Año 10, Núm. 25 (Enero – junio 2017)

Revista de Investigación Académica sin Frontera
ISSN: 2007-8870

http://revistainvestigacionacademicasinfrontera.com

Recibido el 29 abril de 2017 Dictamen favorable el 20 de mayo de 2017.

SEGURIDAD INFORMÁTICA UNA PROBLEMÁTICA DE LAS ORGANIZACIONES EN EL SUR DE SONORA

Edgar Alberto Espinoza Zallas
Rodolfo Rodríguez Pérez

Universidad Estatal de Sonora

Introducción

En la actualidad el funcionamiento de una empresa, así como la como el desarrollo de sus objetivos, depende en gran parte del funcionamiento correcto del sistema y uso adecuado de los equipos informáticos. Cualquier parte del equipo de cómputo que se vea afectado tendrá repercusiones en la organización en general.

A continuación en el siguiente trabajo se presenta el desarrollo de un caso práctico involucrado en la empresa GRUPO OSUNA S.A. enfocado sobre la seguridad informática. Considerando algunos puntos muy importantes como conceptos básicos y claves que es de suma importancia tenerlos siempre presentes, también seguridad lógica, seguridad física, niveles de seguridad, etc.

Se realizó un análisis sobre la circunstancia en la que se está la empresa, encontrando algunos detalles que hay que trabajar, haciendo algunas recomendaciones para poder mejorar los puntos débiles como se muestra en durante el desarrollo del trabajo.

Descripción del Proyecto

Aunque el fin específico de la Informática se refiera a beneficiar a la humanidad algunos hacen mal uso, en casos muy graves a la sociedad entera. Facebook, Youtube, Twitter etc son usadas por lo general para ocio y pérdida de tiempo, pero hay otros problemas muy peligrosos como lo son los hackers, virus, malware, y cualquier clase de problemática que pueda afectar el medio informático.

La Seguridad Informática es un Tema que sin duda se debe de tratar para la sociedad en general. Todos estamos propensos y vulnerables a recibir cualquier tipo de ataque, algunos simples como robo de cuentas de correos y redes sociales, pero algunos otros extremadamente delicados como

desde las micro hasta las macro-empresas, que están propensos a ser bombardeados por algún hacker, ya sea robo de información sumamente valiosa, modificaciones o pérdida total del Sistema.

Algunos usuarios están bien resguardados, mientras que en algunos lados este tema se desconoce, están propensos y libres a recibir cualquier tipo de ataque informático. Por ello se planteó la siguiente pregunta principal: ¿Cuáles son los procedimiento habrán de llevarse a cabo para mantener la integridad de la información en los sistemas informáticos de la empresa GRUPO OSUNA S.A?

Justificación del problema

Como todo en la Informática se dan algunos problemas, pero el tema más enfocado a esta investigación es el de la Seguridad que se debe de tener en la empresa. Años atrás el enfoque administrativo que se tenía era más mecánico y de papeles, el manejo de información y documentación demoraba más tiempo y era un poco más compleja. Con la Informática se han logrado agilizar y automatizar demasiados procesos, pero el manejo de información requiere de extremo cuidado. Con la informática la consulta de información puede ser automatizada en gran parte, siempre y cuando sea manejada y administrada con mucha responsabilidad. Información confidencial o vital de la empresa en manos de personal no autorizado, o externos a la organización puede ser un grave problema tanto así como para llevarla a su desaparición.

Objetivo General

Analizar el procedimiento que habrá de llevar a cabo para mantener la integridad de la información en los sistemas informáticos de la empresa GRUPO OSUNA S.A

Hipótesis

Con la implementación de un plan de contingencia computacional se reducirá la posibilidad de ataques informáticos.

Delimitación

La investigación se desarrolla en el municipio de Navojoa, la cual está ubicada en el sur del estado de Sonora, colinda con municipios como Cajeme y Quiriego en el norte, al este con Álamos, al sudoeste con Huatabampo y al oeste con Etchojoa.

En el municipio de Navojoa cuenta con una población de 157,729 habitantes hasta el 2010 según la información el Instituto Nacional de Estadística y Geografía (INEGI).

La actividad económica del municipio ha estado sustentada en la producción agropecuaria, el comercio y los servicios, siendo las actividades principales la agricultura y la ganadería, mientras que la industria ocupa el segundo lugar en generar empleos de toda la población ocupada.

Referencia teórica

La seguridad simplemente es una necesidad básica, estando previendo sobre la vida y las posesiones. Los primeros con conceptos de seguridad se evidencian en los inicios de la escritura con los sumerios (3000 AC) o el Hammurabi (2000 AC). También la biblia, Homero, Cicerón, Cesar han sido autores de obras en donde aparecen ciertos rasgos sobre seguridad respecto a las Guerras y el Gobierno.

Algunos descubrimientos arqueológicos, marcan sin duda, algunas pruebas de seguridad en tiempo atrás, como en las pirámides egipcias, el palacio de Sargon,el templo de Karnak en el valle Nilo; el dios egipcio Anubi representado con una llave en su mano.

Tiempo atrás los primitivos solían evitar amenazas con métodos defensivos contra los animales, luchando o huyendo (fight or flight), para evitar o eliminar la causa. Así los problemas de la vida siempre han sido inevitables y algunos conceptos referentes a la seguridad ya eran manejados por nuestros antepasados tales como alertar, alarmar, detectar, evitar, reaccionar, etc.

Con el paso del tiempo el término seguridad se ha ido desarrollando y ha seguido evolucionando dentro de todos los órganos sociales. Dentro de la sociedad se han estado conformando nuevas estrategias para que el atacante se haga a la idea de que tendrá mucho que perder y poco que ganar.

Desde las primeras evidencias de Seguridad se pueden apreciar la seguridad externa y la interna. La externa es aquella que se está al tanto de amenazas exteriores hacia la organización. La seguridad interna es la que se preocupa por las amenazas de nuestra organización misma. De estas dos se pueden desprender en seguridad pública y privada.

En la Revolución Industrial la seguridad comenzó a tener una gran importancia por tratar de combatir los delitos y movimientos laborales, tan comunes en aquella época. En ese entonces un teórico y pionero de la management, Henry Fayol en 1919 identifica a la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Fayol definió el objetivo de seguridad como: “salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Generalmente hablando, es todas las medidas para conferir la requerida paz y tranquilidad (Peace of Mind) al personal.

Las medidas de seguridad a las que Fayol se refiere que solamente se restringían exclusivamente lo físico de la instalación porque era de lo más importante como los equipos, no tanto como el empleado. Con la aparición de las maquinas que se podrían considerar como cerebros electrónicos de aquellos tiempos, aunque hoy en día muchos aun lo conceptualizan así, porque

¿Quién sería capaz de entender aparato complicados actuales como para tener en peligro la integridad de los datos por ellos utilizados?

Hoy en día la seguridad se puede apreciar mucho más desde un enfoque legislativo, porque está en manos de los políticos, ya que son los que le tocan decidir sobre su importancia, las consecuencias que podrían tener es decir los delitos, su respectivo castigo que le podría incurrir. Esta forma de contemplar la seguridad a conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo.

Si vemos la seguridad desde un punto de vista técnico, esta se encuentra en manos de la dirección de las organizaciones y, en última instancia en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento.

Como pudo ser visto el proceso de evolución por qué ha pasado la seguridad se puede apreciar que desde mucho tiempo hacia atrás se percibía la seguridad, y a la actualidad no se ha añadido ningún concepto a los ya conocidos, solo se han hecho perfeccionamientos como: llaves, cerraduras, caja fuerte, puertas blindadas, trampas, vigilancia, etc.

Concepto de Seguridad

El termino seguridad proviene del latín *Securitas*. Cotidianamente se puede definir a la seguridad como ausencia de riesgo o también a la confianza en algo o alguien. La seguridad puede ser entendida de varias formas por la gente, de tal forma que se maneja con un cierto grado de incertidumbre. Para conceptualizar el término seguridad de manera adecuada es necesario eliminar la incertidumbre.

Una aceptación en la sociedad es que los problemas nunca se resuelven; es decir que la solución no hace que la energía del problema desaparezca por completo, solo se transforma en problemas mínimos que son más pequeños y aceptables. Por ejemplo:

Si en una organización que se esté trabajando con personal, y se decida la implementación de un sistema informático ayudaría en mucho solucionando el problema de la velocidad de algún procesamiento, pero abrirá otros problemas más pequeños como personal sobrante y reciclable, o en caso de que haya problemas con el sistema o servidos la organización tendría estancamientos laborales por depender de una máquina para realizar el trabajo.

Analizando el término seguridad se pueden apreciar 3 figuras:

1. El poseedor del valor - **Protector.**
2. Un aspirante a poseedor - **Competidor/Agresor.**
3. Un elemento a proteger - **Valor.**

De lo siguiente se puede concluir que entre el Protector y el competidor o agresor siempre surgirá una dinámica en donde el competidor quiere obtener el valor tratado, y el protector tiene que resguardar el bien, sea de su propiedad o para externo, para que el agresor no consiga su objetivo.

Aclaraciones:

1. El protector no siempre es el poseedor.
2. El agresor no siempre es el aspirante o poseedor.
3. Ambas figuras pueden ser delegadas a terceros por el cambio de otro valor.
4. El valor no puede ser concreto, por ejemplo se tendría que cuidar el honor, intimidad, conocimiento, etc.
5. La situación global indica que no será lo mismo el robo de un comercio en Argentina que en Andorra sus habitantes se ven obligados para sustituir.

Los **competidores** se pueden apreciar según su interés como:

- **Competidor interno:** aquel que piensa en el interés de la organización está por encima de sus intereses, y por lo tanto, actúa para sobreponer su interés personal, provocando daños en la organización.

- **Competidor externo:** es aquel que actúa para arrebatar al poseedor lo que para el significa un valor empresarial o personal (clientes, mercado, información, etc.).

"La seguridad es un problema de competencia y rivalidad, si no existiera un competidor-amenaza el problema no es de seguridad".

En general desde un plano social, comercial e industrial hemos evolucionado la técnica, y científicamente desde una era primitiva agrícola la fecha de hoy, siempre se han estado usando los mismos principios (en algunos casos inferiores).

En el presente, cuando se habla de información se está haciendo referencia a la información que es procesada por un sistema informático. Un sistema informático se puede definir como el conjunto de personas, computadoras (hardware y software), papeles, medio de almacenamiento digital, el entorno en donde actúan y sus interacciones.

Entonces de aquí podemos decir que el objetivo de la Seguridad Informática será mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora.

Análisis del objetivo de la seguridad informática

En la Seguridad Informática hay que tener muy en claro que lo que se pretende proteger es la información. Dentro de la información que vamos a proteger se administra en Datos.

La **Información** "es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Desde el punto de vista de la ciencia de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo.

Así, definamos **Dato** como "una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

Los datos convenientemente agrupados, estructurados e interpretados se consideran que son la base de la información humanamente relevante que se pueden utilizar en la toma de decisiones, la reducción de la incertidumbre o la realización de cálculos.

Por ejemplo si tenemos los datos 9, 1, 0, podemos obtener la agregación 1990 que es la información que nos mostrara la representación de tal vez el año de 1990.
Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

La información puede ser pública o no según su importancia o valor. La información pública puede ser visualizada por cualquier persona. Mientras que la privada solo puede ser vista por un grupo selecto de personas que trabaja con ella. Algunas características para preservar de la información son las siguientes:

1. Es crítica: es indispensable para garantizar la continuidad operativa.
2. Es valiosa: es un activo con valor en sí misma.
3. Es sensitiva: debe ser conocida por las personas que la procesan y solo por ellas.

La **disponibilidad** u **operatividad**de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. También se requiere que se mantenga correctamente almacenada con el hardware y con el software funcionando perfectamente y que de alguna manera en caso de algún problema que sea fácil la recuperación y en forma satisfactoria.

La **integridad** de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea restringida para posteriores controles o auditorias. Se puede llegar a presentar alguna falla de integridad a causar de un mal software, falla de hardware, modificación del sistema por el mismo personal o algún tipo de virus informático.

El **control** en las organizaciones es primordial, toda información se debe de clasificar con cierto grado de importancia, para poder asegurar que los usuarios autorizados puedan decidir cuándo y cómo permitir el acceso a la misma.

La **autenticidad** nos permitirá afirmar que la información con la que contamos es válida y utilizable en forma, tiempo y distribución. Una vez teniendo información verídica nos permite asegurar el origen de la misma, validando al emisor de la misma, para evitar suplantación de identidades.

Según las características anteriores sobre la información, se pueden adherir algunos aspectos particulares tales como:

- **Protección a la Replica:** Esta característica nos asegura que una transacción sólo puede realizarse una vez, a no ser por alguna determinación del usuario. No se podrá grabar una transacción para luego reproducirla, mucho menos si el propósito es copiar la transacción para después hacer parecer que se recibieron múltiples peticiones con el mismo remitente original.
- **No repudio:** con un buen flujo y manejo de la información, se evita que cualquier entidad que envió o recibió información alegue de que no la envió o recibió en su defecto.
- **Consistencia:** En un sistema computacional es de suma importancia que el sistema tenga disponibilidad completa, que se comporte siempre como se supone como debería hacerlo, ante los usuarios debidos.
- **Aislamiento:** Este aspecto permite regular y controlar el acceso al sistema, así administrar quien puede y quien no entrar a ver información valiosa, impidiendo que personas no autorizadas hagan uso del sistema.
- **Auditoria:** Es la capacidad simplemente de revisar y corroborar que las acciones y procesos se están llevando a cabo en el sistema, cuando se realizan y que sea el usuario adecuado.

El término **Amenaza** puede entenderse como algún hecho que puede producir algún daño provocado por algún evento natural o antrópico, es decir originado por alguna actividad humana. Viéndolo desde un entorno informático, se puede considerar como cualquier elemento que comprometa al sistema.

Las amenazas pueden ser analizadas de 3 formas según su proximidad: antes del percance, durante y después. En base a lo anterior se conformaran políticas para garantizar la seguridad del sistema informático.

a. **La prevención (antes):** se implementaran mecanismos que reforzaran la seguridad de un sistema.
b. **La detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Por lo general estas revisiones se dan en auditorias.

c. **La recuperación (después):**una vez que en el sistema ya se haya detectado alguna violación, se aplican criterios de seguridad para retornar el sistema a su funcionamiento normal.

Cualquier persona encargada de un Sistema de Información, debe de estar consciente que ante un problema de seguridad, normalmente las medidas defensivas que estén definidas no solucionan un problema dado, si no solo lo transformaran o retrasaran. La amenaza o riesgo siempre seguirá allí, y entonces se debe de cuestionar lo siguiente:

- ¿Cuánto tardara la amenaza en superar la "solución" planteada?
- ¿Cómo se hace para detectarla e identificarla a tiempo?
- ¿Cómo se hace para neutralizarla?

Para poder comprender mejor las preguntas definiremos **Riesgo** como la proximidad o posibilidad de daño sobre un bien.
Cuando hablamos de riesgo en nuestro Sistema Informático, se puede referir amenazas de actos naturales, errores u omisiones humanas y actos incondicionales.

La reducción de riesgo se logra a través de la implementación de medidas de protección, que se basan en los resultados del análisis y la clasificación de riesgo.

- Medidas físicas y técnicas: Construcción de edificio, control de acceso, planta eléctrica, antivirus, datos cifrados, contraseñas inteligentes, etc.
- Medidas personales: Contratación eficaz del personal que dará uso al sistema, sensibilización, capacitación del personal, etc.
- Medidas organizativas: Normas y reglas, seguimiento de control, auditorias, etc.

Analizando cualquier riesgo, el propósito de las medidas de protección para nuestro Sistema Informático, solo se tiene un efecto sobre los componentes de probabilidad de la amenaza, es decir, una vez aumentando nuestra capacidad técnica, personal y organizativa, reducen las vulnerabilidades ante las amenazas que nos enfrentamos. Para amenazas muy comunes se pueden tomar algunas medidas de protección tales como:

- Medidas dependiendo del grado del riesgo
  - -Medio riesgo: Medidas parciales para mitigar el daño
  - -Alto riesgo: Medidas exhaustivas para evitar daño
- Verificación de funcionalidad
  - -Respaldo por coordinación
  - -Esfuerzo adicional y costos VS eficiencia
  - -Evitar medidas pasadas o molestas
- Fundado en normas y reglas
  - -Actividades, frecuencia y responsabilidades

-Publicación

Considerando que la implementación de medidas de protección está directamente en relación con inversiones de recursos económicos y procesos operativos, la mayoría de las organizaciones opta por tener medidas de medio riesgo, ya que resulta mucho más costoso y complejo, que las que solo mitigan el daño.

Una medida de protección no se puede poner simplemente de la nada, se tiene que hacer un estudio donde se verifique su factibilidad, es decir que técnicamente funcionaran y cumplirán con el propósito, que tendrán una buena operatividad institucional, y que el personal fácilmente se apropiara a estas. De no ser así, podrían paralizar u obstaculizar los procesos operativos de la organización.

Ante cualquier tipo de riesgo que pudiera terminar en tragedia sobre nuestro sistema, debemos de tener en claro los siguientes objetivos que perseguimos para el bien de la organización:

1. Minimizar la posibilidad de ocurrencia.
2. Reducir al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseñar de métodos para la más rápida recuperación de los daños experimentados.
4. Corregir las medidas de seguridad en función de la experiencia recogida.

Otro concepto que debe de quedar claro es el Daño es el resultado de alguna amenaza. Este por lo general se produce porque el protector no supo identificar adecuadamente la amenaza.
El protector es el encargado de detectar cada una de las vulnerabilidades del sistema que pueden ser explotadas y empleadas por la amenaza, para comprometerlo. Una vez detectadas las debilidades aplicara medidas de protección adecuadas.
La seguridad que se logre alcanzar indicara la situación en que se encuentra el sistema informático, si está libre de todo daño, peligro o riesgo, aunque es muy difícil conseguir una totalidad de fiabilidad. Para poder garantizar el 100% tiene que tener total integridad, operatividad, privacidad, control y autenticidad.

Seguridad en nuestro sistema informático
Como visto anteriormente es vital hay algunas funciones que se tienen que asegurar para tener un óptimo desempeño en el sistema tales como:

1. **Reconocimiento:** Cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con mencionada identificación. El propósito de esta función es conseguir que no se produzca acceso y/o manipulación indebida de los datos o que en su defecto, quede registrada para posteriores aclaraciones según se requiera.
2. **Integridad:** Un sistema integro en el que todas las partes que le constituyen funcionan de forma correcta en su totalidad proporcionan una herramienta de trabajo muy eficaz.
3. **Aislamiento:** Los datos utilizados por los distintos tipos de usuarios, deben ser independientes unos de los otros lógica y físicamente (usando técnicas de ocultación y/o

compartimiento). En este punto los datos que se les debe de tomar más consideración son los accesibles y los críticos.

4. **Auditoria:**En esta función se hace un análisis mediante exámenes, demostraciones, verificaciones, o comprobaciones del sistema. Estas comprobaciones se deben de realizar a como sea necesario, con tal de obtener datos precisos y que aporten confianza a la dirección.
5. **Controlabilidad:** Todo el sistema en general debe de estar bajo un control permanente.
6. **Recuperabilidad:** En caso de emergencia, se debe de tener una opción para recuperar recursos perdidos o dañados, y tenerla habilitada en todo momento.
7. **Administración y custodia:** La vigilancia nos permitirá conocer en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una retroalimentación del sistema de seguridad, de tal forma de mantenerlo actualizado contra nuevas amenazas.

¿Qué hay que asegurar en un sistema informático?

Existen 3 elementos que básicamente son los que hay que proteger: **el hardware, software y los datos.**

Por **hardware** se entiende que es el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresora, CD-ROM, cintas, componentes de comunicación.

El **software** son todos los elementos lógicos que hace funcional al hardware: sistema operativo, aplicaciones, utilidades.

Lo más importante en toda organización son los **datos**, refiriéndose a la información lógica que maneja el software y el hardware: base de datos, documentos, archivos.
Además de estos 3 elementos, muchas veces se habla otro denominado **fungible;** que son aquellas herramientas que se gastan o desgastan con el uso continuo: papel, tóner tinta, cintas magnéticas, disquetes, etc.

Todos los elementos mencionados arriba tienen gran importancia en toda organización, ya que son el resultado del trabajo realizado. Pero analizando, si se daña el hardware, los elementos fungibles, o el mismo software, se pueden volver a adquirir desde su medio original. En cambio los datos obtenidos en base el esfuerzo y trabajo son imposibles de recuperar porque solamente son nuestros, a no ser que se tengan respaldos, copias de seguridad, pero aun así es difícil devolver absolutamente todos los datos a la forma anterior del daño.

Hablando en general de los elementos a proteger, existen una gran cantidad de riesgos, amenazas, y ataques que podemos clasificar de la siguiente manera:

1. **Ataques pasivos:** el atacante no altera la comunicación, si no que únicamente la monitoriza la información que está siendo transmitida (intercepción de datos y análisis del tráfico). Por lo general se emplean para:
    - Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitoreados.
    - Control del volumen de tráfico de intercambio, obteniendo así información acerca de actividad o inactividad inusuales.
    - Control de las horas habituales de intercambio de datos, para extraer información acerca de los periodos encontrados con actividad.
2. **Ataques activos:** estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Por lo general estos ataques son propiciados por los hackers, piratas informáticos o intrusos. Estos ataques se pueden subdividir en 4 categorías:
    - INTERRUPCION: Si hace que un objeto del sistema se pierda, quede inutilizable totalmente no disponible.
    - INTERCEPCION: Si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
    - MODIFICACION: Además de conseguir acceso modifica el objeto.
    - FABRICACION: Se crea un objeto similar al original del sistema pero ya atacado, de forma que le sería difícil distinguir uno de otro al usuario.
    - DESTRUCCION: Es una modificación que deja totalmente inutilizable el objeto.

Relación operatividad-seguridad (costo beneficio)

Para poder selección e implantar una medida de seguridad que sea realmente eficaz, se necesita hacer un análisis para poder encontrar un punto de equilibrio entre los intereses referidos a seguridad (beneficio), contra los requerimientos operacionales (costo).

Por ejemplo se puede plantear un caso relacionado con la operatividad-seguridad, mostrando una computadora extremadamente segura con las siguientes características:

- Instalada 20 metros bajo la tierra en un recinto de hormigón.
- Aislada informáticamente de otras computadoras.
- Aislada eléctricamente y alimentada por un sistema autónomo.

Con esto se refleja una computadora completamente segura, inversamente proporcional en su utilidad. Es decir que incrementar demasiado la seguridad en un sistema informático su operatividad desciende y viceversa.

Como se observa en el grafico esta función se vuelve exponencial al acercarse al 100% de seguridad. Los costos se disparan (tendientes a infinito) por los complejos estudios que se deberán realizar para mantener este grado de seguridad.

A pesar de por mas costos que se inviertan en tener la mejor seguridad, no existe una prueba total contra engaños, sin embargo si hay que considerar niveles mínimos exigibles. Este nivel

dependerá del análisis de los riesgos que se están dispuestos a correr tomando como referencia el costo sobre las medidas a tomar en su caso.

Seguridad física

Concepto

Esta punto es importante concientizar que por más segura que sea nuestra organización ante ataques externos, hackers, virus, etc.; habrá vulnerabilidad desde algún desastre físico como incendios, terremotos, daños físicos por mal manejo de equipo, etc.

La seguridad física es uno de los puntos que hay que resaltar, por ser uno de los menos considerados a la hora de hacer un diseño informático. La **Seguridad Física** consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". En relación a la informática se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo así como de los medios de acceso al remoto, implementados para proteger el hardware y medio de almacenamiento de datos.

Amenazas contra la seguridad física

El sistema y su implementación es único para cada empresa, a pesar de poder estar usando algunas el mismo no lo implementan tal cual, por lo tanto la seguridad a implementar será única. Así podemos decir que para el edificio en que nos encontraremos, se recomiendan pautas de aplicación general, pero no procedimientos específicos. Para ejemplificar esto depende la posición Geográfica en la que se encuentra la Organización, si se encuentra entre ríos, actividades sísmicas, etc.

La seguridad física está enfocada a eliminar o suavizar daños posibles de amenazas ocasionadas por el hombre o por la naturaleza del medio físico en el que se encuentra el ubicado nuestra organización.

Las principales amenazas que se ubican en la seguridad física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios sabotajes internos y externos deliberados.

No es necesario tener lo máximo en seguridad, ya que la solución sería extremadamente cara, en algunos casos basta con optar por el sentido común para darse cuenta que dejando la puerta

cerrada con llave, o cortar la electricidad en ciertas aéreas, son técnicas sencillas que aún siguen siendo válidas en muchas partes.

A continuación algunos de los factores que atentan con las instalaciones físicas de la empresa. Para así poder considerar acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

Incendios

Un incendio es una ocurrencia de fuego no controlada que puede abrasar algo que no está destinado a quemarse. Por lo general son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas, el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es considerado como una de las amenazas más peligrosas contra el equipo de cómputo, ya que por lo general se ocasionan por accidentes a deshoras de trabajo donde no se pudiera combatir, y que este puede destruir fácilmente los archivos de información y programas.

Algo malo al momento de combatir el fuego es que siguen dejando casi o igual que el mismo daño propiciado por el fuego, sobre todo a los componentes electrónicos. El dióxido de carbono, resulta peligroso para los propios empleados si se quedan atrapados en la sala de cómputo.

Algunos de los factores que se pueden considerar para reducir los riesgos de ser afectado por un incendio nuestro centro de cómputo son los siguientes:

1. El área en la que se encuentra el centro de cómputo debe de estar apartado de cosas no combustibles o inflamables.
2. El local no debe de estar en un lugar encima, debajo o adyacente algún área donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos, o sustancias radiactivas.
3. No debe estar permitido fumar en el área de proceso.
4. Deben emplearse muebles incombustibles, cestos de basura metálicos, deben evitarse materiales de plástico e inflamables.
5. Contar con equipo de ventilación y detección de incendio adecuado, además de contar con extinguidores de fuego.
6. Mantener el equipo sobre una temperatura que no sobrepase los 18º C y el límite de humedad no supere el 65% para el no deterioro del equipo.

Inundaciones

Una inundación se define como la ocupación por parte de agua de zonas que habitualmente están libres de esta. Esta invasión de agua se puede dar pos escurrimientos superficiales o por acumulación de agua en un terreno plano donde no se cuente con drenaje natural o artificial.

Además de las causas naturales, pueda que haya alguna inundación provocada por la necesita de apagar algún incendio en un piso superior, o por algún percance de las tuberías del edificio.

Para poder reducir los riesgos ante inundaciones se pueden tomar medidas como: construir un techo impermeable para evitar el paso de agua desde un nivel superior, y poner el centro de cómputo en una planta segura si se cuenta con más de un piso.

Terremotos

Son fenómenos de una sacudida brusca y pasajera de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas. Estos fenómenos pueden llegar a ser una catástrofe a tal grado de destrucción de edificios, pérdidas humanas, o poco intensos que solamente instrumentos muy sensibles los detectan. El problema en la actualidad que estos fenómenos han estado ocurriendo en lugares donde no había detectado alguna actividad sísmica, pero por fortuna los daños suelen ser ligeros.

Instalación eléctrica

El motor enérgico de un sistema informático es la electricidad. Por lo tanto es una de las áreas principales a considerar en la seguridad física. A medida que los sistemas se vuelven más complicados se requiere de un especialista para que evalúe los riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Los riesgos más comunes para el cableado son:

1. Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipo de radio o microondas.
2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. Daños en el cable: los daños normales con el uso se pueden dañar material del cable, dañado ya no preservaría la integridad de los datos transmitidos o dañar el propio cable, lo que hace que las comunicaciones dejen de ser fiables.

Robo

El robo es clasificado como un delito contra el patrimonio, consiste en el apoderamiento de bienes ajenos, con intención de lucrarse, empleando para ello fuerza en las cosas, violencia o intimidación en la persona.

Las computadoras son vistas como posesiones muy valiosas en las empresas expuestas a hurto o algún tipo de daño. Más que daño o hurto del equipo la información importante o confidencial puede ser fácilmente copiada por alguno de los operadores de la organización. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan una maquina o una calculadora. El software es una propiedad que muy fácilmente puede ser copiado en cintas o discos sin dejar ningún rastro.
Evaluar y controlar permanentemente la seguridad física del edificio es la base para comenzar a integrar la seguridad como una función primordial de cualquier organismo.
Estar prevenidos ante desastres ambientales o acceso físico ante personal no autorizado permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Según sea el caso de cada empresa, las alternativas estudiadas le serán de ayuda para que en todo momento saber su situación, y poder tomar decisiones sobre la base de información brindada por los medios de control adecuados.

Seguridad lógica

Concepto
Después de ver todas las amenazas que nos podrían afectar al no invertir sobre la Seguridad Física, no podemos dejar pasar o no tomar en consideración nuestra Seguridad Lógica, ya que la mayoría de los daños no se dan sobre nuestros medios físicos, si no sobre la información almacenada y procesada.
Como ya mencionado anteriormente, el activo más importante y valioso que poseemos es la información, entonces aparte de cuidarnos de percances naturales o daños físicos, hay otro tipo de amenazas que no se pueden percatar, pueden estar haciéndonos daño sin darnos cuenta, para ello debemos de implementar técnicas para integrar una buena seguridad lógica en nuestra organización.
La Seguridad Lógica involucra todas aquellas medidas establecidas en la administración (usuarios y administradores de recursos de tecnología de la información) para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. Esta consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo nos permita acceder a ellos personas autorizadas.

Algunos de los objetivos que trata la seguridad lógica son:

- Restringir el acceso a los programas y archivos a personal no autorizado.

Revista de Investigación Académica sin Frontera
ISSN: 2007-8870

http://revistainvestigacionacademicasinfrontera.com

- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa, para que no puedan modificar los programas ni los archivos que no les correspondan.
- Asegurar que estén siendo utilizados los programas, archivos y datos correctos en sus labores.
- Que la información sea transmitida única y necesariamente al destinatario que la ocupa y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos, por si llegara a ofrecerse en caso de algún problema con el medio principal.

Control de acceso

Mejor conocidos como access control se refiere a la habilidad ya sea de permitir o denegar el uso de algún recurso a una entidad en particular. Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, base de datos, en un paquete especifico de seguridad o en cualquier utilitario.

Un control de acceso nos brinda una gran ayuda para proteger el sistema operativo de las redes, al sistema de aplicación y nuestra base de datos de la utilización o peor aún de la modificación o eliminación sobre los archivos por personas no autorizadas. Hay que mantener una integridad sobre la información involucrada, otorgando privilegios y determinar modo de uso de la aplicación y datos, para resguardar la información confidencial de accesos no autorizados.

Identificación y autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es a base de la mayoría de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina **identificación** al momento en que el usuario se da a conocer al sistema; y **autentificación** a la verificación que realiza el sistema ante la identificación. Existen 4 tipos de técnicas que permiten realizar la autentificación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Algo que solamente el usuario conoce: por ejemplo clave secreta de acceso, password, clave criptógrafa, PIN, etc.
- Algo que el usuario posee: por ejemplo una tarjeta magnética.
- Algo que el usuario es y lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el usuario es capaz de hacer: por ejemplo los patrones de escritura.

De las técnicas que se acaban de mostrar, cabe resaltar los primeros dos enunciados mencionados, ya que es común y muy frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autentificación biométricos serían los más

apropiados y fáciles de administrar, pero resultando algo costosos, ya que es muy difícil su implementación eficiente.

Para el sistema, le es conveniente que el usuario se identifique y autentifique solo una vez, una vez que el sistema valide la autentificación se pueda acceder a las aplicaciones y los datos a los que su perfil le permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota.

La seguridad informática se basa, en gran medida en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autentificación y autorización de accesos.

Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de los usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o la aplicación según corresponda.
- Además de la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
- Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
- Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad

para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

En este último caso, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible, para en caso de despido, el permiso de acceder se anule previamente a la notificación de la persona.

4.4 ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Por decir, el programador, líder del proyecto, gerente de área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

4.5 LIMITACIONES A LOS SERVICIOS

Estos se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Por ejemplo, en una organización se dispone de un cierto número de licencias para la utilización simultánea de un determinado producto de software, considerando que se tienen 5 licencias que son las que usaran lo ya planteado, a un sexto usuario no se le dará acceso al sistema.

4.6 MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario tener interacción sobre los recursos y a la información.

- **Lectura:** el usuario únicamente podrá leer y visualizar la información o material, pero este no podrá alterarla. Debe considerarse también si podrá ser copiada o impresa.
- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar los programas.
- **Borrado:** Permite al usuario eliminar recursos del sistema (programas, campos de datos, archivos, etc.). El borrado es considerado como una forma de modificación.

Control de acceso interno

Por lo general se usan para realizar la autentificación del usuario, protegiendo los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave son accesibles y de muy bajo costo. Pero cuando el usuario hace uso de varias aplicaciones a la vez, y en cada una de ellas tiene asignado una distinta clave para autentificarse, utilizando varias palabras, le podría ser dificultoso recordarlas. Por otra parte si se usaran claves sencillas y fácilmente deducibles, se vería disminuida la utilidad y eficiencia de esta técnica.

Hay dos técnicas de gran ayuda en el control de acceso interno:

Sincronización de password: Consiste en permitir que esa clave única que le sea designada al usuario, sea tal vez un poco compleja, pero que esté interrelacionada con los distintos sistemas y aplicaciones, es decir con una sola clave podrá autentificarse en todo lo que le haya sido designado. Podría parecerque esto sea negativo para la seguridad de un sistema, ya que una vez descubierta tendrían acceso a todos lo demás, pero estudios han demostrado que cuando las personas manejan más de una clave o password, generalmente tienden a guardar la clave escrita para no olvidarla, lo cual significa un riesgo mayor.

Caducidad y control: Este mecanismo controla cuando pueden y/o deben cambiar las claves de los usuarios. El administrador define un periodo, ya sea corto o largo.

Control de acceso externo

- **Dispositivos de control de puertos:** Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un modem.
- **Firewall o puertas de seguridad:** Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo internet). Los firewall permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de los atacantes o virus a los sistemas de la organización.
- **Acceso de personal contratado o consultores:** Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.
- **Accesos públicos:** Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada, deben tenerse medias especiales de seguridad, ya que se incremente el riesgo y se dificultas su administración.

dministración

Una vez que se hayan establecido los controles de acceso en la organización sobre los sistemas y aplicaciones, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, pruebas, modificaciones, y a todo esto darle el seguimiento correcto sobre el acceso de los usuarios al sistema.

Las políticas de seguridad que se vayan a desarrollar respecto a la seguridad lógica deben ayudar a resolver y determinar los controles de acceso, especificando cuidadosamente consideraciones necesarias para el establecimiento del perfil de cada uno usuario. La definición de los permisos de usuario requiere determinar cuál será el nivel de seguridad para nuestro sistema y datos.

Para comenzar con la implementación, es conveniente tener identificado la información más sensible, o las aplicaciones más críticas, de ahí partir y avanzar con un orden de prioridad descendiente.

A continuación se muestra un proceso para organizar el personal que consiste en los siguientes 4 pasos:

1. **Definición de puestos:** Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
2. **Determinación de la sensibilidad del puesto:** para esto es necesario determinar si la función requiere de permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
3. **Elección de la persona para cada puesto:** se basa en considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Así mismo, para los puestos definidos como críticos puede requerirse una verificación de antecedentes personales.
4. **Entretenimiento inicial y continuo del empleado:** cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que le sean asignadas, debe de hacerse saber las políticas organizacionales haciendo hincapié en la política de seguridad. El individuo debe de conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

NIVELES DE SEGURIDAD INFORMÁTICA

CLASIFICACIÓN DE NIVELES DE SEGURIDAD INFORMÁTICA
Los niveles de seguridad son distribuidos de acuerdo con el sistema operativo que se está utilizando sobre la red de la empresa o institución ya sea pública, privada, gubernamental, entre esos se tienen los siguientes:

Nivel D1	El sistema entero no es confiable
Nivel C1	Protección de hardware
Nivel C2	Resuelve problemas del nivel C1 y C2
Nivel B1	Protección de seguridad etiquetada
Nivel B2	Protección estructurada
Nivel B3	Dominio de seguridad
Nivel A	Diseño verificado

CLASIFICACIÓN DE NIVELES DE SEGURIDAD INFORMÁTICA

NiveL D1
Es la forma más baja de seguridad, esta norma establece que el sistema entero no es confiable. No dispone de protección para el hardware; el sistema operativo se compromete fácilmente y no existe autentificación respecto a los usuarios y sus derechos a tener acceso a la información almacenada en la computadora.

Nivel C1
Se requiere identificación de usuarios que permite el acceso a la distinta información que hay. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene el control de total acceso. Los usuarios deben de identificarse ante el sistema mediante su login y contraseña, se emplea esta combinación para determinar los derechos de acceso a programas e información que tiene cada usuario.

Estos derechos de acceso son los permisos de archivo y directorio, los controles de acceso discrecional permiten al dueño del archivo o directorio, así como al administrador del sistema evitar que ciertas personas o grupos tengan acceso a dichos programas o información. Sin embargo, no se impide que la cuenta del administrador del sistema realice ninguna actividad, en consecuencia un administrador poco escrupuloso puede comprometer fácilmente la seguridad del sistema sin que nadie lo sepa.

Además, muchas de las tareas cotidianas de administración del sistema solo pueden ser realizadas por el login de usuario llamado raíz (root). Con la actual descentralización de los sistemas de cómputo, no es raro que en una organización se encuentren dos o tres personas que conocen la clave del usuario root, esto si es un grave problema pues no habría forma tal de distinguir cual de los usuarios que ingresa como root realizo cualquier tipo de cambio en el sistema o aplicación.

Nivel C2
Está diseñado para ayudar a resolver los problemas anteriores, además de las funciones del nivel C1, el nivel C2 cuenta con características adicionales que crean un ambiente de acceso controlado. Este ambiente tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, con base no solo en los permisos, sino también en los niveles de autorización.

Este nivel de seguridad requiere que se audite al sistema, lo cual implica registrar una auditoria por cada acción que ocurra en el sistema. La auditoría se utiliza para llevar registros de todas las acciones relacionadas con la seguridad como puede ser las actividades efectuadas por el administrador del sistema. La desventaja de la auditoria es que requiere de recursos adicionales del procesador y subsistema de disco.

Con el uso de autorizaciones adicionales, es posible que los usuarios de un sistema C2 tengan la autorización para realizar tareas de administración del sistema sin necesidad de la contraseña del root, esto permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

La auditoría se usa para llevar registros de todas las acciones relacionadas con la seguridad como puede ser las actividades efectuadas por el administrador del sistema. La auditoría requiere autentificación adicional pues, sin esta ¿Cómo estar seguros de que la persona que ejecuta el comando realmente es quien dice ser?; la desventaja de la auditoria es que requiere recursos adicionales del procesador y del subsistema de disco.

Con el uso de autorizaciones adicionales, es posible que los usuarios de un sistema C2 tengan la autorización para realizar tareas de administración del sistema sin necesidad de la contraseña root. Esto permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Nivel B1
Es también llamado protección de seguridad etiquetada, es el primer nivel con soporte para seguridad multinivel, como el secreto y el ultra secreto. En este nivel se establece que el dueño del archivo no puede modificar los permisos de un objeto que este bajo control de acceso obligatorio.

CASO PRÁCTICO

Caso práctico empresa: Grupo Osuna S.A.

Grupo Osuna S.A.es una cadena comercial de súper mercados que cuenta con más de 9 sucursales distribuidas en la región del mayo, como lo son Navojoa, Villa Juárez, Bacobampo, Álamos, San Ignacio, Huatabampo, Etchojoa, etc. A parte de las sucursales se tienen almacenes donde se guardan productos abarrotes, fruta y verdura, carnes, etc.

Las sucursales son como cualquier tienda o súper encargada de vender distintos productos como abarrotes, lácteos, cárnicos, embutidos, botanas, secos, granos, etc. los cuales son dirigidos y suministrados por la matriz central que son las oficinas de Super1 o Súper Canal 1.

SISTEMA ACTIENDA
El sistema principal que se usa en las tiendas, almacenes y oficina es ACTIENDA, este sistema puede ser conseguido empaquetado con funciones ya determinadas y bien definidas, pero en Grupo Osuna S.A. se pidió a la medida para un mejor funcionamiento y automatización de muchos procesos, es algo completo respecto a las funciones diarias, como lo es descrito a continuación:

CATALOGO DE VENTAS: Este apartado se usa en el punto de venta, tiene muchas funciones operantes, y se mantiene el registro de todo respecto a la venta en la base de datos de cada equipo. Los datos que se guardan sobre las ventas son detalles como si se pago con dinero en efectivo, tarjeta de crédito, débito, vales de despensa, etc.

CATALOGO DE PEDIDO: Este apartado se usa en los almacenes de Grupo Osuna S.A., y en las bodegas de cada tienda. Las funciones que tiene son respecto a los distintos movimientos que se pueden capturar como compras, salida por traspaso, entrada por traspaso, salida por ajuste, entrada por ajuste, salida por merma, etc. Aquí el sistema registra todo lo que entra y sale al almacén o bodega, aplicando el tipo movimiento correcto amparando todo con lo que se cuenta en la bodega. Hay que hacer bien los registros cuando entra mercancía por compra a proveedor, si se le da salida para traspasar producto a otra tienda, si se le dio entrada por ajuste por faltante en algún inventario que se hizo, si se le dará salida por merma por producto en mal estado que ya no es apto para la venta, entre muchos más casos.

CATALOGO DE REPORTES: Este catálogo es muy usado en la oficina, y parte en las tiendas y/o almacenes. La función es simple, solamente sirve para mostrar toda la información generada por cada uno de los movimientos registrados. La ventaja aquí que el catalogo tiene una gran variedad de opciones para solicitar la información de manera que nos sea más cómoda la consulta de datos según nuestra necesidad. Una vez generado el reporte el sistema también nos da la opción de poder imprimirla, o para trabajar más a fondo con esa información exportarla a documento de texto, hojas de cálculo Excel, o formato para cargar pólizas a CONTPAQ.

USO DE LICENCIA ACTIENDA Y CONTPAQ

Cualquier máquina que use ACTIENDA debe de tener su respectiva licencia. En todas las tiendas se necesita ACTIENDA, una licencia por cada computadora que se tenga en caja, o en recibo. Al igual que los almacenes. Lo único que varía es que la contabilidad de las tiendas se hace la oficina, la póliza de Diario e Ingreso, y en los almacenes se hace la póliza de diario por no tener ventas, más que solamente traspasos a las tiendas y movimientos de mercancía.

Entre las distintas tiendas de la región del mayo se les provee un ACTIENDA previamente configurado y detallado según el sitio. La administración de cada tienda es independiente de la otra, suele ser muy parecida pero no igual en su totalidad. Es decir, el caso de algunas ofertas se hace directamente a todas las sucursales por igual, de manera global, pero si en alguna de las tiendas se conoce que la competencia tiene mejor precio entran modificaciones de ofertas internas en la tienda.

Las licencias de ACTIENDA usadas en las tiendas y almacenes se administran desde una CPU sencillo con Windows XP usado como servidor, en donde se guarda toda la información en una base de datos.

Para la contabilidad de los almacenes, las computadoras se conectan a un escritorio remoto enlazado con el servidor de la oficina Windows Server 2008, en donde pueden trabajar con Contpaq.

COMUNICACIÓN EN LA EMPRESA GRUPO OSUNA S.A.

Los medios de comunicación que se basa las oficinas, almacenes y tiendas de Grupo Osuna S.A. son en base a teléfonos de Red por plan con llamadas ilimitadas, correos electrónicos, y un servidor gratuito de mensajes instantáneos llamado SPARK. Las llamadas se usan por lo general para acordar cosas de manera rápida, y clara. Los correos electrónicos para dar formalidad y respaldar cualquier tipo de movimiento. Y el sistema Spark para detalles mínimos y velocidad en la transmisión de archivos, fotos, sacan o cualquier documento. Lo bueno del Sistema Spark es que la administración de los contactos la ve directamente el departamento de sistemas, evitando distracciones o mal uso del programa de mensajería instantánea.

Las oficinas de Grupo Osuna S.A. se componen por varios departamentos como:

- Archivo
- Compras
- Ingresos
- Contabilidad
- Sistemas
- Inventarios
- Cuentas por pagar
- Egresos
- Presupuestos
- Recursos Humanos
- Gerencia General
- Dirección

ACTIVIDADES POR DEPARTAMENTO EN EL SISTEMA

En cada uno de los departamentos varia el número de personas según las actividades que se encomienden o se apoyen unos con otros. Es decir que en los departamentos se les provee de una maquina cada usuario, pero esta varia el sistema según las funciones que se le determinen.

Archivo: por sus actividades encomendadas es el único departamento donde no le es designada alguna computadora, son pocas las actividades y todas fuera del sistema, y cuando se le presentan toma la computadora de uso común, o en casos extraordinarios la información se le entrega impresa por algún otro departamento.

Compras: Es uno de los departamentos que mas interacción tienen con las tiendas y el sistema. Por el volumen de compras y variedad, están repartidas las compras en varios usuarios como compra de abarrotes, papelería y granos, mantenimiento, cárnicos, frutas y verduras. A cada uno de los usuarios se le tiene un ordenador en el que se les encomienda desarrollar la actividad de abastecer de mercancía suficiente, manteniendo un margen y un stock que se debe respetar. Para poder concretar la compra se tiene que checar los correos con los pedidos de las tiendas, y echar un vistazo en las existencias de cada tienda. Compras tiene acceso a todos los ACTIENDA, ya sea de almacenes o sucursales, ya que con frecuencia necesita información en general de movimientos, compras bien capturadas y registradas con o sin IVA, existencias de productos, etc.

Ingresos: El departamento de ingresos se encarga de recopilar información de las tiendas referente a todo tipo de ventas. Las ventas que se dan en las tiendas tienen que ser muy bien registradas y conceptuadas según su tipo. Es importante distinguir muy bien entre vender con efectivo, vales de despensa, e incluso distinguir compra de una tarjeta de débito y crédito. La interacción con el sistema es un poco simple, se consulta la información referente a las ventas de cada tienda, y se exporta a un archivo con formato compatible para cargar con el sistema de contabilidad CONTPAQ, de ahí se hacen ajustes necesarios y modificaciones para cerrar las pólizas de ingreso.

Contabilidad: Todas las pólizas en general referentes a las sucursales y la oficina se hacen en el departamento de contabilidad, y próximamente de los almacenes también. Al igual que el departamento de ingresos en el sistema se consulta información pero más global, registrando todos los movimientos que se hicieron en cada una de las tiendas al día, para después exportar al archivo compatible con CONTPAQ y cargar la póliza.

Sistemas: Como bien se reconoce es el principal usuario y administrador del sistema. Las actividades que desarrolla están relacionadas con todo el personal en general de la organización. Es el principal encargado de ver todo lo referente a mantenimiento, soporte, composturas, administración de usuarios, asesorías, algunas capacitaciones, reparaciones técnicas, cableados, suministros de todos lo referente a equipo de cómputo, alarmas, grabaciones de cámaras, etc.

Inventarios: En cada sucursal una persona se encarga de llevar el control de inventarios, pero en la oficina esta una persona viendo toda la información en general de tiendas y almacenes, tiene una maquina designada viendo todos los movimientos que se hacen, control de mermas, ajustes, existencias, checando faltantes o excedentes de todas las tiendas en general.

Cuentas por pagar: Entre los soportes para la póliza de diario que mandan las tiendas vienen registrados todos los movimientos que se hicieron en el día, pero lo que se procura en el departamento de cuentas por cobrar solamente son las facturas del producto recibido, para programar su posterior liquidación. Para esto se necesita estar checando todos los movimientos que se hacen en la tienda, sobre todo el producto que le dio entrada con dichas facturas.

Egresos: El departamento de pagos necesita se apoya mucho en el departamento de cuentas por cobrar. Las facturas previamente ordenadas y programadas por cuentas por cobrar, pasan a ser liquidadas mediante cheques, depósitos, transferencias bancarias, etc. Antes de asegurar el pago es necesario confirmar que el monto a pagar coincida con la entrada, que no haya ninguna diferencia y de ser así solicitar alguna nota de crédito. El departamento necesita conexión con el sistema ACTIENDA para checar todo cualquier movimiento mas no modificar, solamente leer reportes, y el sistema de CONTPAQ para registrar en pólizas de egresos de todos los pagos liberados.

Presupuestos: Este departamento se encarga de ver la situación financiera en la que está la empresa. Todos los gastos y cargos extraordinarios se ven con este departamento, para ver donde se puede cargar y abonar las cuentas según sea la situación, checar que toda la contabilidad este a la par con el sistema ACTIENDA. A parte de presentar los estados financieros.

RecursosHumanos: Este departamento solamente interactúa con el sistema CONTPAQ para registrar todo lo referente a nómina de los empleados en General.
GerenciaGeneral: Aquí no se tiene alguna interacción con algún sistema, solamente se encargar de dar seguimiento algunas cosas, y orientar la buena administración en general de la empresa.

Dirección: Es la máxima autoridad encargada de la empresa y dueña. No tiene alguna interacción con ningún sistema a pesar de tener interacción y dominio sobre todos los puestos, solamente revisa información redactada y procesada para dar seguimiento y tomar decisiones.

LOGIN Y CARACTERISTICAS DE LOS EQUIPOS DE CÓMPUTO

Como ya visto anteriormente, cada computadora en general esta previamente configurada para cada usuario, según sus necesidades en el sistema. Primeramente se tiene limitado el acceso libre al sistema operativo usado “Windows XP Service Pack 3”, para poder iniciar sesión y navegar en las utilerías del equipo de cómputo se requiere de una clave previamente definida por el administrador (departamento de sistemas), la cual es responsabilidad del usuario mantener la confidencialidad de la clave, ya que cualquier alteración por proporcionar la clave a terceros el usuario es responsable.

Para el sistema de contabilidad CONTPAQ se usa solamente en la oficina, y los almacenes. En los almacenes los equipos están configurados para poder acceder a un escritorio remoto que los enlaza con el servidor de la oficina, una vez que estén dentro del servidor, necesitan también hacer login en el sistema CONTPAQ. En la oficina para los que tienen uso frecuente y son de confianza se les tiene instalado el programa de contabilidad y pueden acceder sin hacer login. En otras computadoras de la oficina que el uso no es común, se les tiene un escritorio remoto para logear en el servidor general, todas las claves son administradas por los sistemáticos.

El modo de login del sistema ACTIENDA varía un poco que los demás, porque aquí los usuarios son clasificados y según sus responsabilidades y actividades, el tipo de usuario determina los

privilegios que se le otorgaran. Según sea el origen del ACTIENDA es el ID del usuario. Por ejemplo si estamos hablando de la sucursal Villa Juárezlas iniciales serán VL001 (el 001 es el índice que lo genera automático el sistema, el segundo usuario pasara a ser 002), y así se va por tiendas.

En el caso de las tiendas y almacenes, las claves predeterminadas que se designan solamente funcionaran para el ACTIENDA que se dio de alta. Es decir que si una persona con el ID VL001 perteneciente a la sucursal de Villa Juárez, no podrá entrar a la tienda de Huatabampo por que solamente pueden entrar los usuarios con HP001.

En la oficina pasa a ser OF001, y con este tipo de usuario es posible ingresar a cualquier ACTIENDA en general, pero ya dependen las limitantes que ponen los sistemático, por lo general los privilegios son mínimos, de solo lectura de información.

Existe otro tipo de usuarios muy parecidos a los sistemáticos, los AD001 que son administradores, los privilegios que se les brindan son mucho mayores, este tipo de usuario se le designa en la oficina a personal que tiene cargos especiales, como editar o autorizar movimientos muy importantes.

Así se administran los usuarios, pero el sistemático tiene el poder de ejercer tantos privilegios quiera, según sea el caso de cada trabajador y su puesto.

ESTRUCTURA DE LA INFORMACION

La información más importante se trabaja en el sistema ACTIENDA y CONTABILIDAD. Las pólizas de contabilidad se guardan en el servidor principal, y del sistema ACTIENDA son guardados en sus respectivos equipos, con SQL SERVER.

Para poder trabajar la información en la oficina, el programa ACTIENDA está configurado para que el servidor en un lapso entre 2 a 4 horas que este actualizando la información de todas las sucursales.

SEGURIDAD LOGICA

La seguridad lógica interna tanto externa, no es completa en sí, hay detalles que no se han cubierto, tal vez por confianza en los empleados, o por la idea de que los daños que pudiera haber serian mínimos, pero en el tiempo que he estado me ha tocado ver detalles originados por esos descuidos, algunos sencillos, como un caso que se presentó en una tienda, en una computadora de cajas.

PROBLEMA 1

Las computadoras de cajas están configuradas para iniciar normalmente con el sistema operativo. El sistema ACTIENDA es un ejecutable, el cual se utiliza para las ventas y demás movimientos,

las existencias, precios, detalles de los artículos están guardados y capturados en la base de datos. Un servicio que se tiene en las tiendas de Super1 es el de las recargas telefónicas (telcel, movistar, nextel, unefon, etc.). En la empresa para poder realizar la recarga se necesita ingresar a un navegador de internet, el predeterminado que se tiene es el internet Explorer, por poseer mayor compatibilidad con las paginas, y con un certificado de la página de telefonías, se ingresa al sitio donde se hace la petición, con un usuario y contraseña brindado por los sistemáticos es posible realizar toda la operación sin problemas, a excepción de problemas con el servidor de recargas.

Como mencionado anteriormente, las computadoras se entregan configuradas según puesto en donde se utilizara, si el puesto requiere de acceso a internet se le proporciona navegadores pero solo se les permite entrar a páginas que se tenga la necesidad por trabajo, y las demás paginas como de ocio y entretenimiento son bloqueadas para evitar daños o mal uso del equipo de cómputo.

El problema fue que un cajero de la tienda, al ver que el navegador de internet explorer tenia bloqueados los HOST y no poder entrar a la página de Facebook, descargo e instalo otro navegador, Mozilla Firefox, para él fue algo sencillo, pudo ingresar a la página de Facebook, pero no pensó que dañaría las propiedades del certificado que tenia de la página mediante la cual hacían las recargas.

El equipo al ser des configurado ya no hizo recargas telefónicas, y esta anomalía fue reportada hasta el tercer día, posteriormente el departamento de sistemas se encargó de cambiar el equipo momentáneamente mientras volvían a configurar el dañado. Las consecuencias a este problema fue que no pudieron expedir recargas telefónicas durante 3 días, además de reparación por mal uso del equipo.

SOLUCION 1

Para poder lograr que los usuarios sigan con los host bloqueados, que no desconfiguren el navegador de internet, y que no instalen algunas aplicaciones, estos permisos se los quitaron iniciando sesión en el sistema operativo como segundo usuario, y no como administrador, restringiendo de tareas y movimientos que no tengan que ver con sus labores encomendadas.

PROBLEMA 2

Un problema con muchamás gravedad que se presento fue en la oficina, precisamente en el servidor principal, el centro de toda la información. En la oficina algunas personas tienen acceso a cualquier página, por sus labores y responsabilidades, se les confía el acceso y que harán un buen uso del equipo. Se cuenta con una computadora que es de uso común, para lo que se ofrezca, mandar algún correo, escanear, imprimir, etc. Esa computadora tiene internet abierto y se puede ingresar a cualquier página que sea, ya que no se tiene un uso frecuente por los usuarios.

Al parecer la confianza no había sido un problema, pero por la vulnerabilidad y mal uso de los equipos permitieron el paso de un gran virus, que dejo sin sistema a las oficinas por más de 3 días.

Las sucursales y almacenes trabajan con la información del mismo CPU que tienen como servidor, siendo independiente la información de las oficinas para ellos. Por las sucursales no se tuvo algún problema, siguieron con sus ventas y movimientos comúnmente, pero desde la oficina no pudimos trabajar con nada de los sistemas

ACTIENDA y CONTPAQ.

Para poder restablecer todo el sistema, les llevo algo de tiempo, además de asesoría por terceros a la empresa, ya que por la cuestión de las licencias no se tenían los documentos con los cuales se podrían aceptar términos legales.

SOLUCION 2

El problema de un intruso mediante un virus, que haya ocasionado pérdida total del sistema, tal vez no sea tan grave, la solución pudo haber sido sencilla como reinstalar el sistema operativo del servidor, equipar con las aplicaciones y componentes, vaciar los backup, configurar y entrelazar todos los equipos, eso no llevaría tanto tiempo, pero por el extravío de la documentación legal para poder hacer uso adecuado del sistema, le demoro demasiado tiempo a las personas externas que nos ayudaron a encontrar los archivos para validar original y legalmente la reinstalación del sistema operativo que tiene el servidor, posteriormente los miembros de la organización de GRUPO OSUNA S.A. nos encargamos de terminar de restablecer todo el sistema y actualizar toda la información para seguir con las labores al día.

CONCLUSION

La seguridad implica una ausencia de riesgo, o confianza y aceptación sobre algo específico, pero esto no implica que la energía del problema desaparezca por completo.

Hay que ser cuidadoso de que en la organización, internamente los software tanto los equipos de cómputo estén siendo utilizados de una forma adecuada, y externamente poner todas las restricciones necesarias para no sufrir algún tipo de daño.

Para que la organización de GRUPO OSUNA S.A. refuerce su seguridad informática es necesario comprender la vitalidad de la información, lo importante que es, ir más allá de cualquier amenaza, y si se llegara a tener una buena seguridad, ser conscientes que estamos aún propensos a recibir algún daño.

Se hizo la recomendación de armar un plan de contingencia para la seguridad de la información, con el fin de equiparse con medidas preventivas y de recuperación, con los siguientes puntos definidos:

*Hacer un plan de respaldo: Ante cualquier amenaza, se apliquen medidas preventivas para evitar que se introduzca algún daño, conservar copias de toda la información en un lugar seguro, siempre tener un servidor extra como tipo espejo donde la información pasada y actual siempre estén a la mano en caso de problemas con el servidor principal.

*Plan de emergencia: Contemplar medidas cuando se esté materializando cualquier tipo de amenaza y tratar que no termine de producirse. En caso de daños mínimos si es necesario reestablecer bases de datos. A falta de extintores colocar 3 entre toda la oficina. Abastecer de cada uno de los equipos ya sea de las sucursales, tiendas y almacenes con No break, ya que de toda la organización son menos de 4 las que tienen No break.

*Plan de recuperación: En caso de haberse desarrollado algún daño o desastre, primeramente evaluar el impacto, y regresar lo antes posible al último estado de funcionamiento normal de todo el sistema. Durante el problema tratar de tener un lugar alternativo donde seguir con las actividades, como mencionado anteriormente un servidor alterno con información real y vigente.

*Plan de confidencialidad y privacidad: Se recomienda crear un grupo de privacidad, para que solo ciertos usuarios puedan tener acceso a los recursos compartidos, aprovechando la computadora servidor que tiene Windows Server 2008, evitando mal uso de la información o daños por internos de la empresa ya sea por ignorancia o por intención.

Con lo visto en el desarrollo de la presente investigación podemos deducir que con la implementación de un plan de contingencia computacional se reducirá la posibilidad de ataques informáticos.

BIBLIOGRAFIA

Bell, J. (2002). Cómo hacer tu primer trabajo de investigación. Guía para investigadores en Educación y ciencias sociales. Barcelona, Ed. Gedisa.

ConceiçãoMenezes, P. A., & González-Ladrón-de-Guevara, F. (2010). Maximización de los beneficios de los sistemas ERP . JISTEM: Journal of InformationSystems and TechnologyManagement , 7 (1), 5-32.

Laudon, K. C., & Laudon, J. P. (2008). *Sistemas de información gerencial: Administración de la empresa digital.* D.F., MEXICO: PRENTICE HALL HISPANOAMERICANA.

Conceição Menezes, P. A., & González-Ladrón-de-Guevara, F. (2010). Maximización de los beneficios de los sistemas ERP . *JISTEM: Journal of Information Systems and Technology Management, 7* (1), 5-32.

Rodríguez, Roció(2012). Antecedentes y consecuencias del uso de las ntic por parte de los vendedores. Tesis, Facultad de Economía y Empresa, Universidad de Murcia.

O´Brien, J. (2001). Sistemas de información gerencial, Colombia. Editorial McGraw-Hill Interamericana, S.A.

Pressman, R. (2002). Ingeniería del Software. Un enfoque práctico.

HONG y KIM, 2002; LIGHT, 2005; SOH y otros, 2000

Somers, M. T., & Nelson, K. (2002, Diciembre 22). A taxonomy of players and activities across the ERP project life cycle. *Information& Management,* **41** (2004): 257-278.

Stratman, J. K., &Aleda, V. R. (2002, Fall). Enterprise resource planning (ERP) competence constructs: Two-stage multi-item scale development and validation. *DecisionSciences,* **33** (4): 601.