MODELO DE ESTRATEGIAS INTEGRALES DE SEGURIDAD PARA LA INFRAESTRUCTURA DE RED DE DATOS. CASO DE ESTUDIO: UNIVERSIDAD DE ORIENTE NÚCLEO MONAGAS.

Márquez, Dolystrini
Unidad de Cursos Básicos, Programa de Ingeniería de Sistemas, Universidad de Oriente, Núcleo de Monagas, Maturín, Venezuela. E-mail: dolystrinimarquez@gmail.com
Marcano, Ana Victoria
Unidad de Cursos Básicos, Programa de Ingeniería de Sistemas, Universidad de Oriente, Núcleo de Monagas, Maturín, Venezuela. Email: amarcano@udo.edu.ve.

RESUMEN

La investigación que se presenta estuvo basada en el estudio y formulación de un modelo de estrategias de seguridad organizacional y herramientas informáticas para la infraestructura de red de la Universidad de Oriente Núcleo Monagas, con el fin de identificar las carencias y vulnerabilidades en el campo de seguridad informática, verificando la integridad de los dispositivos, distribución lógica de la red y las consideraciones administrativas. Debido a que los controles de seguridad son escasos, se expone la red a un diverso número de amenazas, tanto internas como externas, las cuales requieren ser reconocidas para así mitigar los riesgos en las telecomunicaciones dentro de la universidad. Con esta investigación, se busca fortalecer la plataforma tecnológica, realizando un estudio exhaustivo sobre las condiciones actuales y la propuesta de posibles controles viables de protección para la red. Para el desarrollo de la investigación se manejo un híbrido entre la metodología EBIOS, Expresión de las Necesidades e Identificación de los Objetivos de Seguridad, y PSSI, Política de Seguridad de los Sistemas de Información, concluyendo que la implementación de las estrategias formuladas es de gran importancia, ya que las actividades dentro de la universidad cada vez son más dependientes de sistemas informáticos y equipos automatizados.

Palabras Clave: Redes, seguridad informática, integridad, recursos de red.

ABSTRACT

The research reported was based on the study and development of strategies models for organizational security and computer tools for the network infrastructure at the University of East Kernel Monagas, in order to identify gaps and vulnerabilities in the field of computer security, verifying the integrity of the devices, logical distribution of the network and administrative considerations. Because the security checks are scarce, it exposes the network to a diverse number of threats, both internal and external, which require be recognized to mitigate the risks in telecommunications within the university. With this research, it seeks to strengthen the technological platform, conducting a comprehensive study on the current conditions and the proposal of possible controls viable protection for the network. For the development of research management is a hybrid between the methodology EBIOS, Expression of the Needs and Identification of Objectives for Safety, and PSSI, Security Policy of the Information Systems, concluding that the implementation of the strategies developed is of great importance, since the activities within the university are increasingly dependent on computer systems and automated equipment.

Keywords: Networks, Computer Security, Integrity, Network Resources.

1. INTRODUCCION

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La carencia de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización; la propia complejidad de las redes es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas.

Para garantizar la seguridad de la infraestructura de las redes en organizaciones modernas, se requiere un enfoque global y un sólido conocimiento de las vulnerabilidades y las medidas de protección asociadas. Aunque tal conocimiento no puede frustrar todos los intentos de ataque al sistema o de incursión en la red, sí que ayuda a los administradores de redes a eliminar ciertos problemas de carácter general, a reducir considerablemente los posibles daños y a detectar infracciones con rapidez. Teniendo en cuenta que el número y la complejidad de los ataques están en constante aumento, es imprescindible adoptar una actitud vigilante por lo que respecta a la seguridad, tanto en grandes como en pequeñas redes.

La Universidad de Oriente (UDO) Núcleo Monagas, como institución de educación superior, condiciona la existencia de una infraestructura de red robusta y segura para la consecución de sus actividades, ya que cada vez es mayor la dependencia de activos informáticos y sistemas.

Las estrategias son un modelo coherente, unificador e integrador de decisiones que determina y revela el propósito de la organización en términos de objetivos, tratando de lograr una ventaja sostenible a largo plazo y respondiendo adecuadamente a las oportunidades y amenazas surgidas en el medio externo de la misma, teniendo en cuenta las fortalezas y debilidades de la organización. Por otro lado, hoy en día las estrategias se ha convertido en una herramienta obligatoria dentro de la actividad gerencial, estas se enfoca hacia el lado de establecer un planteamiento ya que dentro de las organizaciones en un principio es vista como una guía, un modo de acción futura que generara posteriores beneficios si se realiza correctamente.

En este contexto, se ha elaborado esta investigación, con la que se propone facilitar las tareas de todos aquellos que se encuentran actualmente involucrados en las decisiones respecto de las redes de información y de sus modos de administración dentro de la universidad, al tiempo de alertar sobre la importancia crítica de la seguridad. Se destaca que un adecuado tratamiento de esta problemática resulta absolutamente vital, debido a las amenazas cada vez mayores a las que la información se encuentra expuesta. Dado que se trata dentro de un tipo de investigación proyectiva, se exhorta este artículo hacia un estudio diagnostico el cual propondrá las bases para una posterior implementación.

2. DESARROLLO

Las Universidades son catalogadas como una comunidad con diversos intereses que reúne a profesores y estudiantes en la tarea de buscar la verdad y afianzar los valores trascendentales del hombre, y como una organización donde la gestión del conocimiento debe estar enmarcada dentro de la realidad de un mundo cada vez más globalizado y competitivo. Hoy en día existe una tendencia en las universidades hacia el uso de la tecnología, ya que facilita que la información tenga vehículos de entrega y difusión accesibles y de amplio alcance, así como la creación de software de administración académica y el uso de bibliotecas electrónicas.

Según (Annan, 2003). Las tecnologías de la información y la comunicación no son ninguna panacea ni fórmula mágica, pero pueden mejorar la vida de todos los habitantes del planeta. Se disponen de herramientas para llegar a los Objetivos de Desarrollo del Milenio, de instrumentos que harán avanzar la causa de la libertad y la democracia, y de los medios necesarios para propagar los conocimientos y facilitar la comprensión mutua.

El Núcleo de Monagas de la UDO, se encuentra desprovisto de elementos de protección en cuanto a la infraestructura de red se refiere, ésta no cuenta con normas de seguridad para salvaguardar los activos, y la intrusión a los sistemas se tratan de manera reactiva, ya que no se tienen establecidas herramientas y guías de procedimientos para tratar estos eventos. En general, la universidad carece de mecanismos de seguridad que la proteja de los ataques que se producen vía Internet.

Debido al ambiente abierto que reina en ella está poco extendido el uso de cortafuegos que limiten el acceso por defecto y dejen abiertos sólo los servicios necesarios, en su lugar suele seguirse una política inversa de permitir por defecto y filtrar sólo los servicios imprescindibles, como correo y web por ejemplo; esta condición deja caminos abiertos para la intrusión a los sistemas y ocasiona daños que perjudican las operaciones de la organización, e inclusive la incursión de códigos maliciosos que pueden dañar los equipos.

Se han registrado intrusiones que han generado inactividad a los servicios ofrecidos por la universidad vía Internet, trayendo como consecuencia carga de trabajo adicional al personal administrador de la red, en cuanto a la determinación del ataque y corrección del mismo, además el descontento de los usuarios; comunidad estudiantil, profesores, personal administrativo y foráneos, durante la ausencia de estos servicios.

En cuanto a la seguridad física de los dispositivos de red, es notable la ausencia de controles de acceso a los cuartos de datos y escasez de vigilancia en los mismos, no existen mecanismos instalados para tal fin, lo cual trae como consecuencia incidentes por la incursión en ellos por personal no autorizado, poniendo en riesgos los equipos y data vitales para el buen desenvolvimiento de las actividades dentro de la universidad.

Cabe destacar que en la UDO Núcleo de Monagas se encuentran varias aplicaciones administrativas en vía de desarrollo e implementación, es decir, sistemas de automatización de los procesos realizados en diversas áreas, las cuales precisarán de una infraestructura de red bajo una perspectiva de disponibilidad de servicio, integridad y confiabilidad de la información donde ésta se maneje de forma rápida, eficaz y segura de manera de facilitar las gestiones de la dependencia.

Según (Gallo et al., 2002). La seguridad de las redes se refiere a la adecuada salvaguarda de todo lo asociado con una red. Esto incluye datos, medios y equipos. La seguridad implica funciones administrativas tales como la estimación de amenazas, herramientas y facilidades técnicas, tales como productos criptográficos, y productos de control de acceso a la red como los firewalls. La seguridad también implica asegurarse de que los recursos de la red se usen de acuerdo con una línea de acción prescrita y sólo por gente autorizada para usar esos recursos.

Por tal motivo, se hace necesaria la formulación de estrategias de seguridad que permitan proteger los activos y medios de comunicación dentro de dicha infraestructura de red, para así minimizar los riesgos y vulnerabilidades antes incidentes de diversas índoles, como el vandalismo, intrusiones a los sistemas, manipulación incorrecta de los equipos y catástrofes naturales.

Este trabajo fue realizado en la Universidad de Oriente, específicamente en el Núcleo Monagas - Venezuela, considerando sus dos (02) campus (Juanico-Guaritos), y se delimitó a realizar las fases de investigación, análisis y redacción de las estrategias integrales de seguridad.

Para efectos del desarrollo del proyecto, se decidió tomar como base la metodología EBIOS, Expresión de las Necesidades e Identificación de los Objetivos de Seguridad, combinada con PSSI, Política de Seguridad de los Sistemas de Información, desarrolladas por la Dirección Central de la Seguridad de los Sistemas de Información (DCSSI), organismo perteneciente al Ministerio de la Defensa Francés; ya que tienen por esencia la especificación de los objetivos de seguridad para la elaboración de las estrategias, su debida redacción y justificación, para de esta manera alcanzar satisfactoriamente los objetivos propuestos.

El estudio fue llevado a cabo en cuatro (04) fases, descritas en la tabla 1.

Tabla 1. Metodología Operativa.

Fases	Actividades	Metodología	Objetivos
Fase I	1. Realización de entrevistas. 2. Conceptualización del contexto organizacional. 3. Observación directa en el área. 4. Búsqueda de información técnica de la infraestructura de red actual de la UDO Núcleo Monagas. 5. Revisión documental.	Etapa I: EBIOS	Estudiar la situación actual de la infraestructura de red de la Universidad de Oriente Núcleo Monagas.
Fase II	1. Observación directa en el área. 2. Revisión Documental 3. Realización de entrevistas. 4. Determinación de las amenazas y riesgos. 5. Confrontación entre las amenazas y criterios de seguridad. 6. Análisis de riesgos.	Etapa II: EBIOS	Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la infraestructura de red de la Universidad de Oriente Núcleo Monagas.
Fase III	1. Análisis de los datos obtenidos. 2. Establecimiento de los principios de seguridad. 3. Definición de perspectivas de seguridad para las estrategias. 4. Especificación general de las propuestas.	Etapa III y IV: EBIOS. Fase 2: PSSI	Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en la infraestructura de red de la Universidad de Oriente Núcleo Monagas.
Fase IV	1. Redacción de las estrategias integrales de seguridad. 2. Validación de los principios de seguridad propuestos. 3. Elaboración de estudio costo- beneficio.	Etapa V: EBIOS Fase 3: PSSI	Definir las estrategias de seguridad acorde a las necesidades identificadas en la infraestructura de red de la Universidad de Oriente Núcleo Monagas.

3. RESULTADOS

Los resultados se obtuvieron a través de las distintas fases, desarrollando así la metodología operativa implementada en la investigación.

3.1 FASE I

Esta fase abarcó la primera etapa de la metodología EBIOS, estudio del contexto, que se enfoca en el estudio del organismo, estudio del sistema objetivo y determinación del perímetro del estudio. Aquí se realizó la visualización de la situación actual en la institución, haciendo uso de herramientas como, las entrevistas no estructuradas al personal del Centro de Computación, específicamente en el área de Teleinformática, lo que llevó a obtener información acerca del problema existente.

Se realizó un estudio general, valiéndose de la observación directa y revisión documental, para obtener información técnica sobre la infraestructura de red que actualmente opera en la Universidad de Oriente Núcleo de Monagas; obteniendo la distribución de la red y sus modos de administración.

En esta fase se logró reconocer y formular el planteamiento del problema, así como también, definir los objetivos y estimar el alcance del proyecto.

3.2 FASE II

Esta fase comprendió la segunda etapa de la metodología EBIOS; expresión de las necesidades de seguridad, donde se conceptualiza el proyecto con la finalidad de obtener un sólido conocimiento del sistema actual y distinguir los elementos sensibles existentes, para ello en esta fase, al igual que la anterior, se implementó técnicas

de recolección de datos como la entrevista no estructurada, la observación directa y la revisión documental.

En esta fase se recaudó la información referente a la estructura corporativa y funcional de la organización, determinándose las necesidades de seguridad presentes en su infraestructura de red, así como las amenazas y riesgos que se enfrentan. Resaltando que la necesidad creciente de garantizar la disponibilidad de los servicios informáticos, debido al auge tecnológico a nivel educacional y la automatización de los procesos administrativos, hace pertinente que el personal de las áreas de Computación y Teleinformática realicen arduos trabajos, en muchos casos de manera improvisada, para mantener en funcionamiento la red corporativa. Estos casos, traen consigo el nacimiento de vulnerabilidades y amenazas para los sistemas de información y redes de la institución.

Definiendo las vulnerabilidades como las debilidades del sistema que pueden ser explotadas y utilizadas para comprometerlo; y una amenaza, como cualquier elemento que comprometa el sistema a situaciones de inoperatividad; todo aquello capaz de manifestarse en forma de ataque a la red y provocar daños en los activos.

Las vulnerabilidades detectadas, y expresadas por los administradores de la red, de mayor incidencia se relacionan con la negación de servicios, el daño o pérdidas de equipos por la incursión de personal no autorizado o vandalismo, virus informáticos y el uso poco extendido de los Firewalls. Puntualizando las vulnerabilidades existentes, se visualizan tres elementos sensibles en la infraestructura de red, dados por: **Elemento 1:** Seguridad Física. **Elemento 2:** Seguridad Lógica. **Elemento 3:** Seguridad Organizacional.

Estos elementos están vinculados con un conjunto de entidades de distintos tipos: hardware, software, redes y personal de la universidad; y cada elemento esencial tiene una necesidad de seguridad. Esta necesidad se expresa según distintos criterios de seguridad de la información, tales como la disponibilidad, la integridad y la confidencialidad.

La Disponibilidad de la información se refiere la capacidad de estar siempre disponible para su uso por personas autorizadas.

La Integridad de la información es la característica de permanecer intacta en su origen, a menos que sea modificada por personas con permiso para hacerlo, y dicha modificación sea registrada, esta se puede ver afectada por problemas de hardware, software, virus o personas mal intencionadas.

La Confidencialidad es la necesidad de privacidad, y se refiere a que la información sólo puede ser conocida por individuos autorizados.

El impacto de no respetar estas necesidades adopta distintas formas, como deficiencias en la consecución de las actividades, daños o pérdidas de información y equipos, daño de la imagen de la universidad, descontento de los usuarios, entre otros. En la figura 1 se puede observar la relación establecida entre los elementos sensibles y los criterios de seguridad.

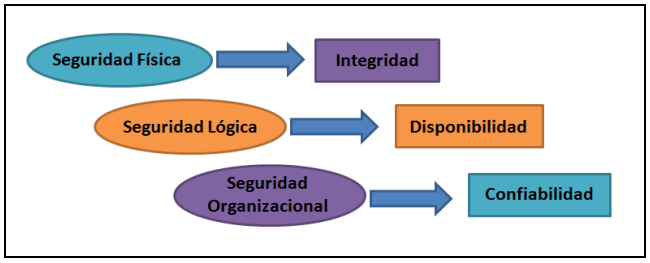

Figura 1. Relación entre Elementos Sensibles y Criterios de Seguridad.

Identificando estos factores dentro de la infraestructura de red, se procedió a realizar el análisis de riesgos; se asume un riesgo como la proximidad o posibilidad de daño sobre un bien, ya se trate de actos naturales, errores u omisiones humanas y actos intencionales; asignándole un valor estimado a la pérdida de un recurso, al multiplicar éste por su importancia se obtiene la evaluación general de riesgo del recurso ($WR_i = R_i * I_i$) Luego el riesgo general de los recursos de la red viene dado por la siguiente fórmula: $W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + \ldots + WR_n * I_n)}{I_1 + I_2 + \ldots + I_n}$.

Este método es definido por ArCERT, Coordinación de Emergencias en Redes Teleinformáticas de la República Argentina. (ArCERT (1999), Manual de Seguridad en Redes, Pág. 31).

En la tabla 2 se presentan los recursos relevantes de la red, su ponderación de riesgo e importancia.

Tabla 2: Valuación de Riesgos.

Recurso	Riesgo (R_i)	Importancia (I_i)	Riesgo Evaluado (R_i*I_i)
Servidores	9	10	90
Router	9	10	90
Switch Central	9	10	90
Base de Datos	9	10	90
Software administrativo, de aplicación, S.O	9	9	81
Backup	9	9	81
Transceivers	8	8	64
DTU	8	8	64
Datos en tránsito y medios externos	8	8	64
Modems, A.P., PABX	7	7	49
Cableado, antenas, hubs, swtches	7	7	49
Documentos de Conf. de red, programas, sistemas y procedimientos administrativos.	6	6	36
PC's, impresoras, fax	5	5	25
Insumos, Datos de usuarios	3	3	9

Resultando el riesgo total: $W_R = 8,02$. Sobrepasando así la media de los valores asignados (0 – 10).

3.3 FASE III

Esta fase abarcó la tercera y cuarta etapa de la metodología EBIOS, el estudio de las amenazas e identificación de los objetivos de seguridad, así como también la selección de principios y redacción de normas correspondientes a la fase 2 de la metodología PSSI.

Aquí se analizaron y estudiaron los datos obtenidos relacionados con las amenazas genéricas, vulnerabilidades y riesgos que enfrenta la infraestructura de red. Esta fase permitió determinar la exposición de los sistemas y redes a intrusiones y otros factores de riesgos; este reconocimiento define las bases para la selección de los principios de seguridad y la redacción de las estrategias que pueden ser implementadas a futuro.

En esta fase se formalizaron las perspectivas generales de las normas para cada elemento sensible, tomando la premisa de que un sistema de seguridad es un conjunto de elementos tanto físicos como lógicos que se encarga de prevenir o remediar posibles riesgos o problemas que se puedan presentar en un determinado momento, una de sus principales características es ser proactivo, un buen sistema de seguridad ayuda bastante en el trabajo y la consecución de las actividades, ya que se minimiza la tarea de corrección.

En este sentido se planteó una perspectiva de seguridad física, que denota la importancia de la protección de los activos, sistemas de información presentes en la Universidad de Oriente Núcleo Monagas, y los equipos que les brindan apoyo, como hardware, dispositivos de red, dispositivos electrónicos, así como el entorno, requiriendo la inclusión de medidas contra desastres naturales, instalaciones inadecuadas (cables mal ubicados o en mal estado, cercanía de cables eléctricos a los cables de red, infraestructura en condiciones no adecuadas), robo u ataques hostiles contra equipos y el control de acceso a los dispositivos importantes.

Una perspectiva de seguridad lógica, que se orienta hacia la aplicación de barreras y procedimientos que resguarden el acceso a los datos en la red de la Universidad de Oriente Núcleo Monagas, permitiendo el acceso sólo a las personas autorizadas. Con acciones como: restringir el acceso a programas y archivos dependiendo del usuario. Definir y verificar la complejidad de las claves de acceso a los sistemas. Asegurar que los operadores

puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan. Certificar que se estén utilizados los datos, archivos y programas correctos en y con el procedimiento correcto. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. Que se disponga de pasos alternativos de emergencia para la transmisión de información, entre otros.

Y una perspectiva de seguridad organizacional, que se orientó en proporcionar controles a las acciones del personal que opera con los activos de información. El objetivo de esta área es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información, haciendo hincapié en la concienciación de sus actividades, haciéndolos más responsables y partícipes de las medidas de seguridad, ya que son los principales involucrados.

3.4 FASE IV

Esta fase contuvo la quinta etapa de la metodología EBIOS, determinación de los objetivos de seguridad, y la fase de finalización correspondiente a la metodología PSSI, que en conjunto determinan la redacción y validación de las estrategias de seguridad.

En esta etapa se utilizó la información recopilada sobre la situación actual de la infraestructura de red con respecto a seguridad y los requerimientos expresados por los administradores de la misma, para así realizar la redacción y validación de las estrategias de seguridad aplicables al sistema. Estableciendo que las estrategias de seguridad son una medida que busca constituir los estándares de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos de la red informática de la Universidad de Oriente, Núcleo Monagas. Es una forma de suministrar un conjunto de normas internas para guiar la acción de los usuarios y encargados de la red. Es el primer paso para aumentar la conciencia de la seguridad en las personas, pues está orientada hacia la formación de hábitos, por medio de manuales de instrucción y procedimientos operativos.

El propósito de proponer este Plan de Seguridad Informática, es proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los usuarios mientras permanezcan en uso de la red de datos de la universidad.

Estas estrategias emergen como el instrumento para concientizar a los usuarios acerca de la importancia y sensibilidad de la información y servicios críticos. El proponer estas estrategias o políticas de seguridad requiere un alto compromiso con la institución, y por parte de ésta, constancia para renovar y actualizar dicha política en función de un ambiente dinámico. Estos lineamientos describen los pasos a seguir para generar un sistema seguro y estable, que permita tanto a usuarios como al sistema en sí, mantener sus bienes de información seguros y optimizar el rendimiento de la red. En este sentido, se formularon las siguientes estrategias:

3.4.1 ESTRATEGIA DE USO DE LA RED.

Estableciendo las Consideraciones Generales: Los recursos de la Red de Datos de la Universidad de Oriente Núcleo de Monagas, son para el estricto uso de las actividades propias, directas y obviamente relacionadas con las funciones de la Institución: Gerencia, Administración, Docencia, Investigación, Extensión y Gestión Universitaria.

Definiciones: Recursos de la red, Se define a los recursos de la red a todas aquellas facilidades telemáticas que la UDO, a través de la Delegación de Teleinformática, las Unidades de Informática de las Escuelas, y por otras vías proveen, tanto de manera local, como a través de Internet, a todos los miembros de la comunidad universitaria.

Usuarios Finales: Desde el punto de vista del tipo de conexión, los usuarios finales se denominarán:

Usuario Básico: Aquel que puede acceder únicamente a los recursos de la Red e Internet.

Usuario Avanzado: Aquel con capacidad de administrar los recursos del equipo y que además tiene acceso a los recursos de red e Internet. Este tipo de acceso implica responsabilidad total por ese dispositivo informático.

Administrador de Red: aquella persona o grupo de personas que tiene la responsabilidad de instalar o manejar los sistemas de red, ya sea en un nodo o en un departamento.

Estableciendo los Derechos y Responsabilidades:

De los Usuarios.

Normas generales: Todo miembro de la Comunidad Udista, Profesor, Estudiante o Personal Administrativo que, por razón de sus actividades académicas, administrativas, de investigación o extensión, puedan acceder a una estación de trabajo (ET), podrán disfrutar de algunos de los recursos de la red.

Uso de los recursos de la red: Cada usuario es el responsable del correcto uso de los recursos de red. El mismo debe ser racional, legal y debe evitar la saturación

Seguridad: Cada usuario debe contribuir a la seguridad total del sistema.

Integridad y Mantenimiento del Sistema: Los usuarios se comprometen a no interferir, voluntariamente, en el uso adecuado de los recursos de red

Acuerdos: documentos donde se establece y acepta la responsabilidad por la administración del recurso informático asignado.

Normas específicas de los Usuarios: establece las normas para el uso de los recursos de red por parte de Docentes e Investigadores, Estudiantes, Personal Administrativo, Personal de Extensión/Asistenciales y Personal Gerencial.

3.4.2 ESTRATEGIA DE SEGURIDAD FÍSICA.

Especificaciones Técnicas sobre el Sistema de Cableado Estructurado para Redes de Área Local de la UDO-Monagas.

Distribución del Cableado Horizontal: El sistema del cableado estructurado debe permitir la distribución del servicio de datos desde el cuarto de cableado mas cercano hasta los puestos de trabajo de los usuarios.

Generalidades Sobre la Red Horizontal de Datos: La red de cableado estructurado deberá hacerse atendiendo a las especificaciones y normas contenidas en el estándar EIA/TIA 568-A-B para cableado UTP Categoría 5E o superior.

Distribución del Cableado Vertical (Backbone): La distribución del cableado vertical permitirá la interconexión de cada una de las redes de datos. La interconexión de las redes de datos se hará directamente con el cuarto de cableado principal, o con algún punto de interconexión directo al backbone de la red, utilizando fibra óptica (multimodo o monomodo) de seis hilos o superior, o cable UTP para Gigabit Ethernet.

Cuartos de Datos: A medida de lo posible, los cuartos de datos de la Universidad deben ser ubicados según el estándar TIA 942, en Tiers de nivel II o superior. Prever el albergue de sistemas y componentes asociados con una tasa de crecimiento de mínimo 15% en cinco años. Incluyendo copias de seguridad y suministro de energía eléctrica redundante, conexiones de comunicaciones de datos en stand by, controles ambientales y dispositivos de seguridad en el acceso.

Componentes Activos: se especifican los tipos de componentes activos que se pueden instalar en los cuartos de datos.

Consideraciones de aterramiento: establecida de acuerdo a la **Norma ANSI/J-STD-607: Tierras y Aterramientos para los Sistemas de Telecomunicaciones de Edificios Comerciales.**

Consideraciones Generales: Todos los materiales utilizados e instalados deben poseer una certificación de garantía de fábrica de al menos Quince (15) Años y Cinco (5) Años contra defectos en la Instalación.

3.4.3 ESTRATEGIA DE SEGURIDAD LÓGICA.

En esta estrategia se especifican los tipos de controles a implementar, tal es el uso de IDS (Intrusion Detection System, siglas en inglés), monitoreo y análisis de logs, configuración de servidores en prevención de ataques DoS y bloqueo de aplicaciones P2P externas, establecimiento de firmas electrónicas, aplicación de virtualización para los servicios críticos de la red y el establecimiento de contraseñas seguras para aplicaciones y equipos.

3.4.4 ESTRATEGIA DE SEGURIDAD ORGANIZACIONAL.

Se estableció los **Deberes y Restricciones por parte de los Usuarios Finales de la Red de Datos de la UDO – Monagas:** Párrafos destinados a proveer un marco referencial de actuación a los usuarios finales pertenecientes a las distintas dependencias que hacen uso de la Red de Datos de la Universidad de Oriente, Núcleo Monagas, en materia de seguridad de la información y resguardo de los equipos asignados, a fin de que sea incorporado a sus rutinas de trabajo, lo cual contribuirá a garantizar una plataforma corporativa estable y segura, que permita realizar sus funciones administrativas y/o académicas.

De los Deberes: se establecieron los deberes y responsabilidades de los usuarios con el fin de no comprometer la seguridad de la red y resguardar los recursos asignados para realizar sus actividades institucionales.

De la protección contra virus: todo usuario deberá reportar al personal de la Delegación de Teleinformática cuando haya detección o sospecha de la existencia de virus informáticos y/o software malicioso en el equipo.

De las restricciones: se especifican todas aquellas acciones que deben evitar ejecutar los usuarios de los recursos de red corporativa.

1. CONCLUSIONES Y RECOMENDACIONES

a) La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las organizaciones para mejorar su productividad y poder explorar más allá de sus fronteras, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información, por lo que la seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles.

b) Los riesgos que enfrentan las organizaciones, han llevado a que se desarrollen documentos y directrices que orientan en el uso adecuado de estas tecnologías y recomendaciones para obtener el mayor provecho de estas ventajas y así evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones.

c) La seguridad en la información no es posible sin la cooperación del usuario. Se puede tener la mejor tecnología para protegerlos y aún así, sufrir una ruptura de seguridad.

d) Se pudo apreciar que con el hecho de utilizar un conjunto de preguntas y procedimientos se logra concretar una excelente imagen de las vulnerabilidades a las que es susceptible la red de la UDO – Monagas.

e) Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles dentro de la universidad, es vital el desarrollo de documentos y directrices que orienten a los usuarios en el uso adecuado de las tecnologías para aprovechar mejor sus ventajas. En este sentido, las estrategias de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la universidad sobre la importancia y sensibilidad de la información y servicios críticos que permiten a UDO crecer y mantenerse activa. Ante esta situación, el proponer o identificar estas estrategias requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dichas estrategias en función del dinámico ambiente que rodea las organizaciones modernas.

f) Finalmente debe quedar claro que la Seguridad Informática es un aspecto muchas veces descuidado en los sistemas, pero de vital importancia para el correcto funcionamiento de todos ellos. Seguridad es un proceso, no un producto.

Dentro de las recomendaciones se plantearon:

a) Desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo de la información, así como su impacto a nivel de las operaciones de la universidad.

b) Contribuir en la capacitación y adquisición de nuevos conocimientos en el área de seguridad informática del personal del Centro de Computación y Teleinformática, con el fin de favorecer la motivación por el trabajo y su crecimiento profesional.

c) Establecer métodos de culturización del personal de la universidad y usuarios generales, estimulando el cultivo de principios morales hacia la seguridad de la información que tengan repercusión a nivel institucional.

d) Mejorar los métodos de registros de eventos desarrollando alguna aplicación que permita elaborar reportes, estimaciones y proyecciones de los incidentes en la infraestructura de red de la UDO Monagas.

REFERENCIAS

Annan, Kofi. (2003). *Discurso Inaugural de la Primera Fase de la WSIS.* Ginebra.

Andrew Lockhart. (2006). *Seguridad de Redes, Los Mejores Trucos.* Editorial ANAYA. Segunda Edición. Madrid.

Cerini, María. Prá, Pablo. (2002). *Plan de Seguridad Informática.* Tesis de Pregrado de Ingeniería de Sistemas. Universidad Católica de Córdoba. Argentina.

Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (ArCERT). (1999). *Manual de Seguridad en Redes.* Buenos Aires.

Dirección Central de Seguridad de los Sistemas de Información. (2004). *EBIOS. Compendio.* Paris.

Dirección Central de Seguridad de los Sistemas de Información. (2004). *PSSI. Compendio.* Paris.

Gallo, Michael. Hancock, William. (2002). *Comunicación entre Computadoras y Tecnologías de Redes.* Editorial THOMSON. Primera Edición. México.

Pereira, A. (2008) *Diseño de una Arquitectura de Interconexión entre los Campus Guaritos – Juanico de la Universidad de Oriente, Núcleo Monagas.* Tesis de pregrado. Universidad de Oriente. Maturín.

Stalling, William. (2004). *Fundamentos de Seguridad en Redes. Aplicaciones y Estándares.* Editorial PEARSON Prentice Hall. Segunda Edición. Madrid.

Vicente Aceituno Canal. (2004). *Information Security Management Maturity Model*. ISECOM. Primera Edición.

Cisco. *Data Center. Mejores Prácticas.* [Documento en línea] Disponible en: http://www.cisco.com/assets/cdc_content_elements/flash/dcap3/

Conformidad Metodológica. EBIOS. [Documento en línea] Disponible en: http://www.isdecisions.com/es/conformidad/metodologica/ebios.cfm

Data Center. [Documento en línea] Disponible en: http://www.compusoluciones.com.do/index2.php?option=com_content&do_pdf=1&id=50

EBIOS. PSSI. Servidor Temático sobre la Seguridad de los Sistemas de Información. [Documentos en línea] Disponibles en: http://www.ssi.gouv.fr/archive/es/confianza/methods.html

Introducción a la seguridad informática. [Documento en línea] Disponible en: http://es.kioskea.net/contents/secu/secuintro.php3

Autorización y Renuncia

Los autores autorizan a LACCEI para publicar el escrito en las memorias de la conferencia. LACCEI o los editores no son responsables ni por el contenido ni por las implicaciones de lo que esta expresado en el escrito.