FICA, Vol. XX, No. X, MES 20XX

ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.

Ana Cristina OREJUELA PÉREZ
Empresa Eléctrica Regional Norte S.A. – EMELNORTE

kristy_op@hotmail.com

Resumen—*El presente artículo tiene como finalidad dar a conocer el trabajo de grado con el manual de políticas y normas de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la entidad beneficiaria que es la EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.*

En términos generales estas políticas y normas de seguridad informática, propende por englobar los procedimientos más adecuados, tomando como lineamientos principales los siguientes criterios: Seguridad Organizacional, Seguridad Lógica, Seguridad Física y Seguridad Legal.

Palabras Claves

Políticas de seguridad informática, Normas de Seguridad, Estándares.

Abstract—*This paper aims to present the degree work with manual policies and information security standards to be observed by service users of information technology to adequately protect it assets and information from the beneficiary which is the EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE.*

In general, these policies and information security standards, aims for include appropriate procedures, using as main guidelines the following criteria: Organizational Security, Logical Security, Physical Security and Legal Security.

INTRODUCCIÓN

ANTECEDENTES

MISIÓN: Generar, distribuir y comercializar energía eléctrica bajo estándares de calidad para satisfacer las necesidades de sus clientes, con servicios de excelencia, personal calificado y comprometido, contribuyendo al desarrollo del país.

VISIÓN: EMELNORTE, será una empresa competitiva, técnica, moderna, modelo y referente del sector eléctrico, por la calidad de sus productos y servicios, gestión transparente y por su efectiva contribución al desarrollo del país.

ORGANIZACIÓN DE LA EMPRESA

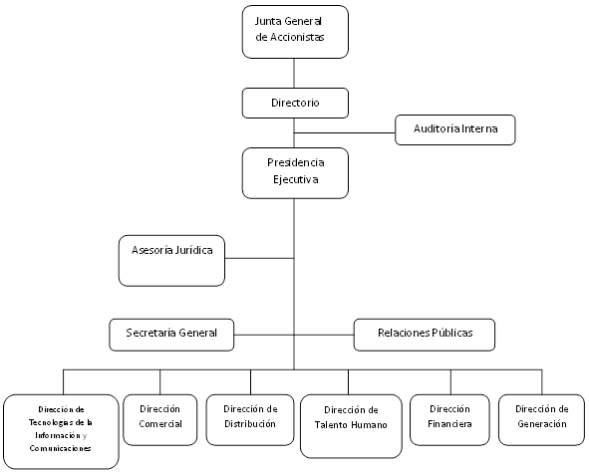

ILUSTRACIÓN 1: Estructura orgánica de la empresa
Fuente: EMELNORTE S.A.

PROBLEMA

La Empresa Eléctrica Regional Norte S.A. – EMELNORTE, es una empresa que posee una red de comunicaciones que integra a todos los usuarios que manejan equipos de computación. Es indispensable contar con políticas de seguridad que ayuden a desarrollar de mejor manera las actividades de intercambio de información y uso de sistemas.

Actualmente existen pocas políticas internas de seguridad, lo que ocasiona muchos inconvenientes en toda el área de concesión de EMELNORTE, tanto en los sistemas, comunicaciones, equipos de computación y la causa de malestar tanto a los abonados como a los usuarios de los sistemas de la empresa. Por ejemplo, la instalación de programas no permitidos en los equipos como los proxy que pueden crear huecos de seguridad en la red o el cambio de lugar de equipos sin previo conocimiento y autorización del Centro de Cómputo lo que causa errores en los registros e inventarios de equipos.

Por lo antes mencionado se ve imperiosa la necesidad de elaborar e implementar políticas y normas de seguridad basándose para su desarrollo en las NORMAS ISO.

JUSTIFICACIÓN

Ante el esquema de globalización de la tecnologías de la información han originado principalmente por el uso masivo y universal de la internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear y robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir, en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país existen muchas instituciones que han sido víctimas de ataques en sus instalaciones, tanto desde el interior como del exterior, por lo que es necesario tratar de contrarrestar y anular estas amenazas reales.

Así pues, ante este panorama surge el proyecto de políticas rectoras que harán que el departamento de Tecnologías de la Información y la Comunicación de EMELNORTE, pueda disponer de los ejes de proyección que en materia de seguridad informática la institución requiere.

ALCANCE

El resultado de la investigación es proveer a EMELNORTE de un manual que contendrá las políticas y normativas de seguridad informática.

Este manual de políticas de seguridad será elaborado de acuerdo al análisis de riesgos y de vulnerabilidades de EMELNORTE, por consiguiente el alcance de estas políticas se encuentra sujeto a la empresa.

SEGURIDAD INFORMÁTICA

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Los objetivos de la seguridad informática se enfocan en:

Integridad: Certificar que los datos sean los que se supone que son.

Confidencialidad: Asegurar la disponibilidad de los recursos únicamente a los individuos autorizados.

Disponibilidad: Garantizar el correcto funcionamiento de los sistemas de información.

Evitar el rechazo: Garantizar de que no pueda negar una operación realizada.

Autenticación: Asegurar que sólo los individuos autorizados tengan acceso a los recursos.

AMENAZAS

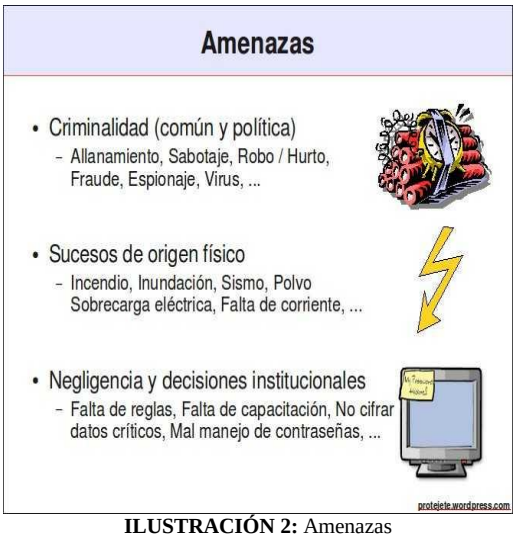

ILUSTRACIÓN 2: Amenazas

Una Amenaza, en el entorno informático, puede ser cualquier elemento que comprometa al sistema. Pueden presentarse circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables.

ANÁLISIS DE RIESGOS

La información es lo más importante dentro de una compañía y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Después de efectuar el análisis debemos determinar las acciones a tomar respecto a los riesgos residuales que se identificaron.

POLÍTICAS DE SEGURIDAD

ILUSTRACIÓN 3: Política de Seguridad: Procesos, Reglas y Norma Institucionales

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación.

RESPALDO

La información constituye puede verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup).

Es vital para las empresas elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables: Continuo, Seguro, Remoto y Mantención de versiones anteriores de los datos.

NORMA TÉCNICA ECUATORIANA INEN-ISO/IEC 27002:2009

Se elaboró las políticas considerando la Norma Técnica Ecuatoriana INEC-ISO/IEC 27002:2009, considerando lo siguiente:

- ✓ Evaluación y tratamiento de riesgos
- ✓ Política de la seguridad
- ✓ Organización de la seguridad de la información
- ✓ Gestión de activos
- ✓ Gestión de comunicaciones y operaciones
- ✓ Control del acceso
- ✓ Adquisición, desarrollo y mantenimiento de sistemas de información
- ✓ Gestión de los incidentes de la seguridad de la información
- ✓ Gestión de la continuidad del negocio
- ✓ Cumplimiento

MANUAL DE POLÍTICAS DE SEGURIDAD

Este manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y vulnerabilidades en las direcciones de la Empresa Eléctrica Regional Norte S.A. – EMELNORTE, por consiguiente el alcance de estas políticas, se encuentra sujeto a la institución.

Se consideraron los siguientes temas:

- ✓ **Activos**
  - ➢ De información
  - ➢ De software, físicos y servicios
- ✓ **Equipos de cómputo**
  - ➢ De la instalación
  - ➢ Para el mantenimiento
  - ➢ De la actualización
  - ➢ De la re-ubicación
  - ➢ De la seguridad
- ✓ **Comunicaciones y operaciones**
  - ➢ Procedimientos y responsabilidades
  - ➢ Planificación y aceptación del sistema**¡Error! Marcador no definido.**
  - ➢ Protección contra códigos maliciosos y móviles
  - ➢ Respaldo
  - ➢ Seguridad en las redes
  - ➢ Manejo de los medios
  - ➢ Monitoreo

- ✓ **Control de acceso**
  - ➢ Gestión del acceso de los usuarios
  - ➢ Responsabilidad de los usuarios
  - ➢ A las redes
  - ➢ Al sistema operativo, las aplicaciones, información
  - ➢ Computación móvil y trabajo remoto
  - ➢ A la web
- ✓ **Software**
  - ➢ De la adquisición
  - ➢ De la instalación
  - ➢ De la actualización
  - ➢ De la auditoria de software instalado
  - ➢ Del software propiedad de la institución
  - ➢ De la propiedad intelectual
- ✓ **Incidentes de la seguridad de la información**
  - ➢ Reporte sobre los eventos
  - ➢ Reporte sobre las debilidades
  - ➢ Gestión de incidentes y mejoras en la seguridad de la información
- ✓ **Supervisión y cumplimiento**
  - ➢ Cumplimiento de las políticas y normas de seguridad
  - ➢ Verificación del cumplimiento técnico
  - ➢ Consideraciones de la auditoría de los sistemas de información

CONCLUSIONES

1. Es responsabilidad de los usuarios de equipos y servicios tecnológicos de EMELNORTE cumplir las políticas y normas del MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA.

2. La Dirección de TIC's emitirá y revisará el cumplimiento de las políticas y normas de seguridad informática que permitan realizar acciones correctivas y preventivas para el cuidado y mantenimiento de los equipos que forman parte de la infraestructura tecnológica de la empresa.

3. La organización y ejecución de pruebas, inspecciones y auditorias (internas y externas) para asegurar la continuidad de la integridad funcional del MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA.

4. Todas las acciones en las que se comprometa la seguridad de la empresa y que no estén previstas en este manual, deberán ser revisadas por la Dirección de TIC's para dictar una resolución sujetándose al estado de derecho y a la normativa vigente.

5. El incumplimiento a cualquiera de las políticas establecidas en el manual acarreara las sanciones de tipo disciplinario y legal a que hubiera lugar de acuerdo a la normativa vigente.

RECOMENDACIONES

1. Legalizar ante los estamentos jurídicos el "MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA".

2. Mantener siempre actualizado el "MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA".

3. Socializar con todos los empleados y trabajadores de la empresa el "MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA".

4. Recomendar la elaboración de manuales de políticas y normas de todas las actividades que se realizan en el departamento de TIC's.

5. Crear un Sistema Informático de Gestión de Seguridad de la información, que supervise y normalice, toda actividad relacionada con la seguridad informática.

6. Recomendar que durante la etapa estudiantil dentro de la Universidad Técnica del Norte las materias impartidas sean teóricas y prácticas para tener un mejor desarrollo en la vida profesional.

7. Crear en la Universidad Técnica del Norte un registro con las necesidades de la comunidad para que las carreras técnicas desarrollen la mejor solución.

AGRADECIMIENTOS

A Dios, por haberme guiado por un buen camino y lograr con éxito esta etapa de mi vida estudiantil.

A todos los miembros de mi familia, por sus ánimos y su apoyo incondicional.

A la Universidad Técnica del Norte, por abrirme sus puertas y prepárame adecuadamente en sus aulas y con los mejores docentes que me impartieron sus conocimientos.

A mi director de tesis, Ing. Edgar Daniel Jaramillo, por sus recomendaciones, consejos y su amistad.

A todos los docentes de la UTN, por su paciencia durante toda mi etapa estudiantil.

A todos los amigos que han estado presentes en las buenas y en las malas.

A EMELNORTE por permitir mi formación en el ámbito profesional.

BIBLIOGRAFÍA

1. Costas Santos, J. (2011). SEGURIDAD Y ALTA DISPONIBILIDAD. CFGS. Ra-ma.

2. Dante Cantone, M. (2011). ADMINISTRACION DE STORAGE Y BACKUPS. Ra-ma.

3. Escrivá Gascó, G., Romero Serrano, R. M., Ramada, D. J., & Onrubia Pérez, R. (2013). SEGURIDAD INFORMÁTICA. Macmillan Profesional.

4. Gomez Vieites, A. (2011). ENCICLOPEDIA DE LA SEGURIDAD INFORMATICA. Ra-ma.

5. Gomez Vieites, A., & García Tomé, A. (2011). GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA. Starbook Editorial, S.A.

6. Gomez Vietes, A., & García Tomé, A. (2011). SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS. Starbook Editorial, S.A.

7. Instituto Ecuatoriano de Normalización. (2009). SISTEMAS DE GESTIÓN DE LA CALIDAD. REQUISITOS. Quito: INEN.

8. Instituto Ecuatoriano de Normalización. (2009). TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE LA SEGURIDAD - CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Quito: INEN.

9. Instituto Ecuatoriano de Normalización. (2011). TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) - REQUISITOS. Quito: INEN.

10. Lacasta, R., Sanmartí, E., & Velasco, J.

11. Merino Bada, C., & Cañizares Sales, R. (2011). IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Fundación Confemetal.

12. Purificación, A. (2010). SEGURIDAD INFORMÁTICA. Nivel: formación profesional. Ra-ma.

13. Scrib. (2009). Seguridad de la información. Tipos de ataques Informáticos. Recuperado el 9 de Julio de 2013, de Scrib: http://www.scribd.com/doc/19397003/Tipos-de-Ataques-informaticos

14. Vallecilla Mosquera, J. (2009). Seguridad de las TIC bajo protocolos TCP/IP. Recuperado el 9 de Julio de 2013, de Vallecilla Mosquera, Juan: http://biblioteca.cenace.org.ec:8180/jspui/handle/123456789/86

15. Vieites Gomez, A., & García Tomé, A. (2011). AUDITORÍA DE SEGURIDAD INFORMÁTICA. Starbook Editorial, S.A.