UNIVERSIDAD
Rafael Belloso Chacín.

Revista Electrónica de
Estudios Telemáticos

TÉLÉMATIQUE

ANÁLISIS SITUACIONAL DE LA INFRAESTRUCTURA TECNOLÓGICA DEL TRIBUNAL SUPREMO DE JUSTICIA

Leal l. Solange A.
Universidad Rafael Belloso Chacín
Maracaibo - Estado Zulia
solangeleal@yahoo.com

José Bermúdez
Universidad Rafael Belloso Chacín
Maracaibo - Estado Zulia

RESUMEN

En la presente investigación se estableció un análisis situacional de la infraestructura Tecnológica del TSJ, específicamente en el Departamento Ejecutivo de la Magistratura que realiza funciones administrativas que ameritan el manejo de información vital y sensitiva; por lo tanto, el propósito de la misma fue proponer estrategias de seguridad para la infraestructura tecnológica, a través, del análisis obtenido de los criterios de la auditoria informática tomando en cuenta los factores que determinan el comportamiento de la continuidad operativa y los controles de seguridad organizativa. La investigación es de campo, de estudio descriptivo y de tipo documental. Su diseño fue no experimental, transeccional descriptiva. La población fue conformada por 168 usuarios, con una muestra de 105 usuarios, para la recolección de datos se aplicaron dos instrumentos (ficha de observación y el cuestionario). Por último se procedió a realizar un análisis de los resultados, lo cual permitió concluir que los factores que determinan el comportamiento de la continuidad operativa estaban en menor percepción, productos de faltas de controles adecuados y de administración. Asimismo, se recomienda planificar, analizar e implantar normas, políticas y procedimientos de seguridad en cuanto al registro del sistema, cuenta de acceso, identificación y autenticación, igualmente establecer un plan de seguridad, que contenga estrategias a seguir.

Palabras clave: Infraestructura, continuidad, controles, factores, seguridad.

ABSTRACT

In the present investigation a situational analysis of the Technological infrastructure of the TSJ was settled down, specifically in the Executive Department of the Magistracy that carries out administrative functions; therefore, the purpose was to propose safe-deposit strategies for the

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

technological infrastructure, the analysis of the computer audit was made taking in account the factors that determine the behaviour of the operative continuity and the controls of organizational security. The investigation is of field and documental type. Their design was not experimental and descriptive. The population was conformed by 168 users, with a sample of 105 users, for the gathering of data two instruments were applied (observation record and the questionnaire). An analysis of the results was made, concluding: that the factors that determine the operative continuity were in smaller perception, products of lacks appropriate controls and of administration. Also it is recommended to plan, analyze and implant norms, political and safe-deposit procedures for the registration of the system, access bill, identification and authentication.

Key Word: Infrastructure, continuity, controls, factors, security.

INTRODUCCIÓN

Durante los últimos años las organizaciones están adquiriendo nuevas tecnologías de la información y comunicación para implementarlo en su infraestructura tecnológica, debido a que se obtiene mejor efectividad organizativa, disponibilidad de información y comunicación entre organizaciones e individuos. Sin embargo, en la medida que la tecnología avanza se requiere conocer, desarrollar y establecer nuevas medidas de seguridad que garanticen la continuidad operativa de la misma.

El estudio en este organismo se debe a que el plan de acción que ejerce en su plataforma tecnológica, no ha podido identificar de manera efectiva los riesgos que se han presentado y han ocasionado retrasos en sus actividades. No obstante, la presente investigación esta orientada a proponer estrategias de seguridad, a través, del análisis situacional de la infraestructura tecnológica del

Tribunal Supremo de Justicia en el área de la Dirección Ejecutiva de la Magistratura ubicado en el estado Mérida, dada la necesidad de optimizar el funcionamiento de su plataforma tecnológica, y asegurar la información que se maneja en esta sede. Tomando en cuenta, los factores que garanticen la integridad, disponibilidad y continuidad de la información, así como también, los controles de seguridad organizativa.

Por otro lado, los análisis obtenidos se basarán en los criterios de la auditoria informática, para garantizar que su infraestructura este en óptimas condiciones, cumpliendo con las normas y procedimientos de seguridad que garantice la factibilidad y disponibilidad de la organización.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Tomando en consideración, ciertos aspectos vinculados al entorno de ésta investigación, se analizaron varios trabajos, por lo cual, fueron tomados en cuenta por sus aportes al mismo. El trabajo de grado, presentado por Prada (2000), titulado Diseño de redes de seguridad de datos de una empresa de servicios de tecnología de información, el propósito del autor es proponer un diseño de redes de seguridad de datos que permita mitigar los riesgos y poder identificar y reducir las amenazas.

Del mismo modo, Ugas (2001), elaboró un trabajo especial de grado titulado Seguridad en organizaciones con tecnologías de información, formulando un modelo que sirva de referencia para la implementación de un esquema de seguridad en función de los objetivos de su investigación; enfocado en la protección lógica de los activos de información, el cual incluye el análisis y evaluación de los niveles de riesgos, basados en un estudio de identificación de los factores internos de la organización y del entorno. Asimismo, Hernández (2003), llevó a cabo un estudio titulado Propuesta de gestión de recursos de red para la administración de la seguridad, desempeño y detección de fallas, la gestión de recursos incluye análisis de los parámetros para la medición de ciertos factores de la administración centralizada de la red.

Por otra parte, el trabajo de Chourio (2004), titulado Criterio de auditoría de seguridad para la plataforma Windows 2000 Server en empresas de tecnología, esta documentación aporta aspectos teóricos que describen el funcionamiento de la seguridad, identificación y autenticación, control de recursos perisologías y registro de eventos de auditoría, por último se ubicó la investigación de Rodríguez (2004), el cual realizó la investigación Modelo de gestión auditable para la instalación, operación y mantenimiento de Switches y Routers, proponiendo un modelo para la auditoria de la instalación, mantenimiento y operación de estos dispositivos.

- **Infraestructura tecnológica:** Se define como un conjunto de bienes y servicios utilizados para la integración y convergencia de la computación, las tecnologías y las técnicas para procesamientos de datos en apoyo a las actividades del hombre, sus principales componentes son: el factor humano, el software, el hardware, tipo y topología de red y los mecanismos de interconexión de transmisión de información.

- **Seguridad de la información:** Según Maiwald (2003), la palabra seguridad es un factor primordial de una red, debido a que se utiliza como medio para poder trasmitir datos sensible, desde su origen hacia su destino, de hecho una buena seguridad de la información es un conjunto de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

soluciones de muchos conceptos de seguridad y “solamente cuando éstas se toman en conjunto proporcionarán los fundamentos sobre los cuales una organización puede manejar eficientemente el riesgo de un incidente de seguridad de la información” (Maiwald, 2003, p. 162). La seguridad sigue siendo el área principal a auditar, hasta el punto de que en el inicio la función de la auditoria informática se basa en la seguridad, auque después se han ido ampliando los objetivos.

- **Auditoria informática:** Comprende la revisión y la evaluación de las normas, controles, técnicas y procedimientos que se tienen establecidos en una organización, a través, del análisis de la infraestructura tecnológica existente y poder tomar dediciones que permitan corregir los errores en caso de que existan, o bien mejorar la forma de actuación.

- **Control interno informático:** El enfoque principal del control interno informático, es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas, dentro de las medidas que se deben considerar están: políticas, normas, procedimientos plan de seguridad.

ASPECTOS METODOLÓGICOS

La investigación se clasificó como una investigación de campo, de estudio descriptivo y de tipo documental, en cuanto al diseño fue de naturaleza no experimental transeccional descriptivo, ya que la variable de estudio de esta investigación fue analizada en su estado natural, así como sus dimensiones e indicadores, sin la intervención de la investigadora, permitiendo caracterizar los elementos de la infraestructura tecnológica y establecer los factores que inciden en la seguridad, tanto en la disponibilidad, integridad y confiabilidad de la información, para poder proponer estrategias de seguridad para la infraestructura tecnológica del TSJ.

Para la recolección de datos se aplicaron dos instrumentos (Ficha de observación y el cuestionario), fue utilizado como tratamiento estadístico de datos el análisis de la varianza un solo factor, siendo una generalización de la prueba de comparación de medias con datos independientes, para aquellas situaciones en las que los grupos a comparar sean tres o más; luego se aplico la prueba T- test, prueba de medias Tukey, entre otros, donde los resultados reflejaron que si existen diferencia altamente significativas asociadas entre las ponderaciones asociadas a los controles de segurización organizativa y los factores de la continuidad operativa.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

DISCUSIÓN DE LOS RESULTADOS

Con respecto, a la ficha de observación, se pudo analizar que cuenta con una infraestructura tecnológica de Hardware actualizada, bajo herramientas de software aptas para un buen desempeño de la red, no obstante, se observó con respecto a la topología en estrella implantada en este organismo, que no es la más recomendada, debido a que se observó un desempeño de los dispositivos en cuanto a colisión de un nivel bajo, ya que la información es transmitida por el único nodo central.

Por tal motivo, se sugiere cambiar a una topología en estrella extendida para obtener mayor seguridad y control en la capa de distribución con respecto a las ACL y VLAN, por otro lado, también se obtiene mayor seguridad en las estaciones de trabajo ubicado en la capa de acceso.

De igual manera, se observó recursos en ciertas oficinas producto de que no están interconectados a los quipos de red, otras oficinas poseen conexión con Internet vía Dial-UP, sin ningún control, bajo ninguna supervisión, ocasionando faltas de seguridad con respecto a entrada y salida de la información, así como también, un mayor potencial de invasión de virus informáticos.

Otro punto importante, fue la observación de que no se cuenta con planos de distribución, donde se pueda apreciar los puntos de conexión de las estaciones de trabajo y de todos sus recursos, igualmente, no cuenta con un buen rotulado ó identificación de los cables de conexión.

Luego, se realizó el estudio de la prueba *One-Way ANOVA*, y T-test con las dos dimensiones (Controles y factores), con la finalidad, de contrastar hasta que punto pueden diferir o no significativamente, (ver anexo 1) sé identificaron que tanto los entre-grupos, intra-grupo y totales, existen diferencias altamente significativas entre las ponderaciones asociadas a los controles de segurización organizativa y los factores de la continuidad operativa.

Tales resultados concuerdan con los datos obtenidos de la test de variable o T de Student, donde en el análisis estadístico de las dos dimensiones o grupos, se observó una t negativa con nivel de significación inferior a 0.001 que nos permite concluir con un pequeño margen de error que existe una diferencia entre la media de la dimensión de factores y de la dimensión de controles de segurización organizativa, indicando que sí hay que mejorar o realizar cambios en la infraestructura tecnológica del TSJ en el área del DEM, hay que empezar por identificar y resolver cuales son los

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

factores que inciden en la continuidad operativa y ajustar ciertos controles para asegurar la fiabilidad de la gestión organizativa.

Luego, se aplicó la prueba *One-Way AOV y la prueba de medias Tukey* a la dimensión de factores, observando que se obtuvo valores entre, dentro y totales de los grupos de 6 a 734 respectivamente, con un valor positivo de F de 25.9 y un valor de P menor de 0.001, del mismo modo, se observó la presencia de tres grupos A, B, C, donde en el grupo C esta la disponibilidad de la información con un valor de 2.4619, (ver anexo 2) donde se encontró con menor percepción, debido a que la población opinó que se ha presenciado la falta de disponibilidad, producto de frecuentes interrupciones originando retrasos para poder acceder a los recursos y la información, por tal motivo, se debe considerar la revisión y configuración de recuperación de fallas a los dispositivos de red como los muros de fuegos, enrutadores y conmutadores, tal como lo sugiere Echenique (2003), que los sistemas configurados con recuperación de fallas pueden detectar los fallos y restablecer los accesos a la información o comunicación.

Por otro lado, para mejorar el factor de integridad de la información se deben tomar medidas con respecto a los controles de acceso y autorización de los archivos y mecanismo de identificación y autenticación. Y para resguardar la información durante la transmisión se debe implementar el uso de tecnología de encriptación, concordando con lo expuesto por Echenique (2003), que la tecnología de encriptación puede evitar la mayor parte de las formas de ataques de modificación durante la transmisión como por ejemplo la firma digital.

Por último se encuentra el grupo A, donde el factor que se debe considerar dentro del grupo es la seguridad de la información, no obstante, para poder realizar una discusión de los resultados, la autora lo clasificó en dos grupos: seguridad física y seguridad lógica.

Dentro de la seguridad física, se presenció que en esta organización no se toma medidas con respecto al uso de equipos de soporte, tales como: aire acondicionado, equipo de control de incendio, planta de energía, por tal motivo, se recomienda considerar controles tanto preventivo como de detección a la infraestructura física para minimizar los riesgos, debido que las amenazas pueden ser muy diversas, y como el Palacio de Justicia es un órgano público, con más razón, se deben tomar medidas con respecto a las entradas y salidas al personal y personas en general.

La autora concuerda con lo señalado por Prada (2000), sugirió en su propuesta de modelo de seguridad, donde recomienda la utilización de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

energía eléctrica, supresión de fuego, control de acceso físico y control de visitas, entre otros.

De acuerdo, con los resultados concernientes al mantenimiento y administración de las computadoras y equipos de red, donde los resultados fueron parcialmente significativos, la autora recomienda la elaboración de documentos dirigidos por una parte al usuario y por otro como manual de referencia a los analistas informáticos del TSJ, tal como se asemeja con lo señalado por Ugas (2001) en su investigación que indico como alternativa cuatro un desarrollo de un marco referencial de seguridad que sirva de guía o base de comparación para el desarrollo de cualquier solución con respecto a seguridad.

En cuanto, a la seguridad lógica correspondiente a la administración, mantenimiento y actualización del software, se pudo apreciar que los analistas deben reforzar todos los mecanismos de seguridad con respecto al sistema operativo, en la configuración de los dispositivos, como también, en la prohibición de divulgación e intercambios de códigos o password, para evitar la entrada a personas no autorizadas a la información y al sistema de computo, por otro lado, administrar el acceso a la información dependiendo de las funciones que tiene las personas que laboran en todas las áreas del DEM.

Para determinar el análisis de la varianza de los controles de segurización organizativa de la infraestructura tecnológica del TSJ, se aplicó de igual manera, la prueba *One-Way AOV* para los itemes: control de acceso y autorización, identificación y autenticación, normas de seguridad, políticas de seguridad, procedimientos de seguridad, protección de virus, (ver anexo 3), obteniéndose la formación de solo dos grupos A y B, donde en el grupo A se presencia solo un indicador *identificación y autenticación* con un valor de la media de 3.3869.

Analizando el indicador de protección de virus que dio como resultado una valor de la media menor que todos los indicadores, la autora enfatiza que los analistas deben reestructurar las medidas de seguridad con relación a que información y de que manera se debe acceder, guardar o modificar la información, de igual manera, se recomendable instalar un antivirus que de forma automática reconozca o no la existencia de alguna anomalía ya sea por diferentes medios discos flexibles, disco duro, Internet, entre otros.

A este respecto, la autora concuerda con lo expuesto por Echenique (2001) donde define virus como “pequeñas subrutinas escondidas en los programas que se activan cuando se cumple alguna condición” (p. 193), por

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

lo tanto la autora acota que los virus informáticos tienen la capacidad de causar daño y pueden replicarse a sí mismo y propagarse a otras computadoras. Infecta entidades ejecutables, cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador vaya a ejecutar, y lo que es más preocupante redes informáticas no regulados.

Retomando este último punto la autora observó que este organismo utiliza como antivirus VirusScan Enterprise 7.0, siendo el más actualizado en el mercado, por lo tanto se recomienda, tener más control con las fuentes de entrada y salida de la información electrónica, implantando medidas de control de acceso y establecer mecanismos de solo lectura, solo escritura, lectura escritura, dependiendo de las actividades laborales del usuario.

Asimismo, continuando el análisis del estudio del grupo B, con los indicadores de normas, políticas y procedimientos de seguridad, se presenció diferencias significativas, debido a que se observó que los trabajadores no toman estos indicadores como deberes e incumpliendo con los procedimientos de seguridad ya que las acciones que toman en cuanto se presencia alguna irregularidad son de manera verbal, dicho en otras palabras, sólo se procede a llamar la atención.

Por tal motivo, la autora comparte con lo establecido por Ugas (2001) en documentar políticas de seguridad en los sistemas de información, para salvaguardar la infraestructura tecnológica, así como también, su información.

Ugas (2001), enfatiza que “las normas redactadas en términos sencillos y comprensible, para todos los empleados de la organización, serán obligatorias por lo que debe ser conocidas por los mismos”, concordando con Chourio (2004), el cual indica que las políticas de seguridad informáticas establecen el canal formal de actuación del personal en relación con los recursos y servicios informáticos importantes de la organización. Igualmente, las normas y procedimientos son operativos que tienen como finalidad describir la forma y las responsabilidades ejecutorias que conlleve a un óptimo manejo de control en la organización.

Siguiendo con la descripción de los resultados, al control de acceso y autorización, la autora observó que no se están aprovechando las ventajas que presta el uso de la tecnología de software y hardware que ellos tienen con respecto al manejo, uso y chequeo del mecanismo de control de accesos, producto en una parte del rechazo y de la poca capacitación que el organismo le ha prestado a los empleados. Por tal motivo, se recomienda

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

tomar estrategias de seguridad ya que este indicador resulta ser un factor preponderante con el resto de los indicadores.

Razonamiento que concuerda con la investigación de Chourio (2004), con respecto a que se debe de analizar políticas y procedimientos de control de acceso con la finalidad de minimizar los puntos de ataques el sistema.

Para finalizar se encontró el indicador identificación y autenticación como único factor del grupo A, indicando que se encuentra en mejor percepción comparado con el resto de los indicadores de la dimensión control de segurización organizativa, por motivo de que el DEM tiene implantado una herramienta de identificación y autenticación del individuo, no obstante, la autora manifiesta que sin un control de acceso bien definido, la identificación y autenticación no tendría mayor peso. Tal como lo señala Chourio (2004), el control de acceso a los recursos consiste en controlar quien utiliza el sistema o cualquiera de los recursos que ofrece y como lo hace.

ESTRATEGIAS DE SEGURIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL TSJ

Las estrategias de seguridad representan las tácticas que se debe seguir para que los mecanismos de control organizacional, ligado con los factores de la continuidad operativa garanticen la calidad de los sistemas. Asimismo, proporcionar un instrumento de manera sencilla a los administradores y usuarios del DEM para el respaldo seguro de la información con criterios de eficacia y eficiencia para el mejor desenvolvimiento de sus funciones informáticas. En tal sentido, se establecieron ciertos criterios de seguridad basados en algunos indicadores más resaltantes.

CONCLUSIONES

En relación a la identificación de las características actuales de la infraestructura tecnológica, se realizó una serie de observaciones, los cuales permitieron concluir que en cuanto a la tecnología de hardware, la organización está a la vanguardia de la tecnología ya que posee equipos de información y comunicación actualizados.

De igual manera, en cuanto a la tecnología de software se puede decir, que el organismo posee herramientas aptas para un buen desempeño en la red, así como: aplicaciones, manejador de base de datos, antivirus, aunque se evidenció que estas no son aprovechadas en su totalidad para mejorar la gestión de seguridad de la infraestructura tecnológica, además se determinó la falta de mecanismos de detección de intrusos, controles de validación y

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

autorización.

Posteriormente, se observó una serie de situaciones entre las cuales se puede mencionar que sólo se encuentra interconexión de equipos de red en el piso tres del DEM y del CJL del piso cuatro, por otro lado, algunas oficinas tienen conexión Internet, sin ningún control de seguridad vía Dial-Up, además, el DEM no posee planos de distribución y formato de identificación del cableado.

En relación con la disponibilidad de la información sé comprobó que se ha presenciado interrupciones del sistema, lo cual ocasiona problemas para acceder a los recursos y a la información, por lo tanto los analistas informáticos deben considerar la revisión del sistema y la configuración de protocolos que suministren mecanismos de recuperación de fallas, tales como enrutadores y conmutadores de paquete, de igual manera, deben constantemente evaluar todas aquellas acciones que puedan ocasionar colisiones o retrasos para poder acceder y obtener la información, ya sea por: impresiones, base de datos, entre otros.

Referente a la integridad, confiabilidad y confidencialidad, que los usuarios almacenan la información en diversos lugares, dando origen a informaciones corruptas, es decir, copias no actualizadas que traen como consecuencia falta de integridad y confiabilidad en la información, por otro lado, se observó que no se preserva la confidencialidad debido a que incumple con los lineamientos de seguridad en cuanto a cambios de las contraseñas y divulgación de la misma.

Desde el punto de vista de seguridad de la información, se determinó que este organismo no tienen lineamientos con respecto a la seguridad física, en lo que respecta al uso de equipos de soporte, controles de entradas y salidas al personal y personas en general, además no cuentan con una documentación de todos aquellos equipos que han presenciado fallas y cuáles han sido sus posibles soluciones.

Haciendo referencia a la seguridad lógica, se observó que en la implementación de los programas de soporte no sé esta aprovechando al máximo, todas las ventajas que tanto los programas como los dispositivos puedan ofrecer a la organización, de igual manera se presenció de manera relevante la falta de capacitación del personal que labora en este organismo, la cual debilita la gestión de seguridad y no garantiza la eficiencia de la infraestructura tecnológica

En cuanto a la protección de virus, se observó que no tienen establecidos

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

mecanismos de detección de intrusos, así como también registros de los tipos de virus que se han presenciado en el DEM, principalmente donde se inicio la fuente de infección, en que computadora, así como el usuario que maneja dichaestación de trabajo.

Asimismo, se observó que el organismo no posee normas, políticas y procedimientos de seguridad por escrito, ocasionando que el personal trabaje sin ninguna restricción y pueda en numerosas ocasiones cometer transgresiones que perjudique la continuidad operativa del organismo, por otro lado, se evidenció que si el personal se les descubre de alguna falta y no realizan amonestaciones al mismo, sólo se le llama la atención de manera verbal.

De igual forma, en la identificación y autenticación dio como resultado una mejor percepción entre las ponderaciones asociadas a la media de los factores de la dimensión control de segurización organizativa, no obstante, se pudo constatar faltas en las responsabilidades del usuario con los deberes de no divulgación de sus claves, como de caducidad de la misma, lo cual trae como consecuencia que personas no autorizadas acceden a datos o información que mal interpretada o utilizada puede crear un clima de inestabilidad para la organización.

RECOMENDACIONES

Se debe elaborar documentos del estado actual de la infraestructura tecnológica, incluyendo: registros, reportes, formato de identificación del cableado, igualmente, es importante la utilización de planos de distribución actualizados de los puntos de red de cada uno de las estaciones de trabajo instalados en el organismo.

Asimismo, se sugiere cambiar a una topología de estrella extendida para obtener mayor seguridad y control en la capa de distribuición y en la capa de enlace, del mismo modo, implantar sistemas de detección de intrusos híbridos basados en censores IDS network-based y host-based.

Se recomienda, planificar, analizar e implantar normas, políticas y procedimientos de seguridad en cuanto al registro del sistema, cuenta de acceso, identificación y autenticación, sistema de cómputo, elaboración de respaldo de la información y de la data almacenada, igualmente, establecer un plan de seguridad, que contengan estrategias a seguir para que los mecanismos de control organizacional, ligado con los factores de la continuidad operativa garanticen la calidad de los sistemas. No obstante, documentar toda esta información de manera sencilla y comprensible por todos los empleados de la organización.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Por otro lado, los analistas de esta organización deben establecer políticas de seguridad tanto prohibitivas como permisibles desde el punto de vista de seguridad, tiempo de caducidad y longitud, tomando en consideración que el personal pueda acceder a su información con su clave sólo en una máquina asignada, e inclusive que la contraseña esté formada por una combinación de letras mayúsculas y minúsculas, números y caracteres especiales y poseer un mínimo de ocho caracteres y no mayor de 64.

AL configurar una estación de trabajo, es recomendable instalar la última versión aprobada del Service pack del sistema operativo, ya que esto permite mantener actualizados los dispositivos contra vulnerabilidades.

Igualmente, se debe utilizar las cuentas de administración para labores comunes y deshabilitar ciertos documentos, desde el punto de vista de control informático, tales como: crear sólo lectura, lectura y escritura, borrar archivos, entre otros.

Se recomienda incentivar al usuario a regirse por las normativas y procedimientos de seguridad, con respecto al uso de la infraestructura tecnológica, para que tenga la cultura y principio de responsabilidad con la estación de trabajo con la cual labora y de esta manera velar por la seguridad de los datos, no obstante, la estación de trabajo debe ser bloqueada al ausentarse del escritorio.

Por otra parte, se debe tomar en cuenta la restricción de la configuración del antivirus en las estaciones de trabajo, para evitar la desinstalación y la deshabilitación de las propiedades del antivirus.

Por último, se recomienda la realización de otras investigaciones para que sirva de marco referencial en función de proporcionar bases sólidas de seguridad a la infraestructura tecnológica de un organismo público o privado, permitiendo con ello, poder identificar, determinar y analizar que parámetros se deben considerar a la hora de realizar un análisis situacional.

REFERENCIA BIBLIOGRÁFICA

Arciniega, L. (2004). *Criterios tecnológicos para el diseño de edificios*

Inteligentes. Tesis de Maestría en Telemática, Universidad Dr. Rafael Belloso Chacín, Maracaibo – Venezuela

Arias, F. (1999). *El proyecto de investigación guía para su elaboración. Episteme,* Caracas

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Bellos, C. (1998), *Manual de seguridad en redes,* [Documento en línea]. Disponible Http://www.seguridad.unam.mx/semAU/AdminUNAM 2002/

Adminin-UNAM-Ocbre/Auditoria.pdf [Fecha de consulta 8/03/05].

Canaves P, (2003), Auditoria informática [Documento en línea]. Disponible: http://gestiopolis.com/recursos/documentos/auditoinfo.htm [Fecha de consulta 23/10/04]

Castillo, j. (s.f.), *Virus informáticos*, [Documento en línea]. Disponible: Http://www.monografia.com/trabajos13/virin/virin.shtml [Fecha de consulta 13/01/05].

Chávez, N. (1991), *Introducción a la metodología educativa,* Caracas, Venezuela. ARS Grafía, SA Editorial Addisson-Wesly. Iberoamericana, México.

Chávez, N. (1994). *Metodología de la Investigación educativa* Caracas, Venezuela. ARS Grafía, SA Editorial Addisson-Wesly. Iberoamericana, México.

Chourio. J, (2004). *Criterios de auditoria de seguridad para la plataforma Windows 2000 Server en empresas de tecnología.* Tesis de Maestría en Telemática. Universidad Dr. Rafael Belloso Chacín, Maracaibo.

CISCO, *Programa semestre 1, 2, 3 y 4 del CCNA,* [Documento en línea]. Disponible Http://www.urbe.cisco.edu [Fecha de consulta 198/09/04].

Corsico, I. (s.f.), *Trabajo de Auditoria: Normas COBIT* [Documento en línea]. Disponible: http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml [Fecha de consulta 13/01/05].

Echenique, J. (2001). *Auditoria en Informática*, Editorial Mac Graw-Hil. México

Enciclopedia de telecomunicaciones (s.f.), *técnicos en redes y comunicaciones para computadoras* comercialización editorial y sistema lyda, codesis

Falcón. A, (s.f.), *Tecnología,* [Documento en línea]. Dirección electrónica: www.monografia.com/trabajos16/tecnologia [Fecha de consulta 21/03/05].

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Gutierre, J (s.f.), *Auditoria aplicada a la seguridad en redes de computadoras.* [Documento en línea]. Dirección electrónica: www.monografia.com/trabajos10/auditoria.html [Fecha de consulta 10/07/04].

Hernández. J, (2003). *Propuesta de gestión de recursos de red para la administración de la seguridad, desempeño y detección de fallas.* Tesis de Maestría en Telemática. Universidad Dr. Rafael Belloso Chacín. Maracaibo – Venezuela

Hernández R., Fernández P., Baptista L:, (1998) *Metodología de la investigación* 2da edición, México, Mc Graw – Hill, Interamericana editores, S.A.

Karanjit S (1995), *Internet y seguridad en redes*, Presentice may, Hispano Americana, México.

León, D. (2001). *Guía para el administrador de redes.* México. 1ra Edición McGraw Hill.

Maiwald. E, (2003), *Fundamentos de seguridad de redes*, 1ra edición, México, Mc Graw - Hill interamericana.

Mendez, C. (1998). *Metodología* 1ra Edición, México, Mc Graw - Hill interamericana.

Naranjo. A, (2000), *Conceptos de la auditoria de sistemas* [Documento en línea]. Disponible: http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml [Fecha de consulta 07/08/04]

Peroso Beatriz (2002), *Factores de riesgo que influyen la inoperatividad de la red VPN. Con tecnología Frame relay y X.25.* Universidad Rafael Belloso Chacín. Tesis de Maestría. Maracaibo.

Piattini. M, (2001). *Auditoria Informática un enfoque práctico,* 2da edición Alfaomega Ra- Ma, México.

Pineda, M. (1996), *Sociedad de la información nuevas tecnologías y medios masivos*, colección Postscriptim, 1° Edición.

Prada, J. (2001). *Diseño de redes de seguridad de datos de una empresa de servicios de tecnología de información.* Universidad Dr. Rafael Belloso

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Chacín. Decanato de investigación y postgrado, maestría en gerencia de proyectos industriales. Maracaibo - Venezuela.

Rodríguez, J. (2004). *Modelo de gestión auditable para la instalación, operación y mantenimiento de switches y routers.* Universidad Dr. Rafael Belloso Chacín. Tesis de Maestría en Telemática. Maracaibo – Venezuela.

Romero. H, (s.f.) *Auditoria de Sistema y políticas de Seguridad Informática* [Documento en línea]. Disponible: http://www.monografias.com/trabajos12/ichagr/fichagr.shtml [Fecha de consulta 07/08/04].

Hernández, Fernández y Baptista (1998) *Metodología de la Investigación*, México: Mc Graw - Hill.

Sanchez, J. (2004). *Vigilancia tecnológica como palanca para la generación e innovaciones,* Universidad Dr. Rafael Belloso Chacín. Tesis de Maestría en Gerencia de Proyectos de Investigación y Desarrollo. Maracaibo – Venezuela.

Sandoval. C (2004) *Auditoria de red* [Documento en línea]. Disponible: http://monografias.com/trabajos10/auap/auap.shtml [Fecha de consulta 14/11/04]

Sulbaran, Y. (2001). *Evaluación de los dispositivos de interconexión a nivel de la capa 2,3 y 4 del modelo OSI,* Universidad Dr. Rafael Belloso Chacín. Tesis de Maestría en Telemática. Maracaibo – Venezuela.

Sierra. R, (1991). *Diccionario practico de estadística y técnicas de investigación científica* Madrid.

Tamaño y Tamaño. M, (1998). *El proceso de la investigación científica.3*ra edición. México. Editorial Limusa.

Tamaño. M, (1997) *El proceso de la investigación científica* México, Editorial limusa.

Ugas, L. (2001). *Seguridad en organizaciones con tecnología de información,* Universidad Dr. Rafael Belloso Chacín. Tesis de Maestría en Telemática. Maracaibo – Venezuela.

Visauta, V. (2002) *Análisis Estadístico con SPSS para Windows, 2*da edición.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005

Volumen I McGraw –Hill Interamericana de España. SAU

Visauta, V. (2003) *Análisis Estadístico con SPSS para Windows, 2*da edición. Volumen II Estadística multivariante, McGraw – Hill Interamericana de España. SAU

ANEXOS

Anexo 1

Cuadro 8
Resultado del AVAR, un solo factor.

Fuente	Suma de cuadrados	GL	Media cuadratica	F	Sig.
Entre	15.190	82	.185	9.239	.000
Dentro	.441	22	.020		
Total	15.631	104			

Fuente: La Autora.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	dimension de factores	2.9783	105	.36575	.03569
	dimension C de segurización organizativa	3.2280	105	.38768	.03783

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	dimension de factores & dimension C de segurización organizativa	105	.762	.000

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	dimension de factores - dimension C de segurización organizativa	-.24979	.26099	.02547	-.30029	-.19929	-9.807	104	.000

Anexo 2

Cuadro 10
Análisis de la varianza para los indicadores de factores.

Fuente	DF	SS	MS	F	P
Entre	6	73.868	12.3114	25.9	0.0000
Dentro	728	345.511	0.4746		
Total	734	419.379			

Fuente: La Autora.

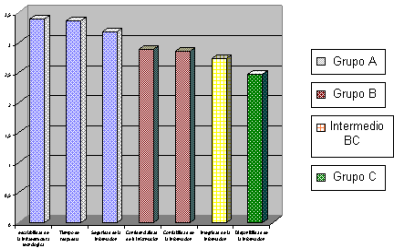

Figura 21. Resultados de la prueba de Tukey para los itemes de la dimensión factores Fuente: La Autora.

Anexo 3

Cuadro 12
Análisis de la varianza para los indicadores de Controles de segurización organizativa.

Fuente	DF	SS	MS	F	P
Entre	5	17.683	3.53655	10.4	0.0000
Dentro	624	212.408	0.34040		
Total	629	230.090			

Fuente: La autora.

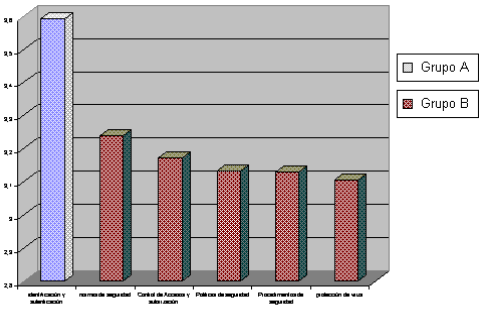

Figura 22. Resultados de la prueba de Tukey para los itemes de la dimensión Controles de segurización organizativa Fuente: La Autora.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 4 Edición No 2 – Año 2005