

UNIVERSIDAD POLITECNICA DE HONDURAS

SEDE DANLÍ

CARRERA DE: INGENIERIA EN SISTEMAS COMPUTACIONALES



**Como Mejorar La Seguridad Informática en Clasificadora y
Exportadora de Tabaco S.A.**

Grupo Plasencia

Danli, El Paraíso

FRANCISCO JAVIER GUZMAN LAGOS

Número de Cuenta: 0409010055

PREVIO OPCIÓN AL TITULO DE:

INGENIERO EN SISTEMAS COMPUTACIONALES

Contenido

DEDICATORIA.....	1
AGRADECIMIENTOS.....	2
INTRODUCCIÓN.....	3
Breve Descripción.....	4
JUSTIFICACIÓN	5
Planteamiento del Problema.....	6
Hipótesis General	8
Objetivo General	8
Objetivos Específicos.....	8
DEMANDA	9
Formulando el Problema.....	9
Limitaciones y alcances de la investigación	10
Limitaciones de la investigación	10
Alcances de la investigación	10
Resumen Ejecutivo	11
I Generalidades de la empresa	12
Reseña histórica.....	13
Misión	16
Visión	16
Política de Calidad.....	16
Objetivos estratégicos	16
Organigramas.....	17
Estructura del departamento de informática.....	17
Estructuras Empresarial del Grupo Plasencia:	18
II	
Marco Teórico.....	19
La seguridad informática.....	20
2.2	
Los resultados del análisis de riesgos y políticas de seguridad.....	32
Los resultados que la empresa obtendría del análisis de riesgos.	33

Políticas de seguridad	33
Elaboración de la política.....	34
Acompañamiento de la política.....	34
Implantación de la política.....	34
Temas de la Política.....	35
Usos de la Política	35
2.3	
Acciones Hostiles.....	37
Acciones a tomar.....	38
2.4	
Seguridad lógica y controles de acceso.	40
Seguridad lógica	41
Control de acceso externo.....	42
2.5	
Delincuencia Informática	44
Delitos informáticos	45
Tipos de delitos informáticos.....	45
Delincuentes informáticos	46
Legislación en Honduras	47
Artículos del código penal de Honduras	47
DELITOS CONTRA LA LIBERTAD Y LA SEGURIDAD.....	47
DELITOS CONTRA LA PROPIEDAD	48
2.6	
Medidas de prevención	49
Repuesta a incidentes de seguridad.....	50
Contención de los efectos de un ataque.....	50
Funcionamiento: Estabilización, y desarrollo de medidas preventivas.....	51
Personal.....	51
Recomendaciones que la empresa puede tomar con sus empleados:	53
Comunicación	54

2.6

Ataques.....	55
Ataques posibles a la empresa.....	56
Ingeniería Social.....	56
Ingeniería Social Inversa.....	56
Trashing.....	57
Ataques de Monitorización que se pudieran dar en la empresa.....	57
Shoulder Surfing.....	57
Ataques de Autenticación.....	57
Spoofing – Looping.....	57
IP Slicing – Hijacking.....	57
Obtención de Password.....	58
Jamming o Flooding.....	58
Net Flood.....	58
E-Mail Bombing – Spamming.....	58
Ataques de modificación – daño.....	59
Tampering o Data diddling.....	59
¿Cómo defenderse de estos y otros ataques?.....	59
Creación y difusión de virus.....	60
Técnicas de propagación de virus.....	60
Algunos Tipos de virus.....	61
Archivos ejecutables.....	61
Virus en el sector de arranque (virus anterior a la carga del sistema operativo).....	61
Virus residente.....	61
Macro virus.....	62
Virus de Mail.....	62
Virus de sabotaje.....	62
Hoax los virus fantasmas.....	62
Reproductores gusanos.....	62
Caballos de Troya.....	62
Bombas lógicas.....	63

Tipos de daños ocasionados por los virus.....	63
Programa Antivirus	64
2.8	
Administración de seguridad para la empresa.....	65
Administración de la seguridad en la empresa.....	66
Firewalls	67
Gestión de claves seguras	67
Normas para que la empresa pueda proteger una clave.....	68
III	
Entrevistas.....	70
Entrevista con Manuel Antonio Rodríguez (Jefe del departamento de Informática).....	71
Entrevista con Ibrahim Salmerón (Gerente Administrativo de Clasificadora y Exportadora de Tabaco S.A.)	74
IV	
Conclusiones Generales.....	75
V	
Recomendaciones.....	77
Políticas de seguridad	78
Identificación de una amenaza.....	79
Evaluación de costos.....	80
Los costos derivados	81
Puntos de equilibrio.....	81
Estrategia de seguridad.....	81
Implementación de las políticas de seguridad.....	82
Auditoría y control	84
Plan de contingencia.....	84
Equipos de respuesta a incidentes.....	85
BACKUPS.....	85
Consejos de la Guía de Seguridad para el resguardo de información (ESET)	86
Pruebas.....	87
Nivel Físico.....	87

Amenaza no intencionada (desastre natural)	88
Nivel Humano.....	88
Mejoramiento de información en fincas	90
Certificar la empresa	90
ISO 27001 Sistemas de Gestión de Seguridad en la Información	90
ISO/IEC 27001	91
Beneficios	91
Implantación	92
Certificación	92
Pasos como la empresa puede ser certificada por ISO 27,000.....	93
Implantación del SGSI	93
Auditoría y certificación.....	95
La entidad de certificación	97
VI	
Recomendaciones en resumen.....	98
VII	
Marco Metodológico y referencial.....	102
Marco Metodológico.....	103
Tipo De Investigación.....	103
Diseño de la investigación.....	103
Marco Referencial	103
VIII	
Análisis, Técnicas e información de la investigación.....	108
Análisis de la demanda de la investigación.....	109
Población y Muestra.....	109
Grafico de empleados por sucursales.....	110
Presupuesto Asignado de TI a la seguridad Informática.....	110
Técnicas e Instrumentos de recolección de datos:.....	111
IX	
Anexos.....	112

POLITICAS Y PROCEDIMIENTOS TECNOLOGIA DE LA INFORMACION	
GRUPO PLASENCIA TABACOS	113
Bibliografía.....	128

DEDICATORIA

Grande es la sabiduría y el entendimiento de tantas cosas, por lo que dedico este trabajo a quien me ha dado todo eso, en primer lugar a Dios.

A toda mi familia que me han apoyado incondicionalmente y siempre han estado a mi lado en toda esta etapa estudiantil. Pero sobre todo al esfuerzo de dos personas que creyeron en mí y pusieron todas sus esperanzas en mí, que me inspiraron a alcanzar metas con esfuerzo y trabajo, y me han motivado a mirar alto, dedico este esfuerzo a quienes me dieron la vida, y que han hecho de mi una mejor persona. Lo dedico a mis padres.

Lo dedico a mis catedráticos que me dieron sus conocimientos para ser de mí una mejor persona y aportar como profesional al desarrollo de esta gran nación.

Dedico este trabajo por último, pero no menos importante a la Universidad Politécnica de Honduras (Sede Danlí).

AGRADECIMIENTOS

Agradezco a DIOS por la vida que poseo, porque se me ha permitido vivirla y llegar hasta este momento tan importante en mi vida y en la de mi familia.

Agradezco a mi familia y a mis padres por la oportunidad que me dieron para llegar a ser un profesional.

Agradezco a todas personas que de cualquier forma contribuyeron a ser de mí una mejor persona.

A mis compañeros de la carrera de Ingeniería en Sistemas Computacionales, a todos mis catedráticos, a la Universidad Politécnica que sin ellos esto no sería realidad, también a la empresa Clasificadora y Exportadora de Tabaco S.A y todas las empresas del Grupo Plasencia, sus empleados, la Gerencia y al señor Manuel Antonio Rodríguez por facilitarme toda la información necesaria para realizar este documento.

Y finalmente y no menos importante a las dos asesoras de este trabajo, La Lic. Eva Ávila y a mi asesora temática Ing. Sandra Gradiz que me ayudaron y asesoraron durante estos meses para contribuir en este trabajo y poder culminar de buena forma mi carrera de pre-grado.

Gracias a Todos

INTRODUCCIÓN

Con el propósito de mejorar la seguridad de la información en las empresas me he decidido por este tema para mi tesis basándome en los conocimientos adquiridos en la clase seguridad de la información incluida dentro del plan de estudios de la universidad y aplicándola enfocándome en Clasificadora y Exportadora de Tabaco S.A de C.V empresa en la cual realice mi práctica profesional.

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). 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.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

En otras palabras la información de una empresa se considera lo más importante de una empresa. Este documento será basado en una forma de que la empresa pueda crecer en el tema de seguridad y que esto ayude a la empresa bajo las normas ISO 20,000 o 27,000. Durante los meses de Enero a Abril se estuvo investigando, recopilando y procesando información para poder mediante este documento aportar conclusiones y recomendaciones que orienten a la empresa en el tema de la seguridad informática. Sabiendo que un sistema, una red, una computadora o unas instalaciones nunca serán totalmente seguras ya que se han robado información de sistemas súper seguros como el del Departamento de Defensa de EE.UU, pero la empresa puede llegar a tener un nivel de seguridad informática aceptable.

Gracias por visitar este Libro Electrónico

Puedes leer la versión completa de este libro electrónico en diferentes formatos:

- HTML(Gratis / Disponible a todos los usuarios)
- PDF / TXT(Disponible a miembros V.I.P. Los miembros con una membresía básica pueden acceder hasta 5 libros electrónicos en formato PDF/TXT durante el mes.)
- Epub y Mobipocket (Exclusivos para miembros V.I.P.)

Para descargar este libro completo, tan solo seleccione el formato deseado, abajo:

