ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE CONTROLES PARA PROTECCIÓN DE ENDPOINTS APLICANDO LA NORMA ISO 27001"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

CHRISTIAN ORLANDO VARGAS JARAMILLO

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

A **Dios** por todas las bendiciones que me han extasiado de felicidad y por cada obstáculo que me ha ayudado a crecer.

A **mi familia** por apoyarme en cada uno de mis proyectos y decisiones.

A **mis amigos** que me impulsaron a culminar esta meta con sus consejos y empuje.

A **DARCON** por facilitarme herramientas para buscar alternativas y afrontar circunstancias, reconociendo que “querer es poder”.

DEDICATORIA

Para mis padres, hermanas y cuñados por brindarme su amor y apoyo incondicional. Y para mis sobrinos que me fortalecen como ser humano con su candidez y ternura.

TRIBUNAL DE SUSTENTACIÓN

.....

MGS. LENIN FREIRE COBOS

DIRECTOR DEL MSIA

.....

MGS. ROBERT ANDRADE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

.....

MGS. NESTOR ARREAGA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

Crear una cultura organizacional sobre la importancia de la Seguridad de la Información, mediante la detección común, pero nada despreciable como es la vulnerabilidad de los virus informáticos que se encuentra latente en las empresas.

Se ha realizado la gestión que involucra la implementación de un SGSI orientada solamente a lo que se definió en el Alcance de este documento.

El objetivo principal es aprovechar un incidente informático ocurrido en el equipo de un funcionario y exponer el riesgo latente y crítico que puede ver afectada la operación de la Empresa, por no tener los controles necesarios de protección contra virus. Para ello se ha considerado la norma ISO 27001 con sus respectivos controles del Anexo 2, para promover la importancia de la aplicación de esta norma en la empresa y proteger el activo más importante que es la Información.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

MAGERIT :	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, la misma que es promovida por el Ministerio de Administraciones Públicas de España.
SGSI :	Siglas de Sistema de Gestión de Seguridad de la Información
SOA:	"Declaración de Aplicabilidad" que se la conoce como SoA por sus términos en inglés (Statement of Applicability).
WSUS:	Por sus siglas en Inglés (Windows Server Update Services). El servidor WSUS proporciona las características que los administradores necesitan para administrar y distribuir actualizaciones mediante una consola de administración.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el entorno empresarial actual de nuestro país recién se está considerando a la seguridad de la información como un proceso de importancia de manera institucional. Por tal motivo es que se le ha propuesto a TASESA C.A. desarrollar un [1] SGSI con el alcance específico a la protección contra código malicioso de los equipos computacionales de los usuarios, donde se expone la importancia de contar con un sistema de manera integral y transversal cuyo objetivo principal es el iniciar un cambio en la cultura organizacional con respecto al manejo prudente y conscientemente de los activos de información.

Inicialmente se ha empezado con el incidente del virus RansonWare y se ha desarrollado la implementación del SGSI que se presenta en este documento y que se lo ha definido respectivamente en el alcance.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

La seguridad de la información en el ambiente empresarial es actualmente un punto neurálgico en toda institución, por tanto el protegerla de: eliminaciones, daños, uso inapropiado; son factores que deben ser considerados prioritariamente por la Alta Gerencia.

La información de los usuarios como: correos electrónicos, libros de Excel, informes, reportes confidenciales o críticos, son parte del flujo de información que cotidianamente rota en una institución ya sea esta pequeña, mediana o grande.

En la actualidad existen vulnerabilidades que afectan a los activos de información y que atacan por diferentes frentes, como lo son:

- Externamente: Virus (como el RansonWare que inhabilita los archivos como .PST, DOC, XLS, etc), Phishing, etc.
- Internamente: Fuga de Información por parte de los funcionarios, mala utilización de los recursos tecnológicos (utilización de Software: Juegos, Torrent, Redes Sociales).

1.2. Solución propuesta

Se aplicará la implementación de controles basados en la norma ISO 27001, con el alcance de proteger los equipos de los usuarios (End Points), y cumplir con dos objetivos fundamentales indicados en orden prioritario de la siguiente manera:

1. Proteger los equipos de los usuarios finales con la aplicación de controles de la Norma ISO 27001.
2. Creación de una cultura en el uso correcto de los recursos informáticos para proteger la información.
3. Inteligenciar a la Alta Gerencia con la importancia de proteger los activos de información, exponiendo las vulnerabilidades que actualmente la información debe enfrentar.

Para realizar la implementación del **Sistema de Gestión de Seguridad de la Información (SGSI)** se utilizó la herramienta **SECURIA SGSI** que es una solución basada en código abierto y de libre distribución dirigida a este tipo de implementaciones.

SECURIA SGSI es una herramienta que soporta la implantación, puesta en marcha, mantenimiento y mejora continua de un SGSI basado en la norma ISO 27001. Esta solución viene con parámetros y configuraciones preestablecidas, las mismas que se han mantenido en esta implementación.

1.3. Alcance

El SGSI que se propone implementar solamente abarcará los controles específicos para la protección de los equipos computacionales de la empresa contra las vulnerabilidades existentes de código malicioso, así mismo se expondrá el incidente reportado en el mes de diciembre sobre la infección de un equipo con el virus RansonWare.

Se elaborarán las políticas principales que son:

- Política Institucional de Seguridad de la Información.
- Protección contra código malicioso.
- Uso correcto de correo electrónico.
- Uso correcto de Internet.
- Uso correcto de servidores de archivos

Así mismo cualquier otro procedimiento o proyecto tecnológico que se derive de la implementación de los controles seleccionados en el SGSI, será mencionado en este documento con el fin que se realicen las gestiones necesarias con los directivos de la empresa para la aprobación, elaboración y aplicación de los mismos, según corresponda.

CAPÍTULO 2

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y ANÁLISIS DE RIESGOS

2.1. Alcance de la implementación de controles basados en ISO 27001

El alcance de esta implementación de controles basados en la norma ISO 27001 será para los equipos computacionales de la Empresa TASESA C.A., para lo cual se regirán bajo los controles establecidos en el Anexo A de la Norma ISO 27001:2005, y de los cuales solo se considerarán los controles que contemplen el aseguramiento de los computadores de los usuarios internos.

2.2. Política de Seguridad según el alcance definido.

Como parte de la implementación de la Norma se ha establecido la política institucional de seguridad de la información que se presenta en el **Anexo 01**, y que se ha clasificado en el documento "SGSI.POL.01.00 POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION". Así mismo también se desarrollaron 4 políticas más:

- SGSI.POL.01.01 - Política de Protección contra código malicioso se la puede observar en **Anexo 02**.
- SGSI.POL.01.02 - Política de Uso correcto de correo electrónico se la puede observar en **Anexo 03**.
- SGSI.POL.01.03 - Política de Uso correcto de internet se la puede observar en **Anexo 04**.
- SGSI.POL.01.04 - Política de Uso correcto de servidores de archivos se la puede observar en **Anexo 05**.

2.3. Identificación de activos de información.

La identificación de los activos se lo realizó mediante la categorización de los activos que la herramienta los define también como DOMINIOS:

Tabla 1. Categorías de Activos de Información

CATEGORIA / DOMINIO	NOMENCLATURA
ORGANIZACIÓN	OR
UBICACIÓN FISICA	U
RED COMUNICACIONES	COM
HARDWARE	HW
SOFTWARE	SW
SERVICIOS	S
ACTIVO DE INFORMACION	D

Con esta categoría se procedió a identificar los activos y categorizarlos según correspondían, esta categorización se expone en la siguiente tabla:

Tabla 2. Levantamiento de activos categorizados

ACTIVO DE INFORMACIÓN	CATEGORIA ASIGNADA
Enlace de Datos e Internet	COM
Servidor de Archivos	HM
Antivirus	SW
Sistemas de Información	S
Servidor de Correo Electrónico	S
Servicio de Correo Electrónico	D
Equipos Informáticos de usuarios	D
Información de usuarios	D

2.4. Valoración de los activos de información.

Para la valoración de los activos de información se mantuvieron las dimensiones y criterios que vienen en la herramienta SECURIA SGSI:

Tabla 3. Dimensiones y Criterios para el análisis.

ATRIBUTO DE INFORMACIÓN	CODIGO CRITERIO	CRITERIO DE IMPACTO POSIBLE
Confidencialidad	C1	¿Qué impacto tendría la divulgación de los datos internamente?
	C2	¿Qué impacto tendría la divulgación de los datos externamente?
Integridad	I1	¿Qué impacto tendría la perdida de información? (Sin que se pudiera recuperarla de ninguna forma)
	I2	¿Qué impacto tendría que la información contenga errores?
Disponibilidad	D1	Interrupción de la prestación de servicios o procesos de negocios hasta 1 día.
	D2	Interrupción de la prestación de servicios o procesos de negocios hasta 1 semana.
	D3	Interrupción de la prestación de servicios o procesos de negocios hasta 2 semanas.

2.5. Análisis de riesgos

Las amenazas y vulnerabilidades encontradas y que se identificaron se las presenta en las siguientes figuras que se detallan a continuación, vale la pena recordar que la herramienta a la categoría también la representa como dominio:

AMENAZA	DESCRIPCIÓN	VULNERABILIDAD	DOMÍNIO	CON	DIS	INT
Ataque destructivo	El personal o las entidades externas contratadas son las más familiares con sus organizaciones ICT. Este conocimiento provee a ellos de la capacidad de causar la interrupción máxima a la organización por saboteando los sistemas informáticos. El número de los incidentes de sabotaje de empleado, como se cree, es menos que para el Robo y el Fraude pero las pérdidas individuales pueden ser altas. Los ejemplos de sabotaje incluyen: Destrucción de hardware y infraestructura Cambios en los datos Entrada de datos errónea Eliminación de software Introducción de virus	Archivos de respaldo y sistemas no disponibles.	D	X	X	
Ataque destructivo	El personal o las entidades externas contratadas son las más familiares con sus organizaciones ICT. Este conocimiento provee a ellos de la capacidad de causar la interrupción máxima a la organización por saboteando los sistemas informáticos. El número de los incidentes de sabotaje de empleado, como se cree, es menos que para el Robo y el Fraude pero las pérdidas individuales pueden ser altas. Los ejemplos de sabotaje incluyen: Destrucción de hardware y infraestructura Cambios en los datos Entrada de datos errónea Eliminación de software Introducción de virus	Archivos de respaldo y sistemas no disponibles.	OR	X	X	

Figura 2.5.1. Identificación de amenazas y vulnerabilidades página 1 de 3

AMENAZA	DESCRIPCIÓN	VULNERABILIDAD	DOMÍNIO	CON	DIS	INT
Difusión de software dañino	(Virus, troyanos etc)	Carencia de actualización regular del Antivirus.	OR		X	
Difusión de software dañino	(Virus, troyanos etc)	Carencia de actualización regular del Antivirus.	SW		X	
Difusión de software dañino	(Virus, troyanos etc)	Educación Inadecuada de personal sobre Antivirus.	OR		X	
Difusión de software dañino	(Virus, troyanos etc)	Educación Inadecuada de personal sobre Antivirus.	D		X	
Difusión de software dañino	(Virus, troyanos etc)	Educación Inadecuada de personal sobre Antivirus.	SW		X	
Difusión de software dañino	(Virus, troyanos etc)	Descarga Incontrolada y empleo de software de la Internet.	OR		X	
Difusión de software dañino	(Virus, troyanos etc)	Descarga Incontrolada y empleo de software de la Internet.	D		X	
Difusión de software dañino	(Virus, troyanos etc)	Descarga Incontrolada y empleo de software de la Internet.	SW		X	
Difusión de software dañino	(Virus, troyanos etc)	Carencia de política para abrir adjuntos de correo electrónico.	D		X	
Difusión de software dañino	(Virus, troyanos etc)	Carencia de política para abrir adjuntos de correo electrónico.	SW		X	
Difusión de software dañino	(Virus, troyanos etc)	Carencia de control de mensajería inmediata.	SW		X	
Difusión de software dañino	(Virus, troyanos etc)	Carencia de comprobaciónes para software no autorizado.	SW		X	
Difusión de software dañino	(Virus, troyanos etc)	Carencia de política contra utilización de dispositivos de almacenaje portátiles y medios de comunicación antes de exploración por Antivirus.	SW		X	
Uso de software pirata o no autorizado	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	Carencia de política que restringe al personal en empleo de software autorizado.	D		X	X
Uso de software pirata o no autorizado	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por	Control inadecuado de distribución de software.	SW		X	X

Figura 2.52. Identificación de amenazas y vulnerabilidades página 2 de 3

AMENAZA	DESCRIPCIÓN	VULNERABILIDAD	DOMÍNIO	CON	DIS	INT
	personas ajenas a la Organización o por personal contratado temporalmente.					
Uso de software pirata o no autorizado	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	Carencia de revisión de software.	SW		X	X
Uso de software pirata o no autorizado	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	Copia sin restricción de software.	SW		X	X
Difusión de software dañino	(Virus, troyanos etc)	Inexistencia de software de Antivirus	OR		X	
Difusión de software dañino	(Virus, troyanos etc)	Inexistencia de software de Antivirus	SW		X	

Figura 2.3. Identificación de amenazas y vulnerabilidades página 3 de 3

El test inicial de los controles realizados con la herramienta se los puede observar en el **Anexo 06** "Test Inicial" de controles.

Los valores de probabilidades se han definido de la siguiente manera

Tabla 4. Descripción de Probabilidades definidas.

IDENTIFICADOR DE PROBABILIDAD	NIVEL	DESCRIPCIÓN
1	Muy Bajo	Improbable que ocurra
2	Bajo	1 vez cada dos años
3	Medio	1 vez cada año
4	Alto	Hasta una vez al mes
5	Muy alto	Más de una vez al mes

Con la tabla antes mencionada se determinaron las probabilidades de ocurrencia de las amenazas para cada una de las "Categorías / Dominio", así como se observa en la siguiente figura:

CATEGORÍA	AMENAZA	DESCRIPCIÓN	PROBABILIDAD
D	Difusión de software dañino	(Virus, troyanos etc)	4
SW	Difusión de software dañino	(Virus, troyanos etc)	4
OR	Difusión de software dañino	(Virus, troyanos etc)	3
D	Ataque destructivo	El personal o las entidades externas contratadas son las más familiares con sus organizaciones ICT. Este conocimiento provee a ellos de la capacidad de causar la interrupción máxima a la organización por saboteando los sistemas informáticos. El número de los incidentes de sabotaje de empleado, como se cree, es menos que para el Robo y el Fraude pero las pérdidas individuales pueden ser altas. Los ejemplos de sabotaje incluyen: Destrucción de hardware y infraestructura Cambios en los datos Entrada de datos errónea Eliminación de software Introducción de virus	3
D	Uso de software pirata o no autorizado	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	4
SW	Uso de software pirata o no autorizado	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	4

Figura 2.4. Definición de Probabilidades para cada amenaza según la Categoría/Dominio afectado.

Esta valoración de probabilidades arrojo los siguientes resultados:

Riesgo Intrínseco por Categoría:

C = CONFIDENCIALIDAD
D = DISPONIBILIDAD
I = INTEGRIDAD

					C			D			I	
CATEGORÍA	ACTIVO	IMPACTO	AMENAZA	PROB.	I	E	1D	1S	2S	A	B
SW	Antivirus	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	20	16	16
SW	Antivirus	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	20	16	16
SW	Antivirus	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	20	16	16
SW	Antivirus	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	20	0	0
SW	Antivirus	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	20	0	0
SW	Antivirus	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	20	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Ataque destructivo	3	3	6	9	12	15	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Ataque destructivo	3	3	6	9	12	15	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Ataque destructivo	3	3	6	9	12	15	0	0

Figura 2.5. Resultado - Riesgo Intrínseco por Categoría, página 1 de 3

C = CONFIDENCIALIDAD
D = DISPONIBILIDAD
I = INTEGRIDAD

					C		D			I	
CATEGORÍA	ACTIVO	IMPACTO	AMENAZA	PROB.	I	E	1D	1S	2S	A	B
D	Servicio de Correo Electrónico	nul null null null null null null	Ataque destructivo	3	6	6	6	9	12	0	0
D	Servicio de Correo Electrónico	nul null null null null null null	Ataque destructivo	3	6	6	6	9	12	0	0
D	Servicio de Correo Electrónico	nul null null null null null null	Ataque destructivo	3	6	6	6	9	12	0	0
D	Informacion de Usuarios	nul null null null null null null	Ataque destructivo	3	3	3	6	9	15	0	0
D	Informacion de Usuarios	nul null null null null null null	Ataque destructivo	3	3	3	6	9	15	0	0
D	Informacion de Usuarios	nul null null null null null null	Ataque destructivo	3	3	3	6	9	15	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Difusión de software dañino	4	0	0	12	16	20	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Difusión de software dañino	4	0	0	12	16	20	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Difusión de software dañino	4	0	0	12	16	20	0	0
D	Servicio de Correo Electrónico	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	16	0	0
D	Servicio de Correo Electrónico	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	16	0	0
D	Servicio de Correo Electrónico	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	16	0	0

Figura 2.6. Resultado - Riesgo Intrínseco por Categoría, página 2 de 3

C = CONFIDENCIALIDAD
D = DISPONIBILIDAD
I = INTEGRIDAD

					C		D			I	
CATEGORÍA	ACTIVO	IMPACTO	AMENAZA	PROB.	I	E	1D	1S	2S	A	B
D	Informacion de Usuarios	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	20	0	0
D	Informacion de Usuarios	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	20	0	0
D	Informacion de Usuarios	nul null null null null null null	Difusión de software dañino	4	0	0	8	12	20	0	0
D	Equipos Informáticos de Usuarios	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	12	16	20	20	20
D	Equipos Informáticos de Usuarios	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	12	16	20	20	20
D	Equipos Informáticos de Usuarios	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	12	16	20	20	20
D	Servicio de Correo Electrónico	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	16	20	16
D	Servicio de Correo Electrónico	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	16	20	16
D	Servicio de Correo Electrónico	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	16	20	16
D	Informacion de Usuarios	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	20	16	16
D	Informacion de Usuarios	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	20	16	16
D	Informacion de Usuarios	nul null null null null null null	Uso de software pirata o no autorizado	4	0	0	8	12	20	16	16

Figura 2.7. Resultado - Riesgo Intrínseco por Categoría, página 3 de 3

La herramienta utilizada, para una definición más aproximada del riesgo, nos permite definir si existe algún tipo de salvaguarda que al implementarse pueda reducir el impacto del riesgo. Estos [2] salvaguardas que se definieron se

basaron en los controles que se van a implementar, los mismos que se definirán y mencionarán más adelante.

En la siguiente tabla se describen los Salvaguardas que al aplicarlos reducirían el impacto del riesgo:

Tabla 5. Definición de salvaguardas utilizadas.

SALVAGUARDA	AMENAZA	CATEGORÍA /DOMINIO	REDUCE IMPACTO
Sociabilización de las Políticas creadas para concientización y educación a los empleados sobre Seguridad de la Información. Instalación de Antivirus Corporativo.	Difusión de software dañino	[D]	SI
		[SW]	SI
		[OR]	SI
Sociabilización y enseñanza a los usuarios sobre la importancia de la seguridad de la Información.	Ataque destructivo	[D]	NO
Concientización y aprendizaje de los empleados sobre los riesgos de uso de Software Ilegal	Uso de software pirata o no autorizado	[D]	NO
		[SW]	SI

Aplicando las salvaguardas antes indicadas la herramienta ha calculado los porcentajes de reducción que se muestran en la siguiente figura:

CATEGORIA	AMENAZA	PROB. INI	PROB. EFECTIVA	% REDUCCIÓN
OR	Difusión de software dañino	3	3	28 %
SW	Uso de software pirata o no autorizado	4	5	27 %
SW	Difusión de software dañino	4	5	28 %
D	Uso de software pirata o no autorizado	4	5	0 %
D	Difusión de software dañino	4	4	28 %
D	Ataque destructivo	3	2	0 %

Figura 2.8. Porcentaje de reducción del impacto al aplicarse los salvaguardas.

Finalmente con la aplicación de las salvaguardas la herramienta ha realizado los cálculos y nos presenta el resultado de Riesgo Efectivo que lo podemos visualizar en dos importantes agrupaciones:

- Riesgo Efectivo de cada “CATEGORIA / DOMINIO” por cada una de las amenazas:

C = CONFIDENCIALIDAD D = DISPONIBILIDAD I = INTEGRIDAD		C		D			I	
CATEGORÍA	AMENAZA	I	E	1D	1S	2S	A	B
D	Ataque destructivo	4	4	6	8	10	0	0
D	Difusión de software dañino	0	0	9	12	14	0	0
SW	Difusión de software dañino	0	0	7	11	18	0	0
D	Uso de software pirata o no autorizado	0	0	15	20	25	25	25
SW	Uso de software pirata o no autorizado	0	0	7	11	18	15	15

Figura 2.9. Riesgo Efectivo por “Categoría / Dominio” y sus respectivas amenazas

- Riesgo Efectivo de cada “Activo” por cada una de las amenazas:

						C = CONFIDENCIALIDAD D = DISPONIBILIDAD I = INTEGRIDAD		C		D		I	
CAT	ACTIVO	AMENAZA	PRB.I	PRB.R	% R	I	E	1D	1S	2S	A	B
SW	Antivirus	Difusión de software dañino	4	5	28%	0	0	7	11	18	0	0
SW	Antivirus	Uso de software pirata o no autorizado	4	5	27%	0	0	7	11	18	15	15
D	Equipos Informáticos de Usuarios	Ataque destructivo	3	2	0%	2	4	6	8	10	0	0
D	Equipos Informáticos de Usuarios	Difusión de software dañino	4	4	28%	0	0	9	12	14	0	0
D	Equipos Informáticos de Usuarios	Uso de software pirata o no autorizado	4	5	0%	0	0	15	20	25	25	25
D	Informacion de Usuarios	Ataque destructivo	3	2	0%	2	2	4	6	10	0	0
D	Informacion de Usuarios	Difusión de software dañino	4	4	28%	0	0	6	9	14	0	0
D	Informacion de Usuarios	Uso de software pirata o no autorizado	4	5	0%	0	0	10	15	25	20	20
D	Servicio de Correo Electrónico	Ataque destructivo	3	2	0%	4	4	4	6	8	0	0

Figura 2.10. Riesgo efectivo por Activo para cada "Categoría / Dominio"

2.5.1. Metodología utilizada de la herramienta SECURIA para análisis de riesgos.

Esta herramienta al ser una solución española utiliza a [4] “Magerit” como metodología para el Análisis de Riesgo.

Un breve resumen del esquema de Magerit se lo puede observar en la siguiente figura:

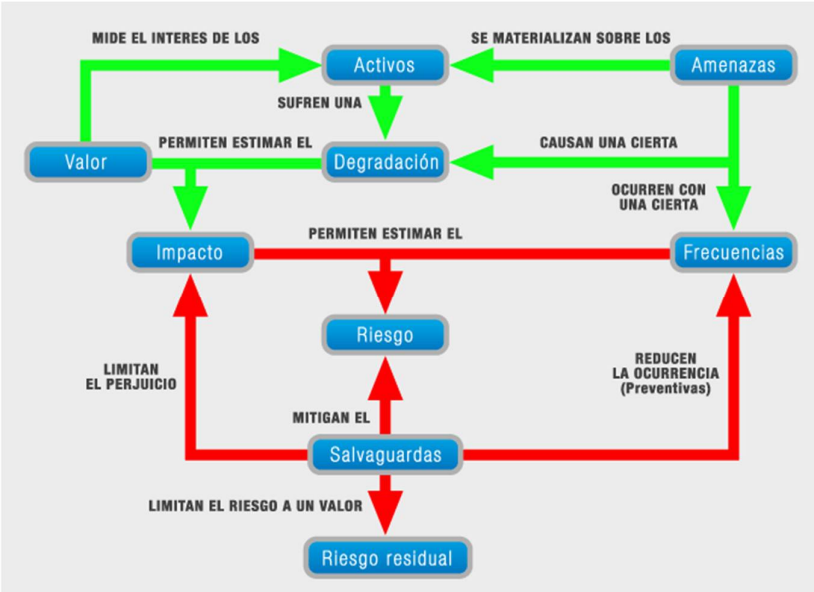

Figura 2.11. Flujo de funcionamiento de metodología Magerit

2.6. Selección de controles a implementar.

Con lo expuesto en los capítulos anteriores y teniendo definido los riesgos con sus respectivos impactos, se define la “Declaración de Aplicabilidad” que también se la conoce como [3] SoA por sus términos en inglés (Statement of

Applicability), esta es la definición más importante porque aquí se determinan prácticamente los controles que se implementarán en el SGSI.

ID CONTROL	CONTROL	APLICA	JUSTIFICACIÓN SELECCIÓN/EXCLUSIÓN
5.1	Documento de Política de Seguridad de la Información	X	el 06 de Diciembre del 2016, se creó la Política de Seguridad de la Información
5.1.2	Revisión de la política de seguridad de la información	X	El 06 de Diciembre del 2016, se creó la Política de Seguridad de la Información, y esta para la revision y aprobación del Gerente
6.1.1	Comisión de gestión de la seguridad de la información		Actualmente aun no esta conformado la Comisión, para ello se esta preparando un proyecto que motive a la Gerencia para que se realice la implementación de un SGSI
6.1.2	Coordinación de la seguridad de la información		Actualmente aun se define una coordinación de Seguridad de la Información, para ello se esta preparando un proyecto que motive a la Gerencia para que se realice la implementación de un SGSI
6.1.3	Asignación de las responsabilidades sobre Seguridad de la Información		Se ha iniciado un proyecto en el cual se ha definido el alcance de proteccion de equipos de los usuarios contra codigo malicioso, en el cual se ha generado Políticas donde se definen ciertas responsabilidades
6.1.4	Proceso de autorización de recursos para el tratamiento de la información		No existe un procedimiento, pero si existe una política donde se define que se deben realizar la instalación de un Antivirus para la proteoción de los equipos
6.1.5	Acuerdos de confidencialidad		
6.1.6	Contacto con las autoridades		
6.1.7	Contacto con grupos de interés especial	X	Se tiene los contactos del personal de Tecnologia y Comunicaciones para reportar las incidencias y soporte tecnico
6.1.8	Revisión independiente de la Seguridad de la Información		
11.7.1	Ordenadores y comunicaciones móviles		En la empresa no se cuenta con uso de equipos portatiles.
6.2.1	Identificación de riesgos relativos a partes externas		
6.2.2	Direocionamiento de la seguridad en el trato con los clientes		
6.2.3	Direocionamiento de la seguridad en los contratos con teroeros		
7.1.1	Inventario de Activos	X	El personal de TICs mantiene un inventario de los equipos computacionales existentes en las Agencias, asi mismo para el desarrollo de este proyecto se han identificado Activos de Información que pueden verse afectados por codigo malicios (virus)
7.1.2	Propiedad de los activos	X	Los equipos se definen en dos grupos: Servidores y Telecomuncaciones: Definidos como propietarios el personal de TICs Computadores, Laptops e Impresoras: Definidos como propietarios los funcionarios de la Empresa

Figura 2.12. Declaración de Aplicabilidad, página 1 de 6

ID CONTROL	CONTROL	APLICA	JUSTIFICACIÓN SELECCIÓN/EXCLUSIÓN
7.1.3	Uso aceptable de los activos	X	Al estar iniciando la creación de la Política de Seguridad se han definido políticas de uso aceptable de los siguientes activos: servicio de correo electrónico, servicio de internet y servicio de recursos compartidos
7.2.1	Guía de clasificación		
7.2.2	Marcado y tratamiento de la información		
8.1.1	Funciones y Responsabilidades		
8.1.2	Investigación de antecedentes		
8.1.3	Términos y condiciones de contratación		
8.2.1	Gestión de responsabilidades		
8.2.2	Concienciación, educación y formación en seguridad de la información	X	Al estar iniciando la creación de la Política de Seguridad se deben definir tambien los procedimientos para que el área Administrativa-Financiera coordine la educación (capacitación) para la concientización y aplicación de Seguridad para cada uno de los funcionarios
8.2.3	Proceso disciplinario		
8.3.1	Finalización de responsabilidades		
8.3.2	Retorno de activos		
8.3.3	Retirada de derechos de acceso		
9.1.1	Perímetro de seguridad física		
9.1.2	Controles físicos de entrada		
9.1.3	Seguridad de oficinas, despachos y recursos		
9.1.4	Protección contra las amenazas externas y entorno		
9.1.5	Trabajo en áreas seguras		
9.1.6	Áreas de acceso publico , de carga y descarga		
9.2.1	Instalación y protección de equipos	X	Se va a presentar un proyecto para la implantación del WSUS (Solución de Microsoft para la distribución centralizada y controlada de los parches de Sistemas Operativos) Con las sociabilización de las Politicas creadas mas la planificación de capacitación se pretende mejora una educación y culturización organizacional sobre el uso correcto de los activos de información.
9.2.2	Instalaciones de suministro		
9.2.3	Seguridad de cableado		
9.2.4	Mantenimiento de equipos	X	Se va a sugerir la instalación de un Servidor de Actualizaciones de Parches de Sistemas Operativos (WSUS) para que los S.O. se encuentren actualizados
9.2.5	Seguridad de los equipos fuera de los locales de la organización		
9.2.6	Seguridad en la reutilización o eliminación de equipos		

Figura 2.13. Declaración de Aplicabilidad, página 2 de 6

ID CONTROL	CONTROL	APLICA	JUSTIFICACIÓN SELECCIÓN/EXCLUSIÓN
9.2.7	Extracción de pertenencias		
10.1.1	Procedimientos operacionales documentados		
10.1.2	Gestión de cambio		
10.1.3	Segregación de tareas		
10.1.4	Separación de los recursos de desarrollo , ensayo y operacionales		
10.2.1	Entrega de servicio		
10.2.2	control y revisión de los servicios por tercera parte		
10.2.3	Gestión de cambios de los servicios por tercera parte		
10.3.1	Gestión de la capacidad		
10.3.2	Aceptación del sistema		
10.4.1	Controles contra código malicioso	X	Despues del Incidente del Ataque del Virus RansonWare se ha iniciado la protección de los equipos con un Antivirus. Se ha creado la politica "SGSI.POL.01.01 _Politica-Proteccion-Codigo-Malicioso" para la proteccion de codigo malicioso. Asi mismo se esta preparando un proyecto para solicitar la adquisicion de una solución que permita gestionar de manera centralizada la configuración y actualizacion del antivirus en los equipos de los usuarios.
10.4.2	Controles contra código ambulante	X	Esta contemplado en la politica "SGSI.POL. 01.01_Politica-Proteccion-Codigo-Malicioso"
10.5.1	Información de copias de seguridad	X	El área de TICs tiene un procedimiento para obtener copias de Seguridad, el mismo que se va a revisar para optimizarlo o corregirlo segun sea necesario.
10.6.1	Controles de red		
10.6.2	Seguridad de los servicios de red		
10.7.1	Gestión de los soportes desmontables	X	Se ha creado la politica "SGSI.POL.01.01 _Politica-Proteccion-Codigo-Malicioso" en la que se menciona los cuidados que deben tener los usuarios en el uso de los soportes desmontables.
10.7.2	Retirada de soporte		
10.7.3	Procedimiento de tratamiento de la información		
10.7.4	Seguridad de la documentación del sistema		
10.8.1	Políticas y procedimientos de intercambio de información		
10.8.2	Acuerdos de intercambio		
10.8.3	Soportes físicos en transito		
10.8.4	Envío de mensajes electrónicos	X	Al estar iniciando la creación de la Política de Seguridad se deben definir tambien la Política de uso correcto del Correo Electrónico.

Figura 2.14. Declaración de Aplicabilidad, página 3 de 6

ID CONTROL	CONTROL	APLICA	JUSTIFICACIÓN SELECCIÓN/EXCLUSIÓN
10.8.5	Sistemas de información del negocio		
10.9.1	comercio electrónico		
10.9.2	Transacciones On-line		
10.9.3	Información públicamente disponible		
10.10.1	Registro de auditoria		
10.10.2	Seguimiento del uso del sistema		
10.10.3	Protección de los registros de información.		
10.10.4	Diario de operaciones y administración		
10.10.5	Registro de fallos		
10.10.6	Sincronización del reloj		
11.1.1	Políticas de control de acceso		
11.2.1	Registro de usuario		
11.2.2	Gestión de privilegios		
11.2.3	Gestión de contraseñas del usuario		
11.2.4	Revisión de derechos de acceso de usuario		
11.3.1	Uso de contraseñas		
11.3.2	Equipo de usuario desatendido		
11.3.3	Política de puesto de trabajo despejado y pantalla limpia		
11.4.1	Política de uso de los servicios de red		
11.4.2	Autentificación de usuario para conexiones eternas		
11.4.3	Identificación de equipo en las redes		
11.4.4	Diagnostico remoto y configuración de la protección de puerto		
11.4.5	Segregación de redes		
11.4.6	Control de la conexión de red		
11.4.7	Control del direccionamiento de red		
11.5.1	procedimientos de entrada seguros		
11.5.2	Identificación y autentificación de usuario		
11.5.3	Sistema de gestión de contraseñas		
11.5.4	Uso de los recursos del sistema		
11.5.5	Tiempo de la conexión de la sesión		
11.5.6	Limitación de tiempo de conexión		
11.6.1	Restricción de acceso a la información		
11.6.2	Aislamiento del sistema sensible		
11.7.1	Ordenadores y comunicaciones móviles		En la empresa no se cuenta con uso de equipos portatiles.
11.7.2	tele trabajo		
12.1.1	Análisis y especificación de los requisitos de seguridad		

Figura 2.15.Declaración de Aplicabilidad, página 4 de 6

ID CONTROL	CONTROL	APLICA	JUSTIFICACIÓN SELECCIÓN/EXCLUSIÓN
12.2.1	Validación de los datos introducidos		
12.2.2	Control del procesamiento interno		
12.2.3	Integridad de los mensajes		
12.2.4	Validación de los datos resultantes		
12.3.1	Política acerca del uso de controles criptográficos		
12.3.2	Gestión de las claves		
12.4.1	Control del software operativo		
12.4.2	Protección de los datos de prueba del sistema		
12.4.3	Control de acceso al código fuente de los programas		
12.5.1	Procedimientos de control de cambios		
12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		
12.5.3	Restricciones de los cambios a los paquetes de software		
12.5.4	Fugas de información		
12.5.5	Externalización del desarrollo de software		
12.6.1	Control de las vulnerabilidades técnicas		
13.1.1	Comunicación de los eventos de seguridad de la información	X	En las políticas que se han creado esta definido a quien deben notificar en caso de eventos de seguridad
13.1.2	Comunicación de puntos débiles de seguridad	X	Actualmente los usuarios lo realizan hace a traves del personal de TICs, pero se deben optimizar ya que es una actividad que aun no esta establecida en un Procedimiento o Manual
13.2.1	Responsabilidades y procedimientos	X	Actualmente se tiene definido los responsables para reportar los incidentes y eventos de Seguridad, pero se deben optimizar ya que aun no esta establecido en un Procedimiento o Manual
13.2.2	Aprendizaje de los incidentes de la seguridad de la información	X	Actualmente no se tiene establecido ningun mecanismo ni metodología. Con el plan de capacitación que se tiene tratan sobre seguridad de la información.
13.2.3	Recopilación de pruebas		
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio		
14.1.2	Continuidad del negocio y evaluación del riesgo		
14.1.3	Desarrollo e implantación de planes de continuidad que incluyan seguridad de la información		
14.1.4	Marco de referencia para la planificación de la continuidad del negocio		
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad de negocio		
15.1.1	Identificación de la legislación aplicables		
15.1.2	Derechos de propiedad intelectual	X	Con las sociabilización de las Políticas creadas mas la planificación de capacitación se pretende mejora una educación y

Figura 2.16.Declaración de Aplicabilidad, página 5 de 6

ID CONTROL	CONTROL	APLICA	JUSTIFICACIÓN SELECCIÓN/EXCLUSIÓN
			culturización organizacional sobre el uso correcto de los activos de información en el mismo que se incluye la responsabilidad de los empleados sobre el uso de software ilegal..
15.1.3	Protección de los registros de la organización		
15.1.4	Protección de datos y privacidad de la información personal		
15.1.5	Prevención del uso indebido de las instalaciones de procesamiento de la información		
15.1.6	Regulación de los controles criptográficos		
15.2.1	cumplimiento de las políticas y normas de seguridad	X	La politica de seguridad de la informacion como las otras politicas recien fueron creadas el 06 Diciembre 2015 as mismas qe deben ser aprobadas por la Genrencia General y cumplir con este control.
15.2.2	Comprobación del cumplimiento técnico		
15.3.1	Controles de la auditoria de los sistemas de información		
15.3.2	Protección de las herramientas de auditoria de los sistemas de información		

Figura 2.17. Declaración de Aplicabilidad, página 6 de 6

CAPÍTULO 3

IMPLEMENTACIÓN DE CONTROLES DEFINIDOS

3.1. Determinación de controles específicos.

Como resultado del análisis de riesgo se determinó que para el aseguramiento de los equipos por las amenazas detectadas y los impactos de las mismas se deben aplicar controles que no solamente son tecnológicos sino también de gestión e incluso se pretende profundizar con una culturización organizacional, con lo cual, como se indicó en el objetivo de esta tesis, se pretende educar a los funcionarios para que sepan reconocer que las diversas herramientas o elementos con los cuales interactúan cotidianamente en sus labores, en realidad son elementos importantes dentro de la seguridad de la información, porque en el marco de trabajo del SGSI se los define con su nombre propio: "activos de información".

Más adelante se podrá observar la lista de controles que se necesitan implementar en el SGSI.

3.1.1. Definición, desarrollo y creación de Políticas.

Se definió la Política institucional de seguridad de la información que se la puede observar en **Anexo 01**, en la misma se han definido los controles principales que ayudaran a asegurar los equipos computacionales de los usuarios, se realizó un desglose de la política institucional, mediante definición y creación de 4 políticas adicionales que se mencionan a continuación:

- SGSI.POL.01.01 - Política de Protección contra código malicioso se la puede observar en **Anexo 02**.
- SGSI.POL.01.02 - Política de Uso correcto de correo electrónico se la puede observar en **Anexo 03**.
- SGSI.POL.01.03 - Política de Uso correcto de internet se la puede observar en **Anexo 04**.
- SGSI.POL.01.04 - Política de Uso correcto de servidores de archivos se la puede observar en Anexo 05.

3.1.2. Controles relacionados al aseguramiento de los computadores.

En esta implementación después del análisis de riesgo se ha determinado que se requieren implementar los siguientes controles para cumplir con el objetivo y alcance de este proyecto, a continuación se detallan los controles:

Tabla 6. Lista de controles que se deben implementar para cumplir con el objetivo y alcance.

CÓDIGO DE CONTROL	NOMBRE DEL CONTROL
5.1	Documento de Política de Seguridad de la Información
5.1.2	Revisión de la política de seguridad de la información
6.1.7	Contacto con grupos de interés especial
7.1.1	Inventario de activos
7.1.3	Uso aceptable de los activos
8.2.2	Concienciación, educación y formación en seguridad de la información
9.2.1	Instalación y protección de equipos
9.2.4	Mantenimiento de equipos
10.4.1	Controles contra código malicioso
10.4.2	Controles contra código ambulante
10.5.1	Información de copias de seguridad
10.7.1	Gestión de los soportes desmontables
10.8.4	Envío de mensajes electrónicos
11.7.1	Ordenadores y comunicaciones móviles
13.1.1	Comunicación de eventos de seguridad de la información
13.1.2	Comunicación de puntos débiles de seguridad
13.2.1	Responsabilidades y procedimientos
13.2.2	Aprendizaje de los incidentes de la seguridad de la información
15.1.2	Derechos de propiedad intelectual
15.2.1	Cumplimiento de las políticas y normas de seguridad

3.2. Selección y justificación de los controles

A continuación se detalla en esta tabla el Plan de Acción con los controles escogidos para cumplir el alcance de la implementación del SGSI:

Tabla 7. Detalle de los controles que se van a implementar, mencionados en el Plan de Acción.

ID CONT	CONTROL	ESTADO INICIAL	ESTADO DESTINO	ACCIONES REQUERIDAS
5.1	Documento de Política de Seguridad de la Información	DEFINIDO	DEFINIDO	La Política institucional de seguridad de la información debe ser revisada y aprobada por la Gerencia
5.1.2	Revisión de la política de seguridad de la información	INICIADO	INICIADO	Esta Política como recién fue creada esta para la revisión de la Gerencia General y su aprobación respectiva
6.1.7	Contacto con grupos de interés especial	DEFINIDO	DEFINIDO	Se actualizará el listado de contactos de manera bi-mensual.
7.1.1	Inventario de Activos	INICIADO	INICIADO	Se establecerá un procedimiento para mantener actualizada la lista de activos
7.1.3	Uso aceptable de los activos	INICIADO	INICIADO	Se evaluará a los empleados para verificar que estén plenamente conscientes de la importancia de la Seguridad de la Información, y por ende del uso apropiado de los activos
8.2.2	Concienciación, educación y formación en seguridad de la información	INICIADO	INICIADO	Se evaluará a los empleados para verificar que estén plenamente conscientes de la importancia de la Seguridad de la Información.
9.2.1	Instalación y protección de equipos	INICIADO	INICIADO	Se revisará la ejecución del proyecto de WSUS
9.2.4	Mantenimiento de equipos	INICIADO	INICIADO	Se revisará la ejecución del proyecto de WSUS
10.4.1	Controles contra código malicioso	INICIADO	INICIADO	Se verificará que se adquiera una solución antivirus que proteja los correos electrónicos de los usuarios, detectando adjuntos que contengan archivos dañinos y se han bloqueados automáticamente por la esta solución.

				Se revisarán los indicadores que midan la cantidad de equipos que tienen actualizada la base de definición de virus.
10.4.2	Controles contra código ambulante	INICIADO	INICIADO	Se revisarán los indicadores que midan la cantidad de equipos que tienen actualizada la base de definición de virus.
10.5.1	Información de copias de seguridad	INICIADO	INICIADO	Se revisará que exista un procedimiento para la obtención/revisión de respaldos, y se evidenciará que estén correctamente etiquetados los respaldos, así como que su contenido sea reproducible
10.7.1	Gestión de los soportes desmontables	INICIADO	INICIADO	Se verificará que la Política de Protección de código malicioso se esté cumpliendo. Se evidenciará que exista el antivirus instalado y actualizado en los equipos, con una política de revisión de unidades removibles.
10.8.4	Envío de mensajes electrónicos	INICIADO	INICIADO	Se evaluará que se esté cumpliendo la Política de uso correcto de correo electrónico, así como también si se han desarrollado algún procedimiento para uso de correo electrónico.
13.1.1	Comunicación de los eventos de seguridad de la información	INICIADO	INICIADO	Se medirá que los empleados estén cumpliendo con la notificación de incidentes de seguridad, conforme se lo ha expuesto en la Política de Seguridad de la Información
13.1.2	Comunicación de puntos débiles de seguridad	INICIADO	INICIADO	Se medirá que los empleados estén cumpliendo con la notificación de incidentes de seguridad, conforme se lo ha expuesto

				en la Política de Seguridad de la Información
13.2.1	Responsabilidades y procedimientos	INICIADO	INICIADO	Se deben cumplir las políticas creadas
13.2.2	Aprendizaje de los incidentes de la seguridad de la información	INICIADO	INICIADO	Se va a crear un procedimiento donde se formalicen los mecanismos de información que actualmente se realizan.
15.1.2	Derechos de propiedad intelectual	INICIADO	INICIADO	Se evaluará al personal sobre las políticas que se sociabilizarán además de las capacitaciones sobre seguridad de la información que se impartirán.
15.2.1	cumplimiento de las políticas y normas de seguridad	INICIADO	INICIADO	Se evidenciará que la Política institucional de Seguridad de la Información este aprobada y socializada en la organización.

Cabe indicar que para la implementación de los controles a parte de la definición de políticas que ya han sido desarrolladas y se presentan en los Anexos de este documento, también se está proponiendo lo siguiente:

- Creación de procedimientos los mismos que se detallan en la sección siguiente.
- Se debe gestionar 2 proyectos para implementar en la empresa y proteger los equipos de ataques o código malicioso, los que se detallan a continuación:
    - [5] WSUS (Windows Server Update Services) Servidor de actualizaciones centralizadas de Sistemas Operativos y soluciones Microsoft.

- Instalación de un Servidor con Consola centralizada que permita la administración de los clientes antivirus en los equipos de los usuarios, y además que permita configurar las protecciones de: correo electrónico e internet. La solución que se sugiere es Kaspersky.

3.3. Políticas y Procedimientos específicos.

Las políticas a implementarse son las que se han creado y se han anexado a este documento, y los procedimientos que se van a definir para la creación serán como mínimo los siguientes:

- Procedimiento para revisión de equipos computacionales y unidades extraíbles.
- Procedimiento para notificación de incidentes seguridad y comunicación con contactos de interés especial.
- Procedimiento para solicitar la creación de recursos en el servidor de archivos.
- Procedimiento para la obtención, etiquetado y pruebas de los respaldos.
- Procedimiento para protección de equipos desatendidos y de oficinas seguras.
- Procedimiento para uso correcto de correo electrónico, internet y servidor de archivos.

3.4. Registros de incidentes

En el mes de diciembre se presentó un incidente que se lo pudo controlar inmediatamente y fue afectado mayor y únicamente el equipo que se infectó con el RansonWare, y unos archivos en la carpeta compartida del Servidor al que se accesaba ese equipo por una unidad de red.

El registro de los incidentes se los realizó por medio de la herramienta SECURIA, y básicamente los pasos que se efectuaron para registrar el incidente fueron los siguientes:

1. Cuando se presenta una incidencia se deben registrar la siguiente información relacionada con el incidente:
    a. Fecha
    b. Asunto que identifique el incidente.
    c. Hora aproximada
    d. Prioridad (la misma que deberá ser evaluada por el responsable de Tics) y se basa en esta categoría: Baja, Normal, Alta, Emergencia
    e. Tipo de incidencia, que debe seleccionarse según las siguientes categorías:
        i. Copias de seguridad y recuperación.
        ii. Denegación de Servicio.
        iii. Derechos de acceso.
        iv. Fallos del sistema.
        v. Fallos de Hardware o Software
        vi. Perdida de servicio, equipo o instalaciones.

vii. Información comprometida

viii. Otros.

f. Descripción de la incidencia:

g. Causa de la incidencia

2. Después de ser registrada esta incidencia debe ser notificada al responsable de seguridad, él mismo que deberá proceder a:
    a. Clasificar la incidencia como cualquiera de estas dos categorías: “Incidencia Técnica” o “No Conformidad”, para este caso será la primera.
    b. Asignar a un responsable que puede ser el responsable de Seguridad o el responsable de Sistemas.
3. Posterior a la asignación de la incidencia, la persona que haya sido asignada, deberá:
    a. Realizar las acciones correctivas y documentar las mismas y para ello para seguir el flujo de información deberá hacerlo en la misma herramienta y colocar en la incidencia las “Acciones correctivas” ejecutadas.
    b. Y por último “cambiar el estado” colocando como “cerrada” a la incidencia.

Los pasos aquí mencionados son los que se deben colocar como mínimo en el “Procedimiento para notificación de incidentes seguridad y comunicación con contactos de interés especial”.

Como prueba del funcionamiento del registro de incidentes siguiendo los pasos anteriormente descritos se presentan los informes obtenidos de la herramienta:

ID: 1	Fecha Notificación: 27/12/2015	Fecha de cierre: 11/01/2016
Tipo: Informacion Comprometida		Estado: Cerrada
Notificador: Oficial Seguridad de la Informacion		Prioridad: Alta
Asunto: Ataque de Virus RansonWare		

Descripción:
Se comprometió la computadora de un funcionario del área de ventas de respuestos
Causa:
Se ejecutó un archivo que estaba adjunto en un correo electronico

TRATAMIENTO DE LA INCIDENCIA / ACCIONES CORRECTIVAS		
ID: 1		
Descripción:		
1. Se aislo el equipo para que no contaminará los recursos de red compartidos. 2. Se realizó la revision del computador con un un Disco de Rescate (Rescue Live CD Kaspersky) y se detectaron y eliminaron los virus del equipo 3. Se instaló el Antivirus MalwareBytes y se lo ejecuto en modo a prueba de fallos. 4. Se le instaló el Antivirus Kaspersky (Version por 30 días) para que el equipo quede proyegido		
Responsable Implantación: Jefe de Tecnologia	Plazo: 1 dias	Coste estimado: 0.00 €

Método de Control de la Acción		
Descripción del método de control		
1. Se debe revisar que las medidas hayan sido las correctas. 2. Se debe revisar el impaco de la información que se compormetio y/o perdió.		
Fecha Control: 04/12/2015	Responsable Control: Oficial Seguridad de la Informacion	Revisado: Si

Resultado del control
¿Ha sido eficaz? Si
Motivo no eficaz:

Figura 3.1. Informe de Incidencia No. 1 Equipo comprometido con Virus RansonWare

ID: 2	Fecha Notificación: 02/01/2016	Fecha de cierre:
Tipo: Copias de seguridad y recuperación		Estado: Pendiente de revisión
Notificador: Oficial Seguridad de la Informacion		Prioridad: Alta
Asunto: Deshabilitacion de Archivos de Access para el Sistema de Contenedores		

Descripción:
El ataque del Virus del RansonWare comprometio el archivo de access que controlaba los numeros secuenciales del Sistema de Contenedores.
Causa:
Virus RansonWare que afecto al equipo de un usuario y este equipo al tener acceso a la Unidad de Red donde se encontraba el archivo de Access, fue encriptado por el virus.

TRATAMIENTO DE LA INCIDENCIA / ACCIONES CORRECTIVAS

ID: 2
Descripción:
1. Como esta incidencia fue producto de la Incidencia 01 (Ataque del Virus RansonWare) y que fue atendida y solucionada hoy en la mañana 4 de Diciembre, se verificó que el equipo comprometido efectivamente ya no tenía el virus. 2. Se ubicó el respaldo de Access y se lo volvió a copiar en el File Server para que sea accesado por los demas usuarios

Responsable Implantación: Jefe de Tecnologia	Plazo: 1 dias	Coste estimado: 0.00 €

Método de Control de la Acción
Descripción del método de control
1. Se verificó que efectivamente el equipo comprometido ya no estaba encriptando los archivos 2. Se verificó que el respaldo que se cargo al File Server tenia la información correcta para que no afecte al funcionamiento del Sistema de Contenedores.

Fecha Control: 04/12/2015	Responsable Control: Jefe de Seguridad	Revisado: Si

Resultado del control
¿Ha sido eficaz? Si
Motivo no eficaz:

Figura 3.2. Informe de Incidencia No. 2, archivo de Access ubicado en un recurso compartido, comprometido con virus RansonWare

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se ha observado que los usuarios tienen un conocimiento bastante aceptable en el uso de los equipos computacionales, pero como toda persona, igual existe la probabilidad de cometer errores al momento de trabajar con archivos ya sean: adjuntos en correo electrónico, descargados de Internet, manejados en unidades removibles o en el mismo Servidor de Archivos.

2. Se necesita hacer una inversión en la adquisición de infraestructura tecnológica tanto en Hardware como Software para proteger los equipos de los usuarios con

soluciones de protección de: actualización de parches de los Sistemas Operativos y contra código malicioso.

3. Es una empresa que tiene un numero manejable de equipos computacionales y además que tiene un vínculo de comunicación bastante efectivo para solicitar soporte y notificar incidentes. Pese a eso, como normativa falta normarlo en un procedimiento donde se formalicen y estandarice esta gestión.

4. Se ha aprovechado un incidente de seguridad presentado en el mes de diciembre del 2015, para promover un proyecto que fortalezca a la organización, evidenciando ciertas falencias que pueden ser corregidas y mejoradas con la implementación de un SGSI.

Recomendaciones

1. Por medio de campañas de sociabilización y capacitación fortalecer el conocimiento de los empleados en el correcto uso de los recursos y herramientas tecnológicas y sobre todo iniciar una educación institucional sobre seguridad de la información para mitigar los riesgos detectados y sobre todo encaminar a la organización para asimilar de la mejor manera la implementación de un SGSI que abarque un objetivo y alcance más general.

2. La alta gerencia debe estar al tanto de los incidentes que se presenten y sobre todo debe estar abierta a las recomendaciones de protección que se sugieren y exigir que se presenten proyectos viables y a corto tiempo para implementar las soluciones.

3. Al existir actividades que se están realizando actualmente, estas deben ser documentadas para cumplir con la normativa.

BIBLIOGRAFÍA

[1] ISO2700, «SGSI,» [En línea], Available: http://www.iso27000.es/glosario.html#section10a. [Último acceso: Enero 2016].

[2] EAR/PILAR, «salvaguardas,» [En línea], Available: http://www.ar-tools.com/es/glossary/index.html. [Último acceso: Enero 2016].

[3] EAR/PILAR, «SoA,» [En línea], Available: http://www.ar-tools.com/es/glossary/index.html. [Último acceso: Enero 2016].

[4] Magerit, «MAGERIT,» [En línea], Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VpRZq_krIy4 [Último acceso: Enero 2016].

[5] Microsoft, «WSUS» [En linea], Available: https://technet.microsoft.com/es-es/library/hh852345.aspx

ANEXOS

Anexo 01. Documento SGSI.POL.01.00 - Política Institucional de seguridad de la información

1. Definiciones

Las definiciones de los términos utilizados se encuentran en el documento SGSI.MAN.01.00 (Manual de definición de términos usados en los documentos).

2. Objetivo

El Objetivo de Seguridad de la Información es asegurar los 3 componentes básicos de la Información que la norma ISO 27001 los reconoce como C-I-D (Confidencialidad, Integridad y Disponibilidad).

Esta política tiene como objetivo principal velar por:

- La Información y los servicios que ofrece aseguren la Confidencialidad, Integridad y Disponibilidad.
- La información en cualquier medio este protegida contra accesos no autorizados Tasesa.
- Toda incidencia sea reportada y tratada correcta y oportunamente.
- Los empleados tengan pleno conocimiento de las políticas y tratamiento correcto de la Información en cualquiera de sus medios.
- Los empleados conozcan la responsabilidad adquirida en el cumplimiento de políticas, procedimientos, instructivos y demás documentos que se deriven en este documento para el aseguramiento de la Información.
- Los responsables de Tics sean los responsables de velar por el cumplimiento de esta política como también de la correcta ejecución de manuales, procedimientos que se deriven de este documento.

3. Alcance

Esta política se aplica a toda la institución, esto incluye a empleados, dirigentes, proveedores, clientes, servicios de **Tics**.

Inicialmente se ha sesgado esta política para implementar controles de seguridad para asegurar los equipos computacionales de ataques de virus y malware.

4. Políticas

4.1. Protección contra código malicioso y descargable

La política de Protección contra código malicioso se encuentra en el documento SGSI.POL.01.01 (Política de protección contra código malicioso)

POLITICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION					
CÓDIGO	: SGSI.POL.01.00	**APLICACIÓN**	: Toda la Institución	**PÁGINA:**	TASESA CONTAINER TERMINAL
VERSIÓN	: 001	**FECHA**	: 06-ENE-2016	**1** de **2**	

1. Definiciones

Las definiciones de los términos utilizados se encuentran en el documento SGSI.MAN.01.00 (Manual de definición de términos usados en los documentos).

2. Objetivo

El Objetivo de Seguridad de la Información es asegurar los 3 componentes básicos de la Información que la norma ISO 27001 los reconoce como C-I-D (Confidencialidad, Integridad y Disponibilidad).

Esta política tiene como objetivo principal velar por:

- La Información y los servicios que ofrece aseguren la Confidencialidad, Integridad y Disponibilidad.
- La información en cualquier medio este protegida contra accesos no autorizados Tasesa.
- Toda incidencia sea reportada y tratada correcta y oportunamente.
- Los empleados tengan pleno conocimiento de las políticas y tratamiento correcto de la Información en cualquiera de sus medios.
- Los empleados conozcan la responsabilidad adquirida en el cumplimiento de políticas, procedimientos, instructivos y demás documentos que se deriven en este documento para el aseguramiento de la Información.
- Los responsables de Tics sean los responsables de velar por el cumplimiento de esta política como también de la correcta ejecución de manuales, procedimientos que se deriven de este documento.

3. Alcance

Esta política se aplica a toda la institución, esto incluye a empleados, dirigentes, proveedores, clientes, servicios de **Tics**.

Inicialmente se ha sesgado esta política para implementar controles de seguridad para asegurar los equipos computacionales de ataques de virus y malware.

4. Políticas

4.1. Protección contra código malicioso y descargable

La política de Protección contra código malicioso se encuentra en el documento SGSI.POL.01.01 (Política de protección contra código malicioso)

Elaborado por: Ing. Christian Vargas Departamento de TICs	**Revisado por:** Ing. Luis Alfredo Andaluz Responsable de TICs	**Aprobado por:** Ing. Juan Carlos Peña Gerente General

4.2. Uso correcto de correo electrónico

Esta política se encuentra en el documento SGSI.POL.01.02 (Política de uso correcto de Correo Electrónico).

4.3. Uso correcto de internet.

Esta política se encuentra en el documento SGSI.POL.01.03 (Política de uso correcto de internet).

4.4. Uso correcto de servidores de archivos

Esta política se encuentra en el documento SGSI.POL.01.04 (Política de uso correcto de servidores de archivos).

Gerencia General

Anexo 02. Documento SGSI.POL.01.01 - Política de Protección contra código malicioso

POLITICA DE PROTECCION CONTRA CODIGO MALICIOSO					
CÓDIGO	: SGSI.POL.01.01	**APLICACIÓN**	: Toda la Institución	**PÁGINA:**	TASESA CONTAINER TERMINAL
VERSIÓN	: 001	**FECHA**	: 06-ENE-2016	**1** de **1**	

1. Definiciones

Las definiciones de los términos utilizados se encuentran en el documento SGSI.MAN.01.00 (Manual de definición de términos usados en los documentos).

2. Objetivo

Esta política tiene como objetivo principal asegurar que los equipos computacionales estén protegidos ataques de virus y malware, considerando la participación activa de los responsables de Tics. Así como cada uno de los funcionarios que tienen como custodio un equipo computacional como herramienta de trabajo para el desarrollo de sus actividades.

3. Alcance

Esta política se aplica a toda la institución, esto incluye a empleados, dirigentes, proveedores, clientes, servicios de **Tics**.

Inicialmente se ha sesgado esta política para implementar controles de seguridad para asegurar los equipos computacionales de ataques de virus y malware.

4. Política de protección contra código malicioso y descargable

- Todos los equipos computacionales deben contar con una solución antivirus (gratuita o pagada) que garantice la protección de los equipos de ataques de virus y/o malware.
- Todos los equipos de personal externo que necesite tener acceso a la red corporativa debe ser revisado con un antivirus que tenga actualizada la base de definiciones de virus.
- Toda unidad de almacenamiento (pendrives, celulares, disco externos, etc) cuando se necesite ser conectada a un equipo de la empresa debe ser previamente revisado por el antivirus.
- Cualquier archivo que sea descargado por correo electrónico o internet debe ser revisado por el antivirus
- El uso de correo electrónico, Internet y servidores de datos deben cumplir con las políticas respectivas:
  - SGSI.POL.01.02 (Política de uso correcto de Correo Electrónico)
  - SGSI.POL.01.03 (Política de uso correcto de Internet)
  - SGSI.POL.01.04 (Política de uso correcto de Servidores de Archivos)

Elaborado por: Ing. Christian Vargas Departamento de Tics	**Revisado por:** Ing. Luis Alfredo Andaluz Responsable de Tics	**Aprobado por:** Ing. Juan Carlos Peña Gerente General

Anexo 03. Documento SGSI.POL.01.02 - Política de Uso correcto de correo electrónico

POLITICA DE USO CORRECTO DE CORREO ELECTRONICO					
CÓDIGO	: SGSI.POL.01.02	**APLICACIÓN**	: Toda la Institución	**PÁGINA:**	TASESA CONTAINER TERMINAL
VERSIÓN	: 001	**FECHA**	: 06-ENE-2016	**1** de **3**	

1. Definiciones

Las definiciones de los términos utilizados se encuentran en el documento SGSI.MAN.01.00 (Manual de definición de términos usados en los documentos).

2. Objetivo

Exponer y aclarar que el uso del correo electrónico debe ser utilizado para actividades netamente de la empresa, y exponer las directrices de las responsabilidades que se adquieren al tener una cuenta de correo electrónico así como de lo que se debe y no se debe hacer en el uso de este servicio

3. Alcance

Esta política se aplica a toda la institución, esto incluye a empleados, dirigentes, servicios de Tics.

4. Política de uso correcto de correo electrónico.

- Todo empleado que necesite comunicarse tanto internamente como externamente deberá tener asignada una cuenta de correo electrónico.
- El único medio de comunicación de correo electrónico valido de actividades o asuntos de la empresa deberá ser con una cuenta de correo corporativa que identifique plenamente al usuario.
- Bajo ningún motivo se deben utilizar cuentas de correo personales de servicios gratuitos de correo electrónico (Google, Hotmail, Yahoo!, etc.) para actividades relacionadas a la empresa.
- No se deben descargar y mucho menos ejecutar archivos de dudosa procedencia o de emisores desconocidos.
- El envío de información propia de la empresa ya sea por archivos, texto en el cuerpo del mensaje, transcripción de información, o cualquier otro medio, debe ser exclusivamente para las personas que necesitan y deben tener acceso a esa información, con esto se cumple el atributo de la información de confidencialidad.
- Se prohíbe la salida de información de la empresa a cuentas personales de correo electrónico o cualquier otra persona que no sea de la institución.

Elaborado por: Ing. Christian Vargas Departamento de Tics	**Revisado por:** Ing. Luis Alfredo Andaluz Responsable de Tics	**Aprobado por:** Ing. Juan Carlos Peña Gerente General

- Solo se deben adjuntar archivos que sean para uso de alguna actividad o trabajo específico de la empresa.
- No se deben pasar archivos de música, video, programas o cualquier otro archivo que no sea propio de la actividad de la empresa y de las funciones de los empleados.
- El usuario, es responsable ante la institución, del daño que se le pudiera ocasionar a un equipo de cómputo por contaminación de virus informático en los casos que no haya cumplido con esta politica.
- Cada empleado que tenga asignada una cuenta de correo será el único responsable del contenido y adjuntos que sean enviados, e incluso responsable de seleccionar correctamente los remitentes del correo electrónico.
- El correo electrónico se debe utilizar exclusivamente para las actividades laborales no debe usarse para otra finalidad.
- Todos los correos electrónicos pueden ser conservados el tiempo que se determine por reglamentación tanto interna como externa.
- Los correos electrónicos deben ser conservados en el almacenamiento del equipo de cómputo asignado a los empleados, y cada empleado será el responsable del almacenamiento de sus archivos de correo.
- Los respaldos de los correos deben ser administrados por el responsable de Tics.
- Cada empleado deberá tener asignado una cuenta de correo la misma que debe ser creada de manera que pueda identificarse plenamente al empleado, logrando que se cumpla con el atributo de la información que es el no repudio.
- En el caso que se reciba un correo con un emisor y/o archivo adjunto desconocido, se deberá notificar al responsable de Tics y colocar el correo en la bandeja de no deseados, para una posterior revisión y acciones de control en el servidor de correo para evitar que lleguen estos correos.
- No se deben enviar correos masivos de ninguna índole ni internamente, ni externamente.
- Los mensajes contenidos en los correos electrónicos deberán cumplir con la moral y ética. Y bajo ningún motivo enviar imágenes o texto que contengan contenido de sexo, violencia, otro tipo de contenido que afecte a la moral, ética e integridad de las personas u cualquier otro mensaje contrario a las leyes nacionales e internacionales.

- La persona encargada de administrador el correo electrónico debe:
  - Accesar a los correos electrónicos SOLO cuando fuese solicitado o requerido por el propietario de la cuenta de correo de manera escrita e indicando el motivo por el cual lo requiere, o en su defecto, cuando sea justificado el acceso por una autoridad competente (entidad jurídica por ejemplo como un juez) para una acción o evento especifico.
  - Velar por la disponibilidad del servicio, realizando los mantenimientos respectivos y gestionando oportunamente los requerimientos necesarios para mantener funcionando correcta y óptimamente el servicio.
  - No podrá leer, copiar, borrar, reenviar, divulgar o alterar mensajes de terceros sin el conocimiento y aceptación por escrito del emisor o destinatario, justificando la acción requerida.

Anexo 04. Documento SGSI.POL.01.03 - Política de Uso correcto de internet

POLITICA DE USO CORRECTO DE INTERNET					
CÓDIGO	: SGSI.POL.01.03	**APLICACIÓN**	: Toda la Institución	**PÁGINA:**	TASESA CONTAINER TERMINAL
VERSIÓN	: 001	**FECHA**	: 06-ENE-2016	**1** de **2**	

1. Definiciones

Las definiciones de los términos utilizados se encuentran en el documento SGSI.MAN.01.00 (Manual de definición de términos usados en los documentos).

2. Objetivo

Exponer y aclarar que el uso del internet debe ser utilizado para actividades netamente de la empresa, y exponer las directrices de las responsabilidades que se adquieren al tener acceso a Internet así como de lo que se debe y no se debe hacer en el uso de este servicio

3. Alcance

Esta política se aplica a toda la institución, esto incluye a empleados, dirigentes, proveedores, clientes y servicios de Tics.

Y debe ser contemplado para cualquier dispositivo fijo o móvil con capacidad de navegación de internet, así como equipos computacionales., que sea usado dentro de las instalaciones y en el caso que el medio utilizado sea la red inalámbrica corporativa también contemplará el perímetro de las instalaciones de la empresa donde tenga alcance esta red.

4. Política de uso correcto de internet.

- El acceso de internet será controlado por el responsable de Tics.
- Sólo se le dará acceso a internet a los usuarios que las actividades de sus labores requieran accesar internet.
- El uso de internet solo deberá ser utilizado para actividades propias de la institución
- No se debe usar el internet para la navegación de sitios para adultos, sitios que tengan contenido sexual, redes sociales y cualquier sitio que no sea de actividades laborales institucionales
- El responsable de Tics debe tener una solución que permita controlar de manera centralizada los accesos de internet, ya sea por uso de proxys gratuitos o pagados o cualquier otra solución que como mínimo controle y regule los accesos a páginas con contenido no apropiado al uso de las actividades de la empresa.

Elaborado por: Ing. Christian Vargas Departamento de Tics	**Revisado por:** Ing. Luis Alfredo Andaluz Responsable de Tics	**Aprobado por:** Ing. Juan Carlos Peña Gerente General

- Todos los equipos computacionales que tengan acceso a internet utilizando la red corporativa de la empresa deben ser configurados y pasar por la solución mencionada en el ítem anterior.

- Para el uso de internet en los equipos computacionales solo deberá ser a través de la solución implementada por el responsable de Tics, exceptuando las tablets o Smartphone propios del empleado.

- Queda prohibido dentro de las instalaciones de la empresa el uso de soluciones de internet portátil como: Mifi, módems inalámbricos o cualquier otro servicio que provea de internet.

- En los casos que los empleados, clientes, directivos, proveedores tengan un equipo móvil (Smartphone o Tablet) con o sin acceso de internet; queda terminante prohibido capturar (en imagen, video, audio o cualquier otro medio de reproducción) a las personas, documentos, o cualquier acción u objeto que esté en las instalaciones de la empresa.

- Todos los empleados que tengan acceso a internet en cualquiera de los equipos definidos en el alcance de este documento son responsables del uso correcto de Internet y se sujetaran a las acciones y sanciones de los directivos de la empresa como de las entidades externas según amerite el caso.

- Bajo ningún concepto se debe accesar a sitios que promuevan la piratería de software, música o cualquier otro producto/servicio; y mucho menos descargar archivos que puedan comprometer la seguridad de los equipos.

- El empleado es responsable de los daños tanto físicos como lógicos en caso de haber hecho caso omiso de los lineamientos de este documento, y se deberá atener a las sanciones respectivas.

- El responsable de Tics tendrá entre sus actividades y responsabilidades:

  - Podrá bloquear y/o limitar el acceso de Internet a los empleados o proveedores que accesen a internet utilizando la red corporativa.

  - Deberá controlar que el acceso a Internet sea utilizando la solución para controlar el acceso a Internet.

  - Podrá prohibir el acceso a los sitios web de cuentas de correo electrónico (Gmail, Hotmail, Yahoo!, etc) ajenas a la cuenta corporativa propia.

  - Velar por la disponibilidad del servicio, realizando los mantenimientos respectivos y gestionando oportunamente los requerimientos necesarios para mantener funcionando correcta y óptimamente el servicio.

Anexo 05. Documento SGSI.POL.01.04 - Política de Uso correcto de servidores de archivos

POLITICA DE USO CORRECTO DE SERVIDORES DE ARCHIVOS					
CÓDIGO	: SGSI.POL.01.04	**APLICACIÓN**	: Toda la Institución	**PÁGINA:**	TASESA CONTAINER TERMINAL
VERSIÓN	: 001	**FECHA**	: 06-ENE-2016	**1** de **2**	

1. Definiciones

Las definiciones de los términos utilizados se encuentran en el documento SGSI.MAN.01.00 (Manual de definición de términos usados en los documentos).

2. Objetivo

Exponer y aclarar que el uso de las carpetas compartidas que se creen en los servidores solamente son para uso de actividades propias de la empresa, y exponer el correcto uso de la información que debe ser almacenada en los servidores indicando los lineamientos de lo que se debe y no se debe almacenar.

3. Alcance

Esta política se aplica a toda la institución, esto incluye a empleados, dirigentes, servicios de Tics.

4. Política de uso correcto de servidores de archivos.

- Las únicas carpetas compartidas que deben existir en la empresa son las que se encuentren en los servidores y creadas por el responsable de Tics, ningún usuario debe compartir carpetas en sus equipos computacionales.
- La información que se almacene en las carpetas compartidas debe ser de uso exclusivo de actividades propias de la empresa.
- Bajo ningún concepto se debe copiar archivos de música, video, programas ajenos a la institución, ni cualquier otro archivo que no sea de uso exclusivo de las actividades de la empresa.
- Los empleados son los responsables de los daños tanto lógicos como físicos que ocurran por almacenar y/o ejecutar archivos que no son los permitidos en este documento.
- No se debe extraer información para uso personal o cualquier uso ajeno a las actividades de la empresa.
- Los únicos autorizados a realizar respaldos en los servidores serán el o los responsables de Tics.
- La persona encargada de administrador el servidor de archivos debe:

POLITICA DE USO CORRECTO DE SERVIDORES DE ARCHIVOS					
CÓDIGO	: SGSI.POL.01.04	**APLICACIÓN**	: Toda la Institución	**PÁGINA:**	TASESA CONTAINER TERMINAL
VERSIÓN	: 001	**FECHA**	: 06-ENE-2016	**2** de **2**	

- Verificar la capacidad de los servidores así como supervisar que los usuarios estén usando correctamente este recurso.
- Velar por la disponibilidad del servicio, realizando los mantenimientos respectivos y gestionando oportunamente los requerimientos necesarios para mantener funcionando correcta y óptimamente el servicio.
- Deberá realizar los respaldos necesarios para asegurar la disponibilidad de la información que se encuentre almacenada en los servidores.

Elaborado por: Ing. Christian Vargas Departamento de Tics	**Revisado por:** Ing. Luis Alfredo Andaluz Responsable de Tics	**Aprobado por:** Ing. Juan Carlos Peña Gerente General

Anexo 06. Test Inicial de SGSI

TEST INICIAL

FECHA EMISIÓN INFORME
11/01/2016

5. POLÍTICAS DE SEGURIDAD

5.1. Política de Seguridad

5.1. Documento de Política de Seguridad de la Información
ESTADO ACTUAL: INICIADO

Pregunta:	Respuesta:
- ¿Establece un marco para la definición de los objetivos globales de seguridad?	No
- ¿Se ha considerado,para su elaboración, los riesgos a los que está expuesta la organización?	Si
- ¿Establece las directrices y principios de seguridad más importantes para la Dirección?	Si
- ¿Existe un documento de política de seguridad disponible para todos los usuarios aprobado por Dirección?	No

5.1.2. Revisión de la política de seguridad de la información
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Se hacen revisiones regulares de la política de seguridad?	Si

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Organización de la seguridad de la información

6.1.1. Comisión de gestión de la seguridad de la información
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un comité de seguridad que trate las cuestiones de seguridad?	No
- ¿Están definidas las responsabilidades y funciones del Comité?	No
- ¿Revisa y aprueba la política de seguridad?	No

6.1.2. Coordinación de la seguridad de la información
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un comité donde estén representadas las áreas mas importantes de la organización?	No
- ¿Se coordinan las medidas de seguridad entre los distintos departamentos?	No
- ¿Asegura el comité que las actividades de seguridad son ejecutadas de acuerdo con la política de seguridad de la información?	No

6.1.3. Asignación de las responsabilidades sobre Seguridad de la Información
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Están definidas las responsabilidades para proteger y controlar la información y los sistemas?	No

6.1.4. Proceso de autorización de recursos para el tratamiento de la información
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existe un proceso de autorización de la dirección para instalar nuevos equipos o aplicaciones?	No

6.1.5. Acuerdos de confidencialidad
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Firman los empleados un acuerdo de confidencialidad?	No

6.1.6. Contacto con las autoridades
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Suele su empresa mantener contacto con autoridades especialistas de seguridad?	No

6.1.7. Contacto con grupos de interés especial
ESTADO ACTUAL: INICIADO

Pregunta:	Respuesta:
- ¿Suele su empresa pertenecer a grupos de interés, foros, o asociaciones de seguridad externos?	Si

6.1.8. Revisión independiente de la Seguridad de la Información
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se realizan revisiones independientes de la implantación de la seguridad?	No

6.2. Partes Externas

6.2.1. Identificación de riesgos relativos a partes externas
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se han identificado los tipos de acceso y los motivos por los que terceros puedan acceder a los sistemas o la información de la organización?	No

6.2.2. Direccionamiento de la seguridad en el trato con los clientes
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están definidos los requerimientos de seguridad antes de dar accesos al cliente a los activos o información de la organización?	No

6.2.3. Direccionamiento de la seguridad en los contratos con terceros
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están definidos en los contratos subcontratación los requisitos de seguridad de la organización subcontratada?	No

7. GESTIÓN DE ARCHIVOS

7.1. Gestión de Activos

7.1.1. Inventario de Activos
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existen y se mantienen actualizados	No

inventarios de los activos del sistema de información?

7.1.2. Propiedad de los activos
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se han registrado los propietarios de todos los activos del sistema de información?	Si

7.1.3. Uso aceptable de los activos
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Están definidas y documentadas las reglas del uso aceptable de activos de sistemas de información?	Si

7.2. Clasificación de la Información

7.2.1. Guía de clasificación
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un esquema para clasificar la información y los sistemas en función de su confidencialidad o importancia?	No

7.2.2. Marcado y tratamiento de la información
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen procedimientos para identificar y usar la información, en base al esquema de clasificación?	No

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

8.1. Previo a la contratación

8.1.1. Funciones y Responsabilidades
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se incluyen en la definición del puesto de trabajo las responsabilidades de seguridad de cada cual?	No

8.1.2. Investigación de antecedentes
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se verifica que son ciertos los datos aportados en el CV que aporta el personal, cuando solicita un puesto de trabajo?	No

8.1.3. Términos y condiciones de contratación
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están establecidas las responsabilidades relativas a la seguridad en los términos y condiciones del contrato de trabajo?	No

8.2. Durante la contratación

8.2.1. Gestión de responsabilidades
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se asegura que las responsabilidades relativas a la seguridad de cada cual son aplicadas?	No

8.2.2. Concienciación, educación y formación en seguridad de la información
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Reciben los empleados y usuarios de terceras partes la formación apropiada, relativa a políticas y procedimientos de seguridad?	No

8.2.3. Proceso disciplinario
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un proceso disciplinario para tratar las violaciones realizadas por los empleados, de las políticas y procedimientos de seguridad?	No

8.3. Finalización o cambio de puesto de trabajo

8.3.1. Finalización de responsabilidades
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están definidos y asignados claramente las responsabilidades de los empleados y usuarios de terceras partes a la finalización de la contratación?	No

8.3.2. Retorno de activos
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se asegura la devolución de todos los activos de la organización en posesión de los empleados y usuarios de terceras partes a la finalización de la contratación o acuerdo?	No

8.3.3. Retirada de derechos de acceso
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se asegura la retirada de los derechos de acceso de los empleados y usuarios de terceras partes a ala finalización de la contratación o acuerdo?	No

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un perímetro de seguridad para proteger las áreas donde estas los sistemas?	No

9.1.2. Controles físicos de entrada
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están las áreas de seguridad protegidas por controles de entrada, para permitir el acceso sólo al personal autorizado?	No

9.1.3. Seguridad de oficinas, despachos y recursos
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están protegidos las oficinas y despachos que tienen algún requerimiento de seguridad especial?	No

9.1.4. Protección contra las amenazas externas y entorno
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están protegidas las áreas de seguridad contra incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales u origen humano?	No

9.1.5. Trabajo en áreas seguras
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen controles físicos especiales para trabajar en las áreas de seguridad?	No

9.1.6. Áreas de acceso publico , de carga y descarga
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están las áreas de entradas y salidas de mercancías aisladas del área de sistemas?	No

9.2. Seguridad de los equipos

9.2.1. Instalación y protección de equipos
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Están los equipos situados o protegidos para reducir las opciones de acceso no autorizado?	Si

9.2.2. Instalaciones de suministro
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están protegidos los equipos contra fallos de suministro (electricidad, agua, alcantarillado, calefacción, aire acondicionado)?	No

9.2.3. Seguridad de cableado
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están protegidos contra daños o escuchas los cables que trasmitan datos o soporten servicios de información?	No

9.2.4. Mantenimiento de equipos
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Se mantienen los equipos en base a las recomendaciones del fabricante y/o procedimientos documentados?	No

9.2.5. Seguridad de los equipos fuera de los locales de la organización
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se borra la información de los equipos antes de reutilizarlos?	No

9.2.6. Seguridad en la reutilización o eliminación de equipos
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se borra la información de los equipos antes de reutilizarlos?	No

9.2.7. Extracción de pertenencias
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se necesita una autorización para sacar de las oficinas equipos, información o software?	No

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1. Responsabilidades y procedimientos operacionales

10.1.1. Procedimientos operacionales documentados
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están documentados y mantenidos los procedimientos operacionales?	No

10.1.2. Gestión de cambio
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están controlados los cambios de los sistemas y aplicaciones?	No
- ¿Se identifican, registran, planifican y prueban los cambios significativos antes de pasarlos a producción?	No
- ¿Se evalúan los impactos potenciales?	No
- ¿Existe un proceso formal de aprobacion de los cambios propuestos?	No
- ¿Existe un proceidmiento para abortar y recuperar los cambios?	No

10.1.3. Segregación de tareas
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están segregadas las tareas, para reducir la oportunidad de o malos usos de los sistemas?	No

10.1.4. Separación de los recursos de desarrollo , ensayo y operacionales
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están separadas las áreas de desarrollo y pruebas de as de los sistemas en operación?	No

10.2.2. control y revisión de los servicios por tercera parte
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se han identificado e incorporado al contrato los riesgos antes de utilizar servicios de empresas externas?¿Se revisan y auditan periodicamente los informes y registros suministrados por el proveedor del servicio?	No

10.2.3. Gestión de cambios de los servicios por tercera parte
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se controlan los cambios de servicios de terceras partes que afectan a política, procedimientos y controles de seguridad, en especial a los procesos críticos de negocio y al análisis de riesgos?	No

10.2. Gestión de entrega del servicio por tercera parte

10.2.1. Entrega de servicio
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se controla que las terceras partes cumplen con los acuerdos alcanzados sobre los controles de seguridad que deben implantar y los niveles de servicio?	No

10.3. Sistemas de planificación y aceptación

10.3.1. Gestión de la capacidad
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se controla la necesidad de aumentar la potencia eléctrica y la capacidad de proceso y almacenamiento?	No

10.3.2. Aceptación del sistema
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen criterios de aceptación para nuevos sistemas, ampliaciones o nuevas versiones antes de aceptarlos?	No

10.4. Protección contra código malicioso y ambulante

10.4.1. Controles contra código malicioso
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existen procedimientos implantados para proteger a la empresa contra software malicioso?	No

10.4.2. Controles contra código ambulante
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existen procedimientos implantados para proteger a la empresa contra código móvil?	Si

10.5. Copias de seguridad

10.5.1. Información de copias de seguridad
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Se hacen regularmente copias de seguridad?	Si
- Se tiene definidos los datos sensibles y la periocidad de los respaldos?	No

10.6. Gestión de la seguridad de las redes

10.6.1. Controles de red
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se ha implantado algún tipo de control para mantener la seguridad en la red?	No

10.6.2. Seguridad de los servicios de red
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están documentados los atributos de seguridad de todos los servicios de red?	No

10.7. Manejo de los soportes

10.7.1. Gestión de los soportes desmontables
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Hay procedimientos para gestionar soportes removibles con información cono discos, CDS, informes impresos?	Si

10.7.2. Retirada de soporte
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Han desarrollado procedimientos para asegurar el archivo y la destrucción de los soportes informáticos?	No

10.7.3. Procedimiento de tratamiento de la información
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen procedimientos para manejar y almacenar la información, que la proteja de malos usos?	Si

10.7.4. Seguridad de la documentación del sistema
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está la información y los documentos del sistema protegidos de accesos no autorizados?	No

10.8. Intercambio de información

10.8.1. Políticas y procedimientos de intercambio de información
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están documentadas las políticas, procedimientos medidas para intercambio de información a través de todos los tipos formas de comunicación?	No

10.8.2. Acuerdos de intercambio
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se han establecido acuerdos con otras empresas para intercambiar información o aplicaciones?	No

10.8.3. Soportes físicos en transito
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se toma alguna medida especial con los soportes en tránsito con información sensible?	No

10.8.4. Envío de mensajes electrónicos
ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existe una política para el uso del correo electrónico?	Si

10.8.5. Sistemas de información del negocio
ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se han establecido políticas y directrices para controlar los riesgos de seguridad asociados con los sistemas dentro de las oficinas?	No

10.9. Servicios de comercio electrónico

10.9.1. comercio electrónico

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está protegido el comercio electrónico contra actividades fraudulentas (EDI, Email, transacciones on line, etc.)	No

10.9.2. Transacciones On-line

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está protegida las transacciones online contra transmisiones, incompletas, mal enrutamiento, modificación, divulgación o duplicación no autorizada del mensaje?	No

10.9.3. Información públicamente disponible

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un proceso de autorización, para validar la información publica de la empresa antes de publicarla?	No

10.10. Seguimiento

10.10.1. Registro de auditoria

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se mantienen durante un periodo de tiempo determinado los registros del sistema para su monitorización futuras del control de acceso?	No

10.10.2. Seguimiento del uso del sistema

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen procedimientos para monitorizar el uso de servicios de proceso de información?	No

10.10.3. Protección de los registros de información.

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está protegida contra sabotaje y accesos no autorizados los logs de sistemas de información?	No

10.10.4. Diario de operaciones y administración

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se registran y revisan regularmente las actividades de los administradores y operadores?	No

10.10.5. Registro de fallos

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se registran, analizan y aplican las acciones apropiadas a los fallos de sistemas?	No

10.10.6. Sincronización del reloj

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están sincronizados todos los relojes de los ordenadores?	No

11. CONTROL DE ACCESO

11.1. Requisitos de negocio para el control de acceso

11.1.1. Políticas de control de acceso

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están documentados las reglas y los derechos de acceso de los usuarios y los grupos?	No

11.2. Gestión de acceso de usuario

11.2.1. Registro de usuario

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Quedan registrados los accesos de los usuarios a los servicios y sistemas?	No

11.2.2. Gestión de privilegios

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está controlada la gestión de privilegios?	No

11.2.3. Gestión de contraseñas del usuario

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un proceso para la gestión de passwords?	No

11.2.4. Revisión de derechos de acceso de usuario

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se revisan periódicamente los derechos de acceso de los usuarios?	No

11.3. Responsabilidades del usuario

11.3.1. Uso de contraseñas

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se indica a los usuarios que sigan buenas prácticas en la seleción y uso de passwords?	No

11.3.2. Equipo de usuario desatendido

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se solicita a los usuarios adoptar medidas de protección con los equipos desatendidos?	No

11.3.3. Política de puesto de trabajo despejado y pantalla limpia

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe una política de pantallas y mesas limpias para los entornos de trabajo (p.e. no dejar documentos sobre las mesas, o el ordenador sin salva pantallas, etc.)?	No

11.4. Control de acceso de red

11.4.1. Política de uso de los servicios de red

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está garantizado que los usuarios solo pueden	No

acceder a los servicios para los que tienen autorización?

11.4.2. Autentificación de usuario para conexiones eternas

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están autenticadas las conexiones de los usuarios remotos?	No

11.4.3. Identificación de equipo en las redes

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se identifican automáticamente los terminales, para autenticar la conexiones a localizaciones específicas y a equipos portátiles?	No

11.4.4. Diagnostico remoto y configuración de la protección de puerto

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están controlados los accesos a los puertos de diagnóstico de los equipos del sistema?	No

11.4.5. Segregación de redes

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está la red segmentada por los grupos usuarios y servicios	No

11.4.6. Control de la conexión de red

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está controlada la capacidad de conexión de los usuarios en redes compartidas?	No

11.4.7. Control del direccionamiento de red

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Tienen controles que verifiquen las direcciones de origen y destino de las conexiones en las redes compartidas?	No

11.5. Control de acceso al sistema operativo

11.5.1. procedimientos de entrada seguros

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿El acceso a los sistemas se realiza mediante un logon seguro?	No

11.5.2. Identificación y autentificación de usuario

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Tiene cada usuario un identificador único?	No

11.5.3. Sistema de gestión de contraseñas

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Tiene algún sistema de gestión de password que dé passwords difíciles de romper?	No

11.5.4. Uso de los recursos del sistema

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están restringidos y controlados los programas de utilidades del sistema?	No

11.5.5. Tiempo de la conexión de la sesión

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen procedimientos y mecanismos para asegurar que se desconecten los terminales inactivos en localizaciones de riesgo?	No

11.5.6. Limitación de tiempo de conexión

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen restricciones en las horas a las que se realizan conexiones a aplicaciones de alto riesgo, así como en su duración?	No

11.6. Control de acceso a la aplicación y a la información

11.6.1. Restricción de acceso a la información

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Esta restringido el acceso a la información y funciones del sistema de aplicación?	No

11.6.2. Aislamiento del sistema sensible

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están en un entorno aislado y dedicado los sistemas con información sensible?	No

11.7. Ordenadores portátiles y tele trabajo

11.7.1. Ordenadores y comunicaciones móviles

ESTADO ACTUAL: INICIADO

Pregunta:	Respuesta:
-	

11.7.1. Ordenadores y comunicaciones móviles

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existe una política y los controles para la protección contra el riesgo de trabajar con portátiles?	No

11.7.2. tele trabajo

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen políticas y procedimientos para autorizar y controlar las actividades de tele trabajo?	No

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

12.1. Requisitos de seguridad de los sistemas de información

12.1.1. Análisis y especificación de los requisitos de seguridad

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se especifican los controles de seguridad necesarios para nuevos sistemas o mejoras de los actuales,p.e. adquisición o desarrollo de nuevo software?	No

12.2. Procesamiento correcto en las aplicaciones

12.2.1. Validación de los datos introducidos

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se validan los datos introducidos a las aplicaciones?	No

12.2.2. Control del procesamiento interno

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen chequeos de validación incorporados en el sistema para detectar corrupciones de los datos procesados?	No

12.2.3. Integridad de los mensajes

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se ha implantado algún sistema de autenticación de mensajes?	No

12.2.4. Validación de los datos resultantes

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se valida la salida de datos de la aplicación del sistema para garantizar que el procesamiento de la información almacenada es correcto?	No
- ¿Se definen las responsabilidades del personal que interviene en el proceso de salida de datos?	No

12.3. Controles criptográficos

12.3.1. Política acerca del uso de controles criptográficos

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe una política de uso de controles de cifrado para la protección de la información?	No
- ¿Se usan controles criptográficos para alcanzar objetivos de seguridad, p.e. confidencialidad: uso de encriptación para proteger información sensible o crítica, tanto si se almacena o se transmite.?	No
- ¿Se han considerado herramientas criptográficas para protección de información sensible transportada en soportes móviles o a traves de líneas de comunicación?	No

12.3.2. Gestión de las claves

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se protegen las claves de los usuarios para evitar el uso fraudulento?	No
- ¿Se utiliza algún sistema de gestión de claves para soportar el uso de técnicas criptográficas?	No

12.4. Seguridad de los archivos de sistemas

12.4.1. Control del software operativo

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se conservan versiones anteriores de software de las aplicaciones?	No
- ¿Existen procedimientos para controlar la instalación de software en los S.O.?	No
- ¿Existe una estrategia de restauración antes de implementar los cambios?	No
- ¿Se consideran los riegos de contar con software sin asistencia técnica?	No
- ¿Se tienen en cuenta los requisitos empresariales para los cambios y la seguridad de la versión, p.e. introducción de nuevas funcionalidades de seguridad?	No
- ¿Se mantienen registros de auditoría de los cambios efectuados?	No

12.4.2. Protección de los datos de prueba del sistema

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿se autoriza el uso de datos de prueba en el sistema de información?	No
- ¿Se elimina la información de forma segura una vez finalizados todos los procesos de prueba?	No
- ¿Están protegidos los datos de prueba?	No

12.4.3. Control de acceso al código fuente de los programas

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Está controlado el acceso al código fuente y a los elementos relacionados(diseños, especificaciones, planes de verificación y validación)?	No
- ¿Se registra el acceso al código fuente?	No
- ¿Se encuentran inaccesibles las librerias y código fuente del personal no autorizado?	No

12.5. Seguridad en el desarrollo y procesos de asistencia técnica

12.5.1. Procedimientos de control de cambios

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se garantiza el cambio de procedimientos de usuario y operativos para que sigan siendo adecuados?	No
- ¿Se obtiene una autorización formal de las propuestas detalladas antes de iniciar al cambio?	No
- ¿Se garantiza que los cambios sólo se realicen por usuarios autorizados?	No
- ¿Se realiza una evaluación del riesgo, un análisis de los efectos del cambio y una especificación de controles de seguridad necesarios?	No
- ¿Existen procedimientos para el control de cambios?	No
- ¿Se identifica todo el software, información, bbdd y hardware que requieren modificación?	No

12.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se revisan y aprueban los sistemas de aplicación cuando se producen cambios?	No

12.5.3. Restricciones de los cambios a los paquetes de software

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se desaconsejan las modificaciones de los paquetes de software?	No

12.5.4. Fugas de información

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se utilizan productos evaluados y fiables (SW y sistemas)?	No
- ¿Se controla y chequea adquisición, uso y cambios de sw con referencia a posibles puertas traseras y códigos troyanos?	No

12.5.5. Externalización del desarrollo de software

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se aplican controles para asegurar que el desarrollo subcontratado de software cumple con las medidas de seguridad necesarias?	No
- ¿Se realizan pruebas antes de la implantación para detectar código malicioso y Troyano?	No

12.6. Gestión de la vulnerabilidad técnica

12.6.1. Control de las vulnerabilidades técnicas

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Exite un procedimiento para tratar las vulnerabilidades técnicas identificadas o notificadas para identificar posibles riesgos y actuar en consecuencia?	No
- ¿Se definen las responsabilidades del personal técnico con la gestión de vulnerabilidades?	No
- ¿Se obtiene información sobre vulnerabilidades técnicas de los sistemas de información, la exposición de la organización a tales vulnerabilidades y se toman las medidas apropiadas para tratar el riesgo asociado?	No
- ¿Se planifican revisiones periódicas de vulnerabilidades técnicas?	No
- ¿El inventario de activos incluye información del proveedor del software, números de versión, estado actual de implantación y persona/s resposnables del software en la organización?	No

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

13.1. Notificación de eventos y puntos débiles de la seguridad de la información

13.1.1. Comunicación de los eventos de seguridad de la información

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Conocen las responsabilidades en el procedimiento de comunicación de incidencias los empleados, clientes contratados y terceros?	Si
- ¿Existe un canal a través del que ese reporten los incidentes de seguridad?	Si

13.1.2. Comunicación de puntos débiles de seguridad

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Se solicita a los usuarios que comuniquen cualquier debilidad de seguridad o amenaza para el sistema?	Si
- ¿Conocen las responsabilidades en el procedimiento de comunicación de debilidades los empleados, clientes contratados y terceros?	No

13.2. Gestión de incidencias de seguridad de la información y mejoras

13.2.1. Responsabilidades y procedimientos

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Se han establecido procedimientos y responsabilidades para la gestión de incidentes?	No
- ¿Se identifican las causas de las incidencias y se registran las acciones efectuadas para su resolución?	No
- ¿Se establecen procedimientos para la gestión de diferentes tipos de incidentes de seguridad, p. e. fallos del sistema de información, pérdida de servicio, código malicioso, uso indebido del sistema de información, etc.?	No

13.2.2. Aprendizaje de los incidentes de la seguridad de la información

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Existen mecanismos funcionando, para realizar análisis del tipo, volumen y coste de los incidentes y fallos?	No

13.2.3. Recopilación de pruebas

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- Para apoyar una acción contra una persona u organización ¿Se mantienen las evidencias, conforme a las leyes y normas publicadas?	No

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

14.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

14.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un proceso establecido en la organización, para desarrollar y mantener la continuidad del negocio?	No
- ¿Identifica el Plan de Continuidad del Negocio (PCN) los recursos financieros, organizativos, técnicos y de entorno para afrontar las posibles incidentes de seguridad identificados?	No
- ¿Se documenta, se prueba y actualiza y revisa periódicamente el PCN?	No
- ¿Se identifican todos los activos que intervienen en los procesos críticos del negocio?	No

14.1.2. Continuidad del negocio y evaluación del riesgo

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:

- ¿Existe un plan estratégico, basado en la valoración de riesgos, donde se detallen las acciones para la continuidad del negocio?	No

14.1.3. Desarrollo e implantación de planes de continuidad que incluyan seguridad de la información

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se identifican los responsables de mantener y supervisar los PCN?	No
- ¿Existen procedimientos operativos que puedan seguirse hasta la recuperación y restauración de la actividad normal?	No
- ¿Están desarrollados los planes de continuidad para mantener o restaurar las operaciones del negocio y garantizar la disponibilidad de la información en un tiempo requerido después de una interrupción o fallo de procesos críticos?	No
- ¿La copia del PCN está almacenado en un lugar distinto al principal y protegida con el mismo nivel de seguridad aplicado en la ubicación principal?	No

14.1.4. Marco de referencia para la planificación de la continuidad del negocio

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un plan general de trabajo para asegurar que todos los planes son consistentes?	No
- ¿Se definien las responsabilidades de las personas que intervienen en cada plan así como los recursos necesarios para realizar procedimientos de emergencia?	No
- ¿Se definen las condiciones de activación de los planes antes de activar el plan?	No

14.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad de negocio

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se revisan los resultados de la revisión para mejorar los PCN ?	No
- ¿Se prueban regularmente los planes de continuidad de negocio para asegurar que son eficaces?	No

15. CUMPLIMIENTO

15.1. Cumplimiento de los requisitos legales

15.1.1. Identificación de la legislación aplicables

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están definidos y documentados, para cada sistema de información todos los requisitos contractuales, reguladores y estatutarios?	No

15.1.2. Derechos de propiedad intelectual

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Hay procedimientos para asegurar el cumplimiento con las restricciones legales en el uso de material referente a los derechos de propiedad intelectual y uso de productos software registrados?	No
- ¿Se limitan las copias de material con DPI exclusivamente a la creación de copias de respaldo autorizadas?	No
- ¿Se mantienen resguardos y pruebas de adquisición de material con derechos de propiedad intelectual?	No
- ¿Existe una política conocida por todos los usuarios que defina las responsabilidades de todos en el uso legal de software y productos de información?	No

15.1.3. Protección de los registros de la organización

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existe un procedimiento sobre la conservación, el almacenamiento, la manipulación, la eliminación y recuperación de registros e información?	No
- ¿Están protegidos contra pérdida, destrucción y falsificación los registros importantes?	No
- ¿Se clasifican los registros según su tipo, p.e. registros contables, de bases de datos, de autirorías, de accesos,etc., y se detalla su tiempo de conservación y medio de almacenamiento?	No

15.1.4. Protección de datos y privacidad de la información personal

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen controles eficaces para proteger la información personal en base a la legislación vigente? ¿Está adecuado a la LOPD?	No

15.1.5. Prevención del uso indebido de las instalaciones de procesamiento de la información

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Conocen todos los usuarios el alcance exacto del acceso que se les permite y detectar accesos no autorizados?	No
- ¿Firman los empleados una autorización/compromiso por escrito aceptando las restricciones a las que están sujetos para el uso del sistema de información?	No
- ¿Existe autorización de la dirección para usar el sistema para fines no relacionados con el negocio (usos personales)?	No

15.1.6. Regulación de los controles criptográficos

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Existen controles para asegurar el cumplimiento con los acuerdos nacionales para controlar el uso de cifrado?	No

15.2. Cumplimiento de políticas y normas de seguridad y cumplimiento técnico

15.2.1. cumplimiento de las políticas y normas de seguridad

ESTADO ACTUAL: INEXISTENTE

Pregunta:	Respuesta:
- ¿Se establecen acciones para resolver los incumplimientos o no conformidades detectadas?	No

- ¿Se guardan registros de las revisiones?	No
- ¿Dirección revisa periódicamente que se cumplen las políticas, procedimientos de seguridad y otros requerimientos dentro de su área de responsabilidad?	No

15.2.2. Comprobación del cumplimiento técnico

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Se realizan pruebas de intrusión o test de vulnerabilidades periódicamente?	No
- ¿Se chequean regularmente los sistemas de información para verificar el cumplimiento de las normas y procedimientos de seguridad de la información?	No

15.3. Consideraciones de la auditoria de los sistemas de información

15.3.1. Controles de la auditoria de los sistemas de información

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Están planificadas las auditorias de sistemas para reducir el riesgo de interrupciones en el proceso de negocio?	No
- ¿Se garantiza la independencia del auditor/es?	No
- ¿Se registra la realización de la auditoría y se establecen las acciones para detectar y corregir las causas de las incidencias detectadas?	No

15.3.2. Protección de las herramientas de auditoria de los sistemas de información

ESTADO ACTUAL: NADA

Pregunta:	Respuesta:
- ¿Esta protegido el acceso a los registros e informes consecuencia de auditorías?	No
- ¿Esta protegido el acceso a las herramientas de auditoria del sistema?	No

Anexo 06. Temarios para iniciar capacitación a los usuarios en Seguridad de la Información

1. Introducción a la seguridad
    a. Que es la Seguridad
    b. Que debemos Proteger
    c. Actualidad
2. Políticas de seguridad
    a. Que son las políticas y para qué sirven
    b. Políticas de seguridad
    c. Contrato de confidencialidad
    d. Políticas de Claves
    e. Recomendaciones y mejores prácticas
3. Punto de vista del Negocio
    a. Consecuencias
4. En la Organización
    a. Diferentes Amenazas
5. Correo Electrónico
    a. Que es el Spam
    b. Correos Maliciosos
    c. Uso del Correo Electrónico
    d. Amenazas y Consecuencias
6. Mensajería / Chat
    a. Virus y Troyanos
    b. Amenazas y Consecuencias

7. Navegación en Internet
    a. Que es el Phishing
    b. Sitios Maliciosos
    c. Robo de credenciales de usuarios
    d. Uso de Internet
    e. Virus y Troyanos en Internet
    f. Amenazas y Consecuencias
8. Dispositivos Móviles
    a. Uso de dispositivos móviles
    b. Virus y Troyanos
    c. Amenazas y Consecuencias