ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADO A LOS ACTIVOS DE LA EMPRESA CONSTRUCTORA COETECORPZA SA, BASADOS EN EL ESTÁNDAR ISO 27002."

TRABAJO DE TITULACIÓN

Previa la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Rolando Manuel Huayamave Torres

GUAYAQUIL – ECUADOR

AÑO

2017

AGRADECIMIENTO

Un agradecimiento muy especial a Dios por concederme salud, a mis padres y hermanos por formar parte de mi vida y ayudarme siempre en mi desarrollo tanto profesional como personal.

A mi esposa y a mis hijos por ser el motor principal y mi motivo de superación.

Rolando M Huayamave Torres

DEDICATORIA

Dedico este trabajo a Dios en primer lugar por todas sus bendiciones y darme salud para poder estudiar y trabajar.

A mi familia, a mis padres, hermanos, primos y en especial a mi esposa Valkiria por su apoyo incondicional y a mis hijos Saúl y Emma por darme fuerzas para seguir luchando por ellos.

A mis amigos por su total apoyo.

Rolando M Huayamave Torres

TRIBUNAL DE SUSTENTACIÓN

_____

DIRECTOR MSIA

MGS. LENÍN FREIRE COBO

_____

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MGS. LENÍN FREIRE COBO

_____

MIEMBRO DEL TRIBUNAL

MGS. OMAR MALDONADO DAÑIN

DECLARACIÓN EXPRESA

“Declaro de forma expresa que la responsabilidad del contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

_____

Rolando Manuel Huayamave Torres

RESUMEN

Para un correcto manejo de la seguridad de la información se necesita implementar un sistema de gestión de seguridad de la información (SGSI) aplicado al dominio de activos, un sistema con objetivos claros de seguridad y gestión de riesgos a los que está inmersa dicha organización. Con esto logramos identificar los riesgos y determinar las vulnerabilidades.

Para tal objetivo utilizaremos las normas internacionales ISO 27002, se elaborarán políticas de seguridad informática en base a la norma 27002 para beneficiar a la empresa COETECORPZA SA a la cual se proporcionará mejores prácticas de seguridad de la información y gestión de riesgos.

Se documentará el plan de tratamiento de riesgos con las acciones recomendadas a seguir y sus responsables. Se implementará el Sistema de gestión de Seguridad Informática y se entregará el manual de procedimientos.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE TABLAS

INTRODUCCIÓN

En tiempos actuales la información ocupa un papel principal en las organizaciones y brinda ayuda en el posicionamiento de la misma, el salvaguardar dicha información y los sistemas que la gestionan es tarea principal de las organizaciones, por lo tanto, se han adaptado estándares para proteger y mantener segura la información.

La organización debe conocer sus activos más importantes y a los cuales enfocar su mayor esfuerzo con la finalidad de salvaguardar dichos activos, definir políticas procedimientos y dar a conocer a su personal esta información.

El siguiente proyecto de titulación tiene como base la norma ISO 27002:2013 controles de Seguridad, estándar internacional aplicable a cualquier tipo de empresa para nuestro caso de estudio está dirigido a una empresa constructora.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

La empresa COETECORPZA SA radicada en la ciudad de Guayaquil desde el año 2008 se encarga de fiscalización y presupuesto de obras. Cuenta con una oficina en la ciudadela Kennedy en el norte de la ciudad de Guayaquil.

La infraestructura de la empresa consta de un servidor alojado en la oficina del gerente general y ocho computadoras de escritorio, una bodega donde guardan todas las herramientas necesarias para la

ejecución de su trabajo, un departamento de presupuesto para la elaboración de los mismos.

Para la comunicación interna cuentan con un modem de un proveedor local conectado a un Router WI-FI el cual es administrador por personal de la empresa, un Ingeniero de sistemas encargado de la parte tecnológica de la empresa.

Referente a las aplicaciones la empresa COETECORPZA SA cuenta con un sistema de presupuesto de obra SAO-Presupuesto que forma parte del ERP SAO.

Dicha aplicación cuenta con seguridad a nivel de acceso y un usuario asignado con diferentes roles y perfiles dependiendo de la actividad de cada trabajador.

La empresa no cuenta con seguridad física, cámaras de seguridad, alarmas contra incendios, control biométrico para sus empleados. La única seguridad es una puerta de vidrio con llave.

1.2 Descripción del problema

En la actualidad la empresa constructora COETECORPZA SA no cuenta con un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) alguno que incluya políticas de seguridad y procedimientos que definan controles de seguridad con respecto a los accesos y el correcto uso de recursos informáticos.

Con el crecimiento de la empresa y el número de empleados aumenta el riesgo en la seguridad de los activos de información de la empresa constructora COETECORPZA SA. En el periodo de actividad de la empresa constructora se han presentado inconvenientes con respecto a la seguridad, tales como, accesos no autorizados a los sistemas, robo de información, hurto de herramientas y equipos, daño en los servidores de la empresa por fallas ambientales en el centro de cómputo.

Por ejemplo, en las instalaciones donde quedan ubicadas las oficinas de la empresa constructora COETECORPZA SA no tenían ningún control de acceso y un día cualquiera, en la hora del almuerzo nadie se percató que alguien había entrado y sustraído una laptop del departamento financiero con la información contable del negocio y como consecuencias los pagos a los trabajadores demoraron más de 7

días en poder ser efectivos. La pérdida de información y la no política de respaldos ocasionaron a las constructoras inconvenientes con los trabajadores.

Otro caso que podemos mencionar es el daño del servidor principal a causa de unas goteras en la oficina a lo cual no tenían un plan de contingencia y menos de prevención de este tipo de sucesos. El daño del servidor fue total y se tuvo que comprar otro servidor, pero aún no se crean las políticas sobre el cuidado de los equipos informáticos.

La falta de políticas de seguridad incrementa la posibilidad o el riesgo de que se presenten eventos como perdida de equipos, perdida de información o no tener disponible la información cuando se la requiera, trayendo consecuencias negativas para la empresa constructora COETECORPZA SA como por ejemplo una mala imagen ante sus clientes y proveedores ya que la falta de información o información errona dificulta sus relaciones de negocios.

1.3 Solución propuesta

Desarrollar un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) en el que se incluya:

Procedimientos que ayuden a mejorar la relación entre los recursos tecnológicos y humanos, basados en estándar ISO 27002(El estándar ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información).

Definir política de seguridad informática tomando como base los procedimientos antes mencionados.

Aplicar controles de los siguientes dominios del estándar ISO 27002:2013.

- ✓ Gestión de activos.
- ✓ Seguridad física y Ambiental.
- ✓ Aspectos de la SI en la Gestión de la Continuidad de Negocio.

A través de identificación, análisis y tratamiento de riesgos, analizar vulnerabilidades de los activos tecnológicos. Este SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) servirá como base para la implementación de futuros controles de seguridad de la información y ayuda a preservar la confidencialidad, integridad y disponibilidad de la información.

Dentro de los beneficios que nuestra propuesta otorgaría están:

- ✓ Acceso solo a personal autorizado a los sistemas informáticos.
- ✓ Información de las bases de datos integra.
- ✓ Respaldos de información.
- ✓ Mantenimientos preventivos de equipos.
- ✓ Información siempre disponible para cuando los usuarios la requieran.

1.4 Objetivo general

Implementar un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) aplicado a la empresa constructora COETECORPZA SA basado en el estándar ISO 27002.

1.5 Objetivos específicos

1. Identificar y Valorizar los activos de información y la infraestructura tecnológica de la constructora COETECORPZA SA.
2. Analizar y Evaluar los riesgos y así evitar la materialización de las amenazas de la Empresa Constructora COETECORPZA SA.
3. Seleccionar los Controles para el Tratamiento de Riesgos.

4. Desarrollar la Política de Seguridad de la Empresa Constructora COETECORPZA SA.
5. Dar a conocer las políticas para el buen uso de los sistemas de información por parte de los trabajadores de la constructora COETECORPZA SA.

1.6 Alcance

Nuestra propuesta tiene como alcance la protección de los activos de la empresa COETECORPZA SA. En todos aquellos equipos que almacenan la información del negocio y garantizando el correcto uso de los equipos que accedan a dicha información, otorgándoles a estos activos un usuario responsable.

1.7 Metodología

La norma ISO/IEC 27002 proporciona los controles de seguridad, pueden ser aplicados a cualquier tipo de empresa u organización e indistinto de su tipo o naturaleza.

Para garantizar de la seguridad de la información se gestiona correctamente se debe identificar su ciclo de vida.

La norma cuenta con un proceso principal el cual está formado por etapas del ciclo PHVA (Planear, Hacer, Verificar, Actuar). El alcance de este proyecto son las dos primeras etapas de este ciclo.

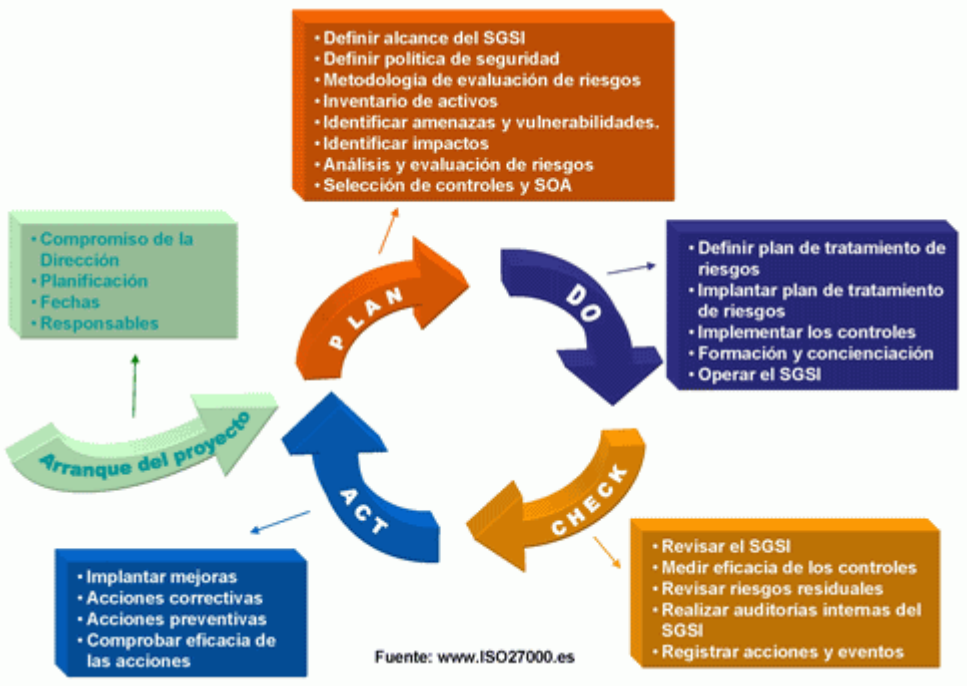

Figura 1.1: Ciclo Deming
Fuente: Www.Iso27000.Es

Planear:

- ✓ Alcance.
- ✓ Política.
- ✓ Metodología de evaluación de riesgos.
- ✓ Inventario de activos.
- ✓ Identificar amenazas y vulnerabilidades.
- ✓ Identificar impacto.
- ✓ Análisis y evaluación de riesgos.
- ✓ Selección de controles y SOA.

Hacer:

- ✓ Definir plan de tratamiento de riesgos.
- ✓ Implementar plan de tratamiento de riesgos.
- ✓ Implementar los controles.
- ✓ Formación y concienciación.
- ✓ Operar el SGSI.

Las metodologías de este proyecto están divididas en etapas enlazadas para garantizar el avance del proyecto.

Bajo esta primicia la metodología que se aplicará estará basada en los siguientes puntos:

1. Análisis y Evaluación de Riesgos.
2. MAGERIT para valorar Riesgos.
3. Norma ISO/IEC 27002 para verificar controles.
4. Análisis de amenazas y vulnerabilidades.
5. Valoración de Riesgos:
    - ✓ Probabilidad de ocurrencia.
    - ✓ Valoración de impacto.
6. Tratamiento de Riesgos, según la norma ISO/IEC 27002.
7. Política y procedimientos organizacionales.
8. Dar a conocer las políticas y normas implementadas.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad de la Información

La seguridad de la información tiene como objetivo principal salvaguardar la información, para esto debe cumplir tres principios básicos dentro del manejo y acceso a la información.

La seguridad de los sistemas de información es una disciplina en continua evolución. La meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión,

implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las TIC de la organización, a sus socios comerciales, clientes, administración Pública, suministradores, etc. [1]

Confidencialidad. - Asegurar que las personas que tengan acceso estén autorizadas, hoy en día la información se ha convertido en el activo más valioso dentro de las organizaciones.

Integridad. - Asegurar que la información sea integra y real o verdadera, esto incluye sus métodos.

Disponibilidad. – Asegurar que la información esté disponible para los usuarios autorizados cuando estos la requieran.
Dentro de los activos tenemos: correos electrónicos, website, imágenes, bases de datos, telecomunicaciones.

La Seguridad de la Información a través de un Sistema de Gestión de Seguridad de la información (SGSI) también protege a la organización contra amenazas que se presentan en su entorno y daños ocasionados por agentes externos o internos.

Para lograr proteger a los mencionados activos se implementan políticas, se aplican controles, se crean procesos y procedimientos organizacionales y desarrollan aplicaciones de software.

Figura 2.2: Seguridad de la Información
Fuente: www.grupsertec.com

2.2 Sistema de Gestión de Seguridad de la información (SGSI)

El Sistemas de Gestión de Seguridad de la información (SGSI) consisten en una serie de actividades de gestión las cuales deben realizarse mediante procesos sistemáticos como, por ejemplo, crear documentación de respaldo y comunicar a todos los miembros de la organización, con la finalidad de proteger a la empresa de ataques o perdidas de información. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y

disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. [2]

Como parte fundamental para garantizar que la seguridad refiriéndose a seguridad de la información se gestiona o es gestionada eficientemente y correctamente se debe primero identificar su ciclo de vida y con esto dar seguridad a que la confidencialidad, integridad y disponibilidad se cumplan.

El manejo de información delicada o sensible llega a ser parte fundamental dentro del negocio ya que ayuda a la empresa a posicionarse y consolidarse dentro del mercado. Con esto, la información, sus procesos y los sistemas que interactúan con esta se consideran activos muy valiosos dentro de la organización.

Dentro de los posibles beneficios que otorga el Sistema de Gestión de Seguridad de la información se nombran los siguientes:

- ✓ Metodología estructurada.
- ✓ Revisión y Mejoras en la Gestión de riesgo.
- ✓ Dar acceso autorizado a la información acorde a los perfiles de usuario.

- ✓ Ganar aceptación en términos de confianza por parte de clientes y proveedores.
- ✓ Plan de continuidad del negocio.

Figura 2.3: SGSI
Fuente: Normas-Iso.Com/Iso-27001

2.3 Norma ISO/IEC 27000

ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) desarrollaron una norma que brindan un escenario de gestión de la seguridad de la información, el mismo que puede ser implementado en cualquier organización o empresa ya sea esta de tipo publica privada e indistinto del tamaño y del tipo de empresa.

A esta normal la denominaron ISO/IEC 27000, esta norma proporciona una visión global de todas las series 27000 así como también el alcance de cada una de ellas y su objetivo principal.

Figura 2.4: ISO Serie 27000
Fuente: Es.Slideshare.Net/Calderonperaza/Introduccion-Iso-27001-Sgsi

2.4 Norma ISO/IEC 27001

La última versión de esta norma fue publicada en el año 2013. Es la norma principal de toda la serie ya que incluye todos los requisitos del Sistema de Gestión de Seguridad de la Información en las organizaciones. La ISO 27001 sustituye a la BS 7799-2 estableciendo unas condiciones de adaptación para aquellas empresas que se encuentren certificadas bajo esta última. En el Anexo A se enumeran los objetivos de control y los análisis que desarrolla la norma ISO27001 para que se puedan seleccionar las empresas durante el progreso de sus Sistemas de Gestión de Seguridad de la Información. La empresa podrá argumentar el hecho de no aplicar los controles que no se encuentren implementados ya que no es obligatorio. [3]

ISO 27001 forma parte de la serie 27000 y es una de las normas más vitales ya que contiene los requisitos del Sistema de Gestión de Seguridad de la Información y sirve como norma de certificación para las organizaciones ya que pueden contratar a empresas o entidades acreditadas para que realicen una auditoria a través de sus auditores externos y con un resultado positivo obtener la certificación.

El objetivo principal de esta norma es proteger la información de la organización y garantizar la confidencialidad, integridad y disponibilidad de los datos.

Figura 2.5: ISO 27001
Fuente: Ukaccreditation.Co.Uk/Iso-27001-2013.Php

2.5 Norma ISO/IEC 27002:2013

ISO/IEC 27002 otorga las mejores prácticas a todos los responsables de empezar, implementar y mantener los Sistemas de gestión de la seguridad de la información (SGSI).

La versión ISO/IEC 27002:2013 cuenta con 35 objetivos de control y 114 controles agrupados en 14 dominios. Dicha norma establece directrices generales para la gestión de la seguridad de la información dentro de una organización.

Los objetivos de control y los controles de la norma ISO 27002:2013 cumplen su objetivo principal que es el de satisfacer los requisitos identificados en la evaluación de riesgos a través de su implementación.

En base a la norma ISO 27002, se comprobara que controles de dicha norma están implantados y a qué nivel en base a un checklist. Con esto, se consigue determinar el estado de madurez en el que se encuentra la compañía, para poder identificar el esfuerzo que hay que hacer en la implementación. [4]

Esta norma no es certificable por ser un conjunto de buenas prácticas y no presentan requisitos específicos que permitan a las empresas poder certificarse.

Figura 2.6: ISO 27002
Fuente*:* Linkedin.Com/Topic/Iso%2Fiec-27002

2.6 Gestión de Riesgo

Tiene como finalidad garantizar la seguridad de los datos, aplicar políticas previamente definidas de acceso en niveles de autorización de acceso e identificar las amenazas que se presenten, vulnerabilidades y riesgos informáticos.

Una buena organización de TI es capaz de identificar la eminente materialización de un riesgo, algo que está por suceder que impactará negativamente las operaciones normales, ejecutar acciones que eliminen o mitiguen la materialización del riesgo y luego eliminen la causa raíz por la cual se incrementó el riesgo operativo de la organización. [5]

La gestión de riesgo informático es en si la probabilidad de ocurrencia de algún incidente que causen algún fallo en los sistemas informáticos y evite cumplir con los objetivos de la organización. Con esto se obtienen perdidas económicas y daño muchas veces irreversibles.

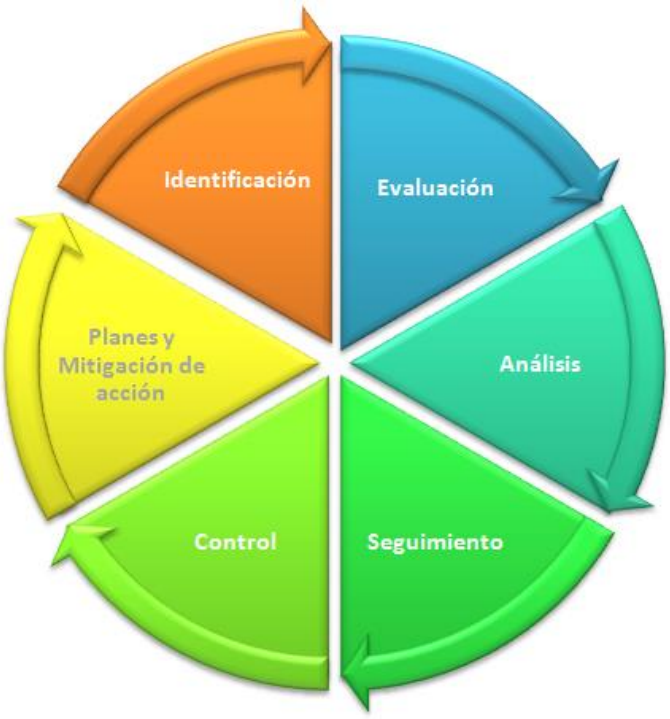

Figura 2.7: Fases Del Tratamiento De Riesgo
FUENTE: BIMPROVEMENT.COM/GESTION-DE-RIESGOS.HTML

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACION

3.1 Identificación de la infraestructura de la empresa

La empresa COETECORPZA SA comenzó sus operaciones en Ecuador en esta última década, siendo su principal actividad todo lo referente al mundo de la construcción tanto para empresas como para público en general.

Al ser una constructora cuenta con personal administrativo y técnico para la realización de las obras que realizan.

Dentro de su infraestructura, encontramos servidores de aplicación y base de datos, así como equipos y maquinaria para la construcción. Dentro de la información que maneja la empresa constructora COETECORPZA SA podemos mencionar que almacena información sensible de sus clientes y trabajadores como por ejemplo contratos, presupuestos, planos, pagos de nómina, etc.

3.2 Identificación y valoración de activos de información

Al momento de identificar los activos de la empresa se utilizaron los datos del último inventario realizado hace menos de 2 semanas a la fecha de este documento.

Los activos de la empresa COETECORPZA SA son:

COETECORPZA SA.					
#	ID-ACTIVO	DESCRIPCION - ACTIVO	USUARIO	CARGO	AREA/DEPARTAMENTO
1	COEGYE1	LAPTOP SONY	PAOLA UQUILLAS	PRESIDENTE	PRESIDENCIA
2	COEGYE2	LAPTOP SONY	NILTON HUAYAMAVE	GERENTE	GERENCIA GENERAL
3	COEGYE3	LAPTOP SONY	SILVIA SALTOS	GERENTE FINANCIERO	FINANCIERO
4	COEGYE4	PC-DESKTOP	MARJORIE CARDENAS	ASISTENTE	FINANCIERO
5	COEGYE5	PC-DESKTOP	ERICKA VILLAMAR	SECRETARIA	GERENCIA GENERAL
6	COEGYE6	LAPTOP SONY	WILLIAN BANCHON	GERENTE TECNOLOGIA	SISTEMAS
7	COEGYE7	PC-DESKTOP	DALTON HERNANDEZ	INFRAESTRUCTURA	SISTEMAS
8	COEGYE8	PC-DESKTOP	LUIS MERA	SOPORTE TECNICO	SISTEMAS
9	COEGYE9	PC-DESKTOP	GALO AVECILLAS	ARQUITECTO/ANALISTA	PRESUPUESTO
10	COEGYE10	PC-DESKTOP	DAVID RODRIGUEZ	ARQUITECTO/ANALISTA	PRESUPUESTO
11	COEGYE11	PC-DESKTOP	DANIELA MONTAÑO	ARQUITECTO/ANALISTA	PRESUPUESTO
12	COEGYE12	SAO PRESUPUESTO	TODOS	SISTEMA SAO	-
13	COEGYE13	SAO TALENTO HUMANO	TODOS	SISTEMA SAO	-
14	COEGYE14	SAO FIN	TODOS	SISTEMA SAO	-
15	COEGYE15	LEXMARK T656	TODOS	IMPRESORA	SISTEMAS
16	COEGYE16	LEXMARK T656	TODOS	IMPRESORA	PRESUPUESTO
17	COEGYE17	LEXMARK T656	TODOS	IMPRESORA	PRESIDENCIA
18	COEGYE18	EPSON	TODOS	PROYECTOR	PRESIDENCIA
19	COEGYE19	SERVID0R	TODOS	ACTIVE DIRECTORY	SISTEMAS
20	COEGYE20	SERVIDOR	TODOS	EXCHANGE	SISTEMAS
21	COEGYE21	SERVIDOR	TODOS	SQL SERVER	SISTEMAS

Tabla 1: ACTIVOS COETECORPZA S.A
FUENTE: AUTOR

3.2.1 Tipos de Activos

La clasificación de activos se realizó agrupando dichos activos según las tareas que realizan.

CLASIFICACION	
1	LAPTOP SONY
2	PC-DESKTOP
3	SISTEMA SAO
4	IMPRESORA
5	SERVID0R
6	PROYECTOR

Tabla 2: Clasificación De Activos
FUENTE: AUTOR

3.2.2 Dimensión De Valoración Y Tabla De Valores

Se considera dimensión de valoración a las características propias de un activo con la cual se le asigna un valor a dicho activo.

Se utiliza para darle valor a las consecuencias de una amenaza.

- ✓ Disponibilidad (D) .- Poder utilizar los equipos cuando sea necesario.
- ✓ Integridad (I) .- Garantizar la integridad de los activos.

- ✓ Confidencialidad (C) .- Solo disponible a las personas autorizadas.

Escala de valores. –

ESCALA DE VALORES		
VALOR		CRITERIO
5	MUY ALTO	AFECTACION MUY ALTA A LA EMPRESA
4	ALTO	AFECTACION ALTA A LA EMPRESA
3	MEDIO	AFECTACION MEDIA A LA EMPRESA
2	BAJO	AFECTACION BAJA A LA EMPRESA
1	NULO	LA EMPRESA NO SUFRE AFECTACION

Tabla 3: Escala De Valores
Fuente: Autor

Criterios de valor. -

CRITERIOS DE VALOR		
VALOR	CRITERIO	
5	DO	DAÑO EN LA OPERACIÓN DEL NEGOCIO
	DSE	DAÑO EN LOS SISTEMAS DE LA EMPRESA (SOFTWARE)
	DI	DAÑO EN LA INFORMACION ALMACENADA EN LAS BASES DE DATOS
4	DS	DAÑO EN UN SECTOR/AREA ESPECIFICAMENTE
	FCR	FALLA EN CUMPLIR UN REGLAMENTO DE LEY
	FAP	FALLA EN LA ATENCION AL PUBLICO
3	ON	EN OCACIONES AFECTA LA OPERATIVA DEL NEGOCIO
	IMC	IMPACTO MEDIO EN LAS COMUNICACIONES
2	PTI	PROBLEMAS EN EL TRABAJO DE UN INDIVIDUO
	IMO	IMPACTO MINIMO EN LA OPERACION DE LA EMPRESA
1	NOA	NO AFECTA LA SEGURIDAD DE LOS DATOS

Tabla 4: Criterios De Valor
FUENTE: AUTOR

VALORACION DE ACTIVOS. –

ID-ACTIVO	DESCRIPCION - ACTIVO	USUARIO	Disponibilidad		Integridad		Confidencialidad		VALOR TOTAL
			valor	criterio	valor	criterio	valor	criterio	
COEGYE1	LAPTOP SONY	PAOLA UQUILLAS	2	PTI	3	ON	2	PTI	2,33
COEGYE2	LAPTOP SONY	NILTON HUAYAMAVE	3	ON	3	IMC	2	PTI	2,67
COEGYE3	LAPTOP SONY	SILVIA SALTOS	4	FAP	4	DS	3	ON	3,67
COEGYE4	PC-DESKTOP	MARJORIE CARDENAS	2	PTI	4	FAP	3	ON	3,00
COEGYE5	PC-DESKTOP	ERICKA VILLAMAR	2	PTI	4	FAP	3	ON	3,00
COEGYE6	LAPTOP SONY	WILLIAN BANCHON	4	DS	3	ON	4	FCR	3,67
COEGYE7	PC-DESKTOP	DALTON HERNANDEZ	4	DS	3	ON	4	FCR	3,67
COEGYE8	PC-DESKTOP	LUIS MERA	2	PTI	3	ON	2	PTI	2,33
COEGYE9	PC-DESKTOP	GALO AVECILLAS	2	PTI	2	IMO	3	ON	2,33
COEGYE10	PC-DESKTOP	DAVID RODRIGUEZ	2	PTI	2	IMO	3	ON	2,33
COEGYE11	PC-DESKTOP	DANIELA MONTAÑO	2	PTI	2	IMO	3	ON	2,33
COEGYE12	SAO PRESUPUESTO	TODOS	5	DSE	5	DI	4	DS	4,67
COEGYE13	SAO TALENTO HUMANO	TODOS	5	DSE	5	DI	4	DS	4,67
COEGYE14	SAO FIN	TODOS	5	DSE	5	DI	4	DS	4,67
COEGYE15	LEXMARK T656	TODOS	2	IMO	1	NOA	1	NOA	1,33
COEGYE16	LEXMARK T656	TODOS	2	IMO	1	NOA	1	NOA	1,33
COEGYE17	LEXMARK T656	TODOS	2	IMO	1	NOA	1	NOA	1,33
COEGYE18	EPSON	TODOS	2	IMO	1	NOA	1	NOA	1,33
COEGYE19	SERVID0R	TODOS	5	DO	4	FAP	4	FAP	4,33
COEGYE20	SERVIDOR	TODOS	5	DO	4	DS	4	FCR	4,33
COEGYE21	SERVIDOR	TODOS	5	DO	5	DI	4	FCR	4,67

Tabla 5: Valoración De Activos
FUENTE: AUTOR

3.3 Identificación de Amenazas y Vulnerabilidades

Vulnerabilidad. - Se considera a la exposición directa a un riesgo dentro del área de sistemas o TI, con los avances tecnológicos la exposición a los riesgos aumenta y cada vez se invierte más en tratar de prevenir o mitigar los riesgos debido a la inseguridad que sufren las conexiones entre los equipos.

Amenaza. - se considera amenaza a un posible evento que se pudiera presentar u ocurrir.

Producto de atentar contra las partes de un sistema ya sea físico o digital esto como consecuencia atenta contra la integridad, disponibilidad, confidencialidad y autenticidad de la información.

Se debe crear acciones para mitigar las vulnerabilidades y amenazas por tal motivo se debe considerar el nivel de inversión acorde a la importancia

	AMENAZA		VULNERABILIDAD
ACTIVO	CODIGO	DESCRIPCION	DESCRIPCION
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC1	TERREMOTO	FALTA DE PROTECCION ANTISISMICA(PREVENCION)
	APC2	INCENDIO	FALLA EN LOS SISTEMAS CONTRA INCENDIOS
	APC3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS
	APC4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS
	APC5	TEMPERATURA	FALLA EN EL ACONDICIONAMIENTO ADECUADO DE TEMPERATURA(AC)
	APC6	ROBO	FALLA/FALTA DE CONTROL ANTIROBO
SERVID0R	AS1	TERREMOTO	FALTA DE PROTECCION ANTISISMICA(PREVENCION)
	AS2	INCENDIO	FALLA EN LOS SISTEMAS CONTRA INCENDIOS
	AS3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS
	AS4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS
	AS5	TEMPERATURA	FALLA EN EL ACONDICIONAMIENTO ADECUADO DE TEMPERATURA(AC)
	AS6	ROBO	FALLA/FALTA DE CONTROL ANTIROBO
	AS7	ATAQUE DENEGACION DE SERVICIO	FALLA DE SEFGURIDAD
	AS8	LENTITUD EN EL SISTEMA	FALTA DE RECURSOS (MEMORIA, PROCESADOR, DISCO DURO)
SOFTWARE ERP SAO	AERP1	ADMINISTRACION DEL SISTEMA	FALTA DE CAPACITACION AL ADMINISTRADOR DEL APLICATIVO
	AERP2	USUARIOS	FALTA DE CAPACITACION A LOS USUARIOS DE LOS DIFERENTES APLICATIVOS.
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	ERROR DE MONITOREO DEL APLICATIVO
	AERP4	INGRESO ERRONEO DE INFORMACION	FALTA DE CONOCIMIENTO DEL APLICATIVO
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	FALLAS EN LA ACTUALIZACION DEL SISTEMA

Tabla 6: Amenaza Y Vulnerabilidades
FUENTE: AUTOR

CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL SGSI

4.1 Análisis e identificación del impacto

Impacto. - se define impacto en relación a seguridad informática como todo hecho que se suscita, indistinto de si se pudo resolver o no y que el mismo provoca algún tipo de repercusión negativa sobre los activos de la empresa u organización.

A continuación, se detallan las consecuencias por impacto:

CONSECUENCIAS DEL IMPACTO	
CODIGO	DESCRIPCION
I1	PERDIDAS MATERIALES
I2	PERDIDAS ECONOMICAS
I3	RESPONSABILIDAD LEGAL
I4	DAÑO A PERSONAS
I5	INCUMPLE OBLIGACIONES FISCALES
I6	PERDIDA DE INFORMACION (ACTIVO)

Tabla 7: Consecuencias Del Impacto
FUENTE: AUTOR

Impacto por amenaza. - Se realiza cuadro del impacto y su afectación tomando en consideración el tipo de activo y la amenaza relacionada.

IMPACTO POR AMENAZA						
ACTIVO	CODIGO	DESCRIPCION	IMPACTO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIABILIDAD
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC1	TERREMOTO	I1, I2, I4	X		
	APC2	INCENDIO	I1, I2, I4	X		
	APC3	FALLA FISICA(HARDWARE)	I1, I2	X		
	APC4	FALLA ELECTRICA (SUMINISTRO)|	I1, I2	X		
	APC5	TEMPERATURA	I1, I2, I4	X		
	APC6	ROBO	I1, I2,I3, I4	X		X
SERVID0R	AS1	TERREMOTO	I1, I2, I4	X		
	AS2	INCENDIO	I1, I2, I4	X		
	AS3	FALLA FISICA(HARDWARE)	I1, I2	X		
	AS4	FALLA ELECTRICA (SUMINISTRO)|	I1, I2	X		
	AS5	TEMPERATURA	I1, I2, I4	X		
	AS6	ROBO	I1, I2,I3, I4	X		X
	AS7	ATAQUE DENEGACION DE SERVICIO	I6, I5, I4, I3, I2	X	X	X
	AS8	LENTITUD EN EL SISTEMA	I5, I6, I2	X		
SOFTWARE ERP SAO	AERP1	ADMINISTRACION DEL SISTEMA	I2, I3, I4	X	X	X
	AERP2	USUARIOS	I1, I2, I5, I6	X		
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	I1, I2	X		
	AERP4	INGRESO ERRONEO DE INFORMACION	I2, I4, I6		X	
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	I2, I5	X		

Tabla 8: Impacto Por Amenaza
FUENTE: AUTOR

4.2 Análisis y evaluación del Riesgo

El análisis y la evaluación de riesgos se encargan de identificar los riesgos a los que están expuestos los activos a través de un análisis completo entre vulnerabilidades, amenazas y el impacto a lo que están propensos los activos en su entorno dentro de la organización o empresa.

Para encontrar medidas preventivas se debe identificar los riesgos en todos los activos de la empresa y determinar una evaluación de dichos riesgos en función de los resultados ocasionados.

Frecuencia. - Para realizar el análisis y evaluación de riesgos se necesita tener como dato la frecuencia que puede suceder dichas amenazas y asignar un valor al impacto ocasionado.

FRECUENCIA	
CODIGO	DESCRIPCION
5	SIEMPRE
4	CASI SIEMPRE
3	A VECES
2	POCAS VECES
1	CASI NUNCA

Tabla 9: Frecuencia
FUENTE: AUTOR

Nivel del Impacto

NIVEL DEL IMPACTO	
CODIGO	DESCRIPCION
5	MUY ALTO
4	ALTO
3	MEDIO
2	BAJO
1	MUY BAJO

Tabla 10: Nivel de Impacto
FUENTE: AUTOR

Matriz de evaluación de Riesgos

ANALISIS Y EVALUACION DE RIESGO					
ACTIVO	CODIGO	DESCRIPCION	FRECUENCIA	IMPACTO	VALOR DEL RIESGO
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC1	TERREMOTO	1	5	5
	APC2	INCENDIO	1	5	5
	APC3	FALLA FISICA(HARDWARE)	2	5	10
	APC4	FALLA ELECTRICA (SUMINISTRO)|	2	5	10
	APC5	TEMPERATURA	2	4	8
	APC6	ROBO	1	5	5
SERVIDOR	AS1	TERREMOTO	1	5	5
	AS2	INCENDIO	1	5	5
	AS3	FALLA FISICA(HARDWARE)	2	5	10
	AS4	FALLA ELECTRICA (SUMINISTRO)|	2	5	10
	AS5	TEMPERATURA	2	4	8
	AS6	ROBO	1	5	5
	AS7	ATAQUE DENEGACION DE SERVICIO	1	5	5
	AS8	LENTITUD EN EL SISTEMA	3	5	15
SOFTWARE ERP SAO	AERP1	ADMINISTRACION DEL SISTEMA	1	5	5
	AERP2	USUARIOS	3	4	12
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	4	5	20
	AERP4	INGRESO ERRONEO DE INFORMACION	3	4	12
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	2	5	10

Tabla 11: Matriz De Análisis Y Evaluación Del Riesgo
FUENTE: AUTOR

4.3 Análisis e implementación del Plan de tratamiento de riesgo

Al encontrar niveles elevados en la matriz de riesgos, necesitamos aplicar medidas para reducir dichos riesgos, para aquello, se necesita elaborar el **Plan de Tratamiento de Riesgo** o **PTR** el cual consiste en seleccionar los controles de la norma ISO27002:2013 adecuados y aplicar dichos controles, con el objetivo de mitigar el riesgo y reducir el impacto.

Formas de tratamiento de riesgos:

- ✓ Reducir el Riesgo.
- ✓ Aceptar el Riesgo.
- ✓ Transferir el Riesgo.
- ✓ Evitar el Riesgo.

Reducir el Riesgo. - Consiste en implementar controles necesarios para reducir los riesgos a niveles aceptados por la empresa.

Se pueden reducir los riesgos bajando la posibilidad que la vulnerabilidad se vea afectada por la amenaza y disminuyendo el impacto si el riesgo se presenta.

Aceptar el Riesgo. - Debido a los costos de implementación para mitigar el impacto cuando el riesgo se presente, algunas empresas deciden no invertir en planes de tratamiento de riesgos y deciden asumir las consecuencias del impacto cuando se presente el riesgo.

Transferir el Riesgo. - una opción para las empresas es la de trasferir el riesgo, existen algunas opciones de transferencia como el caso de empresas aseguradoras que cubren los gastos ocasionados por los resultados del nivel de impacto, otra opción es la de contratar empresas outsorcing y transferir el riesgo a ellas para su mitigación, de esta forma quedamos atentos a monitorear los riesgos, pero no a su mitigación.

Evitar el Riesgo. - consiste en modificar las actividades propias de la empresa (procesos) para evitar correr riesgos y la consecuencia que estos presentan. Se debe establecer procesos adecuados de operación para evitar el riesgo o simplemente evitar realizar algún proceso.

Analizar si los procesos que se dejen de realizar con el fin de evitar riesgos resultan económicamente muy costosos y devastadores para la economía de la empresa.

A continuación, se muestra una tabla con una valoración de riesgo elevada, los mismos que deben ser mitigados.

PLAN DE TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA		VULNERABILIDAD	VALOR DEL RIESGO	Riesgos mitigados
	CODIGO	DESCRIPCION	DESCRIPCION		
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	10	5
	APC4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	10	5
SERVID0R	AS3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	10	5
	AS4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	10	5
	AS8	LENTITUD EN EL SISTEMA	FALTA DE RECURSOS (MEMORIA, PROCESADOR, DISCO DURO)	15	10
SOFTWARE ERP SAO	AERP2	USUARIOS	FALTA DE CAPACITACION A LOS USUARIOS DE LOS DIFERENTES APLICATIVOS.	12	4
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	ERROR DE MONITOREO DEL APLICATIVO	20	10
	AERP4	INGRESO ERRONEO DE INFORMACION	FALTA DE CONOCIMIENTO DEL APLICATIVO	12	8
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	FALLAS EN LA ACTUALIZACION DEL SISTEMA	10	5

TABLA 12: PLAN DE TRATAMIENTO DE RIESGO
FUENTE: AUTOR

4.4 Análisis y selección de los controles del estándar ISO 27002

PLAN DE TRATAMIENTO DE RIESGO				
ACTIVO	AMENAZA		VULNERABILIDAD	Control Seleccionado
	CODIGO	DESCRIPCION	DESCRIPCION	
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	8. Gestión Activos 11.2 Seguridad de los equipos
	APC4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	8. Gestión Activos 11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información
SERVID0R	AS3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información
	AS4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	8. Gestión Activos 11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información
	AS8	LENTITUD EN EL SISTEMA	FALTA DE RECURSOS (MEMORIA, PROCESADOR, DISCO DURO)	8. Gestión Activos 11.2 Seguridad de los equipos
SOFTWARE ERP SAO	AERP2	USUARIOS	FALTA DE CAPACITACION A LOS USUARIOS DE LOS DIFERENTES APLICATIVOS.	8.1.3 uso aceptable de los Activos 11.2 Seguridad de los equipos
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	ERROR EN EL MONITOREO DEL APLICATIVO	11.2 Seguridad de los equipos
	AERP4	INGRESO ERRONEO DE INFORMACION	FALTA DE CONOCIMIENTO DEL APLICATIVO	8.1.3 uso aceptable de los Activos 11.2 Seguridad de los equipos
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	FALLAS EN LA ACTUALIZACION DEL SISTEMA	11.2 Seguridad de los equipos

Tabla 13: Análisis Y Selección De Controles Iso27002
FUENTE: AUTOR

CAPÍTULO 5

DESARROLLO E IMPLEMENTACION DEL SGSI

5.1 Desarrollo e implementación de controles

5.1.1 Control Gestión Activos (8.1)

La institución deberá identificar los activos y asignar un grado de importancia, incluir como parte del inventario todo lo referente al activo (descripción, tipo, fechas, documentación legal y de ser posible un avaluó, de esta manera se agilita la recuperación en el caso de algún desastre.

5.1.2 Control Uso aceptable de los equipos (8.1.3)

Capacitación constante y retroalimentación a los usuarios que utilizan y manejan los activos, sean estos equipos o sistemas informáticos considerados activos de la empresa constructora.

5.1.3 Control Seguridad de los equipos (11.2)

La empresa Coetecorpza SA deberá proteger sus activos (equipos) contra todo tipo de amenazas ya sean estas de tipo físico o ambiental, con la protección lo que se busca es minimizar accesos no autorizados y la mala manipulación del activo (equipo) y que esto pueda conllevar al daño o sustracción del activo. Con una debida protección se reducen el riesgo.

Deberá contar con planes de emergencia ante cualquier eventualidad que se presente y que esta pueda afectar el equipo directa e indirectamente.

Evitar la reubicación física del equipo por personal no autorizado para realizar esas tareas, incluir dentro de los procesos el llevar documentación con firma del responsable del equipo y del personal que lo traslada y el motivo de traslado y que esto sea validado por personal de seguridad física.

Controlar áreas físicas para accesos no autorizado, establecer información visible sobre lugares de reunión, salidas de escape, escaleras y puertas de emergencia.

5.1.4 Control Continuidad de la seguridad de la información (17.1)

Dentro de la planificación sobre continuidad del negocio y recuperación ante desastres naturales se deberá tener presente siempre el proceso de seguridad de la información y sus elementos necesarios.

Garantizar lo mayormente posible que ante cualquier eventualidad o desastre natural siempre la organización contara con controles de seguridad de la información operativos.

La organización deberá tener un plan de contingencia o emergente en el caso de falla en los controles ya no puedan cumplir con sus objetivos para los que fueron implementados.

Revisar periódicamente el plan de contingencias y recuperación ante desastres ya que siempre se puede presentar algún cambio dentro de los procesos que maneja la organización.

PLAN DE TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA		VULNERABILIDAD	Control Seleccionado	Plan de acción
	CODIGO	DESCRIPCION	DESCRIPCION		
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	8. Gestión Activos 11.2 Seguridad de los equipos	Tener actualizado el inventario de equipos. Planificar los mantenimientos preventivos periódicos
	APC4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	8. Gestión Activos 11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información	Realizar el plan de continuidad para saber qué medidas tomar en el caso que se presente un evento o suceso de este tipo, contar con suministro eléctrico alterno, equipos UPS y demás
SERVID0R	AS3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información	Tener actualizado el inventario de equipos. Planificar los mantenimientos preventivos periódicos
	AS4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	8. Gestión Activos 11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información	Realizar el plan de continuidad para saber qué medidas tomar en el caso que se presente un evento o suceso de este tipo, contar con suministro eléctrico alterno, equipos UPS y demás
	AS8	LENTITUD EN EL SISTEMA	FALTA DE RECURSOS (MEMORIA, PROCESADOR, DISCO DURO)	8. Gestión Activos 11.2 Seguridad de los equipos	Realizar un levantamiento de información sobre las características de hardware y software de los equipos y analizar si aquellas características sirven para cumplir con la tarea encomendada

PLAN DE TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA		VULNERABILIDAD	Control Seleccionado	Plan de acción
SOFTWARE ERP SAO	AERP2	USUARIOS	FALTA DE CAPACITACION A LOS USUARIOS DE LOS DIFERENTES APLICATIVOS.	8.1.3 uso aceptable de los Activos 11.2 Seguridad de los equipos	Impartir capacitación sobre los sistemas que utiliza la constructora Coetecorza S.A a todo el personal nuevo y firmar acta de responsabilidad entre el trabajador nuevo y la empresa sobre el uso de los sistemas(Activos)
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	ERROR EN EL MONITOREO DEL APLICATIVO	11.2 Seguridad de los equipos	Capacitación a personal sobre el monitoreo de aplicaciones y estado de los servicios. Establecer el plan de acción ante eventos o sucesos que se presenten.
	AERP4	INGRESO ERRONEO DE INFORMACION	FALTA DE CONOCIMIENTO DEL APLICATIVO	8.1.3 uso aceptable de los Activos 11.2 Seguridad de los equipos	Impartir capacitación sobre los sistemas que utiliza la constructora Coetecorza S.A a todo el personal nuevo y firmar acta de responsabilidad entre el trabajador nuevo y la empresa sobre el uso de los sistemas(Activos)
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	FALLAS EN LA ACTUALIZACION DEL SISTEMA	11.2 Seguridad de los equipos	Plan de contingencia. Tener un plan de recuperación y continuidad del negocio para minimizar el impacto por la caída de los servicios.

Tabla 14: Controles Y Plan De Acción
FUENTE: AUTOR

5.2 Desarrollo de la Política de seguridad informática

Con el día a día el mundo tecnológico avanza a pasos de gigante y trae consigo un mundo de bondades con las cuales facilita la vida a todas las personas. Con la llegada del internet ahora es posible estar conectado siempre a través de un sin número de dispositivos disponibles en el mercado mundial.

Así como bondades también el internet dio cabida a la llegada de amenazas de seguridad lógica y física. Por tal motivo se establece un documento que se debe de cumplir obligatoriamente por parte de todos los trabajadores de la empresa y debe ser difundido por el personal de talento humano para que todos conozcan de las políticas de la empresa en lo referente a gestión de activos. El no cumplir con estas políticas puede traer consigo perdidas monetarias para la empresa y el no cumplimiento de sus objetivos. Estas políticas surgen a partir del análisis de riesgos que se realizó para la elaboración de este proyecto.

5.2.1 Alcance De Las Políticas

La elaboración de este documento de políticas de seguridad basadas en la gestión de activos se obtiene del análisis de riesgos realizado a la

empresa, con el fin de aplicar controles para mejorar o disminuir las amenazas encontradas y mejorar la seguridad de sus activos.

5.2.2 Objetivo de la Política

Desarrollar un documento claro y preciso sobre las políticas establecidas para garantizar el correcto manejo de los activos de la empresa Cotercopza SA y la correcta difusión de las políticas para que sean de conocimiento general por parte de los miembros de la organización.

Obtener el compromiso de todo el personal de la organización para el cumplimiento de las políticas ya que todos forman parte del sistema de Gestión de Seguridad de la información.

5.2.3 Política

Clausula 1.-

Asignación del Comité, el cual estará integrado por personal de la empresa (Gerente TI, Talento Humano, Jefes de Área) el cual se reunirá con la siguiente finalidad:

- ✓ Compra y adquisiciones de activos tecnológicos.
- ✓ Estandarización de equipos de TI, aplicaciones y sistemas.
- ✓ Arquitectura de TI.

El comité dentro de sus responsabilidades encontramos el correcto uso y funcionamiento de los activos de información. Plan de mejora continúa sobre los riegos encontrados, elaboración de las estrategias y velar por la calidad del servicio brindado.

Poseer inventario general de los activos de la empresa y tener la información de dicho inventario disponible y actualizado.

Cumplir y hacer cumplir las políticas establecidas para el uso de los activos e implementar acciones correctivas y sanciones correspondientes a las personas que no acaten las políticas.

Clausula 2.-

La organización asignara a un responsable sobre el cual recaerá la responsabilidad de los activos y servicios y supervisara todas las políticas implementadas y establecidas por el comité.

Inventario de los activos de cómputo

Clausula 3.-

Se deberá llevar a cabo un inventario general de todos los activos y asignar un custodio y las funciones que se realizan con este activo.

Se deberá utilizar un formato creado y aprobado por el comité, a continuación se adjunta un formato de ejemplo.

Sobre las instalaciones físicas de los activos de computo (Equipos)

Clausula 4.-

Se deberá instalar y asegurar los equipos de cómputo en los escritorios de los usuarios, adicionalmente se deberá firmar un acta de entrega del activo al usuario y validar la firma de responsabilidad.

Se deberá tener instalaciones eléctricas y puntos de redes identificados y en correcto funcionamiento. El uso de regletas, extensiones u otros elementos de corriente queda totalmente prohibido.

Se deberá llevar un control semestral sobre los puestos de trabajo y los equipos instalados al personal y establecer planes de mejora sobre estos puntos.

Funcionamiento de los equipos de cómputo

Clausula 5.-

Revisar por medio de cada jefe de área que los activos de cómputo se utilicen de manera correcta y en las condiciones adecuadas establecidas por el proveedor.

Clausula 6.-

Evitar completamente el consumo de alimentos y bebidas en los espacios establecidos para los equipos de cómputo.

Clausula 7.-

Prohibir el ingreso de equipos particulares a las áreas de la organización más críticas y las instalaciones de programas y aplicativos no autorizados.

Clausula 8.-

Implementar software antivirus original en la organización y siempre tener instaladas las últimas actualizaciones. Asignar al área correspondiente para el monitoreo del estado de la aplicación en los equipos instalados.

Se prohíbe el uso de dispositivos de almacenamiento portátil como disco duros externos, memorias extraíbles o pendrive.

Elementos de seguridad y del entorno

Clausula 9.-

La organización deberá contar con todo lo necesario para garantizar el adecuado uso de los equipos de computación. Por ejemplo:

- ✓ Deberá poseer un ambiente climatizado acorde a las necesidades de cada área.
- ✓ Equipos y señalización contra incendio.
- ✓ Rutas de escape por área.
- ✓ Sistemas de fuentes de energía para dotar a los equipos en caso de algún suceso.

- ✓ Deberá contar con políticas y procedimientos definidos ante cualquier suceso que se pueda presentar y que afecte la operación de la organización.

Mantenimiento preventivo y correctivo

Clausula 10.-

Elaborar un plan de mantenimiento preventivo a los equipos de cómputo ya sea por área, por prioridad o a consideración del comité y establecer la frecuencia de cada mantenimiento.

Asignar al personal responsable de los mantenimientos de los equipos y llevar un control de partes y piezas con defectos.

Definir el procedimiento a realizar sobre los mantenimientos correctivos que se presenten en la organización.

Correcto uso de los Activos

Clausula 11.-

Los activos solo pueden estar disponibles para el personal autorizado y deben ser utilizados para cumplir con las funciones establecidas para lo que fueron instaladas.

Internet y redes internas

Clausula 12.-

El acceso a internet es realizado bajo aprobación del comité y para cumplir con alguna función específica dentro de la organización. El departamento encargado de los equipos deberá implementar políticas para el bloqueo de puertos en los equipos y evitar fugas de información o contaminación de virus. Se deberá asignar un puerto de red y llevar un documento formal donde consten los puntos y equipos asignados.

Implementar políticas de seguridad lógica y equipos como firewall, IPS, equipos de filtrado web e email y equipos perimetrales. Realizar monitoreo sobre las redes y los equipos instalados para evitar ataques de personas maliciosas y que estas dañen la información de la empresa.

Clausula 13.-

Elaborar plan de contingencia ante desastres, asegurar los activos de la empresa mediante pólizas de seguros. Elaborar los procedimientos adecuados para que la organización pueda seguir funcionamiento desde un sitio alterno en el caso de desastres totales.

Copias de seguridad de los datos

Clausula 14.-

Elaborar y poner en funcionamiento la generación de respaldos de información entendiéndose como el activo de mayor valor de la empresa, establecer frecuencia de respaldo, establecer área responsable de llevar esta tarea, así mismo de escoger los equipos y sistemas adecuados para cumplir con esta función y otorgarle seguridad física y lógica al lugar donde van a ser almacenados estos respaldos y que solo puedan tener acceso personal autorizado.

Guardar configuraciones de los Servidores y llevar control sobre las modificaciones que se realicen y crear procedimientos de emergencia sobre respaldos mal efectuados o con problemas.

CAPÍTULO 6:

ANÁLISIS DE RESULTADOS DEL SGSI

Con la finalidad de proteger los activos de la empresa y como parte de la gestión de los mismos, se deberá garantizar la continuidad de los sistemas de información, para esto se elaboran las políticas que deben ser difundidas por el personal responsable y deben ser cumplidas en su totalidad.

La organización debe fomentar el cumplimiento de las políticas como cultura organizacional y crear acuerdos de compromiso entre la organización y los trabajadores.

6.1 Dar a conocer la política de seguridad

Se deberá comunicar, transmitir, difundir las políticas de seguridad de la información aplicadas a los activos de la empresa a todo el personal propio de la empresa y sin dejar a un lado a los proveedores y a todo el personal que realice negociaciones con la empresa.

Capacitar a los empleados para que puedan entender y aplicar las políticas dentro de sus funciones y establecer plan de capacitación y frecuencia de capacitación, con la finalidad de reforzar estos temas o aclarar ciertas dudas referentes a las políticas.

6.2 Evaluar si fueron mitigados los riesgos

Se realiza análisis de riesgos mitigados.

ANALISIS Y EVALUACION DE RIESGO						RIESGOS MITIGADOS		
ACTIVO	CODIGO	DESCRIPCION	FRECUENCIA	IMPACTO	VALOR DEL RIESGO	FRECUENCIA	IMPACTO	Riesgos mitigados
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC3	FALLA FISICA(HARDWARE)	2	5	10	1	5	5
	APC4	FALLA ELECTRICA (SUMINISTRO)|	2	5	10	1	5	5
SERVIDOR	AS3	FALLA FISICA(HARDWARE)	2	5	10	1	5	5
	AS4	FALLA ELECTRICA (SUMINISTRO)|	2	5	10	1	5	5
	AS8	LENTITUD EN EL SISTEMA	3	5	15	2	5	10
SOFTWARE ERP SAO	AERP2	USUARIOS	3	4	12	1	4	4
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	4	5	20	2	5	10
	AERP4	INGRESO ERRONEO DE INFORMACION	3	4	12	2	4	8
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	2	5	10	1	5	5

Tabla 15: Riesgos Mitigados
FUENTE: AUTOR

PLAN DE TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA		VULNERABILIDAD	VALOR DEL RIESGO	Riesgos mitigados
	CODIGO	DESCRIPCION	DESCRIPCION		
LAPTOP SONY PC-DESKTOP IMPRESORA PROYECTOR	APC3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	10	5
	APC4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	10	5
SERVID0R	AS3	FALLA FISICA(HARDWARE)	FALLA/FALTA DE MANTENIMIENTOS PREVENTIVOS	10	5
	AS4	FALLA ELECTRICA (SUMINISTRO)|	FALLA EN LOS SISTEMAS DE LOS UPS O GENERADORES ELECTRICOS	10	5
	AS8	LENTITUD EN EL SISTEMA	FALTA DE RECURSOS (MEMORIA, PROCESADOR, DISCO DURO)	15	10
SOFTWARE ERP SAO	AERP2	USUARIOS	FALTA DE CAPACITACION A LOS USUARIOS DE LOS DIFERENTES APLICATIVOS.	12	4
	AERP3	NO DETECCION DE ERRORES EN EL SISTEMA(MONITREO)	ERROR DE MONITOREO DEL APLICATIVO	20	10
	AERP4	INGRESO ERRONEO DE INFORMACION	FALTA DE CONOCIMIENTO DEL APLICATIVO	12	8
	AERP5	CAIDAS EN EL SISTEMAS (FALLA EN LOS SERVICIOS)	FALLAS EN LA ACTUALIZACION DEL SISTEMA	10	5

Tabla 16: PTR Mitigados

FUENTE: AUTOR

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. El uso correcto del sistema de gestión de seguridad de la información garantiza seguridad a los activos de información y con esto la protección de los datos de la empresa.

2. Implementar el sistema de gestión de seguridad de la información otorga a la empresa la seguridad de la continuidad del negocio y un bajo nivel de impacto de los incidentes que se presenten.

3. Gracias a la implementación del sistema de gestión de seguridad informática se pudo mejorar la infraestructura tecnológica de la

empresa y llevar un correcto control sobre la manipulación de los equipos de cómputo.

4. Se realizaron jornadas de capacitación al personal de la empresa sobre el manejo correcto de la información y el uso de los equipos y aplicaciones. Con esto disminuyo el ingreso erróneo de información en las bases de datos de los diferentes aplicativos.

5. Se instalaron cámaras de seguridad y controles de acceso por áreas, gracias a esta gestión se identificó al personal que estaba intentando ingresar en áreas no autorizadas dentro de la empresa.

Recomendaciones

1. Definir claramente los responsables de los activos y documentar acta de responsabilidad.

2. Monitorear constantemente la disponibilidad de la red y controlar el acceso a la misma y hacia los equipos de cómputo por el personal de la empresa.

3. Definir las políticas de seguridad y transmitir la misma al personal de la organización, incluir en la política los procedimientos a realizar en el

caso que se presenten anomalías como robos, accesos no autorizados y/o desastres naturales, etc.

4. Revisar periódicamente a través de análisis de riesgos, los riesgos a los que la organización es expuesta y ejecutar plan de acción y mejora continua para garantizar siempre la operatividad de la organización.

5. Inculcar en el personal de la organización la cultura de seguridad de la información y otorgar capacitación constante al personal en temas de seguridad, manejo de los aplicativos y sistemas de la organización.

BIBLIOGRAFÍA

[1] J. Areitio Bertolín, Seguridad de la información. Redes, informática y sistemas de información, Madrid, España: Paraninfo, 2008.

[2] J. Ruiz Spohr y A. Lopez Neira, «iso27000,» octubre 2012. [En línea]. Available: http://www.iso27000.es/sgsi.html.

[3] isotools, «isotools.org,» [En línea]. Available: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/. [Último acceso: Enero 2017].

[4] . A. Corletti Estrada, Seguridad por niveles, Madrid: DarFe, 2011.

[5] L. Cruz, «gestionyauditoriati,» 30 noviembre 2013. [En línea]. Available: https://gestionyauditoriati.com/2013/11/30/la-medicion-del-riesgo-de-ti/.