UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

INFORME TÉCNICO

TEMA: *PLANEACIÓN DE LA SEGURIDAD INFORMÁTICA*

APLICATIVO: *AUDITORÍA INFORMÁTICA Y DEFINICION DE POLÍTICAS DE SEGURIDAD DE LA COOPERATIVA DE AHORRO Y CRÉDITO "ATUNTAQUI" Ltda.*

AUTORA: *GLORIA GRACIELA SUÁREZ PIÑA*
DIRECTOR: *Ing. Msc. JORGE CARAGUAY*

IBARRA-ECUADOR

INDICE

INDICE 2
OBJETIVOS 3
1. Objetivo General 3
INTRODUCCION 4
2. INTRODUCCION 4
CAPITULO I 5
1. AUDITORÍA INFORMÁTICA 5
1.1. Importancia de la Auditoria Informática 5
CAPITULO II 7
2. AUDITORÍA DE SEGURIDAD INFORMÁTICA 7
2.1. Introducción 7
2.2. OBJETIVO GENERAL 7
2.3. SEGURIDAD LÓGICA 7
2.3.1. OBJETIVO 7
2.4. SEGURIDAD DE LAS COMUNICACIONES 7
2.4.1. OBJETIVO 7
2.5. SEGURIDAD DE LAS APLICACIONES 8
2.5.1. OBJETIVO 8
2.6. SEGURIDAD FÍSICA 8
2.6.1. OBJETIVO 8
2.7. ADMINISTRACIÓN DE LA BASE DE DATOS 8
2.7.1. OBJETIVO 8
CAPITULO III 9
CONCLUSIONES Y RECOMENDACIONES 9
3. CONCLUSIONES 9
3.1. RECOMENDACIONES 10

OBJETIVOS

Objetivo General

- Realizar un estudio y definición de Planeación de la Seguridad Informática, sobre la importancia de los recursos para resolver los nuevos problemas que se presentan en la Institución, en relación a la seguridad y especificar las responsabilidades de aplicar los correctivos o sanciones.

- Realizar una Auditoria Informática en la Cooperativa de Ahorro y Crédito "Atuntaqui" Ltda. con el fin de establecer puntos críticos, desarrollar políticas de seguridad y soluciones de contingencia.

INTRODUCCION

INTRODUCCION

La institución es cada vez más dependiente de sus Sistemas y Servicios de Información, por lo tanto podemos afirmar que son cada vez más vulnerables a las amenazas concernientes a su seguridad.

La información debe considerarse como un recurso de misión crítica con el que cuenta la institución y por lo tanto tiene un considerable valor para ésta, al igual que el resto de los activos, debe estar debidamente protegida.

La Seguridad de la Información, protege a esta de una amplia gama de amenazas, tanto de orden fortuito como destrucción, incendio o inundaciones, o de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, etc.

Con Políticas de Seguridad que se implantaran se puede obtener normas y procedimientos documentados y comunicados, que tienen por objetivo minimizar los riesgos informáticos más probables que involucran el uso de herramientas, y cumplimiento de tareas por parte de las personas involucradas en salvaguardar la información, con el objetivo de recuperar operatividad mínima de un lapso de tiempo adecuado a la misión del sistema afectado, ante emergencias generadas por los riesgos informáticos.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el porqué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios y los gerentes.

CAPITULO I

AUDITORÍA INFORMÁTICA

Es importante definir el término de Auditoria, ya que el mismo se ha usado principalmente para referirse a una revisión cuyo único fin es detectar errores, fraudes, señalar fallas y como consecuencia recomendar el despido o remoción del personal, no obstante, la auditoria es un concepto mucho más amplio que lo define como "El proceso sistemático para evaluar y obtener de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados". El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando los principios establecidos para el caso". [1]

Importancia de la Auditoria Informática

La Auditoria Informática, es importante en las organizaciones por las siguientes razones:

✓ Se pueden difundir y utilizar resultados o información errónea si la calidad de datos de entrada es inexacta o los mismos son manipulados, lo cual abre la posibilidad de que se provoque un efecto dominó y afecte seriamente las operaciones, toma de decisiones e imagen de la empresa.

✓ Las computadoras, servidores y los Centros de Procesamiento de Datos se han convertido en blancos apetecibles para fraudes, espionaje, delincuencia y terrorismo informático.

✓ La continuidad de las operaciones, la administración y organización de la empresa no deben descansar en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.

[1] The American Accounting Association

✓ Las bases de datos pueden ser propensas a atentados y accesos de usuarios no autorizados o intrusos.

✓ En el Departamento de Sistemas se observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.

✓ Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.

CAPITULO II

AUDITORÍA DE SEGURIDAD INFORMÁTICA

Introducción

La auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

OBJETIVO GENERAL

La realización de una Auditoria Informática en la Cooperativa de Ahorro y Crédito "Atuntaqui" Ltda. con el fin de relevar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una Política de Seguridad, donde se definirán los lineamientos para promover la implementación de un modelo de seguridad en toda la organización.

SEGURIDAD LÓGICA

1.1.1. OBJETIVO

Evaluar los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que éstas gestionan, con el fin de señalar las irregularidades que obstaculicen la confidencialidad, exactitud y disponibilidad de la información, y las mejoras que fueran factibles de efectuarse.

SEGURIDAD DE LAS COMUNICACIONES

1.1.2. OBJETIVO

Se deberá evaluar la seguridad de las comunicaciones, los datos transmitidos, los dispositivos usados durante la transmisión, la documentación necesaria para la

realización eficiente e ininterrumpida de esta transmisión, y los sistemas usados para la transmisión de datos de un entorno a otro, comprobando el cumplimiento de las normas de seguridad de la información.

SEGURIDAD DE LAS APLICACIONES

1.1.3. OBJETIVO

Evaluar la seguridad de las aplicaciones utilizadas en la institución, la consistencia de sus datos de entrada y la exactitud de sus datos de salida, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento, de acuerdo a los estándares propuestos.

SEGURIDAD FÍSICA

1.1.4. OBJETIVO

Evaluará que el centro de cómputos, los equipos, los dispositivos, los medios de almacenamientos y las personas que conforman el sistema informático de La Empresa cumplan con las medidas necesarias en lo relativo a la infraestructura física y al mantenimiento de la seguridad de los recursos de la organización.

ADMINISTRACIÓN DE LA BASE DE DATOS

1.1.5. OBJETIVO

Evaluar la correcta organización y administración del área de sistemas (Centro de Procesamiento de Datos), así como la asignación de tareas y responsabilidades del personal que la conforma; a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo a las normas existentes que regulan esta actividad.

CAPITULO III

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El encargado de la seguridad de los centros de cómputo debe garantizar que la información y los activos de la institución, sean confidenciales, íntegros y disponibles para todos los usuarios.

- Somos conscientes de que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo se debe estar preparado y dispuesto a reaccionar con rapidez ya que las amenazas y las vulnerabilidades están cambiando constantemente.

- Disponer de una política de seguridad es importante, pero entendemos que hacer de la política de seguridad una parte del entorno de trabajo diario es esencial. La comunicación con los usuarios del sistema es la clave para hacer que esta política sea efectiva y se genere una "cultura de la seguridad" entre los usuarios de la información que tiene la institución.

RECOMENDACIONES

- Sabiendo el rol estratégico que ocupa la infraestructura de T/SI a lo largo de todas las áreas del negocio en las instituciones, permitiendo el intercambio y el procesamiento de la información, es necesario que sean investigadas, evaluadas, y posteriormente sean divulgadas dentro de cada organización que desee conseguir mejoras productivas y competitivas.

- La institución debe ser capaz de cumplir con su propio modelo de gestión de innovación tecnológica, basado en sus necesidades, relacionadas con su sector y tamaño, pero, sobre todo, con su propia estrategia y visión del futuro.

- Para situar a la innovación como un arma competitiva y un motor de crecimiento de la institución, es importante aprovechar la capacidad estratégica de sus recursos tecnológicos potenciando el liderazgo del Jefe de Sistemas. El esfuerzo de definir la estrategia de innovación tecnológica se hace especialmente necesario para potenciar la atención a las tecnologías de medio y largo plazo, para la planificación de nuevos productos y procesos, y para enmarcar el desarrollo de las necesidades que han surgido.

- Para las correctas creaciones de las Políticas de Seguridad hemos utilizado algunas herramientas que tienen un costo elevado con lo que se ha realizado la comparación Costo/Beneficio para la institución y hemos formulado que es una inversión muy necesaria en la que podemos decir que el beneficio es alto para el costo en el que ha sido adquirido.

TECHNICAL UNIVERSITY OF NORTH

ENGINEERING SCHOOL OF APPLIED SCIENCE

SCHOOL OF COMPUTER SYSTEMS ENGINEERING

TECHNICAL REPORT

THEME: *INFORMATION SECURITY PLANNING*

APPLICATION: *COMPUTER AUDIT POLICY AND DEFINITION OF SECURITY SAVINGS AND CREDIT COOPERATIVE "Atuntaqui" Ltd.*

AUTHOR: *GLORIA GRACIELA SUAREZ PIÑA*
DIRECTOR: *Mr. Msc. JORGE CARAGUAY*

IBARRA, ECUADOR

INDEX

1. General Purpose 3
2. INTRODUCTION 4
1. COMPUTER AUDIT 5
1.1. Importance of Computer Audit 5
2. IT SECURITY AUDIT 7
2.1. Introduction 7
2.2. GENERAL PURPOSE 7
2.3. LOGICAL SECURITY 7
2.3.1. OBJECTIVE 7
2.4. COMMUNICATIONS SECURITY 7
2.4.1. OBJECTIVE 7
2.5. SECURITY APPLICATIONS 8
2.5.1. OBJECTIVE 8
2.6. PHYSICAL SECURITY 8
2.6.1. OBJECTIVE 8
2.7. ADMINISTRATION OF THE DATABASE 8
2.7.1. OBJECTIVE 8
CONCLUSIONS AND RECOMMENDATIONS 9
3. CONCLUSIONS 9
3.1. RECOMMENDATIONS 9

OBJECTIVES

1. General Purpose

• Conduct a study and definition of information security planning, the importance of resources to solve new problems that arise within the institution, in relation to security and specify the responsibilities of implementing corrective measures or sanctions.

• Conduct an audit Informatics in Savings and Credit Cooperative "Atuntaqui" Ltd. to establish critical points, develop security policies and contingency solutions.

INTRODUCTION

2. INTRODUCTION

The institution is increasingly dependent on its information systems and services, therefore we can say they are increasingly vulnerable to threats regarding their safety.

The information should be considered a mission critical application that tells the institution and therefore has considerable value for it, like the rest of the assets, should be appropriately protected.

The Information Security protects this from a wide range of threats, both random order and destruction, fire or flooding, or deliberate order, such as fraud, espionage, sabotage, vandalism, etc.

With Security Policies were implemented can get rules and procedures documented and communicated, which aim to minimize IT risk more likely to involve the use of tools, and task performance by those involved in safeguarding the information, operation in order to recover at least a period of time appropriate to the mission of the affected system, emergency risks generated by computer.

Computer security policies set out the mechanisms and procedures to be adopted by enterprises to safeguard their systems and information they contain. These policies should be designed "to measure" in order to collect the characteristics of each organization. They are not a technical description of security mechanisms, not a legal term that involves sanctions on behaviors of employees, are more a description of what and why you want to protect it, meaning they can be taken as a form of communication between users and managers.

CHAPTER I

1. COMPUTER AUDIT

It is important to define the terms of auditing, since it has been used primarily to refer to a review whose sole purpose is to detect errors, fraud, identify shortcomings and recommend following the dismissal or removal of staff, however, the audit is a much broader concept that defines it as "The systematic process to evaluate and objectively obtain evidence related to economic activity reports and other related events." The end of the process is to determine the degree of overlap of information content with the evidence that gave rise, and to determine whether these reports were prepared to observe the principles established for the case. "

1.1. Importance of Computer Audit

Computer Audit is important in organizations for the following reasons:

- ✓ It can spread and use results or misleading information if the quality of input data is inaccurate or the same are handled, which opens the possibility of causing a domino effect and seriously affect the operations, decision making and Image Company.

- ✓ The computers, servers and data processing centers have become tempting targets for fraud, espionage, computer crime and terrorism.

- ✓ The continuity of operations, administration and organization of the company should not rely on poorly designed systems, since they can become a serious threat to the company.

- ✓ The databases may be prone to attacks and access by unauthorized users or intruders.

- ✓ In the Systems Department observed a disproportionate increase in costs, investments by unreasonable or significant overspending.

- ✓ Risk Level Assessment in regard to logical security, physical security and confidentiality.

CHAPTER II

2. IT SECURITY AUDIT

2.1. Introduction

The audit of computer security covers the concepts of physical and logical security. Physical security refers to protection of the hardware and data carriers as well as the safety of buildings and facilities that house them. The computer auditor should consider situations from fire, flood, sabotage, theft, natural disasters, etc.

2.2. GENERAL PURPOSE

Conducting an Audit Information on Savings and Credit Cooperative "Atuntaqui" Ltd. to survey the existing vulnerabilities in terms of security controls as a means of developing a Security Policy, which will define the guidelines to promote the implementation of a security model across the organization.

2.3. LOGICAL SECURITY

2.3.1. OBJECTIVE

Evaluate controls user access to computer processing platforms and data that they manage, in order to identify irregularities that impede the confidentiality, accuracy and availability of information, and improvements were made feasible.

2.4. COMMUNICATIONS SECURITY

2.4.1. OBJECTIVE

Should assess the security of communications, transmitted data, the devices used during transmission, the documentation required for the efficient and uninterrupted this transmission, and systems used to transmit data from one environment to another, checking compliance of information security.

2.5. SECURITY APPLICATIONS

2.5.1. OBJECTIVE

To evaluate the safety of the applications used in the institution, the consistency of input data and the accuracy of its output data, the integrity of databases and the existence and use of the documentation necessary for its operation, according to the proposed standards.

2.6. PHYSICAL SECURITY

2.6.1. OBJECTIVE

Evaluate the data center, equipment, devices, storage media and people that make the computer system of the Company to comply with the necessary measures with regard to physical infrastructure and the maintenance of security resources the organization.

2.7. ADMINISTRATION OF THE DATABASE

2.7.1. OBJECTIVE

Assess the proper organization and administration of the area of systems (Data Processing Center) and the allocation of tasks and responsibilities of the forms, so that it provides optimal operating conditions that allow an appropriate environment and Control to improve the availability of their services, according to existing rules governing this activity.

CHAPTER III

CONCLUSIONS AND RECOMMENDATIONS

3. CONCLUSIONS

• The security manager of data centers must ensure that the information and assets of the institution are confidential, honest and available to all users.

• We are aware that there is a security scheme to cover fully the potential risks, however you should be prepared and ready to react quickly because the threats and vulnerabilities are constantly changing.

• Have a security policy is important, but we understand that policy making safety a part of daily work environment is essential. Communication with users of the system is key to making this policy effective and generate a "safety culture" among users of the information of the institution.

3.1. RECOMMENDATIONS

• Knowing the strategic role that infrastructure holds the T / SI across all business areas within the institutions, allowing the exchange and processing of information, they need to be investigated, evaluated, and are subsequently released into Each organization that wishes to achieve productivity improvements and competitive.

• The institution must be able to meet its own model of management of technological innovation, based on their needs related to their sector and size, but above all, with its own strategy and vision.

• To bring innovation as a competitive weapon and an engine of growth of the institution, it is important to build the strategic capacity of its technological resources strengthening the leadership of the Head of Systems. The effort to define

the strategy of technological innovation is especially necessary to strengthen the focus on technologies of medium and long term planning of new products and processes and to frame the development needs that have arisen.

• To correct creations Security Policy have used some tools that are expensive to what has been done to compare cost / benefit for the institution and have made it much-needed investment in which we can say that the benefit is high for the cost that has been acquired.