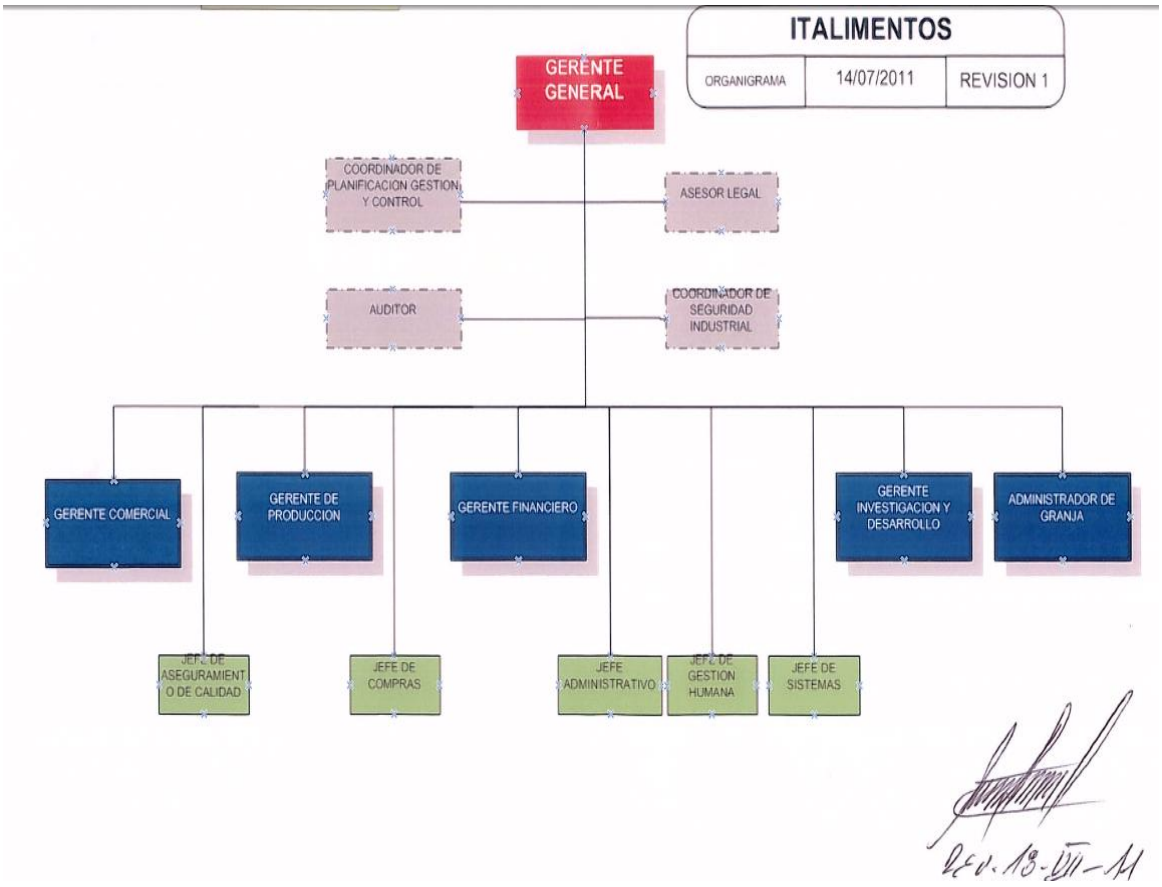
- Cambiar de contraseña de seguridad de ingreso a sesiones de Windows y correo

electrónico cada 3 meses, manteniendo un historial de los mismos.

- No relevar la contraseña a nadie ni escribirla en equipos de otros departamentos.
- Fijar la duración mínima y máxima de vigencia de la contraseña.
- Establecer los procedimientos de bloqueo y desbloqueo de cuenta por utilización reiterada de contraseñas incorrectas.
- Establecer los procedimientos de generación, conservación y almacenamiento seguro de contraseñas.
- Establecer límites de frecuencia en la utilización de contraseñas por lo cual no se podrá repetir las últimas contraseñas que hemos utilizado.
- Solicitar contraseña cada vez que arranque la máquina.
- Añadir contraseña encriptado al menú de edición es decir imposibilitar la edición por cualquier usuario no autorizado y al modo de recuperación.
- Usar herramientas de auditoría de sistema de acceso y nivel de fortaleza de contraseñas como lo es Ophcrack.
- Contratar algún servicio para detección de llamadas con el objetivo de comprobar la llamada entrante que solicitan ayuda.
- Implementar las sugerencias sobre las contraseñas realizadas en el capitulo tres.

ANEXOS

Anexo A. Estructura Organizacional de Italimentos Cía. Ltda.[82]



[82] Recursos humanos de Italimentos Cía. Ltda.

Anexo B. Cuestionario sobre políticas de seguridad.

República del Ecuador	Auditoría en Seguridad Informática	**Proceso:** Norma ISO 27001		
	EVALUACIÓN DE POLITICAS DE SEGURIDAD	**Fecha:**	07/11/2011	

"Con el objeto de evaluar las políticas de Seguridad Informática y de conocer la percepción de las personas entrevistadas en el Área de Sistemas de Información, se desea conocer sus opiniones evaluativas de esta actividad".

Por favor diligencie el siguiente formato.

1. DATOS GENERALES:

FECHA DE AUDITORÍA	**Día**	☑ 0 6	**Mes**	1 1	**Año**	☑ 2 0 1 1	**PROCESO AUDITADO**	☐ **Consideraciones** ☐ **Medidas, Controles, Procedimientos, Normas y Estándares de Seguridad** ☐ **Periodo de Vida de Contraseñas**	☐ **Privilegio del Personal** ☐ **Cifrado de Información**

NOMBRE DEL AUDITOR A EVALUAR	Cristian Bacilima Pulla.		
NOMBRE DEL EVALUADOR			
PERFIL	Departamento Tecnico	**FIRMA**	

A continuación encontrará una serie de preguntas cuya respuesta se debe señalar con una (X) en una escala de valores así:

PREGUNTAS	SI	NO	N/A
1. ¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?	X		
2. ¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?	X		
3. ¿Existen procedimientos de notificación y gestión de incidencias?		X	
4. ¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?	X		
5. ¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?			X
6. ¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?	X		
7. ¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado?		X	
8. ¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?	X		
9. ¿Existe una relación de personal autorizado a acceder a los soportes de datos?	X		
10. ¿Existe un período máximo de vida de las contraseñas?	X		
11. ¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?	X		
12. ¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran o deben estar- documentadas en el Documento de Seguridad?		X	
13. ¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado?	X		
14. ¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?		X	
15. ¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	X		
16. ¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer: • Un número máximo de intentos de conexión. • Un período máximo de vigencia para la contraseña, coincidente con el establecido en el Documento de Seguridad.	✓ ✓		
17. ¿Existen procedimientos de asignación y distribución de contraseñas?	X		

Anexo C.1. Formato de movimientos o bajas de equipos de cómputo.

ITALIMENTOS CIA. LTDA.

FC FORMATO PARA MOVIMIENTOS O BAJAS DE EQUIPOS DE COMPUTO 2011

MOVIMIENTO ☐ BAJA ☐ REPARACIÓN ☐

NOMBRE	NOMBRE	MARCA	MODELO	SERIE (S/N)	ESTADO (Bueno, Malo, Regular)	MOTIVO DEL MOVIMIENTO O LA BAJA (Especificar si el activo es nuevo y no tiene código)

ESPONSABLESPONSABLE (f): _____ DEPARTAMENTO DE SISTEMAS (f): _____

NOM NOMBRE: _____ NOMBRE: _____

SER MOVIM SER MOVIMIENTO): NUEVO CUSTODIO (f): _____

NOMBRE: _____

Página 1/1

Anexo C.2. Cuestionario sobre gestión de activos informáticos.

República del Ecuador	Auditoría en Seguridad Informática	**Proceso:** Norma ISO 27001	
	EVALUACIÓN DE POLITICAS DE SEGURIDAD	**Fecha:** 07/11/2011	

"Con el objeto de evaluar las políticas de Seguridad Informática y de conocer la percepción de las personas entrevistadas en el Área de Sistemas de Información, se desea conocer sus opiniones evaluativas de esta actividad".

Por favor diligencie el siguiente formato.

1. DATOS GENERALES:

FECHA DE AUDITORÍA	**Día**	15	**Mes**	12	**Año**	2011	**PROCESO AUDITADO**	☒ Inventario de Soporte y Actualizaciones ☒ Registro y actualización de entrada o salida de la información ☒ Copias de Seguridad y Recuperación de datos ☒ Medidas adoptar cuando un soporte vaya ser desechado o reutilizado ☒ Almacenamiento de Contraseñas ☒ Lugar de almacenamiento de copias de seguridad ☒ Etiquetado de los Activos ☒ Cuentas de Usuario

NOMBRE DEL AUDITOR A EVALUAR	Cristian Bucheli P.		
NOMBRE DEL EVALUADOR	CHRISTIAN CADME, DIEGO DUBVE		
PERFIL		**FIRMA**	

A continuación encontrará una serie de preguntas cuya respuesta se debe señalar con una (X) en una escala de valores así:

PREGUNTAS	SI	NO	N/A
1. ¿Existe un control sobre el acceso físico a las copias de seguridad?	X		
2. ¿Existe un inventario de los recursos informáticos existentes?	X		
3. ¿Dicho inventario incluye las copias de seguridad?		X	
4. ¿Las copias de seguridad, o cualquier otro soporte, se almacena fuera de la instalación?		X	
5. ¿Existen procedimientos de actualización de dicho inventario?	X		
6. ¿Existen procedimientos de etiquetado e identificación de los soportes informáticos?	X		
7. ¿Existen procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual?		X	
8. ¿Existen estándares de distribución y envío de estos soportes?		X	
9. ¿Se tiene un documento que especifique los archivos que se envían fuera de la empresa, en la que se especifique el tipo de soporte, la forma de envío, el emisor y el destinatario?		X	
10. ¿Se comprueba que todos los soportes incluidos en la pregunta 9 se encuentra también en el soporte de datos mencionado anteriormente?		X	
11. Se obtiene una copia de registros de entrada y salida de soportes y se comprueba que en él se incluyen: • Los soportes incluidos en la pregunta 9 y 10 • Transporte de soportes al exterior (si existiera)	X		
12. ¿Se verifica que el registro de entrada y salida refleja la información requerida por algún reglamento?	X		
13. ¿Se analiza los procedimientos de actualización del registro de entrada y			

Página 1 de 2

República del Ecuador	Auditoría en Seguridad Informática	Proceso: Norma ISO 27001		SALESIANA
	EVALUACIÓN DE POLITICAS DE SEGURIDAD	Fecha:	07/11/2011	

salida en relación con el movimiento de soportes?	X		
14. ¿Existen controles para detectar la existencia de soportes recibidos/enviados que no se escriben en un registro de entrada/salida?		X	
15. ¿Se realiza envíos de soportes fuera de la empresa, con ficheros de nivel alto?			X
16. ¿Se verifica que todos los soportes que contienen ficheros con datos de nivel alto van cifrados?		X	
17. ¿Existen procedimientos para la realización de copias de seguridad?	X		
18. ¿Existen controles para la detección de incidencias de errores en la realización de pruebas de respaldo de copias de seguridad?	X		
19. ¿Existe controles sobre el acceso físico a las copias de seguridad?	X		
20. ¿Se controla que solo las personas con acceso autorizado, en un documento de seguridad, tengan acceso a los soportes que contienen las copias de seguridad?		X	
21. ¿Las copias de seguridad de los ficheros de alto nivel, se almacenan en un lugar diferente?	X		
22. ¿Alguna vez se ha realizado una recuperación de datos de alto nivel, utilizando las copias de seguridad?	X		
23. ¿Alguna vez se ha realizado una recuperación de datos a nivel de usuario, utilizando las copias de seguridad?	X		
24. ¿Se toman medidas de seguridad para impedir cualquier tipo de recuperación posterior de la información almacenada en él?		X	
25. ¿Existe una política para desechar un recurso con información importante?		X	
26. ¿Se reutiliza la información importante de un recurso informático a ser desechado?	X		
27. ¿Los soportes que van a ser desechados, son triturados para ser inaccesible a la información?		X	
28. ¿Existe algún programa que permita gestionar y almacenar claves secretas?	X		
29. ¿Las contraseñas están almacenadas en alguna carpeta compartida en red?	X		
30. ¿Las contraseñas de usuarios están almacenados en algún fichero de claves?		X	
31. ¿Existe un estándar para etiquetar los soportes de datos?		X	
32. ¿Existe un orden lógico en el almacenamiento de soporte de datos?		X	
33. ¿Existe una estructura para crear una nueva cuenta de usuario?	X		
34. ¿Hay en el sistema cuentas de usuario genéricas, utilizadas por más de una persona?	X		
35. En el sistema hay están habilitadas para todas las cuentas de usuario, las opciones que permiten establecer: • Un numero máximo de intentos de conexión • Un periodo máximo de vida vigente de contraseñas, especificados en un documento			X

Anexo D. Cuestionario sobre seguridad relacionada con el personal.

"Con el objeto de evaluar la seguridad de la información relacionada con el personal y de conocer la percepción de las personas encuestadas en la empresa de Italimentos Cía. Ltda., se desea conocer sus opiniones evaluativas de esta actividad".

Nota: Esta información es personal y privada. No repercutirá en su puesto de trabajo.

<table>
<tr><th colspan="10">1. DATOS GENERALES:</th></tr>
<tr>
<td>FECHA DE AUDITORÍA</td>
<td>Día</td>
<td>☐
☐</td>
<td>Mes</td>
<td>☐
☐</td>
<td>Año</td>
<td>☐
☐
☐
☐</td>
<td>PROCESO AUDITADO</td>
<td>☐ Uso de recursos informáticos.

☐ Funciones y Obligaciones del personal.

☐ Acceso de personal a sistemas que tratan datos personales.</td>
<td>☐ Acceso de personal a soporte de datos e información.

☐ Confidencialidad con todo el Personal.

☐ Comunicación de debilidades en materia de seguridad.</td>
</tr>
</table>

NOMBRE DEL AUDITOR A EVALUAR	
DEPARTAMENTO	

A continuación encontrará una serie de preguntas cuya respuesta se debe señalar con una (X):

PREGUNTAS	**SI**	**NO**
1. ¿A sufrido accidentalmente pérdida de información en su puesto trabajo		
2. En caso de pérdida de información ¿Ha logrado recuperar total ó parcialmente la información?		
3. ¿Alguna persona ha divulgado información personal o privada?		
4. ¿Alguna vez ha insertado un Flash Memory en su puesto de trabajo?		
5. ¿Separa la información dependiendo de su importancia?		
6. ¿Existe un procedimiento o manual que ayude al manejo de información privada o restringida?		
7. ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento, con información de la empresa?		
8. ¿Conoce usted el término de encriptación de archivos?		
9. ¿Se ha olvidado de cerrar su sesión?		

10. Cuando está ausente en su puesto de trabajo, ¿Su ordenador se queda prendido?		
11. ¿Ha instalado cualquier tipo de programa en su puesto de trabajo?		
12. ¿Ha intentado ingresar a documentos o archivos y se le ha denegado el acceso?		
13. ¿Ha grabado información en su puesto de trabajo desde algún dispositivo de almacenamiento?		
14. ¿Al terminar sus labores diarias apaga su computadora?		
15. En caso de ausencia en su puesto de trabajo y este prendido su computador ¿cierra usted su sesión?		
16. Cuando se instala un programa nuevo ¿Existe su debida capacitación?		
17. ¿Ha tenido alguna pantalla de advertencia en su monitor?		
18. ¿Ha comunicado al departamento de sistemas por algún mensaje de error de alguna aplicación?		
19. ¿Ha intentado ingresar a otras cuentas de usuario?		
20. Por cualquier motivo ¿Su puesto de trabajo ha sido reemplazado temporalmente por personal interno?		
21. ¿Ha recuperado algún archivo perdido?		
22. ¿Usted cree que la información dentro de la empresa está segura?		
23. ¿Comparten información con otros departamentos mediante carpetas compartidas?		

24. ¿Ha sufrido alguna pérdida de información?		
25. ¿Ha realizado alguna vez un cambio de clave en su computadora?		
26. ¿Graba la información que realiza cuando va a estar ausente?		
27. ¿Ha investigado información por medio de navegadores de búsqueda como Google en su puesto de trabajo?		
28. ¿Ha logrado alguna vez, por su cuenta, arreglar algún error en su computador?		
29. ¿Se ha denegado el acceso a datos o información de otro departamento?		
30. ¿Existe un área restringida en alguna carpeta de su computadora?		
31. ¿Realiza respaldos de su información diariamente en dispositivos de almacenamiento?		
32. ¿Se ha desconectado su computadora por apagones?		
33. ¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo?		
34. ¿Tiene su ordenador información personal como fotos, videos, música, etc.?		
35. ¿El departamento de sistemas realiza el mantenimiento de su computador mensualmente?		
36. ¿Alguna vez le han cambiado su computadora por otra?		
37. ¿En los últimos 6 meses, le han cambiado su computadora?		
38. ¿Conoce usted el término de activos informáticos?		

39. ¿Separa por categorías los documentos públicos, privados, confidenciales, etc.?		
40. ¿Comparte su computador con otro compañero de trabajo?		
41. ¿Alguna vez se ha activado advertencias de antivirus?		
42. ¿Usted cree que la información que usted posee está segura?		
43. ¿Ha intentado arreglar su computadora por su propia cuenta?		
44. En su departamento ¿Tienen definido sus funciones y obligaciones?		
45. A parte de usted ¿Alguna otra persona conoce su contraseña de acceso a su computador?		
46. ¿Guarda información privada en distintas carpetas?		
47. Por cualquier motivo ¿Su puesto de trabajo ha sido reemplazado temporalmente por personal que no trabaja en la empresa?		
48. ¿Ha intentado ingresar a una página web y se ha bloqueado el acceso?		
49. ¿Ha tenido alguna capacitación para el mejor uso de las aplicaciones de su computadora, con el objetivo de mejorar su trabajo diario?		
50. ¿Ha llevado archivos o documentos informáticos fuera de la empresa en Flash Memory, CD, etc.?		
51. Su cuenta de usuario ¿Tiene la misma clave que la de su correo electrónico?		

52. Cuando sale un mensaje en su pantalla ¿Cierra el mensaje?		
53. ¿Ha rotado alguna vez una memoria flash para pasar información?		
54. ¿Se ha realizado algún cambio donde su computador le instalaron en otro departamento?		
55. ¿Ha observado archivos o información que no se relacionan con su departamento en su puesto de trabajo?		
56. ¿Tienen manuales todas las aplicaciones su computador?		
57. ¿Ha utilizado otra cuenta para ingresar a una sesión?		
58. ¿Su contraseña tiene como caracteres nombres de hijos, esposo, padres, mascotas, etc.?		
59. ¿Ha perdido información por apagones?		
60. ¿Se ha instalado alguna aplicación para el mejor manejo de la información?		
61. ¿Ha enviado archivos de la empresa desde su Hotmail o gmail?		
62. ¿Tiene acceso a internet en su puesto de trabajo?		
63. ¿Guarda su trabajo y cierra la aplicación cuando va a estar ausente?		
64. Sabe si su información, donde usted guarda ¿No es visible para otros usuarios?		

BIBLIOGRAFIA

- **Implementación de un sistema automatizado de control de acceso a una red LAN.** (Recuperado el 18 de Septiembre del 2011).

http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/7456/1/ice%20247.pdf

- **Especialista en administración de la seguridad.** (Recuperado el 22 de Septiembre del 2011).

http://repository.unimilitar.edu.co/handle/10654/3215

- **Estándares y protocolos de seguridad lógica en los sistemas de información.** (Recuperado el 29 de Septiembre del 2011)

http://cdigital.uv.mx/bitstream/123456789/28544/1/Salgado%20Almanza.pdf

- **Fundamentos de ISO 27001 y su aplicación en las empresas.** (Recuperado el 05 de Octubre del 2011).

http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=84921327061

- **Ampliar el alcance del sistema de gestión de la calidad para la prestación de servicios de seguridad de la información en la empresa DSC.** (Recuperado el 09 de Octubre del 2011).

http://repository.unilibre.edu.co/handle/10901/5871

- **Modelo de seguridad para el servicio de soporte técnico brindado por empresas Outsourcing.** (Recuperado el 19 de Octubre del 2011).

http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/5532/1/IF7.85.pdf

- **Desarrollo de políticas de seguridad informática e implementación de cuatro dominios en base a la norma27002 para el área de hardware en la empresa Uniplex Systems S.A en Guayaquil.** (Recuperado el 25 de Octubre del 2011).

http://www.dspace.espol.edu.ec/bitstream/123456789/5247/1/Desarrollo%20de%20Pol%C3%ADticas%20de%20Seguridad%20Inform%C3%A1tica%20e%20Implementaci%C3%B3n.pdf

- **Implementación y mejora de la consola de seguridad informática OSSIM una experiencia de colaboración Universidad-Empresa.** (Recuperado el 25 de Octubre del 2011).

http://www.educacioneningenieria.org/index.php/edi/article/view/63/53

- **ISO/IEC 27001.** (Recuperado el 20 de Octubre del 2011).

http://es.wikipedia.org/wiki/ISO/IEC_27001

- **Seguridad de la información ISO/IEC 27001.** (Recuperado el 7 Noviembre del 2011).

http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/

- **Amenazas, utilerías y mantenimiento de software.** (Recuperado el 17 Noviembre del 2011).

http://hecman.jimdo.com/hacker-ycracker/clasificacion-de-crackers/

- **Mi PC, pasado, presente y futuro.** (Recuperado el 22 de Noviembre del 2011).

http://mipc.elrincontecnologico.com/2008/12/definicin-de-servidor.html

- **Privacidad.** (Recuperado el 2 de Diciembre del 2011).

http://www.metroblog.com/privacy

- **Que es una cuenta de usuario estándar?.** (Recuperado el 15 de Diciembre del 2011).

http://windows.microsoft.com/es-US/windows-vista/What-is-a-standard-user-account

- **Protección de datos de carácter personal. Manual informativo y gestión interna. Normas de seguridad.** (Recuperado el 28 de Diciembre del 2011).

http://www.coie.unican.es/includes/manualNormas.pdf

- **Términos informáticos.** (Recuperado el 5 de Enero del 2012).

http://michelleinformate.blogspot.com/?zx=ecf8b073751ae89d

- **Seguridad física - Instalación Eléctrica.** (Recuperado el 10 de Enero del 2012).

http://www.segu-info.com.ar/fisica/instalacioneselectricas.htm

- **Redes telemáticas.** (Recuperado el 14 de Enero del 2012).

http://majandratv.blogspot.com/

- **VNC Scan Enterprise Console.** (Recuperado el 18 de Enero del 2012).

http://vnc-scan-enterprise-console.softonic.com/descargar

- **Seguridad informática: un enfoque desde la auditoria informática.** (Recuperado el 28 de Enero del 2012)

http://www.univalle.edu/publicaciones/journal/journal18/pagina17.htm

- **Plan de seguridad.** (Recuperado el 2 de Febrero del 2012).

http://mgeseguridadinformatica.wordpress.com/paguina2/

- **Políticas y procedimientos en la seguridad de la información.** (Recuperado el 8 de Febrero del 2012).

http://www.ilustrados.com/tema/4923/Politicas-Procedimientos-seguridad-Informacion.html

- **Políticas y procedimientos en la seguridad de la información.** (Recuperado el 15 de Febrero del 2012).

http://www.sabetodo.com/contenidos/EplpVplEZlTOfazBIB.php

- **El cifrado de información es una tarea pendiente en la pyme.** (Recuperado el 20 de Febrero del 2012).

http://www.tecnologiapyme.com/hardware/el-cifrado-de-informacion-es-una-tarea-pendiente-en-la-pyme

- **Plan de gestión de activos.** (Recuperado el 23 de Febrero del 2012).

http://es.wikipedia.org/wiki/Plan_de_gesti%C3%B3n_de_activos

- **TrueCrypt, software para el cifrado de datos.** (Recuperado el 28 de Febrero del 2012).

http://www.tecnologiapyme.com/software/truecrypt-software-para-el-cifrado-de-datos

- **Políticas y procedimientos en la seguridad de la información.** (Recuperado el 1 de Marzo del 2012).

http://www.sabetodo.com/contenidos/EplpVplEZlTOfazBIB.php

- **Políticas y procedimientos en la seguridad de la información.** (Recuperado el 3 de Marzo del 2012)

http://www.ilustrados.com/tema/4923/Politicas-Procedimientos-seguridad-Informacion.html