Empresa Textilera S.A

PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013

Nombre Estudiante: Paula Andrea Maya Arango

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia
Profesor responsable de la asignatura: Carles Garrigues Olivella
Centro: Universitat Oberta de Catalunya

Fecha entrega: 2016/06/06

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013*
Nombre del autor:	*Paula Andrea Maya Arango*
Nombre del consultor/a:	*Antonio José Segovia*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	06/2016
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Área del Trabajo Final:	*Sistemas de Gestión de la Seguridad de la Información*
Idioma del trabajo:	*Español*
Palabras clave	SGSI, ISO 27001:2013; Textilera

Resumen del Trabajo.

El trabajo final del master, describe los objetivos, el alcance, la expectativa del SGSI y la metodología asociada a la definición, planeación, identificación y creación del modelo de seguridad de la información para la organización Textilera S.A, basado en la norma ISO 27001:2013; iniciando desde el entendimiento de la organización desde la óptica de los procesos críticos, ejecución del diagnóstico de seguridad de la información, identificación de las principales vulnerabilidades y amenazas, aplicando una metodología de gestión del riesgos para la gestión de riesgos de seguridad de la información, planeación de los planes de tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para Textilera S.A.
El principal objetivo es sentar las bases del proceso de mejora continua y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). Para ello se abordarán las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Definición clara de la situación actual y de los objetivos del SGSI.
- Análisis de Riesgos.
    - Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.

- Identificación de amenazas, evaluación y clasificación de las mismas
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013 en la organización.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Esquema Documental del sistema de gestión de seguridad de la información.

Abstract

The final work of the master, describes the objectives, scope, the expectation of the SGSI and methodology associated with the definition, planning, identifying and creating model of information security for the organization Textilera SA, based on the ISO 27001: 2013; starting from the understanding of the organization from the perspective of critical processes, execution of diagnostic information security, identifying key vulnerabilities and threats, applying a management methodology risks risk management information security, planning of risk treatment plans and generation of documentary framework of the management system of information security for Textile SA

The main objective is to lay the foundation for continuous improvement process and propose measures to minimize the impact of potential risks actions.

The project proposes the establishment of the basis for the implementation of an SGSI (information security management system). To this end the following steps will be addressed:

• Normative documentation on best practices in information security.

• Definition of the current situation and the objectives of the SGSI.

•Risk analysis.

- Identification and valuation of corporate assets as a starting point to a risk analysis.
- Identification of threats, evaluation and classification of the same.

• Evaluation of the level of compliance with the ISO / IEC 27002: 2013 in the organization.

• Proposed projects face to achieve adequate safety management.

• Documentary Scheme management system information security.

Índice

Índice de Ilustraciones

Índice de tablas

1. Capítulo I. Introducción

1.1 Contexto y justificación del Trabajo

Entre los activos intangibles más valiosos de Textilera S.A se encuentra la información, razón que amerita su protección y la de los sistemas informáticos que la respaldan y la conservan. De hecho, las certificaciones internacionales existentes en el campo de la informática tienen entre sus propósitos, otorgarle a los procesos internos de una organización un alto estándar para conservar la información como una ventaja competitiva y en muchos casos como un secreto empresaria.

Hay que enfatizar que cuando se implementa un Sistema de Gestión de Seguridad de la Información (SGSI) para optar a la certificación ISO27001:2013, es necesario revisar y evaluar en todas las áreas de la organización los controles y procesos, con el fin de buscar estrategias que permitan no sólo obtenerla la primera vez, sino poder permanecer en el tiempo con procesos prácticos y eficientes que sean a la vez fáciles de mantener y permitan renovar la certificación sin sobrecostos o esfuerzos extraordinarios. En este mismo orden de ideas, lo primero será involucrar a todo el personal de la compañía sin importar el área a la que pertenezcan, pues son ellos los que ayudaran a implementar en la cotidianidad los sistemas de gestión y evitar que sólo se queden en documentos escritos. Algunos mecanismos para ello son las campañas de concientización sobre la seguridad de la información, la publicación de resultados y las auditorias de seguridad de la información tipo inspección para verificar el cumplimiento de políticas.

Actualmente Textilera S.A. cuenta con diferentes procesos y procedimientos en el área de tecnología que están enfocados y basados en la Norma ISO 9001, con el transcurso del tiempo estos procesos no se han modificado y se crea la necesidad de evolucionar y actualizar estos procesos a una norma más actualizada y que este enfocada en la Seguridad de la Información.

Basados en la norma ISO 27001:2013 se evaluara el estado actual de los procesos relacionados con la seguridad de la información en Textilera, realizándose un análisis de riesgos en miras a identificar y desarrollar los proyectos a generarse que le permitan la implementación de un sistema de Seguridad de la información.

Los procesos que se tiene implementado hoy en día en Textilera fueron creados para cumplir con la norma ISO 9001, hoy estos procesos deben ser actualizados y mejorados buscando la excelencia y el mejoramiento continuo.

Teniendo presente que la norma ISO 27001:2013 abarca diferentes conceptos se enfocara este proyecto en la implementación de un SGSI en Textilera S.A. teniendo presente los diferentes procesos que se tienen ya enmarcados e identificando que proyectos nuevos deben ser creados para cumplir con la norma.

1.2 Definición de objetivos del plan director de seguridad

El plan director de seguridad se define como hoja de ruta que debe seguir la compañía para conseguir gestionar de forma adecuada la seguridad en los siguientes procesos:

- División informática: Todos los procesos.
- Control interno: Proceso de pólizas, Proceso de manejo de activos, procesos de contratistas.
- Administración servicios al personal: Proceso de contratación.
- Seguridad física: Proceso de control de acceso y seguridad.

1.2.1 Objetivo General:

- Planear, diseñar y recomendar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) enfocado a los procesos de las áreas de: División informática, control interno, administración servicios al personal, seguridad física en Textilera S.A.

1.2.2 Objetivos Específicos:

- Identificar el estado actual de los procesos existentes en el área de TI, control interno: en cuanto a administración de pólizas, manejo de activos, manejo de contratistas. Administración servicios al personal: proceso de contratación. Seguridad física: control de acceso.

- Establecer controles para minimizar los riesgos significativos y de alto impacto para el negocio, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial, la alteración o modificación de la misma, y en general la continuidad de las operaciones.

- Establecer la brecha de seguridad entre los procesos y el SGSI bajo la norma ISO27001:2013.

- Establecer claramente al interior de la compañía los roles y responsabilidades en términos de Seguridad de la Información.

- Desarrollar y mantener una cultura en Seguridad de la Información orientada a la identificación y análisis de riesgos, a través de la sensibilización a los funcionarios y contratistas.

- Realizar un análisis diferencial del estado actual de seguridad de los activos de la compañía, versus el cumplimiento de la norma ISO/IEC 27001 e ISO/IEC 27002, para que a partir de este análisis se identifiquen los recursos necesarios y se puedan establecer los planes de trabajo con el fin de cumplir la norma.

1.3 ENFOQUE Y MÉTODO SEGUIDO

A medida que la seguridad se ha consolidado como una parte cada vez más importante de los sistemas de información, también lo ha ido haciendo la metodología y las 'buenas prácticas' sobre seguridad de la información.

Aun cuando son muchas las aproximaciones, nosotros nos centraremos en el estudio de la ISO/IEC 27002 (que proviene de la ISO 17799)**.** Norma ISO 27001:2013.

ISO 27001:2013 es la norma principal de la serie ISO 27000 y contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). Tiene su origen en el estándar ISO27001:2005 el cual contenía 11 anexos de la norma ISO27002:2005, ahora este nuevo estándar contiene 14 anexos con una mejor distribución de los controles y una simplificación hacia los aspectos que son realmente importantes en un SGSI para un empresa.

El SGSI permite la integración con todos los procesos actuales siendo este par de la organización y estructura de la gestión global, preservando asegurar la confidencialidad, integridad y disponibilidad; siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

Por ese motivo es que la norma ISO27001:2013 comienza definiendo el sistema de gestión que servirá de base para administrar los riesgos, antes de comenzar a tocar siquiera cuestiones relacionadas a la seguridad: sistematizar el descubrimiento, tratamiento y mitigación de los riesgos, y sostener esas actividades en el tiempo, es condición necesaria para considerarse "mínimamente seguro", con todas las dificultades que expresarlo de esa manera podría acarrear. Luego de haber implementado un sistema de gestión del riesgo, con todas las consideraciones mencionadas, incluyendo revisiones periódicas de un Comité de Seguridad que asigne recursos, verifique la implementación de los controles, propicie la mejora continua de los procesos, y ajuste políticas organizacionales que complementen las medidas de seguridad incorporándolas a un plan de capacitación y concientización para todos los

actores que interactúan con la información de la compañía, tendremos apenas un vistazo a lo que significa contar con ISO27001:2013 en una organización.

La certificación agrega un componente fundamental, que son las auditorías externas: éstas son realizadas por auditores profesionales que día a día van ganando experiencia en auditar organizaciones en distintos mercados y tipos de negocio, aportando objetividad al sistema de gestión implementado a través de las observaciones y no conformidades que detectan.

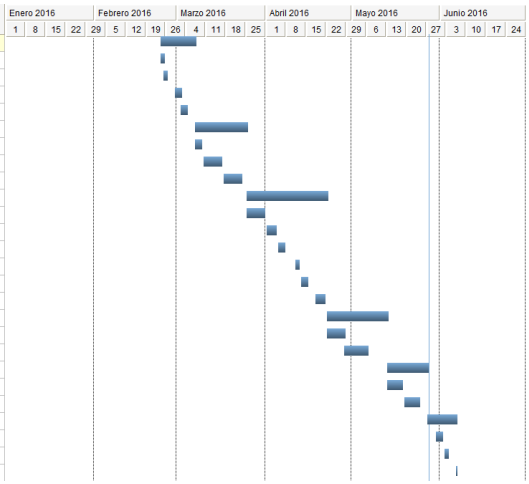
Los hallazgos se definen como resultado de la comparación entre un criterio y la situación actual encontrada en la organización donde se identifican hechos o circunstancias importantes que inciden en la gestión del sistema de gestión de seguridad de la información y que por su naturaleza merecen ser comunicados en un informe. Los hallazgos están relacionados con asuntos significativos e incluyen información (evidencia) suficiente, competente y pertinente, que surge de la evaluación practicada, generalmente los hallazgos corresponden a cualquier situación que se determina como consecuencia de la aplicación de procedimientos de auditoría, sus elementos son: condición, criterio, causa y efecto, con los hallazgos se pueden generar oportunidades de mejora, se pueden desarrollar recomendaciones, señalando la necesidad de efectuar reformas, teniendo en cuenta su análisis de las causas y efectos en las condiciones identificadas; a este respecto se debe tener en cuenta la relación costo-beneficio y los efectos positivos y negativos que podrían resultar de la implementación de la recomendación.

En un sistema de gestión ISO, es deseable que aparezcan aspectos a mejorar, ya que de otra forma para qué desearía uno contar con un sistema basado en la mejora continua, cuando solamente se realizan auditorías internas, estamos perdiendo una oportunidad inmejorable para validar la efectividad de la gestión de riesgos y de listar todas las ventajas que con seguridad contaremos luego de obtener la certificación, siendo conscientes que detrás de un certificado, hay muchos más beneficios para la organización.

1.4 Planificación del Trabajo

Para el desarrollo de este trabajo se realiza el siguiente diagrama de Gantt en el cual se describen los hitos de cada PEC, las tareas a realizar en cada una de ellas, la planificación de cada tarea.

	Nombre	Duración	Inicio	Fin	Predecesoras	Recursos
1	PEC 1.Fase 1: Situación actual: Contextualización, objetivos y aná	9d?	24/02/2016	07/03/2016		
2	Introducción al Proyecto	2d?	24/02/2016	25/02/2016		
3	Enfoque y selección de la empresa que será objeto de estudio.	2d?	25/02/2016	26/02/2016		
4	Definición de los objetivos del Plan Director de Seguridad	3d?	29/02/2016	02/03/2016		
5	Análisis diferencial de la empresa con respecto la ISO/IEC 27001	3d?	02/03/2016	04/03/2016		
6	PEC 2. Fase 2: Sistema de Gestión Documental	15d?	07/03/2016	25/03/2016		
7	Elaboración de la Política de Seguridad	3d?	07/03/2016	09/03/2016		
8	Declaración de aplicabilidad	5d?	10/03/2016	16/03/2016		
9	Documentación del SGSI	5d?	17/03/2016	23/03/2016		
10	PEC 3. Fase 3: Análisis de riesgos	21d?	25/03/2016	22/04/2016		
11	Identificación y valoración de activos	5d?	25/03/2016	31/03/2016		
12	amenazas	2d?	01/04/2016	04/04/2016		
13	vulnerabilidades	3d?	05/04/2016	07/04/2016		
14	cálculo del riesgo	2d?	11/04/2016	12/04/2016		
15	nivel de riesgo aceptable	3d?	13/04/2016	15/04/2016		
16	riesgo residual	4d?	18/04/2016	21/04/2016		
17	PEC 4. Propuesta de Proyectos	16d?	22/04/2016	13/05/2016		
18	Evaluación de proyectos que debe llevar a cabo la Organización p	5d?	22/04/2016	28/04/2016		
19	Cuantificación económica y temporal de los mismos	7d?	28/04/2016	06/05/2016		
20	PEC 5. Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2	11d?	13/05/2016	27/05/2016		
21	Evaluación de controles	4d?	13/05/2016	18/05/2016		
22	madurez y nivel de cumplimiento	4d?	19/05/2016	24/05/2016		
23	PEC 6. Fase 6: Presentación de Resultados y entrega de Informe	7d?	27/05/2016	06/06/2016		
24	Consolidación de los resultados obtenidos durante el proceso de	3d?	30/05/2016	01/06/2016		
25	Realización de los informes y presentación ejecutiva a la Direcció	2d?	02/06/2016	03/06/2016		
26	Entrega del proyecto final.	1d?	06/06/2016	06/06/2016		



Los recursos utilizados para la elaboración del proyecto:

- Fuentes documentales/libros
- Webs
- Recurso humano de Textilera S.A

1.5 Breve sumario de productos obtenidos

El Plan de Implementación de la ISO/IEC 27001:2013 es un aspecto clave en cualquier organización que desea alinear sus objetivos y principios de seguridad a la normativa Internacional de Referencia
El principal objetivo es sentar las bases del proceso de mejora continua en materia de seguridad de la Información, permitiendo a las organizaciones conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). Para ello se abordarán las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Definición clara de la situación actual y de los objetivos del SGSI.
- Análisis de Riesgos.
    - Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
    - Identificación de amenazas, evaluación y clasificación de las mismas
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013 en la organización.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Esquema Documental.

Como entregables del proyecto, deberán presentarse básicamente los productos que se especifican a continuación:

- Informe Análisis Diferencial
- Esquema Documental ISO/IEC 27001
- Análisis de Riesgos
- Plan de Proyectos
- Auditoría de Cumplimiento
- Presentación de resultados

1.6 Breve descripción de los otros capítulos de la memoria

A continuación se describe brevemente el contenido de cada fase para la elaboración del proyecto:

Fase 1: Situación actual: Contextualización y análisis diferencial

El planteamiento del proyecto será por tanto, sentar las bases de un Plan de Director de Seguridad para la empresa. Simplificando, y como iremos viendo, nuestro proceso será el siguiente:

- Analizar y detallar nuestro inventario de activos.
- Estudiar las amenazas a las que están expuestos.
- Estudiar el impacto potencial de dichas amenazas.
- Proponer un plan de acción para luchar contra dichas amenazas.
- Evaluar el impacto residual una vez aplicado el plan de acción

Contextualización
Se deberá concretar el alcance, teniendo en cuenta que lo que nos interesa son los Sistemas de Información que dan soporte a actividades, servicios o procesos de negocio de la Organización.
Análisis diferencial:
Este punto tiene como objetivo realizar un análisis diferencial de las medidas de seguridad y la normativa que tenga la Organización en relación a la Seguridad de la Información. Este análisis diferencial se realizará con respecto la ISO/IEC 27001 e ISO/IEC 27002, y nos permitirá conocer de manera global el estado actual de la Organización en relación de la Seguridad de la Información.

Fase 2: Sistema de Gestión Documental

Todos los Sistemas de Gestión se apoyan en un cuerpo documental para el cumplimiento normativo.
La propia ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el sistema, desarrollaremos los siguientes:

- Política de Seguridad
- Procedimiento de Auditorías Internas
- Gestión de Indicadores
- Procedimiento Revisión por Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos
- Declaración de Aplicabilidad

La existencia de todos estos documentos constituye evidencias palpables de que el Sistema de Gestión está funcionando.

Fase 3: Análisis de riesgos

En esta fase desarrollaremos:

- Proceso a llevar a cabo para gestión de riesgos.
- Inventario de activos
- Valoración de activos
- Dimensiones de Seguridad
- Tabla resumen de valoración
- Análisis de amenazas
- Impacto potencial
- Nivel de riesgo aceptable y residual

Fase 4: Propuesta de Proyectos

Llegados a este punto, conocemos el nivel de riesgo actual en la Organización, por lo que es el momento de plantear proyectos que mejoren el estado de la seguridad.
La descripción de las mejoras propuestas (proyectos) deberá ayudar a mitigar el riesgo actual a la organización y evolucionar el cumplimiento ISO hasta un nivel adecuado. Dichos proyectos deben derivarse de los resultados obtenidos del AARR a tenor de las recomendaciones asociadas a las amenazas identificadas.

Los proyectos planteados serán resultantes de agrupar un conjunto de recomendaciones identificadas en la fase de análisis de riesgos para facilitar su ejecución. Se incidirá no sólo en la mejora en relación con la gestión de la seguridad, sino también en posibles beneficios colaterales como puede ser la

optimización de recursos, mejora en la gestión de procesos y tecnologías presentes en la organización analizada.

Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2013

En esta fase se evaluara hasta qué punto la empresa cumple con las buenas prácticas en materia de seguridad. La ISO/IEC 27002:2013 nos servirá como marco de control del estado de la seguridad.
Para ello se establece una metodología basada en El estándar ISO/IEC 27002:2013.
Posteriormente se evaluara la madurez de la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013.
Esta estimación la realizaremos según el Modelo de Madurez de la Capacidad (CMM).

Fase 6: Presentación de Resultados y entrega de Informes
El objetivo genérico de esta fase es la generación de la documentación que aborde todo el proceso de la implementación del SGSI.

2. Capítulo II. Fases del proyecto

FASE 1: SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN Y ANÁLISIS DIFERENCIAL.

1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN DE ESTUDIO

La empresa seleccionada para la elaboración del trabajo final del Master que consiste en la elaboración de un "Sistema de Gestión de Seguridad de la Información" basados en la implementación y cumplimiento de la normativa ISO/IEC 27001: 2013 y en los controles de la normativa ISO/IEC 27002, es la empresa Textilera S.A, es una empresa ubicada en el municipio de Girardota, a 28 kilómetros de la ciudad de Medellín, Colombia. Dedicada a la industria Textil.

1.2 ACTIVIDAD Y ENTORNO

La compañía fue fundada en 1964 para la producción de polímeros y fibras sintéticas de poliamida (Nylon) y poliéster, destinados a la industria textil y como material de refuerzo para la fabricación de llantas.
Actualmente, se ha convertido en el mayor fabricante de fibras sintéticas del Grupo Andino, ampliando su oferta de productos, atendiendo también a la industria química y del plástico.

Los socios colombianos de Textilera S.A. son empresas de gran trayectoria y experiencia en los sectores textil, seguros, financiero, alimentos y comercio, liderados por el Grupo Empresarial Antioqueño, uno de los más importantes conglomerados económicos de Latino América.

Se produce y comercializa polímeros y fibras químicas de Poliéster y Nylon, materias primas para la industria, en forma de gránulos, fibras, filamentos textiles e industriales y lona para llantas. Con estos insumos cientos de empresas fabrican envases, hilos, telas no tejidas, rellenos, redes de pesca, bandas transportadoras, carpas, telas, cintas, marquillas, elásticos, llantas y muchos otros productos de excelente calidad que mejoran el nivel de vida y permiten el desarrollo de nuestro País.

1.3 TAMAÑO Y ESTRUCTURA ORGANIZACIONAL

Textil SA es una empresa con dos sedes una en el poblado y otra en Girardota y cuenta con 1600 empleados, la compañía cuenta con varias vicepresidencias.

Actualmente Textilera S.A. cuenta con diferentes procesos y procedimientos que están enfocados y basados en la Norma ISO 9001, con el transcurso del tiempo estos procesos no se han modificado y se crea la necesidad de evolucionar y actualizar estos procesos a una norma más actualizada y que este enfocada en la Seguridad de la Información.

Basados en la norma ISO 27001:2013 se evaluara el estado actual de los procesos relacionados con la seguridad de la información, realizándose un análisis de riesgos en miras a identificar y desarrollar los proyectos a generarse que le permitan el fortalecimiento del sistema de Seguridad de la información.

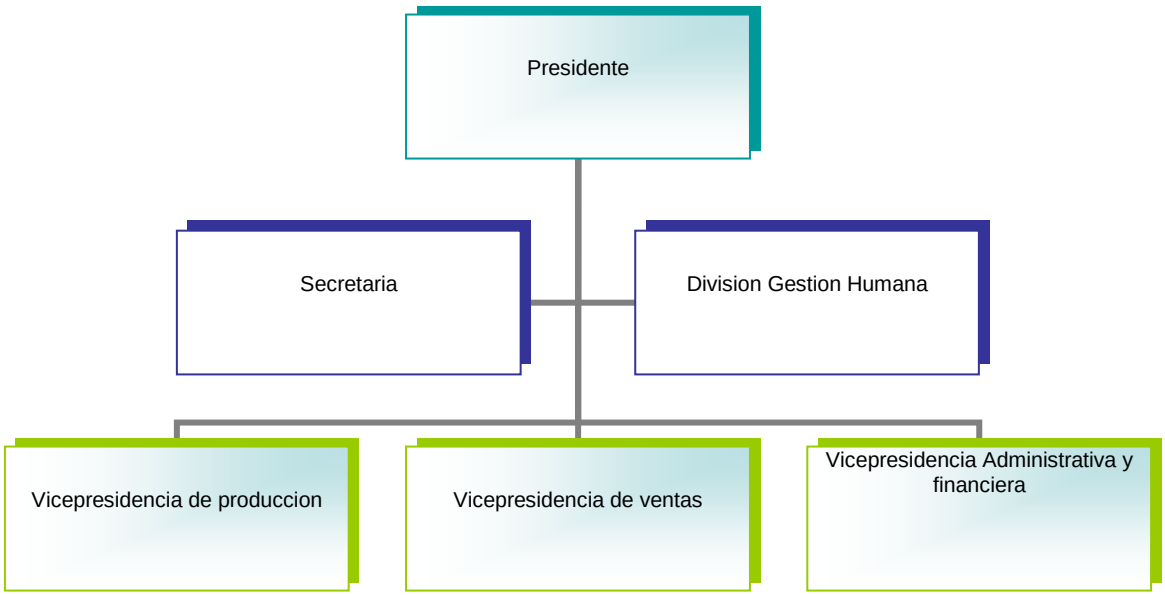


Ilustración 1. Organigrama General.

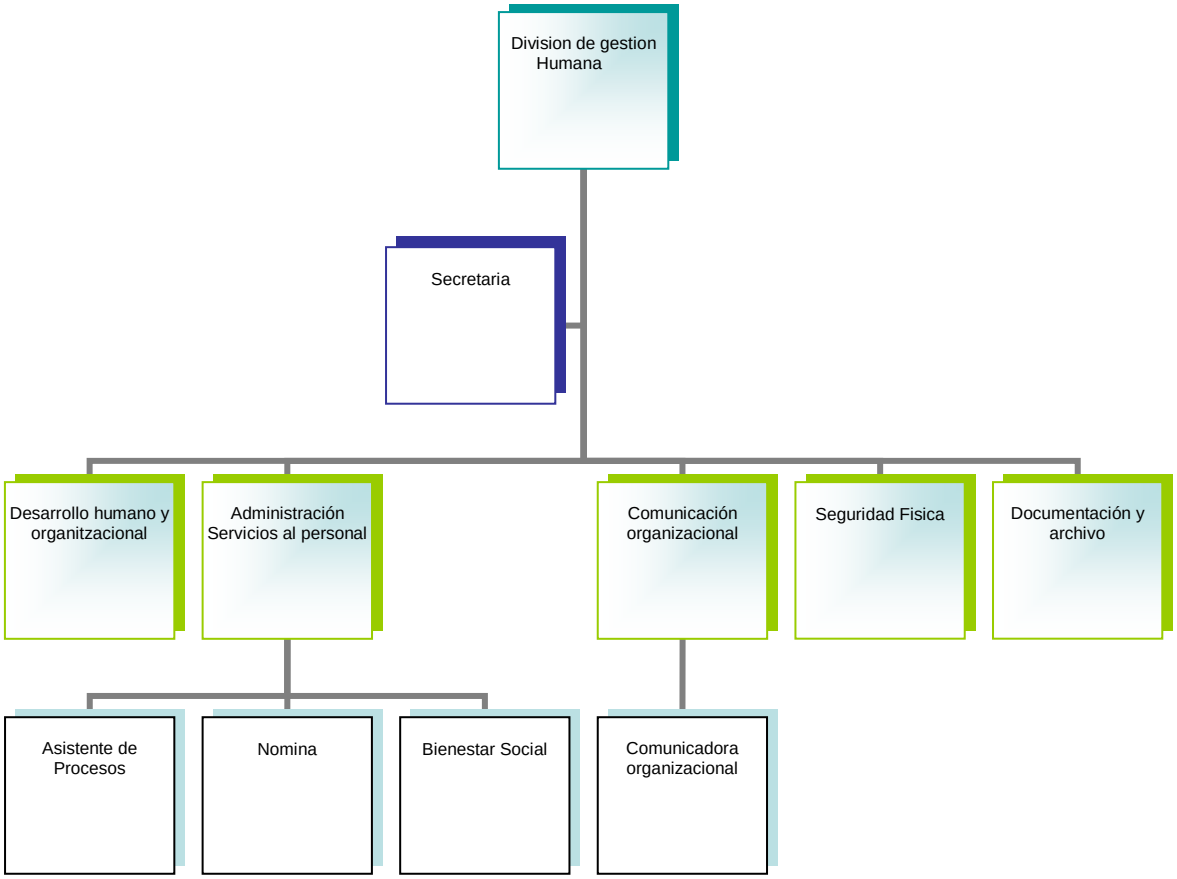


Ilustración 2. **Organigrama División Gestión Humana.**

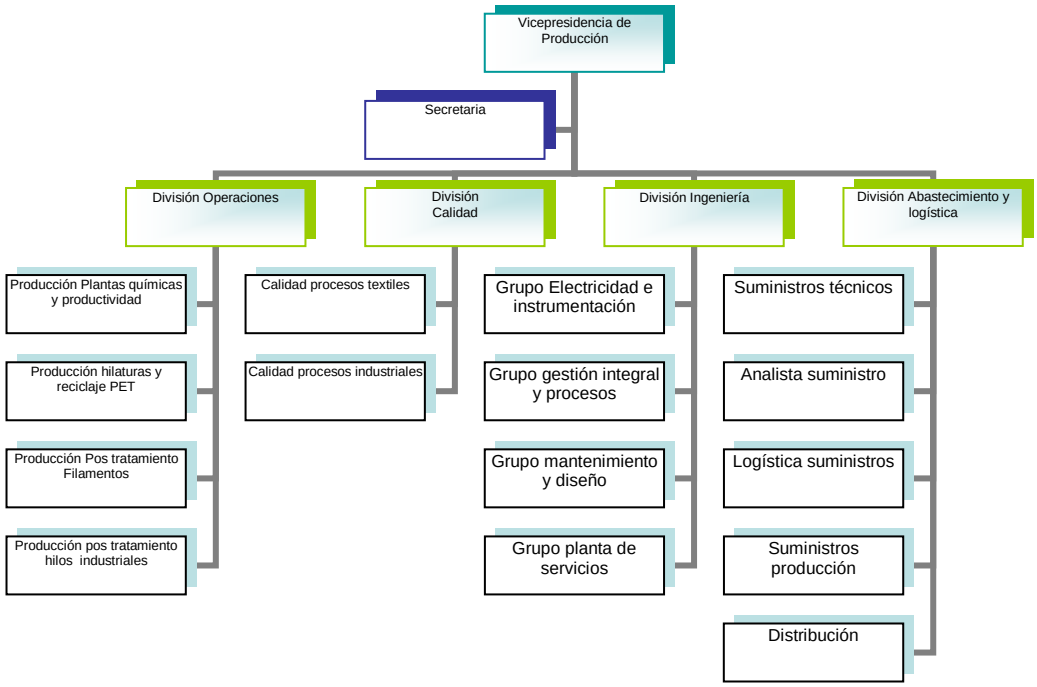


Ilustración 3. Organigrama Vicepresidencia de Producción

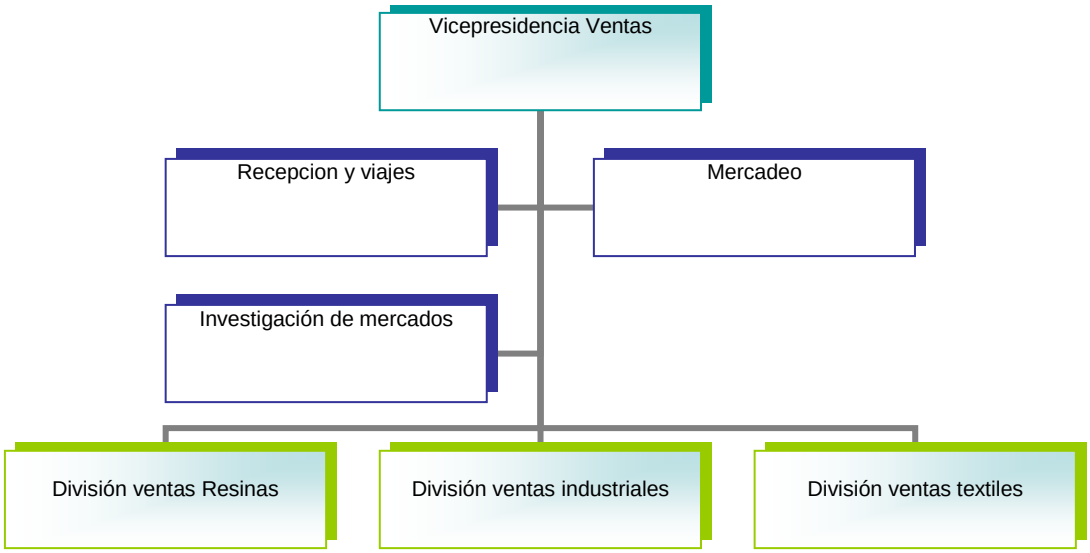


Ilustración 4. Organigrama Vicepresidencia Ventas

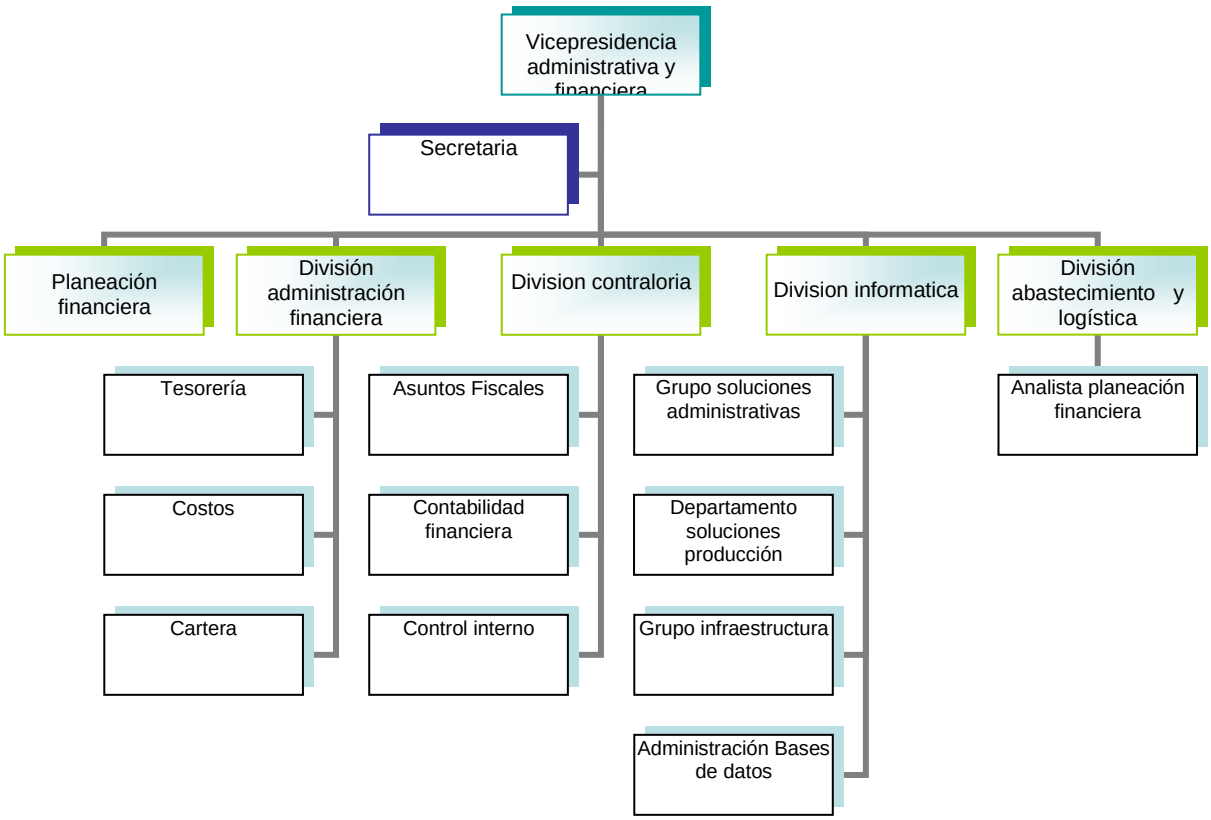


Ilustración 5. Vicepresidencia Administrativa y Financiera

1.4 ANÁLISIS DIFERENCIAL DEL ESTADO ACTUAL VERSUS ISO/IEC 27001 Y 27002

Teniendo como base está definición de la norma ISO27001:2013, este trabajo estará enfocado en analizar todos los controles y requerimientos de seguridad detallados en el Anexo A: ISO/IEC 27002:2013 con los procesos de Textil S.A, para lo cual se mirará en detalle cada uno de los capítulos la misma, empezando por el numeral 5– Políticas de Seguridad de la información y terminando con el 18- Cumplimiento. Dentro de cada capítulo, existen controles que deben también implementarse.

Los hallazgos descritos a continuación son resultados de un análisis de las medidas de seguridad y la normativa que tiene la organización en relación a la seguridad de la información, esta verificación se centró en la revisión de los diferentes controles de las áreas del alcance. Este análisis nos permitirá conocer de manera global el estado actual de textil S.A en relación de la seguridad de la información.
Se agrega un valor a cada control en base al estado en el que se encuentra:

0- No esta implementado.

1- Esta parcialmente implementado.

2- Esta casi completamente implementado.

3- Completamente implementado.

Adjunto el documento base del “hoja de verificación.xlsx”

Norma	Sección	No	Descripción	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
27001-AP.4	**4. Contexto de la organización**	**4.1**	**Entendiendo la organización y su contexto**		No se evidencian registros o actas donde la organización determine los enfoques y propósitos del sistema de gestión de la información	0
27001-AP.4	4. Contexto de la organización	4.2	Entendiéndolas necesidades y expectativas de las partes interesadas		No se tiene evidencia de actas donde se demuestran las partes interesadas que son relevantes en el sistema de gestión de la información	0

27001-AP.4	4. Contexto de la organización	4.3	Determinando el alcance del SGSI		Aunque se tiene un alcance claro no se evidencias actas referenciando el alcance, los requerimientos, interfaces y dependencias	0
27001-AP.4	4. Contexto de la organización	4.4	Administración del sistema de gestión de seguridad de la información		Aunque existe un fuerte compromiso de la alta dirección no se encuentra un registro o acta donde la organización se comprometa a establecer, implementar, mantener y darle continuidad al sistema de información	0
27001 AP.5	**5. Liderazgo**	**5.1**	**Liderazgo y compromiso**	La alta dirección demuestra liderazgo y compromiso con el SGSI	Aunque existe un fuerte compromiso de la alta dirección no se encuentra un registro o acta donde la evidencie el aseguramiento de los objetivos, la integración con otros procesos	0
27001 AP.5	5. Liderazgo	5.2	Política	Existe un documento de política de la información y está publicado en la intranet	A pesar de que existe un documento esta desactualizado, faltan incluir objetivos acordes a las nuevas tecnologías y garantizar la mejora continua, igualmente no se evidencian actas o formatos donde se muestre la	1

					divulgación del documento y la revisiones periódicas del mismo	
27001 AP.5	5. Liderazgo	5.3	Roles de la organización, responsabilidad y autoridad	Existen responsables comprometidos con el SGSI	sin embargo no existe claramente diferenciados los roles para garantizar el cumplimiento, no existe un rol de responsable de seguridad especificado	1
27001 AP.6	**6. Planificación**	**6.1**	**Acciones para dirigir los riesgos y oportunidades**		No se evidencia procesos o documentación que evidencien identificación de riesgos, no se identifican responsables de los riesgos, ni evaluaciones	0
27001 AP.6	6. Planificación	6.2	Objetivos y planes para lograrlo	Existe un documento de políticas	A pesar de que existe un documento de políticas no hay evidencias de métricas, de evaluación, de recursos involucrados, de responsables de seguimiento de objetivos	0
27001 AP.7	**7. Soporte**	**7.1**	**Recursos**	Se cuenta con recurso humano comprometido y dispuesto, igualmente con presupuesto para adquirir los recursos	No se encuentran o actas que evidencien la disponibilidad de los recursos	0
27001 AP.7	7. Soporte	7.2	Competencia	Hay recurso humano interesado	No se encuentran evidencias de planes de formación para auditores internos	0

27001 AP.7	7. Soporte	7.3	Sensibilización	La política de seguridad esta publicada en la intranet la cual tiene acceso todo el personal	No se evidencian actas o divulgaciones de la política, actualizaciones de la misma, estrategias de comunicación	0
27001 AP.7	7. Soporte	7.4	Comunicación	Existe un departamento de comunicación	No se evidencian actas donde se determine el que comunicar, cuando, a quien, quien, como, el SGSI	0
27001 AP.7	7. Soporte	7.5	Información documentada	Por normatividad existen establecidas plantillas y formatos por ISO 9000 que podrían tomarse	No hay formatos para el SGSI se deben crear, proteger, controlar y garantizar una retención	0
27001 AP.8	**8. Operación**	**8.1**	**Planificación y control operativo**		No se evidencian implementación de planes para alcance de objetivos, la claridad de los procesos externalizados,	0
27001 AP.8	8. Operación	8.2	Evaluación riesgos Seguridad de la información		No se evidencia análisis de riesgos.	0
27001 AP.8	8. Operación	8.3	Tratamiento riesgos Seguridad de la información		No se evidencia el plan de tratamiento de riesgos	0
27001 AP.9	**9. Evaluación de desempeño**	**9.1**	**Seguimiento, medición, análisis y evaluación**	Existen procesos de monitoreo, análisis	A pesar de que existen procesos de monitoreo no están claramente definidos para el SGSI se necesita estructurar que monitorear, cuando, quien, métodos, cuando analizar, quien analizara	1

27001 AP.9	9. Evaluación de desempeño	9.2	Auditoria Interna		No está definido ni estructurado el plan de auditorías internas para el SGSI y los auditores lideres	0
27001 AP.9	9. Evaluación de desempeño	9.3	Revisión de la Dirección		No existe un proceso de revisión por la dirección para considerar el estado de acciones, cambios, retroalimentación, resultados, oportunidades de mejora	0
27001 AP.10	**10. Mejoras**	**10.1**	**No-conformidades y acciones correctivas**	Existe un aplicativo desarrollado para el tratamiento de acciones correctivas, mejorativas por iso 9000	No esta definidos un proceso para el tratamiento de no conformidades y acciones correctivas para el SGSI se debe asociar las buenas practicas que ya se tienen en los procesos de la organización a raíz de ISO 9000 para complementarlas con el SGSI iso 27001	
27001 AP.9	10. Mejoras	10.2	Mejora continua		No hay definido un plan para la vigencia, adecuación y efectividad del SGSI	0
27001 - A.5	**5. Políticas de la Seguridad de la Información**	**5.1**	**Orientación de la dirección para la gestión de la seguridad de la información**			

27001 - A.5	5. Política de Seguridad de la Información	5.1.1	Políticas para la seguridad de la información	Las políticas se publican en la intranet, se han divulgado a todos los empleados, se han hecho campañas de conciencia de estas políticas, se tienen controles para monitorizar el cumplimiento de las políticas. Dentro de los hallazgos positivos se tiene el portal de informática las evidencias de los tipos de seguridad mes a mes como parte del proceso de sensibilización al usuario	No se tiene evidencia de los entrenamientos realizados a todos los empleados específicamente en las políticas de seguridad. No se incluye en todos los planes de entrenamiento las políticas de seguridad.	2
27001 - A.5	5. Política de Seguridad de la Información	5.1.2	Revisión de las políticas de seguridad de la información		las políticas se encuentran desactualizadas, no existe un tiempo estimado para la revisión de las mismas	1
27001 - A.6	**6. Organización de la Información**	**6.1**	**Organización Interna**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	
27001 - A.6	6. Organización de la Seguridad de la Información	6.1.1	Funciones de seguridad de la Información y las responsabilidades	Se tiene documentado los roles de la compañía y las responsabilidades de cada rol.	No se tiene un rol específico para el responsable del SGSI	1
27001 - A.6	6. Organización de la Seguridad de la Información	6.1.2	La segregación de funciones	existen roles y cargos definidos		3

27001 - A.6	6. Organización de la Seguridad de la Información	6.1.3	Póngase en contacto con las autoridades	Se tiene un documento donde se plasma el procedimiento disciplinario y su aplicación. Se contacta al personal de seguridad en caso de ser necesario Se registran los incidentes con copia a la hoja de vida del empleado	no se tiene un proceso para la recolección de evidencia informática forense	2
27001 - A.6	6. Organización de la Seguridad de la Información	6.1.4	Póngase en contacto con los grupos de interés especial	dentro de la organización existen personas que tiene contactos con grupos de interés, tales como policía, fiscalía, bomberos, Urgencias, además se tiene un grupo organizado que atiende primariamente urgencias médicas y desastres menores	No se encontró un documento donde se centralice la información de grupos de interés.	1
27001 - A.6	**6. Organización de la Información**	**6.2**	**Dispositivos móviles y teletrabajo**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.6	6. Organización de la Seguridad de la Información	6.2.1	Política de dispositivo móvil		No se tienen políticas de sobre el uso de dispositivos móviles, no hay controles para el uso de dispositivos móviles no se tiene analizados los riesgos para el uso de dispositivos móviles.	0

27001 - A.6	6. Organización de la Seguridad de la Información	6.2.2	Teletrabajo	Si se tiene una política sobre el trabajo remoto se tiene un proceso para lo solicitud de acceso a los servicios remotos las solicitudes solo puede ser autorizadas por vicepresidencia existen controles de para la protección de la información en tránsito en el trabajo remoto.	se debe definir en la política de trabajo remoto el procedimiento para el acceso de terceros (proveedores por webex)	1
27001 - A.7	**7. Seguridad de los Recursos Humanos**	**7.1**	**Antes de la contratación laboral**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.7	7. Seguridad de los Recursos Humanos	7.1.1	Proyección	existe un proceso que define los lineamientos sobre la solicitud de nuevo personal existe un documento donde se especifica el tipo de evaluación por realizar en cada proceso de selección según el rol o cargo a desempeñar, en este documento se especifica la revisión de todos los antecedentes, documentación, se hace visita domiciliaria, de los	no se tiene un documento donde se evalúen o se haga seguimiento a los proveedores no se tiene definido cada cuento se debe hacer la evaluación de proveedores	1

				candidatos Existe un proceso de contratación y compras donde se evalúan las diferentes alternativas de selección de proveedor		
27001 - A.7	7. Seguridad de los Recursos Humanos	7.1.2	Términos y condiciones de empleo	Existen contratos en donde se incluye un cláusula de confidencialidad de la información	En la cláusula de confidencialidad no se tiene estipulado el tiempo por el cual será confidencial la información una vez terminando el contrato	2
27001 - A.7	**7. Seguridad de los Recursos Humanos**	**7.2**	**Durante la contratación laboral**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.7	7. Seguridad de los Recursos Humanos	7.2.1	Responsabilidades de gestión	Existen contratos en donde se incluye un cláusula de confidencialidad de la información, se hacen entrenamientos sobre las políticas, se tienen controles para monitorizar el cumplimiento de las políticas de seguridad y son reportados en una aplicación	no se tienen acuerdos de confidencialidad donde se definan las recomendaciones de seguridad sobre el tratamiento de la información	1
27001 - A.7	7. Seguridad de los Recursos Humanos	7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación	se hacen entrenamientos a todas las personas administrativas cuando ingresan sobre el manejo de la información;	no todas las personas reciben entrenamiento en políticas de seguridad de la información los contratistas externos , no existen	1

				Se envían correos denominados tipos de seguridad donde se educa a los usuarios en buenas prácticas de seguridad	evidencia de que a las personas sean entrenadas en políticas de seguridad en el plan de entrenamientos	
27001 - A.7	7. Seguridad de los Recursos Humanos	7.2.3	Proceso disciplinario	Se tiene un documento donde se plasma el procedimiento disciplinario y su aplicación. Se contacta al personal de seguridad en caso de ser necesario Se registran los incidentes con copia a la hoja de vida del empleado	En la evaluación de los empleados no se tiene en cuenta los incidentes de seguridad de la información. No existe un proceso de recolección de evidencia	1
27001 - A.7	**7. Seguridad de los Recursos Humanos**	**7.3**	**Durante la terminación o cambio del contrato**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.7	7. Seguridad de los Recursos Humanos	7.3.1	La terminación o el cambio de las responsabilidades laborales	se tiene una lista de chequeo de cumplidos que deben tramitarse para el retiro de personal; existe una aplicación que apoya el proceso de retiro de usuarios de manera que facilite a nomina, área y sistemas dar cumplido a las obligaciones del empleado	no se tiene un proceso documentado para el retiro de personal de la compañía	2
27001 - A.8	**8. Gestión de Activos**	**8.1**	**Responsabilidad por los Activos**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**

27001 - A.8	8. Gestión de Activos	8.1.1	Inventario de activos	El área de plataforma maneja varios inventarios de activos de información en Excel (hardware y software) Se tiene uno dedicado solo a equipos de cómputo denominado Microstextil ,otro a impresoras, otro a Acces point y un directorio donde esta cada Switche con toda la información	No se tiene un proceso documentado para el inventario de activos	1
27001 - A.8	8. Gestión de Activos	8.1.2	Propiedad de los bienes	Se tiene un inventario físico y digital de activos de información asignado a cada persona. Se tiene una carpeta de control de facturas de equipos comprados esto con el fin de control, propiedad del bien, indicadores de actualización de plataforma. Control de licenciamiento OEM	No se tiene un proceso documentado para la asignación de activos los equipos suministrados por terceros no están inventariados	1
27001 - A.8	8. Gestión de Activos	8.1.3	Uso aceptable de los activos	En el proceso de inducción de nuevos empleados se hace mención al trato y manejo de equipos que se les asigna, dentro del departamento de infraestructura	no hay un documento de responsabilidad frente a los recursos que se le entregan a los empleados	1

				cada técnico tiene asignadas unas áreas una de las premisas es velar por los equipos asignados y enviar correos a los analistas de cada área cuando se identifica maltrato o falta de cuidado de los activos de computo, esto último queda registrado en el reporte de cada técnico y en la aplicación de track it. en las políticas de seguridad de la compañía en el ítem 2.9 se hace alusión al uso del puesto de trabajo		
27001 - A.8	8. Gestión de Activos	8.1.4	Retorno de los activos	Se tiene un procedimiento que especifica las actividades de retiro de usuario de SI, formato de retiro que se deposita de manera física en una carpeta del centro de cómputo como evidencia para Auditorías internas y externas; Igualmente el correo de paz y salvo que envía el área del empleado a retirarse al área de informática	Se debe complementar el procedimiento ya existente con todo el proceso ya que no menciona el proceso de paz y salvo y no hay una actividad dentro del formato que actualice los inventarios y carpetas físicas	2

27001 - A.8	8. Gestión de Activos	8.2	Clasificación de la Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
27001 - A.8	8. Gestión de Activos	8.2.1	Clasificación de la información	Se tiene un modelo de seguridad para información sensible en servidores. Tip de seguridad que hablan del manejo de directorios compartidos de manera local	No se tiene un proceso formal de clasificación de información, existe información sensible en los equipos de usuarios administrativos	1
27001 - A.8	8. Gestión de Activos	8.2.2	Etiquetado de la información	Se tiene una estándar para el manejo de procesos e instructivos	No se tiene clasificación de la información con marcas de información pública, privada	1
27001 - A.8	8. Gestión de Activos	8.2.3	Manejo de activos	Dentro del archivo de inventario de micros hay un campo de serial y service tag de la maquina único de la misma, modelo, área, responsable, fecha de asignación de la máquina, asi mismo en los archivos impresoras, Acces Pointy switches	No hay el mismo tratamiento para monitores y equipos de terceros , no hay etiquetas físicas, no están clasificados por información	1
27001 - A.8	**8. Gestión de Activos**	**8.3**	**Manipulación de Medios**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.8	8. Gestión de Activos	8.3.1	Gestión de soportes extraíbles	Existe una estrategia que involucra el manejo y manipulación de medios extraíbles para este caso manejo de discos externos, Existen políticas antivirus para	no se tiene una política sobre el uso de medios extraíbles no se tiene controles sobre el uso de medios extraíbles para personal administrativo No se monitoreo periódicamente	1

				el bloqueo de medios extraíbles para la parte operativa de planta, además de políticas de directorio activo que maneja restricciones de accesos a la mayoría de equipos operativos Existen logs donde está el registro de la conexión de medios extraíbles	la conexión de medios extraíbles	
27001 - A.8	8. Gestión de Activos	8.3.2	La eliminación de los medios de comunicación	se hace una disposición adecuada de los activos a dar de baja y se elimina todo tipo de información corporativa antes de esto LA entrega de chatarra tecnológica se realiza a la cooperativa coopérenla	no se tiene un proceso donde se definan los pasos a seguir en caso de la eliminación segura de equipos, eliminación de información y datos	2
27001 - A.8	8. Gestión de Activos	8.3.3	Transferencia de medios físicos	Los discos son trasladados de Girardota a Rose siempre por una misma persona correo interno de la compañía y con un control en cajas, las base de datos van con la los usuarios del esquema de la base de datos, los cuales son con restricciones de acceso.	La información de los discos no está encriptada, contiene información de todas las bases de datos críticas de la compañía, en extensión .bak los cuales desde un SQL pueden ser montadas y se podrían hacer reconocimiento de usuarios sa mediante técnicas de hackeo	1

27001 - A.9	9. Control de Acceso	9.1	Control de Acceso de requerimientos del Negocio	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
27001 - A.9	9. Control de Acceso	9.1.1	Política de control de acceso	Se tiene una política sobre el control de acceso a la información y se sigue un proceso para solicitarlo. Hay una aplicativa que soporta este proceso, el edificio administrativo donde se encuentra la información más sensible y servidores de la compañía maneja control de acceso a través de carnet con banda e igualmente se tienen cámaras.	No Se tiene clasificación de la información ni clasificaciones de perfiles de acceso	1
27001 - A.9	9. Control de Acceso	9.1.2	El acceso a las redes y los servicios de red	Se tiene un proceso de solicitud de ingreso de usuario donde se especifica los servicios a asignarle y recursos; se tiene un procesos para servicio de terceros la herramienta de mesa de ayuda track it están las auditorias periódicas de seguridad y resultados, correo de informes de resultados auditorias de seguridad, se tiene un	Se debe tener un proceso de seguridad en red y actividades de revisiones permisos de acceso, Se debe centralizar las revisiones documentadas en un solo proceso y que existe mucha información dispersa se debe actualizar la información de los procesos "Procedimiento Solicitud de terceros; Actualización de usuarios - Ingreso o	1

				archivo de permisos de carpetas en servidores, check list para revisiones de seguridad en usuarios y servidor de nómina; Se tiene además un proceso y un formato para la solicitud \ de conexión VPN	Retiro"	
27001 - A.9	**9. Control de Acceso**	**9.2**	**Gestión de Acceso de Usuarios**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**Valor**
27001 - A.9	9. Control de Acceso	9.2.1	Registro de usuarios y de la matrícula	Se tienen registros para solicitud de acceso VPN, Solicitud de servicios informáticos para empleado; solicitud de terceros; correo de aprobaciones	se debe actualizar el procedimiento "Actualización de usuarios - Ingreso o Retiro" agregando ítems que apoye el SGSI	2
	9. Control de Acceso	9.2.2	Provisión de acceso al usuario	Se tiene un sistema de control de acceso con carnetizacion para los espacios físicos y un proceso de ingreso, actualización y retiros a los usuarios de los servicios informáticos, tanto para empleados, como contratistas	se debe actualizar el procedimiento "Actualización de usuarios - Ingreso o Retiro" agregando ítems que apoye el SGSI Se debe realizar un estudio de control de acceso para áreas críticas como centros de procesamiento de datos	2

27001 - A.9	9. Control de Acceso	9.2.3	Gestión de derechos de acceso privilegiado	Se tiene dentro del proceso de ingreso a la compañía establecer unos servicios y asignarlo a determinados grupos de directorio activo según la función , se agrega a los sistemas de información y se le da permisos a bases de datos puntuales, todo a través del formato de ingreso y correos que adicionalment e entregan más información para la creación de usuario, el analista igualmente pasa en el formato para los servidores file server a que carpetas debe tener acceso o si es un remplazo se informa vía correo para que se herede el perfil del empleado anterior	en los formatos de ingreso o retiro de usuario no está toda la información hay una parte en correos, otra por solicitud de track it, otra queda a conocimiento de plataforma los detalles y faltantes	1
27001 - A.9	9. Control de Acceso	9.2.4	Gestión de la información de autenticación de secreto de los usuarios	En las políticas de seguridad se describe el manejo de contraseñas igualmente se tienen tips de seguridad enviados a todo el personal	Se debe establecer una política de contraseña segura donde se defina el uso de caracteres especiales se deben generar controles que garanticen el	2

				educando la importancia, uso, creación de contraseñas seguras; se tienen políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de contraseña cada 3 meses,	uso de caracteres especiales en las contraseñas se debe crear una política de control de acceso a las aplicaciones desarrolladas por Textil cuando la aplicación lo requiera.	
27001 - A.9	9. Control de Acceso	9.2.5	Revisión de los derechos de acceso de usuario	Se tiene incorporado por el jefe de infraestructura realizar unas revisiones semanales en cuanto a Directorio Activo, Accesos a internet (Proxy). Diariamente como parte de la operación infraestructura envía informes de conexiones VPN en los cuales salen las conexiones establecidas , usuarios, tiempos. Igualmente previos a las auditorias de Price que son cada 4 meses se sacan reportes de usuarios activos, inactivos, y una serie de	Todas las actividades SGSI no están documentados en el procesos de "Procedimiento de Revisión Seguridad" que defina responsables, periodicidad de revisión y reportes asociados a todo este proceso, existe un proceso pero desactualizado se debe formalizar y actualizar a todas las actividades relacionadas	2

				reportes a nivel de dominio de manera que se logren identificar inconsistencias; se realiza además reportes de vulnerabilidades de servidores cada 3 meses allí se analizan los permisos a directorios compartidos y se valida con archivo seguridad de carpetas servidores		
27001 - A.9	**9. Control de Acceso**	**9.3**	**Responsabilidad de los usuarios**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.9	9. Control de Acceso	9.3.1	El uso de la información secreta de autenticación	se hacen entrenamientos políticas de seguridad donde se establecen las buenas prácticas para el manejo de la contraseña se tiene controles de directorio activo para la creación de contraseñas	Se debe definir una política de manejo de contraseñas y buenas prácticas para el uso de las mismas que incluyan un límite de historia de contraseñas se deben generar controles que garanticen la no reutilización de un límite de contraseña.	1
27001 - A.9	**9. Control de Acceso**	**9.4**	**Control de Acceso a Sistemas y aplicaciones**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.9	9. Control de Acceso	9.4.1	Restricción de acceso Información	Existe un proceso denominado Metodología de desarrollo Textil en las etapas de desarrollo e implementació	No hay un proceso integral que maneje toda la trazabilidad de un usuario es decir desde los permisos que se le otorgan a	1

				n se muestra como es el manejo y configuración de accesos a usuarios, La DBA tiene también un formato de manejo de seguridades, plataforma maneja un proceso de ingreso y retiro donde se especifica el rol del usuario.	la red de datos, pasando por las aplicaciones autorizadas y permisos en las bases de datos, además de los directorios a los cuales tiene acceso en los servidores	
27001 - A.9	9. Control de Acceso	9.4.2	Procedimientos seguros de inicio de sesión	-Se tienen procesos de autenticación por directorio activos para el ingreso a la red de datos. -existe una metodología para la solicitud de acceso a los diferentes recursos y servicios de la compañía -En las políticas de seguridad se describe el manejo de contraseñas creación de contraseñas seguras; se tienen políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de	no se tiene clasificada y documentada la información, las estrategias de autenticación y los procesos de solicitud de permisos a los diferentes sistemas de información	1

				contraseña cada 3 meses, se tiene además una plataforma de doble contraseña proporcionado por PGP		
27001 - A.9	9. Control de Acceso	9.4.3	Sistema de gestión de contraseñas	En las políticas de seguridad se describe el manejo de contraseñas creación de contraseñas seguras; se tienen políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de contraseña cada 3 meses, se tiene además una plataforma de doble contraseña proporcionado por PGP		3
27001 - A.9	9. Control de Acceso	9.4.4	El uso de programas de utilidad privilegiados	Existen políticas de grupo a nivel de dominio que restringe el acceso a utilidades del sistema operativo, Existen grupos de dominio para acceso a internet restringido; Se tienen	se debe actualizar el procedimiento de "revisión de seguridad" ya que no contiene todas las actividades de monitoreo semanal de redes, firewall no están documentadas, no hay un documento que especifique los	2

				reportes de seguimiento y control de servicios de internet, uso de red local;	grupos creados en directorio activo sus privilegios y roles	
27001 - A.9	9. Control de Acceso	9.4.5	Control de acceso al código fuente del programa	Se tiene en la metodología de desarrollo en las etapas de desarrollo e implementación el manejo del código fuente; Se tienen repositorios de los códigos fuente en un servidor con las seguridades adecuadas igualmente una estrategia de backup para estos directorios tanto para aplicaciones CIA como CIU: Se tiene para las aplicaciones Clck once para manejo de versiones	En los documentos "Doc Guía - Etapa Implementación" y "Doc Guía - Etapa Desarrollo; " no se especifica donde se guarda el código fuente de cada división de desarrollo CIA y CIU, la periodicidad, el manejo de versiones, se encuentra desactualizados; no se menciona control de versiones, no se menciona manejo de cambios de estas fuentes	2
27001 - A.10	**10. Criptografía**	**10.1**	**Controles criptográficos**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.10	10. Criptografía	10.1.1	Política sobre el uso de controles criptográficos	se tiene un programa de cifrado denominado PGP para usuarios con información sensible, Presidencia, Vicepresidencias, Jefes de división, Costos, Ventas,	no se tiene una política de controles criptográficos y en qué caso son necesarios, ---------- no se tiene un modelo de inscripción para bases de datos SQL, para datos de aplicaciones administrativas, para discos	1

					externos que salen con información sensible de la empresa	
27001 - A.10	10. Criptografía	10.1.2	Gestión de claves	El sistema de PGP universal ofrece un manejo de llaves optimo esto aplicado a los usuarios que lo tienen instalado,	no se tiene una política de controles criptográficos y en qué caso son necesarios, ---------- no se tiene un modelo de inscripción para bases de datos SQL, para datos de aplicaciones administrativas, para discos externos que salen con información sensible de la empresa	1
27001 - A.11	**11. Seguridad Física y Ambiental**	**11.1**	**Áreas Seguras**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.11	11. Seguridad física y del entorno	11.1.1	Perímetro de seguridad física	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian son certificados por la BASC		3
27001 - A.11	11. Seguridad física y del entorno	11.1.2	Controles de entrada físicas	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados	Los archivos físicos que tienen información sensible e historia de la compañía no tienen control de acceso por	1

				y existen registros que lo evidencian usan carnet y tarjetas de acceso para el ingreso a áreas segura. En algunas zonas se usan estrategias de control de acceso por medio de llaves físicas son certificados por la BASC	carnet ni cámara cercana, el centro de cómputo no tiene control de acceso ni cámara de seguridad	
27001 - A.11	11. Seguridad física y del entorno	11.1.3	Asegurar oficinas, salas e instalaciones	existen procesos y están alineados con la ISO18001	No se menciona en el proceso seguridad física el manejo del control de llaves cómo se maneja, quien es el responsable, por cuanto tiempo se almacena este formato, que personas pueden reclamar las llaves. No hay un control de acceso para el centro de computo	2
27001 - A.11	11. Seguridad física y del entorno	11.1.4	La protección contra amenazas externas y ambientales	existen procesos y están alineados con la ISO18001		3
27001 - A.11	11. Seguridad física y del entorno	11.1.5	Trabajar en zonas seguras	Existen procesos y están alineados con la ISO18001 Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados	No se menciona en el proceso de seguridad física el uso de sistemas seguridad cámaras	2

				y existen registros que lo evidencian usan carnet y tarjetas de acceso para el ingreso a áreas segura. En algunas zonas se usan estrategias de control de acceso por medio de llaves físicas son certificados por la BASC		
27001 - A.11	11. Seguridad física y del entorno	11.1.6	Zonas de entrega y carga	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian usan carnet y tarjetas de acceso para el ingreso a áreas segura. En algunas zonas se usan estrategias de control de acceso por medio de llaves físicas son certificados por la BASC	no se tiene un proceso para el manejo de planilla de control ingreso portátiles No se tiene un proceso manejo de planilla formato ingreso herramientas contratista	1
27001 - A.11	**11. Seguridad Física y Ambiental**	**11.2**	**Equipos**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.11	11. Seguridad física y del entorno	11.2.1	Emplazamiento y Protección del equipo	existen procesos y están alineados con la ISO18001 existen análisis de riesgos ambientales documentados		3

27001 - A.11	11. Seguridad física y del entorno	11.2.2	Apoyo a los servicios públicos	Se tiene incorporado una documentación con las UPS y una vez por año el proceso de mantenimiento con proveedor externo El área de instrumentación-electricidad tiene controles para revisiones periódicas de la energía, mantenimientos a equipos, acciones durante un apagón	No se tiene registro de los mantenimientos de UPS en el proceso, No se menciona en el proceso de instrumentación y electricidad el sistema del centro de cómputo, sus revisiones y mantenimiento	2
27001 - A.11	11. Seguridad física y del entorno	11.2.3	Seguridad del cableado	Se tiene dentro de los proyectos desarrollados a partir del 2010 documentación que especifica el uso de estándares de cableado En el cableado de la empresa en las áreas se tienen tuberías en las zonas externas y canaletas hacia oficinas	No hay cableado certificado en un 80% d la empresa Se detectó falta de canaletas y separación de cables eléctricos y de datos No hay un documento o plano de la compañía que apoye las rutas de cableado estructurado No hay se cumple el estándar en la terminación de cableado	1
27001 - A.11	11. Seguridad física y del entorno	11.2.4	El mantenimiento del equipo	Se tiene un programa de mantenimientos de equipos tanto lógico como físico Se tiene un indicador de mantenimiento que se evidencia cada mes en los grupos	El proceso de mantenimientos preventivos esta desactualizado hace falta incorporar el indicador de mantenimiento No se menciona del programa de mantenimiento	2

				primario	s	
27001 - A.11	11. Seguridad física y del entorno	11.2.5	La eliminación de los activos	Se tiene incorporado un proceso de registro de dar de baja un equipo de SI Se tiene incorporado un proceso de desecho tecnológico	el proceso de desecho tecnológico no está documentado El proceso de dar de baja un equipo y que registros se deben realizar no está documentado	2
27001 - A.11	11. Seguridad física y del entorno	11.2.6	Seguridad de los equipos y de los activos fuera del establecimiento	se tiene un proceso de control de salida de equipos de la empresa	No se tiene sistema de guayas en los equipos portátiles Las personas de seguridad no tienen claridad cuales portátiles son de la compañía y cuales son personales	2
27001 - A.11	11. Seguridad física y del entorno	11.2.7	La eliminación segura o la reutilización de los equipos	se hace una disposición adecuada de los activos de información y se elimina todo tipo de información corporativa antes de esto Los equipos dados de bajo y considerados desechos tecnológicos se les realiza un proceso adecuado y se entrega a la cooperativa	En el proceso "Actualización de usuarios - Ingreso o Retiro" se debe especificar el borrado de la información segura En el formato de Retiro es necesario agregar un ítem para el borrado de información	2
27001 - A.11	11. Seguridad física y del entorno	11.2.8	Equipos de usuario desatendida	Se tiene un proceso para los servidores y uso de servicios terminal services Se tienen tips de seguridad	Se debe crear una política de equipo desatendido. Se debe implementar un control para el tiempo de inactividad de	1

				educando al usuario con tema equipo desatendidos	los equipo de cómputo Se deben realizar más sensibilizaciones a través de la intranet que es de uso diario	
27001 - A.11	11. Seguridad física y del entorno	11.2.9	Política de escritorio y pantalla clear Despejado	Se tienen tips de seguridad educando al usuario con escritorio despejado	se debe crear una política de escritorio y pantalla despejadas se debe monitorizar periódicamente la aplicaciones de la política de escritorio y pantalla despejada	1
27001 - A.12	**12. Seguridad en las operaciones**	**12.1**	**12. Procedimientos Operacionales y Responsabilidades**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.12	12. Operaciones de Seguridad	12.1.1	Procedimientos operacionales, adecuadamente documentados	Se tienen procesos diarios, semanales, mensuales, de todo el SI que soportan la operación	se debe actualizar el documento "Manual de seguridad" colocando las tareas operativas y periodicidad	2
27001 - A.12	12. Operaciones de Seguridad	12.1.2	Gestión del cambio	Existe un proceso de gestión de cambios para desarrollo de software Existe proceso de gestión de cambios para infraestructura Existe un proceso incorporado en manejo de versiones de aplicaciones de software	No se tiene estandarizado el proceso de Actualización de usuario Se encuentra información desactualizada En el proceso de desarrollo de software no se menciona como se manejan las versiones de software en cuanto a los cambios	2

27001 - A.12	12. Operaciones de Seguridad	12.1.3	Gestión de la capacidad	A nivel de desarrollo de software tienen procesos establecidos que les permiten manejar indicadores de calidad y reporte de defectos. Se hacen pruebas de rendimiento bajo demanda de la infraestructura y bases de datos. Se realizan revisiones periódicas de capacidad de base de datos y estado de discos de servidores en la etapa de conceptualización de software se tiene requerimientos operativos En los proyectos desarrollados por infraestructura se analiza los tropud de dispositivos, límite de sesiones, se hace un reconocimiento de empresas para plataformas hibridas	Se debe en el proceso de desarrollo de software detallar el cómo se realiza No se tiene un proceso estandarizado que especifique la gestión de capacidades	1
27001 - A.12	12. Operaciones de Seguridad	12.1.4	Separación de desarrollo, prueba y entornos operativos	Se tiene dentro de las diferentes etapas de metodología de desarrollo de software	No se evidencia el seguimiento del proceso en cuento los controles de calidad.	2

				varios ambientes virtuales el ambiente de desarrollo, ambiente virtual producción en este último se tiene un ambiento idéntico al de producción para realizar todas las pruebas de funcionalidad, rendimiento. Se hacen entrenamiento sobre las buenas prácticas de desarrollo	A pesar de que existe una metodología los departamentos CIA y CIU trabajan sin los mismos lineamientos	
27001 - A.12	**12. Seguridad en las operaciones**	**12.2**	**Protección contra código malicioso**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.12	12. Operaciones de Seguridad	12.2.1	Controles contra mal-ware	existe una política para uso de anti malware se registran lo eventos de seguridad asociados al malware en TRACKIT los casos malware son tratados como incidentes Se tienen reportes diarios, semanales y mensuales de revisiones de seguridad de la plataforma	Se debe ampliar la política de antivirus de las políticas de seguridad de la compañía se debe actualizar procesos relacionados con los monitoreos de la seguridad para que cubran todo lo relacionado con el malware	2
27001 - A.12	**12. Seguridad en las operaciones**	**12.3**	**Copias de Respaldo**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.12	12. Operaciones de Seguridad	12.3.1	Copia de seguridad de la información	Se tiene un proceso de backup y recuperación para servidores,	Los procesos de copias de seguridad no están unificados	2

				bases de datos, información corporativa Una vez al año se tiene incorporadas buenas prácticas para realizar simulacros de recuperación de servidores críticos		
27001 - A.12	**12. Seguridad en las operaciones**	**12.4**	**Registro y Seguimiento**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.12	12. Operaciones de Seguridad	12.4.1	El registro de eventos	Se tiene un proceso de revisiones diarias, semanales y mensuales de seguridad y estado de salud de la plataforma Se tiene una biblioteca en el portal donde se guardan las evidencias y controles por año, por mes, por día.	El procedimiento de revisión de la seguridad se encuentra desactualizado No se tiene protegida la información en cuanto a la manipulación de registros	2
27001 - A.12	12. Operaciones de Seguridad	12.4.2	Protección de la información de registro	Dentro de los controles establecidos las personas no tienen acceso a modificar los log de los sistemas	No se tiene especificado en el procedimiento revisiones de seguridad quienes son los responsables del acceso a los logs, ni la protección a los mismos No está actualizada la información del procedimiento revisiones de seguridad en cuanto a los responsables de los monitoreos de los log	2

					En los procedimientos revisiones de seguridad y manual de seguridad Se deben actualizar los registros faltantes de monitoreo y la ubicación donde se debe guardar los monitoreos	
27001 - A.12	12. Operaciones de Seguridad	12.4.3	Registros de administrador y operador	Se tiene un proceso incorporado de monitoreo diario, semanal por parte del administrador y el operador de los servicios críticos de la compañía Se tiene una biblioteca del portal de informática donde se almacenan estos reportes	No se están almacenando en los registros el monitoreo de dispositivos de red El procedimiento manual de seguridad se encuentra desactualizado	2
27001 - A.12	12. Operaciones de Seguridad	12.4.4	Sincronización de reloj	Se tiene un proceso incorporado para la sincronización de la hora de todos los equipos de textilera desde el servidor NTP en este caso el controlador de dominio	los documentos hora y sincronización de equipos, Situación de hora textilera están bajo formato de correo se debe estructurar como un procedimiento y formalizar	2
27001 - A.12	**12. Seguridad en las operaciones**	**12.5**	**Control de Software Operacional**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**

27001 - A.12	12. Operaciones de Seguridad	12.5.1	La instalación del software en los sistemas operativos	Se tiene incorporado controles de instalación de aplicaciones en equipos de usuarios Se tiene incorporado un sistema de actualización de aplicaciones Microsoft mediante WSUS y en esquema de pruebas para servidores y usuarios	No se tiene control de instalación de aplicaciones para el área administrativa desde medios extraíbles No está documentado el proceso de pruebas de instalación de parches tanto para clientes como para servidores No se tiene implementado un sistema de actualización de parches para programas distintos de Microsoft	1
27001 - A.12	**12. Seguridad en las operaciones**	**12.6**	**Gestión de Vulnerabilidades técnicas**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.12	12. Operaciones de Seguridad	12.6.1	Gestión de vulnerabilidades técnicas	Se tiene incorporado un proceso de chequeo de vulnerabilidades y test de penetración para el servidor y los usuarios de nómina Se tiene incorporado en los mantenimientos de servidores chequeo de vulnerabilidades con el software de Microsoft Baseline Security analyzer	No se tiene documentado el proceso de chequeo de vulnerabilidades en los servidores en el manual del administrador de seguridad, ni la periodicidad con que se realiza, ni los planes de acción No se tiene chequeo de vulnerabilidades y test de penetración para los equipos de red y comunicaciones No se tiene chequeo de vulnerabilidades para los	2

					equipos de usuario críticos de la compañía diferentes a nomina como presidente, vicepresidentes, ventas, costos	
27001 - A.12	**12. Seguridad en las operaciones**	**12.7**	**Consideraciones sobre auditorias de Sistemas de Información**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.12	12. Operaciones de Seguridad	12.7.1	Controles de auditoría de sistemas de información	Se tiene incorporada la periodicidad de auditoria y análisis de vulnerabilidad para el área de nómina Se tiene incorporada la periodicidad de los mantenimientos donde se realiza el chequeo de vulnerabilidades y revisiones para los servidores	No se tiene documentado el manual del administrador de seguridad la periodicidad de las auditorias que se realizan a los servidores	1
27001 - A.13	**13. Seguridad de las Comunicaciones**	**13.1**	**Gestión de la Seguridad de las redes**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.13	13. Seguridad en las Comunicaciones	13.1.1	Controles de red	Se tiene un proceso incorporado para las revisiones de todos los servicios de plataforma Se realizan monitoreos, diarios, semanales, mensuales	El documento Manual del administrador de seguridad informática esta desactualizado las revisiones de los dispositivos de red no se está guardando en el repositorio de los demás equipos La revisión de los log del	2

					firewall no tienen una periodicidad de revisión se realiza muy eventual Las revisiones del router de Une a pesar de que se tiene usuario para revisión de logs no se tiene periodicidad para su revisión ni se guardan los logs	
27001 - A.13	13. Seguridad en las Comunicaciones	13.1.2	Seguridad de los servicios de red	Se tiene para los dispositivos de red configurados los rol de acceso a los dispositivos administrador, operador A nivel de dominio se tiene unos grupos creados y determinados accesos para los servicios de plataforma como internet, uso de aplicaciones	No se tiene documentado como se configuran las seguridades de switches y AP No se tiene dentro del grupo de soporte técnico limitación de acceso al directorio Activo cualquiera puede agregar, modificar o eliminar Se tiene conocimiento de todo el grupo de soporte técnico las contraseñas de administrador de dominio Se tienen varios administradores de dominio	1
27001 - A.13	13. Seguridad en las Comunicaciones	13.1.3	La segregación en las redes	Se tiene incorporada la configuración de subredes para segmentar las redes Igualmente se cuenta con configuración de Vlans para	SE tiene un mapa de red pero no un documento que respalde el detalle de cómo esta segmentada la red, sus configuraciones	2

				la red visitantes y la red de respaldo Se tiene una documentación completa de la red de la empresa por cada switche instalado y que dispositivos están conectados a el		
27001 - A.13	**13. Seguridad de las Comunicaciones**	**13.2**	**Transferencia de Información**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.13	13. Seguridad en las Comunicaciones	13.2.1	Las políticas y los procedimientos de transferencia de información	Se tiene incorporado en los procesos de inducción y entrenamiento del personal nuevo explicar las buenas prácticas para el uso del correo electrónico, la transferencia de archivos, el uso de la red inalámbrica de visitantes y producción. Igualmente los empleados tienen incorporado el uso de la red para proveedores y clientes debe ser apoyado por el área de soporte del departamento de infraestructura	se debe crear una política para el manejo y transferencia de la información a clientes, proveedores, contratistas y empleados se debe divulgar la política de transferencia de información a clientes, proveedores, contratistas y empleados	1

27001 - A.13	13. Seguridad en las Comunicaciones	13.2.2	Los acuerdos sobre la transferencia de información	Dentro de los contratos tanto de contratistas , proveedores se tienen cláusulas de confidencialidad	Se debe establecer acuerdos de confidencialidad y manejo de la información de acuerdo a la ley con los empleados Se debe revisar las clausulas actuales de confidencialidad para contratos de proveedores, clientes de manera que se cubra todo el esquema legal actual	1
27001 - A.13	13. Seguridad en las Comunicaciones	13.2.3	La mensajería electrónica	Se tiene incorporada la metodología Ipsec para las conexiones VPN	Se deben establecer para el servicio de correo electrónico metodologías o canales de encriptados Se debe para el servicio de mensajería instantánea una política adecuada para el manejo de la información	1
27001 - A.13	13. Seguridad en las Comunicaciones	13.2.4	Los acuerdos de confidencialidad o de no divulgación	Se tiene una cláusula de confidencialidad de la información en el contrato laboral (sección 7.3).	no se tiene acuerdos de confidencialidad donde se especifique el manejo adecuado, tiempo de retención y normalización de la información	1
27001 - A.14	**14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**	**14.1**	**Requerimientos de seguridad de los SI**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**

27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.1.1	Análisis de los requisitos de seguridad de la información y especificación	Dentro de la metodología de desarrollo del proyecto de software se estables los requerimientos no funcionales de la seguridad, se elaboran estrategias de tratamiento a los riesgos según la criticidad del proyecto, se tiene listas de chequeo a los requerimientos de seguridad	Se deben oficializar los formatos existentes que se usan en el área de desarrollo adaptándolos a una selección rápida de los ítems de seguridad	2
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.1.2	Asegurar los servicios de aplicaciones en las redes públicas	Se tiene a nivel de Firewall protección IDS Las carpetas web server tienen seguridades	se deben fortalecer las políticas de firewall contra ataques Se debe implementar estrategias y protecciones hacia web server a nivel interno Se debe revisar modelos de firewall interno o estudiar el web server en zona desmilitarizada	1
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.1.3	La protección de las transacciones de servicios de aplicación	Se tiene implementada solo en una aplicación de uso interno y externo en este caso paz y salvo el uso de un proceso de inscripción de datos concatenados de una consulta	se debe establecer para las aplicaciones que manejan y trasmiten información sensible el uso de códigos criptográficos, certificados , firmas digitales	1
27001 - A.14	**14 Adquisición, Desarrollo y Mantenimiento de**	**14.2**	**Seguridad en desarrollo y procesos de soporte**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**

	Sistemas de Información					
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.1	Políticas de desarrollo seguro	se tienen procesos establecidos para el desarrollo de software las personas del área de desarrollo son entrenadas en buenas prácticas de desarrollo seguro	no se tiene documentado la revisión entre compañeros para verificar las buenas practicas no existen manuales de desarrollo seguro	2
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.2	Procedimientos de control de cambios del sistema	se tiene procedimientos de cambios en las aplicaciones y son documentados en TRACK IT y en actas de entrega de proyectos	se deben realizar análisis de riesgos de aplicaciones de cada proyecto, donde se identifiquen las amenazas que estas tiene, impacto, y frecuencia, (OWASP)	1
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.3	Revisión técnica de las aplicaciones después de operar cambios de plataforma	Se tiene incorporado dentro de un proceso de actualización de plataforma realizar reuniones de planeación donde se establecen las actividades , responsables y pruebas Para el caso de cambios en aplicaciones críticas se tiene documentados los casos de pruebas, funcionales y de seguridad, en algunos casos se hacen pruebas de vulnerabilidad externas	Se debe crear un procedimiento para la actualización de plataforma donde describa unos lineamientos a seguir se debe actualizar el proceso de pruebas, incluyendo las pruebas externas	1

27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.4	Restricciones en los cambios a los paquetes de software	En las aplicaciones que son necesaria se establecen logs de pruebas, esto se define en los requerimientos del software Igualmente se establecen bloqueos para aplicaciones como antivirus en los equipos de los usuarios, sistema operativo	se debe establecer un proceso estándar donde se establezca los lineamientos para elegir las aplicaciones que deben tener bloqueos, activación de logs, seguimientos	1
	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.5	Uso de principios de ingeniería en protección de sistemas	Se tiene para la etapa de implementación unos entregables en la etapa de desarrollo que confirman requerimientos, estructura del programa	Se deben revisar	2
	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.6	Seguridad en entornos de desarrollo	Se tienen incorporado prácticas de revisión de seguridad de micros para el área de informática y desarrollo Se tienen implementados dentro de los procesos de mantenimiento de servidores revisión de seguridades de contenedores de códigos fuentes e información de proyectos de desarrollo de software	Se debe planear y documentar una revisión periódica para las estaciones de trabajo, ya que solo se hacen mantenimientos bajo incidentes o cambio de equipo. Se debe tener una estrategia de seguridad para los entornos de desarrollo y estaciones de trabajo para proteger la información de estos equipos	2

27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.7	Desarrollo Outsourced	no aplica		
	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	se tiene dentro de la metodología de desarrollo de software una etapa de pruebas funcionales	Se debe incorporar dentro del proceso de pruebas , pruebas de seguridad.	1
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.2.9	Pruebas de aceptación del sistema	en el plan de pruebas se establecen los criterios de aceptación del software según el sistema de calidad y el monitoreo de defectos reportados en TRACKIT	Se debe dentro de la documentación clasificar los tipos de prueba los documentos solo se remiten a pruebas de datos.	2
27001 - A.14	**14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**	**14.3**	**Datos de prueba**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.14	14. Sistema de adquisición, desarrollo y mantenimiento	14.3.1	Protección de los datos de prueba	Los datos de pruebas, no contienen información sensible para la compañía, sin embargo de requerirse, estos datos son alterados y no reflejan los reales	Se debe revisar el ambiente de desarrollo y pruebas en cuanto accesos, registros de seguridad	2
27001 - A.15	**15 Relación con Proveedores**	**15.1**	**Seguridad de la Información en la relación con los proveedores**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.15	15. Relaciones con los proveedores	15.1.1	Política de seguridad de la información para las relaciones con proveedores	En el contrato se estipulan las condiciones para confidencialidad y política	Se debe incluir en los contratos las formas de tratamiento, retención y transmisión de	1

				de la información	información, y estas deben acordar con los proveedores y contratistas	
27001 - A.15	15. Relaciones con los proveedores	15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	existen un proceso de para la compra de bienes y servicios con proveedores, y se establecen los requerimientos de compras	se deben establecer acuerdos de confidencialidad donde se estipulen la forma para el tratamiento de la información, para los proveedores y contratistas	1
27001 - A.15	**15 Relación con Proveedores**	**15.2**	**Gestión de la prestación de servicios del proveedor**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.15	15. Relaciones con los proveedores	15.2.1	El seguimiento y la revisión de los servicios de proveedores	se hacen un proceso de seleccione de proveedor y se evidencia en estudio de las cotizaciones y el análisis costo beneficio al final de cada contrato se hace evaluación de servicio a los proveedores	No se evalúan periódicamente los proveedores No todos los proyectos tiene evaluación y el mismo proceso, se debe estandarizar para todos los proyectos	2
27001 - A.15	15. Relaciones con los proveedores	15.2.2	Gestión de cambios en los servicios de proveedores	se siguen las buenas prácticas para el cambio de servicios por terceros	No se tiene documentado los procesos y buenas prácticas para el control de cambios. No se monitorizan los servicios prestados por terceros. no se tiene controles de cambios para los servicios prestados por los proveedores	1
27001 - A.16	**16 Gestión de Incidentes**	**16.1**	**Gestión de Incidentes y Mejoras en la**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**

	SI		**SI**			
27001 - A.16	16. Gestión de Seguridad de la Información de Incidentes	16.1.1	Responsabilidades y procedimientos	Se tiene un sistema donde se ingresan todos los incidentes que afectan la disponibilidad, integridad y confidencialidad, los cuales pueden ser reportados por todas personas de la compañía. Dentro de los roles se tiene especificado la función de quienes ingresan y clasifican los incidentes de seguridad (solicitudes de servicios)	no existe una clasificación explicita que defina las solicitudes de servicios como incidentes de seguridad	1
27001 - A.16	16. Gestión de Seguridad de la Información de Incidentes	16.1.2	Informar sobre los eventos de seguridad de información	En el entrenamiento inicial de los empleados se les informa el procedimiento a seguir para el reporte de incidente	no existe una clasificación explicita que defina las solicitudes de servicios como incidentes de seguridad	1
27001 - A.16	16. Gestión de Seguridad de la Información de Incidentes	16.1.3	Presentación de informes de información debilidades de seguridad	Se tiene un proceso de reporte de incidentes tanto para empleados como contratistas internos	los contratistas y proveedores externos no conocen el proceso y pueden reportar incidentes	1
	16. Gestión de Seguridad de la Información de Incidentes	16.1.4.	Valoración de eventos de seguridad de la información y toma de decisiones	Se tiene incorporado en los grupos primarios de informática mensuales el análisis de resultados de las solicitudes atendidas y los reproceso a través de indicadores , allí se	No se tiene clasificación en el sistema de ingreso de incidentes para seguridad, ni la criticidad, ans	1

				establecen acciones correctivas o preventivas, planes de acciones		
27001 - A.16	16. Gestión de Seguridad de la Información de Incidentes	16.1.5	Respuesta a incidentes de seguridad de la información	Se tienen informes de gestión sobre el incidentes los cuales son reportados a la dirección mensualmente existe un acta de resultados donde se registran los incidentes y esta es aprobada por la dirección.	no se tiene documentado el proceso donde se definen los tiempos de revisión y línea de mando	1
27001 - A.16	16. Gestión de Seguridad de la Información de Incidentes	16.1.6	Aprendiendo de los incidentes de seguridad de la información	En cada uno de los incidentes se registra la solución y tratamiento, en caso de requerirse se hacen acciones correctivas, preventivas y de mejoramiento	no se tiene documentado el proceso para el tratamiento de incidentes de seguridad	1
27001 - A.16	16. Gestión de Seguridad de la Información de Incidentes	16.1.7	El acopio de pruebas		No se tiene establecido un proceso para la recolección de evidencia formal	1
27001 - A.17	**17 Gestión de Continuidad del Negocio**	**17.1**	**Continuidad SI**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.17	17. Aspectos de seguridad de información de la gestión de continuidad del negocio	17.1.1	Información de planificación de continuidad de seguridad	Se tienen procesos para el plan de continuidad de negocios que muestran la recuperación de los servidores y servicios críticos de plataforma garantizando	Los documentos del plan de continuidad de negocios se encuentran desactualizado, no se tiene un documento donde se estipulen los tiempos aceptables de	1

				la continuidad de la plataforma en un tiempo asumido por la empresa	recuperación de cada proceso crítico.	
	17. Aspectos de seguridad de información de la gestión de continuidad del negocio	17.1.2	Implantación de la continuidad de la seguridad de la información	Se tiene incorporado a nivel de plataforma unas revisiones de seguridad y se le da continuidad a las revisiones y planes de acciones en caso de incidentes	No se tiene establecido un procedimiento que reúna toda la esfera de seguridad en cuanto a información de la compañía , no hay un comité de seguridad para velar las revisiones, ni periodicidad para el proceso	1
27001 - A.17	17. Aspectos de seguridad de información de la gestión de continuidad del negocio	17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	El departamento realiza una vez al año como mínimo un simulacro para verificar que los procesos si sean efectivos la información queda registrada en actas de grupo de trabajo de CIU, CIA, CITA. Con los resultados de los simulacros se crean Acciones correctivas, preventivas y de mejoramiento.	No se tiene documentado el plan de simulacros y su periodicidad. Los resultados de los simulacros no se usan para hacer ajustes al plan de continuidad de negocio	1
27001 - A.17	**17 Gestión de Continuidad del Negocio**	**17.2**	**Redundancias**	**Hallazgo positivo**	**Hallazgos negativos (Que Falta)**	**valor**
27001 - A.17	17 Gestión de Continuidad del Negocio	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Se tienen procesos para el plan de continuidad de negocios que muestran la recuperación de los	No se tiene documentado en el plan de continuidad de negocios los servidores redundantes y su tiempo de	2

				servidores y su redundancia y servicios críticos de plataforma garantizando la continuidad de la plataforma en un tiempo asumido por la empresa	activación en caso de incidentes	
27001 - A.18	**18 Cumplimiento**	**18.1**	**información**			
27001 - A.18	18. Cumplimiento	18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Existe clausula confidencial; términos legales entre las partes tanto para empleados como para contratistas se tiene clausulas en los contratos para el cuidado de la propiedad intelectual	No se tiene un documento donde se definan y estipulen las leyes aplicables en tema de seguridad informática en la compañía (Marco legal) y los controles efectuados para garantizar el cumplimiento de las mismas.	1
27001 - A.18	18. Cumplimiento	18.1.2	Derechos de propiedad intelectual	Se tiene en los contratos una clausula hacia la propiedad intelectual, cláusula de confidencialidad y manejo de la información Dentro de las políticas existen secciones para la instalación de software. Se monitorea periódicamente el software instalado en los equipos de la compañía	No se tiene un documento donde se defina la periodicidad del monitoreo de software. no se tiene documentos de informes de los monitoreo hechos al software, ni él se encontró incidentes asociados a la instalación de software no autorizado	1

27001 - A.18	18. Cumplimiento	18.1.3	Protección de los registros	Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad y disponibilidad. Los documentos físicos están bajo llave en zonas seguras y solo pueden ser accedidos por personal autorizado -Se tienen portales en share point para gestión documental en las áreas como recurso humano (Archivo), Ingeniería, Informática, áreas de mercadeo, financiera estos portales se tiene bajo permisos y perfiles de acceso a la información. Se tiene dos archivos físicos de manejo de documentos los cuales son controlados por uso de llave y autorización de personas solo autorizadas, Se tiene una estrategia de bakcup para las base de datos y configuración	La información no tiene ninguna clasificación. no se tiene documentación de los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información -No se tiene un proceso establecido , no se tiene estimado tiempo de retención	1

				de share point-		
27001 - A.18	18. Cumplimiento	18.1.4	Privacidad y protección de datos personales	Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad y disponibilidad. los documentos físico están bajo llave en zonas seguras y solo pueden ser accedidos por personal autorizado -Se tienen procesos que muestran que hay seguridades a nivel de servidores, hay evidencias de capacitación a usuario en manejo de permisos en recursos compartidos, hay un centro de llaves para manejo de archivos físicos; dentro de las revisiones del departamento técnico es realizar revisiones de seguridades en cada micro	La información no tiene ninguna clasificación. No se tiene documentación de los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información las personas no están informadas sobre el tratamiento de datos personales que hace la compañía y su finalidad, no todas las zonas y espacios que son monitoreados y gravados son informados a las personas sobre su tratamiento y finalidad. No se tienen procesos establecidos y documentados para el tratamiento de información de grabaciones de video y llamada. -No hay un procedimiento	1

				a su cargo	escrito para el manejo de esta información	
27001 - A.18	18. Cumplimiento	18.1.5	Regulación de los controles criptográficos	Se tiene controles criptográficos establecidos para los servicios de comunicación y transferencia de información -Se tiene un servidor con el software PGP encargado de administrar procesos de inscripción para portátiles críticos de la compañía presidencia, vicepresidencias, jefes de división. Hay proyectos en ejecución por parte de plataforma para inscripción bases de datos SQL server y estudio de herramientas de backup de usuarios	No se tiene documentados los procesos criptográficos de la compañía y en qué casos estos aplican -No se tiene un proceso definido para el manejo de los controles en diferentes ámbitos del área de informática	1
27001 - A.18	**18 Cumplimiento**	**18.2**	**Revisiones de SI**			

27001 - A.18	18. Cumplimiento	18.2.1	Revisión independiente de la seguridad de la información	Se tienen procesos de revisiones diarias, semanales y mensuales en cuanto a seguridad y salud de la plataforma, Se tienen políticas de grupo contraseñas, accesos y manipulación de equipo; se tiene dentro del proceso de plataforma auditorías internas a los procesos de seguridad, 2 veces al año, Se tiene para el área critica nómina y recurso humano, se realizan auditorias trimestral de hacking ético Se hacen auditorías externas las área de informática a los diferentes procesos de plataforma se tiene planes de auditorías a los procesos	se debe incorporar en la programación de auditorías internas el sistemas de gestión de seguridad de la información se debe actualizar el procedimiento de revisiones de seguridad agregando los reportes de servicios y vulnerabilidades técnicas y demás generalidades de SGSI	1

27001 - A.18	18. Cumplimiento	18.2.2	El cumplimiento de las políticas y normas de seguridad	Se tiene dentro del portal de informática los seguimientos, actas que evidencian la gestión , en el sistema track it las actividades y soluciones, en el sistema de acciones correctivas se tiene acciones correctivas frente a incidentes de seguridad con su trazabilidad Dentro de los contratos se tienen estimadas las obligaciones legales de las partes tanto para empleados como contratistas, en el reglamento de la empresa se orienta al cumplimiento de la norma, En las evaluaciones de desempeño se evalúa el compromiso y el acatamiento de las normas	Se debe establecer una política donde se defina el tratamiento de la información segura y buenas practicas se deben establecer controles para monitorizar y reportar todo uso indebido de los sistemas de información Se debe establecer una política que describa la finalidad de los monitoreo a los servicios críticos de plataforma y áreas seguras (monitoreo de red, servicios, llamadas, videos) se debe crear una estrategia de comunicación a todas las personas internas y externas sobre los monitores y su finalidad ---------- No se tiene definido un proceso de revisión periódica del cumplimiento de los requerimientos legales. No se tienen actas de revisión de los requerimientos legales	1
27001 - A.18	18. Cumplimiento	18.2.3	Revisión de cumplimiento técnico	Se tienen reportes que evidencian	No se tiene definido el proceso formal	1

				análisis de vulnerabilidades, test de penetracioncitas calendario para realizar estas tareas, resultado de auditorías de seguridad interna	para la revisión de actividades diarias de los servicios de infraestructura	

Tabla 1. Análisis diferencial

FASE 2: SISTEMA DE GESTIÓN DOCUMENTAL

2.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A continuación se describirá la política de seguridad de la información de la organización: Para la organización la seguridad de la información de los sistemas que se gestionan y/o operan es de vital importancia y se protegerá de cualquier pérdida en su confidencialidad, integridad y disponibilidad.

Con su divulgación se busca que toda la organización incluyendo empleados, contratistas, terceros y directivos conozcan ese marco normativo y de forma individual y colectiva brinden su apoyo para que la organización administre, utilice y disponga de información con niveles adecuados de seguridad.

Textilera S.A, ha definido la política institucional a definido la política institucional y una serie de políticas específicas de seguridad de la información las cuales hacen parte del SGSI y se encuentra en documentos anexos de este documento.

Ver anexo: PW-15-007 Política de seguridad de la información .doc

2.3 DOCUMENTACIÓN DEL SGSI

Como parte de la documentación del Sistema de Gestión de Seguridad de la Información tenemos entre otros los siguientes documentos, considerados procedimientos de seguridad

- Procedimientos de Auditorías Internas
- Gestión de Indicadores
- Procedimiento de Revisión por la Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos

Un Procedimiento de seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los Procedimientos de

Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización. Se describe cómo se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios.

Para cada uno de estos documentos tenemos la misma estructura con el fin de conservar una consistencia en toda la documentación, la estructura del documento contendrá además de un encabezado en donde se registrara título del procedimiento, código establecido por manual de calidad y administración documental, un subtítulo, un responsable, un numero de edición, un campo de aprobación, una fecha, total de páginas y anexos si contiene.
Además de un control de cambios del documento.

- **Procedimientos de Auditorías Internas:**

Verificar si el sistema de gestión de seguridad de la información opera de acuerdo con los planes, procedimientos, registros y controles establecidos y es conforme con los requisitos de la norma ISO 27001:2013 y es eficaz para satisfacer los requisitos relacionados con seguridad de la información

Ver anexo: PQ-01-171 .doc

- **Gestión de Indicadores:**

Se implementarán indicadores de gestión para mantener monitorizado y actualizado del SGSI, los cuales permitirán controlar el funcionamiento de las medidas de seguridad implementadas, eficacia y eficiencia.

Ver anexo**:** PQ-01-013.doc

- **Procedimiento de Revisión por la Dirección:**

El Sistema de Gestión de Seguridad de la Información contempla una evaluación periódica, sistemática y estructurada a cargo de la Alta Dirección que permite asegurar una adecuada planeación y la corrección de las desviaciones en el cumplimiento de los objetivos y como tal, incluye la toma de decisiones sobre acciones necesarias, que dentro de un marco de conveniencia razonable para la organización, promueva el mejoramiento de productos, procesos y capacidades organizacionales que permitan alcanzar resultados de eficiencia, eficacia y efectividad.

Ver anexo: PQ-01-011.doc

- **Gestión de Roles y Responsabilidades:**

El Sistema de Gestión de Seguridad de la Información define los diferentes roles y funciones.

Entre estas definiciones de roles y responsabilidades se podrán identificar alguno de los siguientes ítems:

- Quien es el responsable de la ejecución de cada hito
- Quien toma las decisiones, solo o conjuntamente con otros
- Quien gestiona los recursos y controla el progreso del trabajo
- Quien debe ser informado
- Quien debe ser consultado
- Quien debe participar
- Quien debe dar apoyo o dotar de infraestructura al equipo
- Quien asegura la calidad de los resultados

Ver anexo: PQ-01-012.doc

- **Metodología de Análisis de Riesgos**

La realización del análisis de riesgos tiene como fin identificar de manera clara los riesgos a los cuales está expuesta la organización, y basados en esta identificación de los riesgos determinar cuáles medidas de seguridad serán las adecuadas para los diferentes activos de seguridad de la información, de igual manera permite establecer los planes de contingencia, para este caso realizaremos un análisis de riesgo residual, que es un tipo de análisis que se realiza teniendo en cuentas las medidas de seguridad que la organización ya tiene planteadas, como resultado de este tipo de análisis se obtiene el riesgo real al cual están expuestos los diferentes activos de la información que tiene la organización.

De las diferentes metodologías existentes en el mercado, se optó por utilizar, Magerit.
MAGERIT es un instrumento para facilitar la implantación y aplicación del Esquema Nacional de Seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información

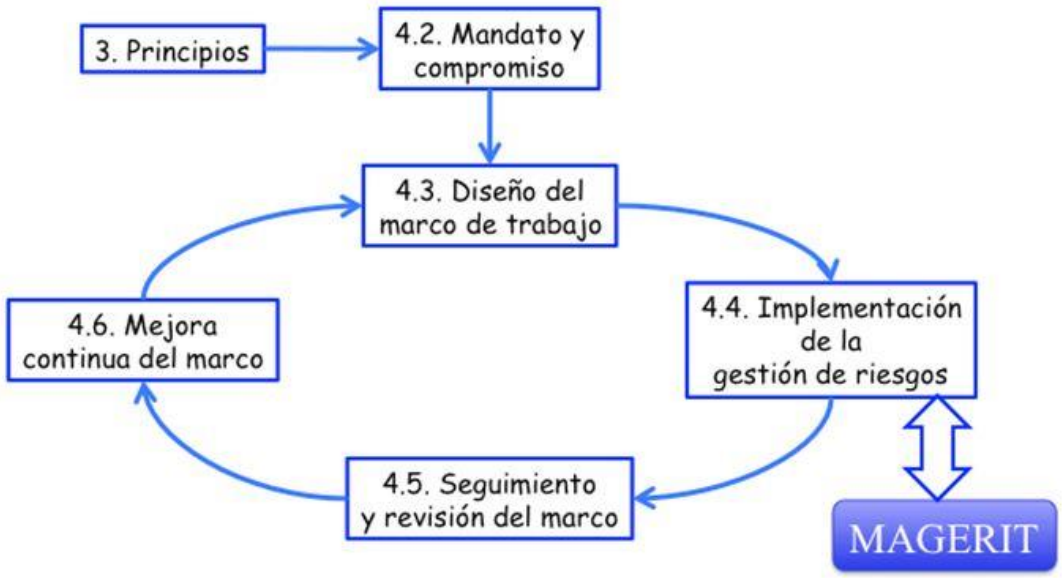


Ilustración 6. Magerit.

MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

El análisis de riesgos considera los siguientes elementos:

1. Activos: Son los recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objeticos propuestos por la dirección.

2. Amenazas: Son las situaciones o hechos que pueden producir daño y que les pueden pasar a los activos causando un perjuicio a la organización.

3. Vulnerabilidades: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo de la información.

4. Impacto: Daño causado sobre el activo de la información una vez se materializa una de las vulnerabilidades, conociendo el valor de los activos es más sencillo estimar el valor del impacto.

5. Riesgo: Es la probabilidad de que una amenaza se materialice y afecte a los activos de la información.

6. Salvaguardas: Mecanismo de protección frente a las amenazas.

Al análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de que perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

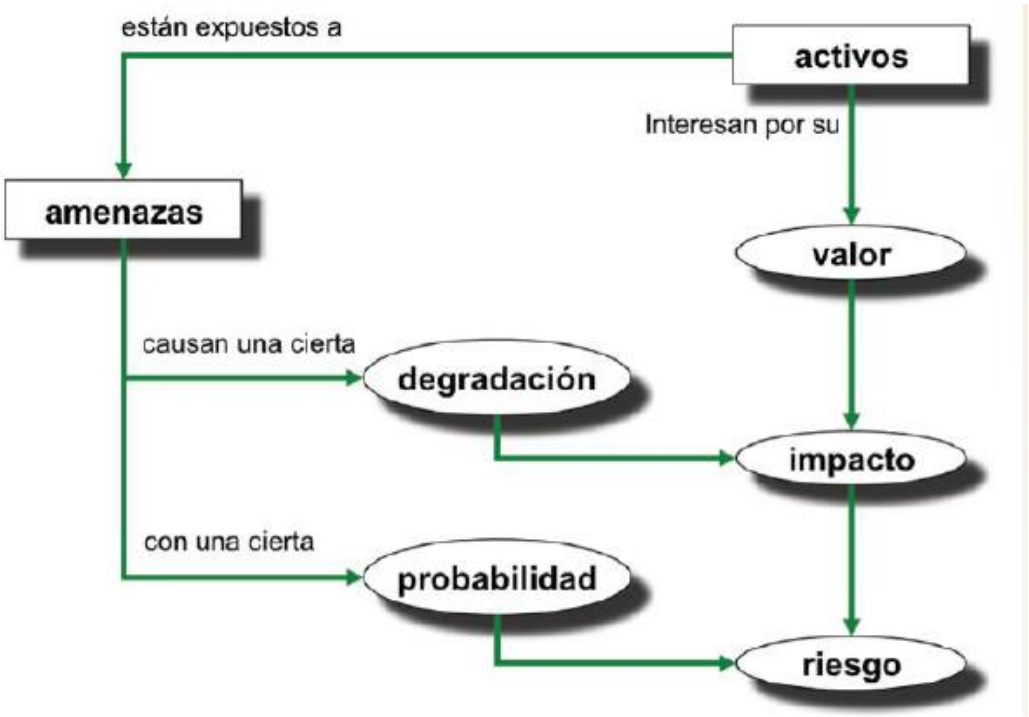


Ilustración 7. Elementos de análisis riesgos potenciales

- **Declaración de aplicabilidad**

  En el documento anexo de declaración de aplicabilidad esta la tabla con todos los controles de la norma en donde se observa si existen controles, y la razón de la selección de cada uno de ellos, resaltando si el control surge de un requerimiento legal, de una obligación contractual, de un requerimiento de negocio o de las mejores prácticas, o si el control surge como resultado del análisis de riesgos realizado a los activo de información de la organización

  Ver anexo**:** Declaración de aplicabilidad y hoja de verificacion.xlsx

3.1 PROCESO DE GESTIÓN DE RIESGOS

La gestión de riesgo se puede definir como un proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si dicha acción sucede, para ilustrar un poco el proceso de gestión de riesgo y cómo interactúan en el sus diferentes elementos, anexamos el diagrama siguiente:

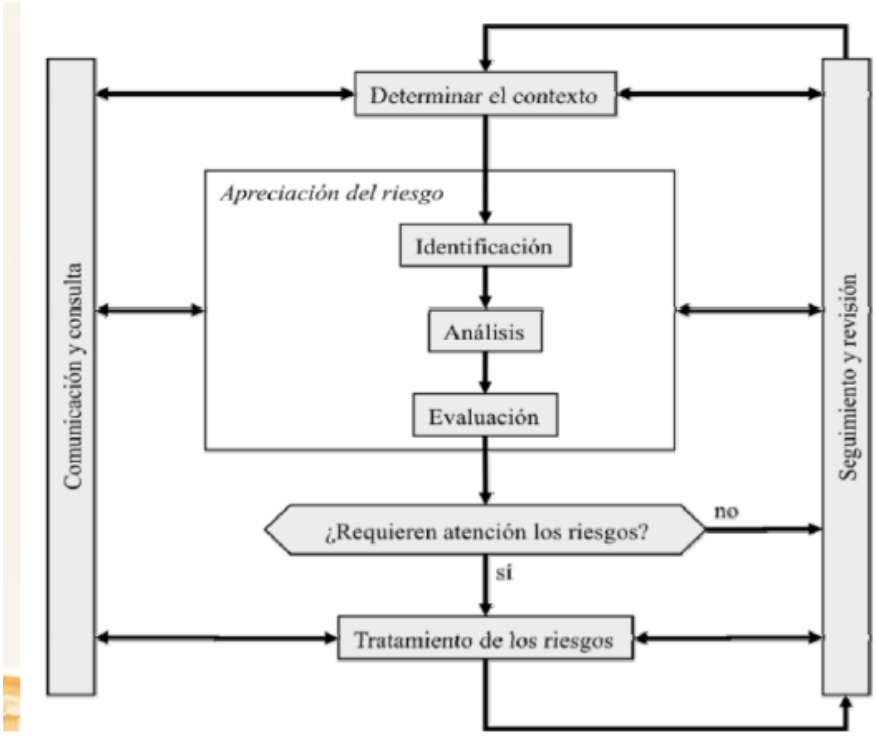


Ilustración 8. Proceso de gestión de riesgos (Tomado Magerit versión 3)

Una vez contemplados los anteriores elementos para el análisis de riesgo, las opciones ante los riesgos son las siguientes:

- Aceptarlo: Significa que la organización en cabeza del comité de riesgos y procesos decide no emprender ninguna acción, en este caso se asume el impacto en caso de que se materialice el riesgo, en tal caso si se produce un incidente se procederá a la recuperación esta opción no debería darse para riesgos altos o que comprometan activos de información relevantes para la organización, es una acción aceptable ante activos de información despreciables (desde el punto de vista de importancia para la organización, así su costo pueda ser alto).

- Mitigarlo: Esta opción es la que más se presenta luego de los análisis de riesgos respectivos, y significa que una vez la organización identifica un riesgo, se aplican salvaguardas o medidas de protección que buscan minimizar o reducir el riesgo, para que en caso de que la amenaza se materialice sus consecuencias no sean tan altas o desastrosas como en caso de que el riesgo no se minimice.

- Transferirlo: Para este acción, y una vez identificado el riesgo la organización decide que a pesar de las medidas tomadas su probabilidad no se puede disminuir más, y que la organización no puede asumirlo, llegados a este punto estos riesgos se transfieren, para lo cual lo usual es usar alguna póliza de seguros que nos proteja en caso de que se materialice el riesgo, un ejemplo común de estos serían las pólizas contra incendios que tomas las organizaciones (a pesar de tener controles para minimizar los riesgos de incendios).

- Evitarlo: Una vez identificado el riesgo la organización decide eliminarlo, bien sea eliminado el activo de información susceptible al riesgo, elimina o cambio el proceso o servicio o elimina la amenaza o la vulnerabilidad que la permitía, esta acción es poco frecuente porque implica eliminar activos de información.

Una vez analizados los riesgos, se debe dar una verificación sobre la viabilidad tanto técnica como económica y operativa de las contramedidas o salvaguardas seleccionadas para mitigar los riesgos, es factible en esta etapa que las acciones sobre los riesgos cambien, debido a la imposibilidad o demora en realizar inversiones económicas, que las viabilidades técnicas no sean factibles, o que operativamente el impacto de implementar las salvaguardas o medidas de mitigación del riesgo sean muy altas (demoras adicionales en los procesos, contratación de gente, impacto en los tiempos de entrega, etc), de igual manera en los temas de costos es importante revisar que la inversión en las contramedidas no sea más alta que el valor de los activos, en cuyo caso no hace sentido realizar estas inversiones y debemos realizar un cambio en la acción que se tomara sobre el riesgo identificado.

Con esta información clara y debidamente costeada en términos económicos y de recursos humanos y de tiempo, la Gerencia de Procesos y riesgos debe determinar los niveles de riesgo que la organización está dispuesta a asumir y sus costos asociados, con este panorama claro se deben determinar los controles a aplicar a los diferentes riesgos identificados.

Para aclarar aún más la metodología Magerit expondré en un ejemplo el proceso con un activo.

Nuestro activo será un servidor web cuyo valor es 4000 dólares.
Lo primero es establecer parámetros:

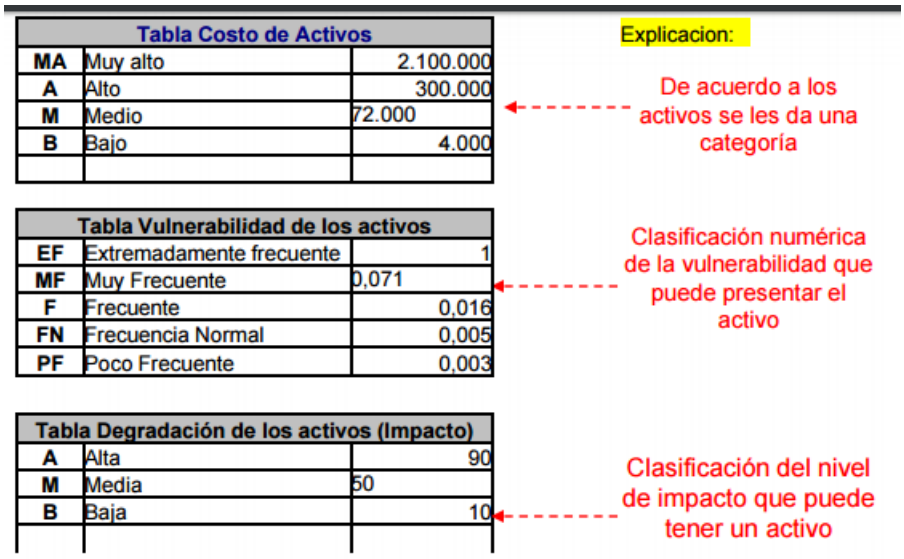


Ilustración 9. Tablas de costos, vulnerabilidad y degradeacion

Luego se identifican las amenazas globales:
Para nuestro caso podriamos tomar A1. daño de hardware, A2. incendio de oficinas, A3. acceso no autorizado oficinas.
Teniendo, la probabilidad, el imacto calculamos el riesgo:

Amenaza		probabilidad		Impacto		Riesgo
A1	daño de hardware	EF	1	M	50	50
A2	incendio de oficinas	PF	0.003	A	90	2.7
A3	acceso no autorizado oficinas	MF	0.071	B	10	0.71

Tabla 2. Tabla Ejemplo

Una vez calculado el riesgo se deben tratar aquellos riesgos que superan un límite que nosotros hayamos establecido. Por ejemplo, se trataran aquellos riesgos “muy altos” y “altos” y se debe a la hora de tratar el riesgo, establecer entre las 4 estrategias, en este caso: aceptarlo, evitarlo, mitigarlo o transferirlo. Estableciendo controles o salvaguardas para disminuir el impacto.

En nuestro ejemplo podríamos tratar daño de hardware (Evitarlo) e incendio de oficinas (Mitigarlo).

Las salvaguardas para daño de hardware, seria plan de monitoreo o aplicativo de diagnóstico que permitan generar alarmas y reportes, renovación de garantía y contratos para atención, partes en inventario en caso de manejar almacén.

El salvaguarda para incendio modelo ARP implementado, plan de continuidad del negocio, pólizas.

Posteriormente se debería calcular el riesgo residual, los riesgos remanentes que existen tras la implementación de salvaguardas, el cual es el resultado de la multiplicación de valor del activo por la probabilidad.

Para nuestro ejemplo seria:

Amenaza		**probabilidad**		**Valor activo**	**Riesgo Residual**
A1	daño de hardware	EF	1	4000	4000
A2	incendio de oficinas	PF	0.003	4000	12
A3	acceso no autorizado oficinas	MF	0.071	4000	284
Total					4296

Tabla 3. Tabla resultante

Con este análisis deberían salir los proyectos que deberán gestionarse en la organización.

3.2 INVENTARIO DE ACTIVOS

Un análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.
El inventario de los activos de la información queda reflejado en la siguiente tabla.

Tabla de Inventario de activos	
Ámbito	**Activo**
Instalaciones	Centro de procesamiento de datos principal
	Centro de procesamiento de datos alterno
	Ubicación local de infraestructura y comunicaciones
	sala eléctrica, ups, telecomunicaciones
Hardware	Servidores
	Equipos escritorio, portátiles
	Equipos de comunicaciones
	Equipos de seguridad perimetral
	Planta telefónica
Software base	Windows server 2008 R2
	Windows server 2012
Aplicaciones	Bases de datos: SQL server 2008 estándar
	Correo electrónico: Exchange
	Antivirus: Symantec Endpoint
	Webserver: IIS

	Sistema de backups: Symantec System recovery
	Erp: JDEdwards
	Aplicaciones scada
Datos	Aplicaciones de desarrollo :Visual studio .Net y SQl developer
	Código fuente aplicaciones de planta y administrativas
	Registros de operación: logs, informes y monitoreo
	Bases de datos corporativas
Red	Backups de usuarios corporativos
	Red de datos
	Red de telefonía
	acceso a Internet
Servicios	Red de control e instrumentación
	Internet
	Intranet
	Telefonía
Equipos adicionales	Correo
	Sistema de alimentación UPS
	Generadores de energía
	Sistema de aire acondicionado
Personal	Equipos de control de temperatura
	Coordinador de infraestructura
	Administrador de base de datos
	Analistas funcionales
	Desarrolladores
	técnicos de operación
	Analista de seguridad de la información Director de informática
Soportes de información	Discos duros de servidores y estaciones de trabajo
	Discos externos información de backups
	Unidades de CD , DVD y Memorias extraíbles

Tabla 4. Inventario de activos

3.3VALORACIÓN DE ACTIVOS

Siguiendo la metodología se define una tabla de valoración de activos con el fin de utilizarla sobre la tabla general de los activos de información.

Las escalas de valoración de los activos quedan definidas con las siguientes categorías muy bajo, bajo, medio, alto y Muy alto, y se han definido unas abreviaturas para cada una de ellas con el fin de poder utilizarlas más adelante.

Valor de los activos		
Descripción	**Abreviatura**	**Valor**
Muy alto	MA	>100000
Alto	A	>40000 <100000
Medio	M	>9000 <40000
Bajo	B	>3000 <90000
Muy Bajo	MB	>500 <3000

Tabla 5. Valor de Activos

En esta tabla quedan establecidos los rangos de valores de los activos de la información en las categorías respectivas, en donde los activos de valor muy bajo esta en un rango de mayor de 500 dólares y menor de 3000 y en donde un activo con valor mayor a 100000 dólares se considera un activo con un valor muy alto.

A continuación se presenta en la siguiente tabla los elementos claves de la organización. Clasificados por activo teniendo en cuenta si criticidad, valor, categoría (Hardware, software, Interfaces, datos, personal), servicios y misión.

Los activos contemplados se seleccionaron pensando que algún incidente o paro de la operación de alguno de ellos impactaría la operación, la continuidad del negocio.

Además del impacto en cuanto a los principios confidencialidad, integridad y disponibilidad de los datos y sistemas de información.

Elementos claves del sistema de la organización										
id	**Activo**	**Criticidad**	**valor**	**categoría**					**Servicios**	**Misión**
				Hardware	**Software**	**Interfaces**	**Datos**	**Personal**		
1	Servidores controladores de dominio	Alta	Medio	**X**	**X**		**X**		Servidor de autenticación centralizada	Autenticación centralizada y servicios de Directorio activo y DNS
2	Servidor web	Medio	Medio	**x**	**x**				Servidor de página Web e intranet	Publicar la información corporativo a nivel web e intranet para empleados, clientes, proveedores
3	Servidores file server	Alto	Alto	**X**	**X**		**X**		Servidor de archivos	Servidor de directorios con información corporativa propia de áreas y usuarios lideres
4	Servidores de correo	Medio	Alto	**X**	**X**		**X**		Servidor correo electrónico de la organización	Intercambio de correo interno y externo
5	Servidor de nomina	Medio	Medio	**X**	**X**		**X**		Servidor de Nomina	Servidor donde se gestiona la nómina de los colaboradores

6	Servidores ERP	Alto	Medio	X	X		X		Servidor de Enterprise Resource Management	Servidor de administración centralizada de recursos empresariales
7	Servidores Base de datos planta	Alto	Alto	X	X		X		Servidor de base de datos	Servidor de administración de las bases de datos corporativas y críticas de la organización
8	Equipos de seguridad perimetral	Alto	Muy Alto	X	X	X			Servicios de seguridad perimetral	Protección de las redes de datos de accesos no autorizados
9	Equipos telecomunicaciones	Alto	Alto	X	X				Transmisión de datos	Gestionar la transmisión de los datos generados en el negocio
10	Código fuente (aplicaciones administrativas/planta)	Alto	Muy Alto		X				Código fuentes de las aplicaciones de negocio de la organización	fuentes de aplicaciones críticas de planta y administrativas
11	Analistas funcionales	Alto	Medio					X	Analistas funcionales de las diferentes áreas de la organización	Proveer soluciones a los procesos críticos de los negocios y gestionar cambios en pro de la organización
12	Coordinador de TI	Alto	Alto					X	Administración de infraestructura, comunicaciones y seguridad	Responsable de mantener los servicios operativos y proveer continuidad en el negocio
13	Desarrolladores de Software	Alto	Medio					X	Desarrollo de software de la organización	Desarrollar e implementar los desarrollos de software de la organización mejorando y optimizando los procesos tanto administrativos como de la planta de producción
14	Aplicaciones scada	Alto	Muy alto	X	X	X	X		Aplicaciones críticas para el funcionamiento y operación de las máquinas de producción	Permitir la operación y la administración de la operación de las máquinas de producción, controlando, mejorando estándares de calidad del producto
15	Discos externos con respaldos corporativos	Alto	Alto				X		Discos externos donde se almacenan la información corporativa	Almacenar backup corporativos y bases de datos de la organización para luego ser trasladados a otra sede y se guardados en la caja fuerte.
16	Jefe De división informática	Alto	Medio					X	Administración de la división informática	Responsable de dirigir las diferentes áreas de la división informática garantizando el cumplimientos de metas y objetivos de la organización

Tabla 6. Elementos claves del sistema de la organización

3.4 DIMENSIONES DE SEGURIDAD

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico.

Identificados los activos se realiza entonces la valoración ACIDA de los mismos. Dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración permitirá a posteriori valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuesto (no cubierto por las salvaguardas en cada una de las dimensiones).

El valor que reciba un activo puede ser propio o acumulado. El valor propio se asignará a la información, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Así pues, los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se apoyan en ellos. Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar.

En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios:

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla 7. Valoración Dimensiones de Seguridad

A continuación la valoración de las dimensiones de seguridad de los activos que incluyen aspectos como Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad.

3.5TABLA RESUMEN DE VALORACIÓN

A continuación la valoración de las dimensiones de seguridad de los activos que incluyen aspectos como Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad.

Valoración Dimensiones de Seguridad de los Activos

			Aspectos Críticos				
Ámbito	**Activo**	**Valor**	**A**	**C**	**I**	**D**	**T**
Instalaciones	Centro de procesamiento de datos principal	Muy Alto				10	
	Centro de procesamiento de datos alterno	Muy Alto				10	
	Ubicación local de infraestructura y	Alto				7	

	comunicaciones						
	sala eléctrica, ups, telecomunicaciones	Muy Alto				10	
Hardware	**Servidores controladores de dominio**	Muy Alto	10	10	10	10	9
	Servidor web	Medio	6	5	6	5	6
	Servidores file server	Muy Alto	10	10	10	8	10
	Servidores de correo electrónico	Muy Alto	10	10	10	9	10
	Servidor de nomina	Muy Alto	10	10	10	10	10
	Servidores ERP	Muy Alto	10	10	10	10	9
	Servidores Base de datos	Muy Alto	10	10	10	10	9
	Servidor de antivirus	Medio	7	6	7	6	7
	Servidor planta	Muy Alto	10	10	10	10	9
	Servidor de impresión	Medio	6	5	5	5	5
	Servidor de Encripcion PGP	Medio	7	6	7	6	7
	Dispositivo almacenamientos NAS para Backups	Muy Alto	10	10	10	8	10
	Servidor filtrado spam	Muy Alto	10	9	9	10	9
	Equipos escritorio, portátiles	Alto	8	6	7	7	7
	Equipos de comunicaciones:HP, D-Link	Muy Alto	10	9	10	10	9
	Equipos de seguridad perimetral:Firewall Fortinet	Muy Alto	10	10	10	10	10
	Planta telefónica: Siemens	Medio	5	6	6	7	7
Aplicaciones	Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	Muy Alto	10	9	8	10	10
	Sistemas Operativos Clientes :windows 7, Winodws 8, windows 10	Alto	7	8	7	6	8
	Bases de datos: SQL server 2008 estándar	Muy Alto	10	10	10	10	10
	Correo electrónico: Exchange	Alto	9	8	8	7	8
	Antivirus: Symantec Endpoint	Alto	9	6	8	6	8
	Webserver: IIS	Medio	6	5	6	5	6
	Sistema de backups: Symantec System recovery, Cobian	Alto	8	8	8	6	8
	ERP: JDEdwards	Muy Alto	10	10	10	10	9
	Sistemas SCADA	Muy Alto	10	10	10	10	9
	Aplicaciones de desarrollo :Visual studio .Net y SQl developer	Medio	7	6	6	6	7
Datos	Código fuente aplicaciones de planta y administrativas	Muy alto	9	9	9	10	9
	Registros de operación: logs, informes y monitoreo	Medio	6	6	6	6	5
	Bases de datos corporativas	Muy alto	10	10	10	10	9
	Backups de usuarios corporativos	Alto	9	8	8	9	8
Red	Red de datos	Muy Alto				10	
	Red de telefonía	Medio				7	
	acceso a Internet	Alto				9	
	Red de control e instrumentación	Muy alto				10	
Servicios	Internet	Alto				9	

	Intranet	Medio				5	
	Telefonía	Medio				7	
	Correo	Muy Alto				10	
Equipos adicionales	Sistema de alimentación UPS	Muy alto				10	
	Generadores de energía	Muy Alto				10	
	Sistema de aire acondicionado	Alto				9	
	Sistema de cableado Eléctrico: Centro de datos principal	Muy alto				10	
	Sistema de cableado Eléctrico: Centro de datos alterno	Muy alto				10	
	Sistema de cableado Eléctrico: Sede alterna	alto				9	
	Sistema de cableado datos: Sede alterna	alto				9	
	Sistema de cableado datos : Centro de datos principal	Muy alto				10	
	Sistema de cableado datos: Centro de datos alterno	Muy alto				10	
	Equipos de control de temperatura	Medio				8	
Personal	Coordinador de TI	Muy alto		10		10	
	Administrador de base de datos	Muy alto		10		10	
	Analistas funcionales	Alto		9		9	
	Desarrolladores	Alto		9		9	
	técnicos de operación	Muy alto		10		10	
	Analista de seguridad de la información	Muy alto		10		10	
	Director de informática	Alto		8		9	
Soportes de Información	Discos duros de servidores y estaciones de trabajo	Muy alto	10	10	10	10	10
	Discos externos información de backups	Muy alto	9	7	10	8	10
	Unidades de CD , DVD y Memorias extraíbles	alto		6	8	7	

Tabla 8. Valoración dimensiones de seguridad de los activos**.**

3.6 ANÁLISIS DE AMENAZAS

Los activos están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad. A nivel metodológico, analizaremos qué amenazas pueden afectar a qué activos.

A continuación identifico el inventario de amenazas clasificadas por:

- Desastres naturales.
- De origen industrial.
- Errores y fallos no interconectados.
- Ataques intencionales.

Igualmente identificada por cada una su agente generados, causa y efecto:

TABLA IDENTIFICACION AMENAZAS							
id	**Amenazas**	**Fuente**			**Agente Generador**	**Causa**	**Efecto**
		Natural	**humana**	**Entorno**			
1	Ejecución de software malicioso			X	Personas malintencionadas , Error humano	Falta de un endpoint (antivirus) ,ausencias de políticas en el endpoint, ausencias de filtrado contenido, filtrado de puertos, malas prácticas de navegación y periféricos	Indisponibilidad, perdida de información, perdida de integridad, robo de información
2	Ataque aplicaciones			X	Personas malintencionadas dentro de la compañía	Desmotivación, competencia desleal entre compañías, malos controles en el desarrollo, mal diseño de la aplicación, malos controles criptográficos	Indisponibilidad, perdida de información, perdida de integridad, robo de información, pérdida de imagen
3	Ataque infraestructura			X	Personas malintencionadas dentro de la compañía	Desmotivación, falta de parches actualizados, mala configuración de políticas	Indisponibilidad, perdida de información, perdida de integridad, robo de información, accesos no autorizados.
4	falta de sistema de parches			X	Personas no capacitadas	Ausencias de proceso en el modelo, falta de un software centralizado para parches	Ataques al sistema vulnerable, inestabilidad del sistema, problemas de compatibilidad entre versiones, lentitud en los procesos
5	Falta de software de control de versiones			X	Personas no capacitadas	Ausencias de proceso en el modelo, falta de un software control de versiones	Perdida de información
6	Robo de información		X		Personas malintencionadas	Falta de controles de acceso, mala configuración de políticas, falta de controles criptográficos, falta de controles en trasporte de información	Ataques al sistema, daño a la imagen corporativa
7	Ausencia de estándares en cableado estructurado			X	Personal no capacitado	Falta de controles en el modelo de calidad, falta de personal capacitado, falta de dinero	Rendimiento, indisponibilidad, eficiencia en la recuperación, ataques a la red

8	Uso de software no oficial			X	Personal no capacitado, personal malintencionado de la compañía	Falta de controles en el proceso de gestión de seguridad, falta de conocimiento del personal, falta de recursos para la compra de herramientas, falta de un proceso de monitoreo	Ataques al sistema, daño a la imagen corporativa, indisponibilidad, rendimiento de las maquinas, integridad en la información, falta de actualización de parches, afectaciones legales
9	Acceso no autorizado		X		Personal no capacitado, personal malintencionado	Falta de controles de acceso, mala configuración de políticas	Ataques al sistema, daño a la imagen corporativa, perdida de información, integridad de la información, indisponibilidad
10	Retiro personal		X		Empleados de la compañía	Desmotivación, mejores oportunidades, ambiente laboral, calamidad domestica	afectación a los tiempos de entrega de proyectos, daño de imagen corporativa, congelación de proyectos en curso, afectación legal
11	Incapacidad		X		Empleados de la compañía	Falta de controles en salud ocupacional, recarga laboral, falta de controles contractuales	afectación a los tiempos de entrega de proyectos, daño de imagen corporativa, congelación de proyectos en curso, afectación legal
12	Poca disponibilidad			X	Empleados de la compañía	mala planeación de mercado, falta de análisis en la capacidad, poco personal, mala distribución de roles, falta de personal de capacitado	afectación en tiempos de entrega, mal diseño en los proyectos, Malas pruebas de calidad de software, afectación legal, mal cumplimiento de los requisitos, congelación del proyecto
13	Copia no autorizada		X		Personal malintencionado interno	Falta de controles de acceso, mala configuración de políticas de grupo, escalamiento de privilegios	Ataques al sistema, daño a la imagen corporativa
14	Borrado y alteración		X		Personal malintencionado	Falta de controles de acceso, mala configuración de políticas, falta de controles criptográficos, falta de controles en trasporte de información	Ataques al sistema, daño a la imagen corporativa
15	Incendio	X			Personal malintencionado, personal no capacitado, amenaza natural, ubicación geográfica	Agentes naturales, Desmotivación, malos controles en seguridad ambiental, seguridad física, mala ubicación geográfica, entorno inseguro, malas prácticas en la eliminación física de información, mala revisión	Perdida de información, indisponibilidad

						del sistema eléctrico, falta de revisión en extintores	
16	Terremoto	X			amenaza natural, ubicación geográfica	Agente natural, ubicación geográfica en una zona de alto riesgo de terremoto	Indisponibilidad, perdida de información
17	Falla eléctrica	X			Personal malintencionado, personal no capacitado, amenaza natural, fallas de servicio con proveedor	Agente natural, falta de controles en sistema de cableado de energía, personal no capacitado, problemas de servicio con proveedor	Indisponibilidad, perdida de información
18	Inundación	X			Personal malintencionado, personal no capacitado, amenaza natural, fallas de servicio con proveedor	Agente natural, falta de controles en sistema de acueducto, personal no capacitado, problemas de servicio con proveedor	Indisponibilidad, perdida de información
19	Terrorismo		X		Personas malintencionadas	Desmotivación, problemas sociales, culturales, religiosos	Suspensión de tareas, muerte, afectaciones legales
20	Desmotivación		X		Empleados de la compañía	Poco apoyo de alta gerencia, acoso laboral, falta de un buen modelo de bienestar laboral, salarios bajos	Ataques al sistema de información, Atentados a la organización, afectaciones legales, afectaciones en tiempos de entrega de proyectos, sindicatos, divulgación de información confidencial.
21	Solo un especialista		X		Personal de la compañía	Falta de un modelo apropiado en la creación de roles, falta de recursos para contratación de personal especializado	afectación en permisos y controles de acceso, pérdida de control del servidor, indisponibilidad, falta de creación de usuarios a tiempo, falta de cambios a tiempo, afectación a los clientes, afectación en los procesos de negociación

22	Negligencia		X		Empleados de la compañía	Problemas de controles en el proceso contractual, no confirmación de nuevos empleados en situaciones laborales en otras empresas, falta de evaluación en el perfil sicológico	afectaciones en tiempos de entrega de las soluciones y proyectos, congelación de proyectos, indisponibilidad del servicio, perdida de información
23	Mal diseño de los procesos			X	Personal de la compañía	mal entendimiento de sus requerimientos, malos procesos de gestión de proyectos	Insatisfacción
24	Líder inexperto			X	Personal de la compañía	mal entendimiento de sus requerimientos, malos procesos en sensibilización, malos procesos de gestión de proyectos	Insatisfacción
25	Analistas inexpertos			X	Personal de la compañía	mal entendimiento de sus requerimientos, malos procesos en sensibilización, malos procesos de gestión de proyectos	Insatisfacción
26	Falta de alcances claros			X	Personal de la compañía	Personal inexperto, falta de procesos claros en los proyectos de actualización de tecnología	Indisponibilidad, falta de integridad, improductividad en los proyectos, congelación de proyectos
27	Robo de equipos		X		Personas malintencionadas	Falta de controles de acceso, falta de un proceso de control de acceso físico, falta de un proceso en seguridad perimetral física, falta de políticas de horarios seguros a la empresa, problemas socioculturales en la ubicación geográfica local	Indisponibilidad, perdida de información, robo de información, congelación de proyectos, congelación de procesos operativos
28	Pérdida de capacidad de servidores			X	Personal de la compañía	falta de capacitación de personal, falta de monitoreo, falta de procesos para monitorear, falta de depuración de la información, falta de concientización en el uso de recursos	Indisponibilidad, perdida de información, congelación de proyectos perdida de rendimiento, afectación en tiempos de entrega en los proyectos

Tabla 9. Identificación de Amenazas

Para continuar con el proceso de valoración de riesgos es necesario definir una tabla en donde estén estimadas las Probabilidades/frecuencias de ocurrencias de las amenazas.

Probabilidad/Frecuencia		
Calificación		**Explicación**
A	1	100%, Alta, siempre ocurre
M+	0.75	75%, Mayor, probable, se espera que ocurra
M+	0.5	50% se espera que no ocurra regularmente
M-	0.25	25%,No esperado pero podría ocurrir algunas veces
B	0.1	10%, Remoto, puede ocurrir en circunstancias excepcionales

Tabla 10. Cálculo de Probabilidad/frecuencias

EL análisis de impacto: El impacto adverso de un evento de seguridad se puede describir en términos de la degradación de una o varias de las metas de seguridad (integridad, Disponibilidad y Confidencialidad).

Perdida de integridad: Se pierde cuando se prestan modificaciones no autorizadas sobre los datos y sistemas, bien sea de manera accidental o intencional.

Pérdida de Disponibilidad: Si un sistema de misión crítica no está disponible para sus usuarios finales, se afecta el logro de la misión de la organización.

Perdida de confidencialidad: La confidencialidad de los datos y sistemas se refiere a la protección contra la divulgación no autorizada.

Las siguientes tablas de impacto valoran de manera cuantitativa el valor del impacto a nivel de operación, financiero y en la información de ocurrencia de las amenazas.

Impacto Financiero		
Calificacion	**Explicacion**	**Detalle**
A	Muy Alto, Mas de 500.000 Dolares Mensuale	La explotacion de la vulnerabilidad puede resultar en altas perdidas financieras por daño de activos o recursos tangibles
M+	Alto , De 250.000 a 500.000 Dolares	Perdida financiera significativa, amenaza con perdida de imagen de la organizacion
M	Medio, De 100.000 a 250.000 dolares	Perdida financiera moderada, no amenaza la imagen y confianza de la organizacion
M-	Bajo, Hasta 100.000 dolares	Perdida financiera menor
B	Menor, Hasta 50.000 dolares	Sin perjuicios, costos asociados bajos

Tabla 11. Impacto Financiero

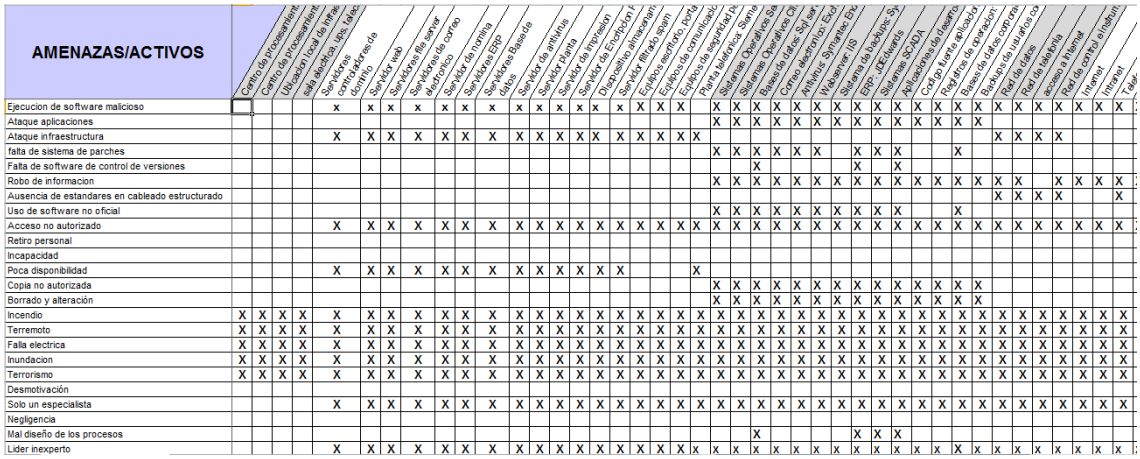
Impacto Operacion		
Calificacion	**Explicacion**	**Detalle**
A	Muy Alto	Hay una indisponibilidad por más de 48 horas, es necesario establecer un mecanismo de procesamiento alterno.
M+	Alto	Hay una indisponibilidad entre 36 y 48 horas, se requiere al proveedor en sitio.
M	Medio	Hay una indisponibilidad entre 12 y 36 horas, se requiere consulta el proveedor
M-	Bajo	Hay una indisponibilidad entre 4 y 12 horas, es necesario escalarlo a 2 nivel
B	Menor	Hay una indisponibilidad menor a 4 y la puede resolver la mesa de ayuda.

Tabla 12. Impacto Operación

Impacto en la información (disponibilidad, confiabilidad, integridad)		
Calificación	**Explicación**	**Detalle**
A (100%)	Muy alto	La información no está disponible por más de 48 horas
M+ (75%)	Alto	La información no está disponible entre 24 y de 48 horas
M (50%)	Medio	La información no está disponible 8 y 24 horas
M- (25%)	Bajo	La información no está disponible 3 y 8 horas
B (10%)	Menor	La información no está disponible por menos de 3 horas.

Tabla 13. Impacto a la información**.**

Después de determinar las tablas es necesario la elaboración del escenario de riesgos por lo que se colocaron las amenazas vs los activos y se identificó su relación.



Ver anexo. Escenario del Riesgo.xlsx

Ahora después de sacar los escenarios se realiza una tabla de activos y dimensiones de seguridad, en la cual se analizara la frecuencia con que puede producirse la amenaza, como su impacto en las distintas dimensiones de la seguridad del activo.

ESCENARIO Amenaza/activo	FRECUENCIA	A	C	I	D	T
Ejecución de software malicioso -- Servidor web	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidores file server	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidores de correo electrónico	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidor de nomina	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidores ERP	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidores Base de datos	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidor de antivirus	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidor planta	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidor de impresión	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidor de Encripcion PGP	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Dispositivo almacenamientos NAS para Backups	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Servidor filtrado spam	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Equipos escritorio, portátiles	0.25	50%	50%	50%	50%	50%
Ejecución de software malicioso -- Equipos de comunicaciones:HP, D-Link	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Equipos de seguridad perimetral:Firewall Fortinet	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.5	50%	50%	50%	50%	50%
Ejecución de software malicioso -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.25	50%	50%	50%	50%	50%
Ejecución de software malicioso -- Bases de datos: SQL server 2008 estándar	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Correo electrónico: Exchange	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Antivirus: Symantec Endpoint	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Webserver: IIS	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Sistema de backups: Symantec System recovery, Cobian	0.5	25%	25%	25%	25%	25%
Ejecución de software malicioso -- ERP: JDEdwards	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Sistemas SCADA	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.25	50%	50%	50%	50%	50%
Ejecución de software malicioso -- Código fuente aplicaciones de planta y	0.5	50%	50%	50%	50%	50%

administrativas						
Ejecución de software malicioso -- Registros de operación: logs, informes y monitoreo	0.5	25%	25%	25%	25%	25%
Ejecución de software malicioso -- Bases de datos corporativas	0.5	25%	25%	25%	25%	25%
Ejecución de software malicioso -- Backups de usuarios corporativos	0.25	25%	25%	25%	25%	25%
Ejecución de software malicioso -- Red de datos	0.25	100%	100%	100%	100%	75%
Ejecución de software malicioso -- Red de telefonía	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- acceso a Internet	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Red de control e instrumentación	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Internet	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Intranet	0.5	25%	25%	25%	25%	25%
Ejecución de software malicioso -- Telefonía	0.5	25%	25%	25%	25%	25%
Ejecución de software malicioso -- Correo	0.5	50%	50%	50%	50%	50%
Ejecución de software malicioso -- Discos duros de servidores y estaciones de trabajo	0.5	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Discos externos información de backups	0.25	75%	75%	75%	75%	75%
Ejecución de software malicioso -- Unidades de CD , DVD y Memorias extraíbles	0.25	25%	25%	25%	25%	25%
Ataque aplicaciones -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.5	100%	100%	100%	100%	75%
Ataque aplicaciones -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.25	75%	75%	75%	75%	25%
Ataque aplicaciones -- Bases de datos: SQL server 2008 estándar	0.5	75%	75%	75%	75%	25%
Ataque aplicaciones -- Correo electrónico: Exchange	0.5	50%	50%	50%	50%	50%
Ataque aplicaciones -- Antivirus: Symantec Endpoint	0.5	50%	50%	50%	50%	50%
Ataque aplicaciones -- Webserver: IIS	0.5	50%	50%	50%	50%	50%
Ataque aplicaciones -- Sistema de backups: Symantec System recovery, Cobian	0.5	50%	50%	50%	50%	50%
Ataque aplicaciones -- ERP: JDEdwards	0.5	75%	75%	75%	75%	75%
Ataque aplicaciones -- Sistemas SCADA	0.25	75%	75%	75%	75%	75%
Ataque aplicaciones -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.5	25%	25%	25%	25%	25%
Ataque aplicaciones -- Código fuente aplicaciones de planta y administrativas	0.5	25%	25%	25%	25%	25%
Ataque aplicaciones -- Registros de operación: logs, informes y monitoreo	0.5	25%	25%	25%	25%	25%
Ataque aplicaciones -- Bases de datos	0.5	25%	25%	25%	25%	25%

corporativas						
Ataque aplicaciones -- Backups de usuarios corporativos	0.5	25%	25%	25%	25%	25%
Ataque infraestructura -- Servidores controladores de dominio	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor web	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidores file server	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidores de correo electrónico	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor de nomina	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidores ERP	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidores Base de datos	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor de antivirus	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor planta	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor de impresión	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor de Encripcion PGP	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Dispositivo almacenamientos NAS para Backups	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Servidor filtrado spam	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Equipos escritorio, portátiles	0.75	50%	50%	50%	50%	50%
Ataque infraestructura -- Equipos de comunicaciones:HP, D-Link	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Equipos de seguridad perimetral:Firewall Fortinet	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Planta telefónica: Siemens	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Red de datos	0.75	100%	100%	100%	100%	100%
Ataque infraestructura -- Red de telefonía	0.75	100%	100%	100%	100%	100%
Ataque infraestructura -- acceso a Internet	0.75	75%	75%	75%	75%	75%
Ataque infraestructura -- Red de control e instrumentación	0.75	100%	100%	100%	100%	100%
Ataque infraestructura -- Discos duros de servidores y estaciones de trabajo	0.75	50%	50%	50%	50%	50%
Ataque infraestructura -- Discos externos información de backups	0.75	50%	50%	50%	50%	50%
Ataque infraestructura -- Unidades de CD , DVD y Memorias extraíbles	0.75	50%	50%	50%	50%	50%
falta de sistema de parches -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.5	75%	75%	75%	75%	75%
falta de sistema de parches -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.5	75%	75%	75%	75%	75%
falta de sistema de parches -- Bases de datos: SQL server 2008 estándar	0.5	75%	75%	75%	75%	75%
falta de sistema de parches -- Correo electrónico: Exchange	0.5	75%	75%	75%	75%	75%

falta de sistema de parches -- Antivirus: Symantec Endpoint	0.5	75%	75%	75%	75%	75%
falta de sistema de parches -- Webserver: IIS	0.5	75%	75%	75%	75%	75%
falta de sistema de parches -- ERP: JDEdwards	0.5	75%	75%	75%	75%	75%
falta de sistema de parches -- Sistemas SCADA	0.75	50%	50%	50%	50%	50%
falta de sistema de parches -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.5	50%	50%	50%	50%	50%
falta de sistema de parches -- Bases de datos corporativas	0.5	50%	50%	50%	50%	50%
Falta de software de control de versiones -- Bases de datos: SQL server 2008 estándar	0.75	75%	75%	75%	75%	75%
Falta de software de control de versiones -- ERP: JDEdwards	0.75	75%	75%	75%	75%	75%
Falta de software de control de versiones -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	75%	75%	75%	75%	75%
Robo de información -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.75	100%	100%	100%	100%	100%
Robo de información -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	100%	100%	100%	100%	100%
Robo de información -- Bases de datos: SQL server 2008 estándar	0.75	100%	100%	100%	100%	100%
Robo de información -- Correo electrónico: Exchange	0.75	100%	100%	100%	100%	100%
Robo de información -- Antivirus: Symantec Endpoint	0.75	100%	100%	100%	100%	100%
Robo de información -- Webserver: IIS	0.75	100%	100%	100%	100%	100%
Robo de información -- Sistema de backups: Symantec System recovery, Cobian	0.75	100%	100%	100%	100%	100%
Robo de información -- ERP: JDEdwards	0.75	100%	100%	100%	100%	100%
Robo de información -- Sistemas SCADA	0.75	100%	100%	100%	100%	100%
Robo de información -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	100%	100%	100%	100%	100%
Robo de información -- Código fuente aplicaciones de planta y administrativas	0.75	100%	100%	100%	100%	100%
Robo de información -- Registros de operación: logs, informes y monitoreo	0.75	100%	100%	100%	100%	100%
Robo de información -- Bases de datos corporativas	0.75	100%	100%	100%	100%	100%
Robo de información -- Backups de usuarios corporativos	0.75	100%	100%	100%	100%	100%
Robo de información -- Red de datos	0.75	100%	100%	100%	100%	100%
Robo de información -- Red de telefonía	0.75	100%	100%	100%	100%	100%
Robo de información -- Red de control e instrumentación	0.75	100%	100%	100%	100%	100%
Robo de información -- Internet	0.75	100%	100%	100%	100%	100%
Robo de información -- Intranet	0.75	100%	100%	100%	100%	100%

Robo de información -- Telefonía	0.75	100%	100%	100%	100%	100%
Robo de información -- Correo	0.75	100%	100%	100%	100%	100%
Robo de información -- Discos duros de servidores y estaciones de trabajo	0.75	100%	100%	100%	100%	100%
Robo de información -- Discos externos información de backups	0.75	100%	100%	100%	100%	100%
Robo de información -- Unidades de CD , DVD y Memorias extraíbles	0.75	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Red de datos	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Red de telefonía	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- acceso a Internet	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Red de control e instrumentación	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Telefonía	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Sistema de cableado datos: Sede alterna	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Sistema de cableado datos : Centro de datos principal	1	100%	100%	100%	100%	100%
Ausencia de estándares en cableado estructurado -- Sistema de cableado datos: Centro de datos alterno	1	100%	100%	100%	100%	100%
Uso de software no oficial -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	50%	50%	50%	50%	50%
Uso de software no oficial -- Bases de datos: SQL server 2008 estándar	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- Correo electrónico: Exchange	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- Antivirus: Symantec Endpoint	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- Webserver: IIS	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- Sistema de backups: Symantec System recovery, Cobian	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- ERP: JDEdwards	0.5	75%	75%	75%	75%	75%
Uso de software no oficial -- Sistemas SCADA	0.75	75%	75%	75%	75%	75%
Uso de software no oficial -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	75%	75%	75%	75%	75%
Uso de software no oficial -- Bases de datos corporativas	0.5	75%	75%	75%	75%	75%
Acceso no autorizado -- Servidores controladores de dominio	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor web	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidores file	0.75	100%	75%	75%	75%	75%

server						
Acceso no autorizado -- Servidores de correo electrónico	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor de nomina	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidores ERP	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidores Base de datos	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor de antivirus	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor planta	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor de impresión	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor de Encripcion PGP	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Dispositivo almacenamientos NAS para Backups	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Servidor filtrado spam	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Equipos escritorio, portátiles	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Equipos de comunicaciones:HP, D-Link	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Equipos de seguridad perimetral:Firewall Fortinet	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Planta telefónica: Siemens	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Bases de datos: SQL server 2008 estándar	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Correo electrónico: Exchange	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Antivirus: Symantec Endpoint	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Webserver: IIS	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Sistema de backups: Symantec System recovery, Cobian	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- ERP: JDEdwards	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Sistemas SCADA	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Código fuente aplicaciones de planta y administrativas	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Registros de operación: logs, informes y monitoreo	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Bases de datos corporativas	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Backups de usuarios corporativos	0.75	100%	75%	75%	75%	75%

Acceso no autorizado -- Red de datos	0.75	100%	100%	100%	100%	100%
Acceso no autorizado -- Red de telefonía	0.75	100%	100%	100%	100%	100%
Acceso no autorizado -- acceso a Internet	0.75	100%	100%	100%	100%	100%
Acceso no autorizado -- Red de control e instrumentación	0.75	100%	100%	100%	100%	100%
Acceso no autorizado -- Internet	0.75	100%	100%	100%	100%	100%
Acceso no autorizado -- Intranet	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Telefonía	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Correo	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Discos duros de servidores y estaciones de trabajo	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Discos externos información de backups	0.75	100%	75%	75%	75%	75%
Acceso no autorizado -- Unidades de CD , DVD y Memorias extraíbles	0.75	100%	75%	75%	75%	75%
Retiro personal -- Coordinador de TI	0.5	100%	100%	100%	100%	100%
Retiro personal -- Administrador de base de datos	0.5	100%	100%	100%	100%	100%
Retiro personal -- Analistas funcionales	0.5	100%	100%	100%	100%	100%
Retiro personal -- Desarrolladores	0.5	100%	100%	100%	100%	100%
Retiro personal -- técnicos de operación	0.5	100%	100%	100%	100%	100%
Retiro personal -- Analista de seguridad de la información	0.5	100%	100%	100%	100%	100%
Retiro personal -- Director de informática	0.5	100%	100%	100%	100%	100%
Incapacidad -- Coordinador de TI	0.75	50%	50%	50%	50%	50%
Incapacidad -- Administrador de base de datos	0.75	25%	25%	25%	25%	25%
Incapacidad -- Analistas funcionales	0.75	25%	25%	25%	25%	25%
Incapacidad -- Desarrolladores	0.75	25%	25%	25%	25%	25%
Incapacidad -- técnicos de operación	0.75	25%	25%	25%	25%	25%
Incapacidad -- Analista de seguridad de la información	0.75	50%	50%	50%	50%	50%
Incapacidad -- Director de informática	0.75	50%	50%	50%	50%	50%
Poca disponibilidad -- Servidores controladores de dominio	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor web	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidores file server	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidores de correo electrónico	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor de nomina	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidores ERP	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidores Base de datos	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor de antivirus	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor planta	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor de impresión	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor de Encripcion PGP	0.5	75%	75%	75%	75%	75%

Poca disponibilidad -- Dispositivo almacenamientos NAS para Backups	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Servidor filtrado spam	0.5	75%	75%	75%	75%	75%
Poca disponibilidad -- Planta telefónica: Siemens	0.5	75%	75%	75%	75%	75%
Copia no autorizada -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Bases de datos: SQL server 2008 estándar	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Correo electrónico: Exchange	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Antivirus: Symantec Endpoint	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Webserver: IIS	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Sistema de backups: Symantec System recovery, Cobian	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- ERP: JDEdwards	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Sistemas SCADA	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Código fuente aplicaciones de planta y administrativas	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Registros de operación: logs, informes y monitoreo	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Bases de datos corporativas	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Backups de usuarios corporativos	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Discos duros de servidores y estaciones de trabajo	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Discos externos información de backups	0.75	75%	75%	75%	75%	75%
Copia no autorizada -- Unidades de CD , DVD y Memorias extraíbles	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Bases de datos: SQL server 2008 estándar	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Correo electrónico: Exchange	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Antivirus: Symantec Endpoint	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Webserver: IIS	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Sistema de backups: Symantec System recovery, Cobian	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- ERP: JDEdwards	0.75	75%	75%	75%	75%	75%

Borrado y alteración -- Sistemas SCADA	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Código fuente aplicaciones de planta y administrativas	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Registros de operación: logs, informes y monitoreo	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Bases de datos corporativas	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Backups de usuarios corporativos	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Discos duros de servidores y estaciones de trabajo	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Discos externos información de backups	0.75	75%	75%	75%	75%	75%
Borrado y alteración -- Unidades de CD , DVD y Memorias extraíbles	0.75	75%	75%	75%	75%	75%
Incendio -- Centro de procesamiento de datos principal	0.1	100%	100%	100%	100%	75%
Incendio -- Centro de procesamiento de datos alterno	0.1	100%	100%	100%	100%	75%
Incendio -- Ubicación local de infraestructura y comunicaciones	0.1	100%	100%	100%	100%	75%
Incendio -- sala eléctrica, ups, telecomunicaciones	0.1	100%	100%	100%	100%	75%
Incendio -- Servidores controladores de dominio	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor web	0.1	100%	100%	100%	100%	75%
Incendio -- Servidores file server	0.1	100%	100%	100%	100%	75%
Incendio -- Servidores de correo electrónico	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor de nomina	0.1	100%	100%	100%	100%	75%
Incendio -- Servidores ERP	0.1	100%	100%	100%	100%	75%
Incendio -- Servidores Base de datos	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor de antivirus	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor planta	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor de impresión	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor de Encripcion PGP	0.1	100%	100%	100%	100%	75%
Incendio -- Dispositivo almacenamientos NAS para Backups	0.1	100%	100%	100%	100%	75%
Incendio -- Servidor filtrado spam	0.1	100%	100%	100%	100%	75%
Incendio -- Equipos escritorio, portátiles	0.1	100%	100%	100%	100%	75%
Incendio -- Equipos de comunicaciones:HP, D-Link	0.1	100%	100%	100%	100%	75%
Incendio -- Equipos de seguridad perimetral:Firewall Fortinet	0.1	100%	100%	100%	100%	75%
Incendio -- Planta telefónica: Siemens	0.1	100%	100%	100%	100%	75%
Incendio -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.1	100%	100%	100%	100%	75%
Incendio -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.1	100%	100%	100%	100%	75%
Incendio -- Bases de datos: SQL server 2008 estándar	0.1	100%	100%	100%	100%	75%

Incendio -- Correo electrónico: Exchange	0.1	100%	100%	100%	100%	75%
Incendio -- Antivirus: Symantec Endpoint	0.1	100%	100%	100%	100%	75%
Incendio -- Webserver: IIS	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de backups: Symantec System recovery, Cobian	0.1	100%	100%	100%	100%	75%
Incendio -- ERP: JDEdwards	0.1	100%	100%	100%	100%	75%
Incendio -- Sistemas SCADA	0.1	100%	100%	100%	100%	75%
Incendio -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.1	100%	100%	100%	100%	75%
Incendio -- Código fuente aplicaciones de planta y administrativas	0.1	100%	100%	100%	100%	75%
Incendio -- Registros de operación: logs, informes y monitoreo	0.1	100%	100%	100%	100%	75%
Incendio -- Bases de datos corporativas	0.1	100%	100%	100%	100%	75%
Incendio -- Backups de usuarios corporativos	0.1	100%	100%	100%	100%	75%
Incendio -- Red de datos	0.1	100%	100%	100%	100%	75%
Incendio -- Red de telefonía	0.1	100%	100%	100%	100%	75%
Incendio -- acceso a Internet	0.1	100%	100%	100%	100%	75%
Incendio -- Red de control e instrumentación	0.1	100%	100%	100%	100%	75%
Incendio -- Internet	0.1	100%	100%	100%	100%	75%
Incendio -- Intranet	0.1	100%	100%	100%	100%	75%
Incendio -- Telefonía	0.1	100%	100%	100%	100%	75%
Incendio -- Correo	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de alimentación UPS	0.1	100%	100%	100%	100%	75%
Incendio -- Generadores de energía	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de aire acondicionado	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de cableado Eléctrico: Centro de datos principal	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de cableado Eléctrico: Centro de datos alterno	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de cableado Eléctrico: Sede alterna	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de cableado datos: Sede alterna	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de cableado datos : Centro de datos principal	0.1	100%	100%	100%	100%	75%
Incendio -- Sistema de cableado datos: Centro de datos alterno	0.1	100%	100%	100%	100%	75%
Incendio -- Equipos de control de temperatura	0.1	100%	100%	100%	100%	75%
Incendio -- Coordinador de TI	0.1	100%	100%	100%	100%	75%
Incendio -- Administrador de base de datos	0.1	100%	100%	100%	100%	75%
Incendio -- Analistas funcionales	0.1	100%	100%	100%	100%	75%
Incendio -- Desarrolladores	0.1	100%	100%	100%	100%	75%
Incendio -- técnicos de operación	0.1	100%	100%	100%	100%	75%
Incendio -- Analista de seguridad de la información	0.1	100%	100%	100%	100%	75%
Incendio -- Director de informática	0.1	100%	100%	100%	100%	75%
Incendio -- Discos duros de servidores y	0.1	100%	100%	100%	100%	75%

estaciones de trabajo						
Incendio -- Discos externos información de backups	0.1	100%	100%	100%	100%	75%
Incendio -- Unidades de CD , DVD y Memorias extraíbles	0.1	100%	100%	100%	100%	75%
Terremoto -- Centro de procesamiento de datos principal	0.1	100%	100%	100%	100%	75%
Terremoto -- Centro de procesamiento de datos alterno	0.1	100%	100%	100%	100%	75%
Terremoto -- Ubicación local de infraestructura y comunicaciones	0.1	100%	100%	100%	100%	75%
Terremoto -- sala eléctrica, ups, telecomunicaciones	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidores controladores de dominio	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor web	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidores file server	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidores de correo electrónico	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor de nomina	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidores ERP	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidores Base de datos	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor de antivirus	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor planta	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor de impresión	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor de Inscripción PGP	0.1	100%	100%	100%	100%	75%
Terremoto -- Dispositivo almacenamientos NAS para Backups	0.1	100%	100%	100%	100%	75%
Terremoto -- Servidor filtrado spam	0.1	100%	100%	100%	100%	75%
Terremoto -- Equipos escritorio, portátiles	0.1	100%	100%	100%	100%	75%
Terremoto -- Equipos de comunicaciones:HP, D-Link	0.1	100%	100%	100%	100%	75%
Terremoto -- Equipos de seguridad perimetral:Firewall Fortinet	0.1	100%	100%	100%	100%	75%
Terremoto -- Planta telefónica: Siemens	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.1	100%	100%	100%	100%	75%
Terremoto -- Bases de datos: SQL server 2008 estándar	0.1	100%	100%	100%	100%	75%
Terremoto -- Correo electrónico: Exchange	0.1	100%	100%	100%	100%	75%
Terremoto -- Antivirus: Symantec Endpoint	0.1	100%	100%	100%	100%	75%
Terremoto -- Webserver: IIS	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de backups: Symantec System recovery, Cobian	0.1	100%	100%	100%	100%	75%
Terremoto -- ERP: JDEdwards	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistemas SCADA	0.1	100%	100%	100%	100%	75%
Terremoto -- Aplicaciones de desarrollo	0.1	100%	100%	100%	100%	75%

:Visual studio .Net y SQl developer						
Terremoto -- Código fuente aplicaciones de planta y administrativas	0.1	100%	100%	100%	100%	75%
Terremoto -- Registros de operación: logs, informes y monitoreo	0.1	100%	100%	100%	100%	75%
Terremoto -- Bases de datos corporativas	0.1	100%	100%	100%	100%	75%
Terremoto -- Backups de usuarios corporativos	0.1	100%	100%	100%	100%	75%
Terremoto -- Red de datos	0.1	100%	100%	100%	100%	75%
Terremoto -- Red de telefonía	0.1	100%	100%	100%	100%	75%
Terremoto -- acceso a Internet	0.1	100%	100%	100%	100%	75%
Terremoto -- Red de control e instrumentación	0.1	100%	100%	100%	100%	75%
Terremoto -- Internet	0.1	100%	100%	100%	100%	75%
Terremoto -- Intranet	0.1	100%	100%	100%	100%	75%
Terremoto -- Telefonía	0.1	100%	100%	100%	100%	75%
Terremoto -- Correo	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de alimentación UPS	0.1	100%	100%	100%	100%	75%
Terremoto -- Generadores de energía	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de aire acondicionado	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de cableado Eléctrico: Centro de datos principal	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de cableado Eléctrico: Centro de datos alterno	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de cableado Eléctrico: Sede alterna	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de cableado datos: Sede alterna	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de cableado datos : Centro de datos principal	0.1	100%	100%	100%	100%	75%
Terremoto -- Sistema de cableado datos: Centro de datos alterno	0.1	100%	100%	100%	100%	75%
Terremoto -- Equipos de control de temperatura	0.1	100%	100%	100%	100%	75%
Terremoto -- Coordinador de TI	0.1	100%	100%	100%	100%	75%
Terremoto -- Administrador de base de datos	0.1	100%	100%	100%	100%	75%
Terremoto -- Analistas funcionales	0.1	100%	100%	100%	100%	75%
Terremoto -- Desarrolladores	0.1	100%	100%	100%	100%	75%
Terremoto -- técnicos de operación	0.1	100%	100%	100%	100%	75%
Terremoto -- Analista de seguridad de la información	0.1	100%	100%	100%	100%	75%
Terremoto -- Director de informática	0.1	100%	100%	100%	100%	75%
Terremoto -- Discos duros de servidores y estaciones de trabajo	0.1	100%	100%	100%	100%	75%
Terremoto -- Discos externos información de backups	0.1	100%	100%	100%	100%	75%
Terremoto -- Unidades de CD , DVD y Memorias extraíbles	0.1	100%	100%	100%	100%	75%
Falla eléctrica -- Centro de procesamiento de datos principal	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Centro de	0.5	25%	25%	25%	25%	25%

procesamiento de datos alterno						
Falla eléctrica -- Ubicación local de infraestructura y comunicaciones	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- sala eléctrica, ups, telecomunicaciones	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidores controladores de dominio	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor web	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidores file server	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidores de correo electrónico	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor de nomina	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidores ERP	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidores Base de datos	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor de antivirus	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor planta	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor de impresión	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor de Encripcion PGP	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Dispositivo almacenamientos NAS para Backups	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Servidor filtrado spam	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Equipos escritorio, portátiles	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Equipos de comunicaciones:HP, D-Link	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Equipos de seguridad perimetral:Firewall Fortinet	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Planta telefónica: Siemens	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Bases de datos: SQL server 2008 estándar	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Correo electrónico: Exchange	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Antivirus: Symantec Endpoint	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Webserver: IIS	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de backups: Symantec System recovery, Cobian	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- ERP: JDEdwards	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistemas SCADA	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Código fuente aplicaciones de planta y administrativas	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Registros de operación: logs, informes y monitoreo	0.5	25%	25%	25%	25%	25%

Falla eléctrica -- Bases de datos corporativas	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Backups de usuarios corporativos	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Red de datos	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Red de telefonía	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- acceso a Internet	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Red de control e instrumentación	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Internet	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Intranet	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Telefonía	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Correo	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de alimentación UPS	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Generadores de energía	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de aire acondicionado	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de cableado Eléctrico: Centro de datos principal	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de cableado Eléctrico: Centro de datos alterno	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de cableado Eléctrico: Sede alterna	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de cableado datos: Sede alterna	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de cableado datos : Centro de datos principal	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Sistema de cableado datos: Centro de datos alterno	0.5	25%	25%	25%	25%	25%
Falla eléctrica -- Equipos de control de temperatura	0.5	25%	25%	25%	25%	25%
Inundación -- Centro de procesamiento de datos principal	0.1	100%	100%	100%	100%	75%
Inundación -- Centro de procesamiento de datos alterno	0.1	100%	100%	100%	100%	75%
Inundación -- Ubicación local de infraestructura y comunicaciones	0.1	100%	100%	100%	100%	75%
Inundación -- sala eléctrica, ups, telecomunicaciones	0.1	100%	100%	100%	100%	75%
Inundación -- Servidores controladores de dominio	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor web	0.1	100%	100%	100%	100%	75%
Inundación -- Servidores file server	0.1	100%	100%	100%	100%	75%
Inundación -- Servidores de correo electrónico	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor de nomina	0.1	100%	100%	100%	100%	75%
Inundación -- Servidores ERP	0.1	100%	100%	100%	100%	75%
Inundación -- Servidores Base de datos	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor de antivirus	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor planta	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor de impresión	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor de Encripcion PGP	0.1	100%	100%	100%	100%	75%

Inundación -- Dispositivo almacenamientos NAS para Backups	0.1	100%	100%	100%	100%	75%
Inundación -- Servidor filtrado spam	0.1	100%	100%	100%	100%	75%
Inundación -- Equipos escritorio, portátiles	0.1	100%	100%	100%	100%	75%
Inundación -- Equipos de comunicaciones:HP, D-Link	0.1	100%	100%	100%	100%	75%
Inundación -- Equipos de seguridad perimetral:Firewall Fortinet	0.1	100%	100%	100%	100%	75%
Inundación -- Planta telefónica: Siemens	0.1	100%	100%	100%	100%	75%
Inundación -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.1	100%	100%	100%	100%	75%
Inundación -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.1	100%	100%	100%	100%	75%
Inundación -- Bases de datos: SQL server 2008 estándar	0.1	100%	100%	100%	100%	75%
Inundación -- Correo electrónico: Exchange	0.1	100%	100%	100%	100%	75%
Inundación -- Antivirus: Symantec Endpoint	0.1	100%	100%	100%	100%	75%
Inundación -- Webserver: IIS	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de backups: Symantec System recovery, Cobian	0.1	100%	100%	100%	100%	75%
Inundación -- ERP: JDEdwards	0.1	100%	100%	100%	100%	75%
Inundación -- Sistemas SCADA	0.1	100%	100%	100%	100%	75%
Inundación -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.1	100%	100%	100%	100%	75%
Inundación -- Código fuente aplicaciones de planta y administrativas	0.1	100%	100%	100%	100%	75%
Inundación -- Registros de operación: logs, informes y monitoreo	0.1	100%	100%	100%	100%	75%
Inundación -- Bases de datos corporativas	0.1	100%	100%	100%	100%	75%
Inundación -- Backups de usuarios corporativos	0.1	100%	100%	100%	100%	75%
Inundación -- Red de datos	0.1	100%	100%	100%	100%	75%
Inundación -- Red de telefonía	0.1	100%	100%	100%	100%	75%
Inundación -- acceso a Internet	0.1	100%	100%	100%	100%	75%
Inundación -- Red de control e instrumentación	0.1	100%	100%	100%	100%	75%
Inundación -- Internet	0.1	100%	100%	100%	100%	75%
Inundación -- Intranet	0.1	100%	100%	100%	100%	75%
Inundación -- Telefonía	0.1	100%	100%	100%	100%	75%
Inundación -- Correo	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de alimentación UPS	0.1	100%	100%	100%	100%	75%
Inundación -- Generadores de energía	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de aire acondicionado	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de cableado Eléctrico: Centro de datos principal	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de cableado Eléctrico: Centro de datos alterno	0.1	100%	100%	100%	100%	75%

Inundación -- Sistema de cableado Eléctrico: Sede alterna	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de cableado datos: Sede alterna	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de cableado datos : Centro de datos principal	0.1	100%	100%	100%	100%	75%
Inundación -- Sistema de cableado datos: Centro de datos alterno	0.1	100%	100%	100%	100%	75%
Inundación -- Equipos de control de temperatura	0.1	100%	100%	100%	100%	75%
Inundación -- Coordinador de TI	0.1	100%	100%	100%	100%	75%
Inundación -- Administrador de base de datos	0.1	100%	100%	100%	100%	75%
Inundación -- Analistas funcionales	0.1	100%	100%	100%	100%	75%
Inundación -- Desarrolladores	0.1	100%	100%	100%	100%	75%
Inundación -- técnicos de operación	0.1	100%	100%	100%	100%	75%
Inundación -- Analista de seguridad de la información	0.1	100%	100%	100%	100%	75%
Inundación -- Director de informática	0.1	100%	100%	100%	100%	75%
Inundación -- Discos duros de servidores y estaciones de trabajo	0.1	100%	100%	100%	100%	75%
Inundación -- Discos externos información de backups	0.1	100%	100%	100%	100%	75%
Inundación -- Unidades de CD , DVD y Memorias extraíbles	0.1	100%	100%	100%	100%	75%
Terrorismo -- Centro de procesamiento de datos principal	0.1	100%	100%	100%	100%	75%
Terrorismo -- Centro de procesamiento de datos alterno	0.1	100%	100%	100%	100%	75%
Terrorismo -- Ubicación local de infraestructura y comunicaciones	0.1	100%	100%	100%	100%	75%
Terrorismo -- sala eléctrica, ups, telecomunicaciones	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidores controladores de dominio	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor web	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidores file server	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidores de correo electrónico	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor de nomina	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidores ERP	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidores Base de datos	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor de antivirus	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor planta	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor de impresión	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor de Encripcion PGP	0.1	100%	100%	100%	100%	75%
Terrorismo -- Dispositivo almacenamientos NAS para Backups	0.1	100%	100%	100%	100%	75%
Terrorismo -- Servidor filtrado spam	0.1	100%	100%	100%	100%	75%
Terrorismo -- Equipos escritorio, portátiles	0.1	100%	100%	100%	100%	75%
Terrorismo -- Equipos de comunicaciones:HP, D-Link	0.1	100%	100%	100%	100%	75%
Terrorismo -- Equipos de seguridad	0.1	100%	100%	100%	100%	75%

perimetral:Firewall Fortinet						
Terrorismo -- Planta telefónica: Siemens	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.1	100%	100%	100%	100%	75%
Terrorismo -- Bases de datos: SQL server 2008 estándar	0.1	100%	100%	100%	100%	75%
Terrorismo -- Correo electrónico: Exchange	0.1	100%	100%	100%	100%	75%
Terrorismo -- Antivirus: Symantec Endpoint	0.1	100%	100%	100%	100%	75%
Terrorismo -- Webserver: IIS	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de backups: Symantec System recovery, Cobian	0.1	100%	100%	100%	100%	75%
Terrorismo -- ERP: JDEdwards	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistemas SCADA	0.1	100%	100%	100%	100%	75%
Terrorismo -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.1	100%	100%	100%	100%	75%
Terrorismo -- Código fuente aplicaciones de planta y administrativas	0.1	100%	100%	100%	100%	75%
Terrorismo -- Registros de operación: logs, informes y monitoreo	0.1	100%	100%	100%	100%	75%
Terrorismo -- Bases de datos corporativas	0.1	100%	100%	100%	100%	75%
Terrorismo -- Backups de usuarios corporativos	0.1	100%	100%	100%	100%	75%
Terrorismo -- Red de datos	0.1	100%	100%	100%	100%	75%
Terrorismo -- Red de telefonía	0.1	100%	100%	100%	100%	75%
Terrorismo -- acceso a Internet	0.1	100%	100%	100%	100%	75%
Terrorismo -- Red de control e instrumentación	0.1	100%	100%	100%	100%	75%
Terrorismo -- Internet	0.1	100%	100%	100%	100%	75%
Terrorismo -- Intranet	0.1	100%	100%	100%	100%	75%
Terrorismo -- Telefonía	0.1	100%	100%	100%	100%	75%
Terrorismo -- Correo	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de alimentación UPS	0.1	100%	100%	100%	100%	75%
Terrorismo -- Generadores de energía	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de aire acondicionado	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de cableado Eléctrico: Centro de datos principal	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de cableado Eléctrico: Centro de datos alterno	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de cableado Eléctrico: Sede alterna	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de cableado datos: Sede alterna	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de cableado datos : Centro de datos principal	0.1	100%	100%	100%	100%	75%
Terrorismo -- Sistema de cableado datos: Centro de datos alterno	0.1	100%	100%	100%	100%	75%

Terrorismo -- Equipos de control de temperatura	0.1	100%	100%	100%	100%	75%
Terrorismo -- Coordinador de TI	0.1	100%	100%	100%	100%	75%
Terrorismo -- Administrador de base de datos	0.1	100%	100%	100%	100%	75%
Terrorismo -- Analistas funcionales	0.1	100%	100%	100%	100%	75%
Terrorismo -- Desarrolladores	0.1	100%	100%	100%	100%	75%
Terrorismo -- técnicos de operación	0.1	100%	100%	100%	100%	75%
Terrorismo -- Analista de seguridad de la información	0.1	100%	100%	100%	100%	75%
Terrorismo -- Director de informática	0.1	100%	100%	100%	100%	75%
Terrorismo -- Discos duros de servidores y estaciones de trabajo	0.1	100%	100%	100%	100%	75%
Terrorismo -- Discos externos información de backups	0.1	100%	100%	100%	100%	75%
Terrorismo -- Unidades de CD , DVD y Memorias extraíbles	0.1	100%	100%	100%	100%	75%
Desmotivación -- Coordinador de TI	0.75	75%	75%	75%	75%	75%
Desmotivación -- Administrador de base de datos	0.75	75%	75%	75%	75%	75%
Desmotivación -- Analistas funcionales	0.75	75%	75%	75%	75%	75%
Desmotivación -- Desarrolladores	0.75	75%	75%	75%	75%	75%
Desmotivación -- técnicos de operación	0.75	75%	75%	75%	75%	75%
Desmotivación -- Analista de seguridad de la información	0.75	75%	75%	75%	75%	75%
Desmotivación -- Director de informática	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidores controladores de dominio	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor web	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidores file server	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidores de correo electrónico	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor de nomina	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidores ERP	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidores Base de datos	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor de antivirus	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor planta	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor de impresión	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor de Encripcion PGP	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Dispositivo almacenamientos NAS para Backups	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Servidor filtrado spam	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Equipos escritorio, portátiles	0.25	75%	75%	75%	75%	75%
Solo un especialista -- Equipos de comunicaciones:HP, D-Link	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Equipos de seguridad perimetral:Firewall Fortinet	0.75	75%	75%	75%	75%	75%

Solo un especialista -- Planta telefónica: Siemens	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Bases de datos: SQL server 2008 estándar	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Correo electrónico: Exchange	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Antivirus: Symantec Endpoint	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Webserver: IIS	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Sistema de backups: Symantec System recovery, Cobian	0.75	75%	75%	75%	75%	75%
Solo un especialista -- ERP: JDEdwards	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Sistemas SCADA	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Código fuente aplicaciones de planta y administrativas	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Registros de operación: logs, informes y monitoreo	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Bases de datos corporativas	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Backups de usuarios corporativos	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Red de datos	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Red de telefonía	0.75	75%	75%	75%	75%	75%
Solo un especialista -- acceso a Internet	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Red de control e instrumentación	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Internet	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Intranet	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Telefonía	0.75	75%	75%	75%	75%	75%
Solo un especialista -- Correo	0.75	75%	75%	75%	75%	75%
Negligencia -- Coordinador de TI	0.1	75%	75%	75%	75%	75%
Negligencia -- Administrador de base de datos	0.1	75%	75%	75%	75%	75%
Negligencia -- Analistas funcionales	0.1	75%	75%	75%	75%	75%
Negligencia -- Desarrolladores	0.1	75%	75%	75%	75%	75%
Negligencia -- técnicos de operación	0.1	75%	75%	75%	75%	75%
Negligencia -- Analista de seguridad de la información	0.1	75%	75%	75%	75%	75%
Negligencia -- Director de informática	0.1	75%	75%	75%	75%	75%
Mal diseño de los procesos -- Bases de datos: SQL server 2008 estándar	0.25	75%	75%	75%	75%	75%
Mal diseño de los procesos -- ERP: JDEdwards	0.25	75%	75%	75%	75%	75%
Mal diseño de los procesos -- Sistemas SCADA	0.25	75%	75%	75%	75%	75%

Mal diseño de los procesos -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidores controladores de dominio	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor web	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidores file server	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidores de correo electrónico	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor de nomina	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidores ERP	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidores Base de datos	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor de antivirus	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor planta	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor de impresión	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor de Encripcion PGP	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Dispositivo almacenamientos NAS para Backups	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Servidor filtrado spam	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Equipos escritorio, portátiles	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Equipos de comunicaciones:HP, D-Link	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Equipos de seguridad perimetral:Firewall Fortinet	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Planta telefónica: Siemens	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Bases de datos: SQL server 2008 estándar	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Correo electrónico: Exchange	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Antivirus: Symantec Endpoint	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Webserver: IIS	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Sistema de backups: Symantec System recovery, Cobian	0.25	75%	75%	75%	75%	75%
Líder inexperto -- ERP: JDEdwards	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Sistemas SCADA	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Código fuente aplicaciones de planta y administrativas	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Registros de operación: logs, informes y monitoreo	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Bases de datos corporativas	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Backups de usuarios	0.25	75%	75%	75%	75%	75%

corporativos						
Líder inexperto -- Red de datos	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Red de telefonía	0.25	75%	75%	75%	75%	75%
Líder inexperto -- acceso a Internet	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Red de control e instrumentación	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Internet	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Intranet	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Telefonía	0.25	75%	75%	75%	75%	75%
Líder inexperto -- Correo	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Bases de datos: SQL server 2008 estándar	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Correo electrónico: Exchange	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Antivirus: Symantec Endpoint	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Webserver: IIS	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Sistema de backups: Symantec System recovery, Cobian	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- ERP: JDEdwards	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Sistemas SCADA	0.25	75%	75%	75%	75%	75%
Analistas inexpertos -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- Coordinador de TI	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- Administrador de base de datos	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- Analistas funcionales	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- Desarrolladores	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- técnicos de operación	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- Analista de seguridad de la información	0.25	75%	75%	75%	75%	75%
Falta de alcances claros -- Director de informática	0.25	75%	75%	75%	75%	75%
Robo de equipos -- Servidores controladores de dominio	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidor web	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidores file server	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidores de correo electrónico	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidor de nomina	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidores ERP	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidores Base de datos	0.5	75%	75%	75%	75%	75%

Robo de equipos -- Servidor de antivirus	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidor planta	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidor de impresión	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidor de Encripcion PGP	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Servidor filtrado spam	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Equipos escritorio, portátiles	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Equipos de comunicaciones:HP, D-Link	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Equipos de seguridad perimetral:Firewall Fortinet	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Planta telefónica: Siemens	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Discos duros de servidores y estaciones de trabajo	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Discos externos información de backups	0.5	75%	75%	75%	75%	75%
Robo de equipos -- Unidades de CD , DVD y Memorias extraíbles	0.5	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidores controladores de dominio	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor web	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidores file server	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidores de correo electrónico	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor de nomina	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidores ERP	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidores Base de datos	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor de antivirus	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor planta	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor de impresión	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor de Encripcion PGP	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Dispositivo almacenamientos NAS para Backups	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Servidor filtrado spam	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Bases de datos: SQL server 2008 estándar	0.75	75%	75%	75%	75%	75%

Pérdida de capacidad de servidores -- Correo electrónico: Exchange	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Antivirus: Symantec Endpoint	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Webserver: IIS	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Sistema de backups: Symantec System recovery, Cobian	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- ERP: JDEdwards	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Sistemas SCADA	0.75	75%	75%	75%	75%	75%
Pérdida de capacidad de servidores -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	0.75	75%	75%	75%	75%	75%

Tabla 14. Activos y dimensiones de la seguridad

3.7IMPACTO POTENCIAL

Una vez realizado el análisis de amenazas podemos determinar el impacto potencial que puede suponer para la empresa la materialización de las amenazas. Se trata de un dato relevante, ya que permitirá priorizar el plan de acción, y a su vez, evaluar cómo se ve modificado dicho valor una vez se apliquen contramedidas.

Para esto calcularemos el riesgo actual. La determinación del riesgo para una amenaza/vulnerabilidad en particular se expresa en función de:

- La probabilidad que una fuente de amenaza intente explotar una vulnerabilidad.
- La magnitud del impacto resultante de la explotación exitosa de una vulnerabilidad.
- LA efectividad de los controles existentes o planeados para mitigar los riesgos.

Para determinar el riesgo se multiplican los valores asignados a la probabilidad de una amenaza por los valores asignados a la magnitud del impacto, como se muestra en la siguiente matriz:

Impacto	A	5	M	M+	M+	A	A
	M+	4	M	M	M+	M+	A
	M	3	M-	M-	M	M	M+
	M-	2	B	M-	M-	M-	M
	B	1	B	B	B	B	M

			0-	21-	41-	61-	81-
			20%	40%	60%	80%	100%
			Probabilidad de ocurrencia				

Tabla 15. Mapa de Riesgo

La escala de riesgo, con los niveles Alto, Medio Alto, Medio, Medio Bajo y Bajo, representa el grado o nivel a que se encuentra expuesto el activo de información evaluado, cuando una vulnerabilidad es explotada exitosamente.

También representa las acciones que se deben tomar la dirección y responsables, en cada uno de los niveles como se indica:

Nivel de Riesgo	Descripción del Riesgo y Acciones necesarias
Alto	Requiere fuertes medidas correctivas, planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de la alta dirección.
Medio Alto	Requiere vigilancia de la alta dirección con planes de tratamiento implementados y reportados a los líderes de proceso.
Medio	Se requieren acciones correctivas controladas por grupos de manejo de incidentes en periodo de tiempo razonable
Medio Bajo	Riesgo Aceptable- Administrado por los grupos de incidentes bajo procedimientos normales de control
Bajo	EL propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo.

Tabla 16. Descripción de Escalas de Riesgo

Procedamos entonces a calcular el riesgo teniendo presente la siguiente información:

Marcaremos un nivel sobre la calificación de las Probabilidades/Frecuencias.

Probabilidad/Frecuencia			
Nivel	**Calificación**		**Explicación**
5	A	1	100%, Alta, siempre ocurre
4	M+	0.75	75%, Mayor, probable, se espera que ocurra
3	M	0.5	50% se espera que no ocurra regularmente
2	M-	0.25	25%,No esperado pero podría ocurrir algunas veces
1	B	0.1	10%, Remoto, puede ocurrir en circunstancias excepcionales

Tabla 17. Calificación probabilidad/frecuencia

Además sobre el impacto en la información:

Impacto en la informacion (disponibilidad, confiabilidad, integridad)			
Nivel	**Calificacion**	**Explicacion**	**Detalle**
5	A	Muy alto	La información no esta disponible por más de 48 horas
4	M+	Alto	La información no esta disponible entre 24 y de 48 horas
3	M	Medio	La información no esta disponible 8 y 24 horas
2	M-	Bajo	La información no esta disponible 3 y 8 horas
1	B	Menor	La información no esta disponible por menos de 3 horas.

Tabla 18. Calificación impacto en la información.

Estos niveles nos facilitaran el cálculo del Riesgo que será la multiplicación entre la probabilidad y el impacto en la información.

ESCENARIO	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo Prob*Impacto
Ejecución de software malicioso -- Servidores controladores de dominio	M	3	M-	2	6
Ejecución de software malicioso -- Servidor web	M	3	M-	2	6
Ejecución de software malicioso -- Servidores file server	M	3	M-	2	6
Ejecución de software malicioso -- Servidores de correo electrónico	M	3	M	3	9
Ejecución de software malicioso -- Servidor de nomina	M	3	M	3	9
Ejecución de software malicioso -- Servidores ERP	M	3	M	3	9
Ejecución de software malicioso -- Servidores Base de datos	M	3	M	3	9
Ejecución de software malicioso -- Servidor de antivirus	M	3	M-	2	6
Ejecución de software malicioso -- Servidor planta	M	3	M-	2	6
Ejecución de software malicioso -- Servidor de impresión	M	3	M-	2	6
Ejecución de software malicioso -- Servidor de Encripcion PGP	M	3	M-	2	6
Ejecución de software malicioso -- Dispositivo almacenamientos NAS para Backups	M	3	M	3	9
Ejecución de software malicioso -- Servidor filtrado spam	M-	2	M-	2	4
Ejecución de software malicioso -- Equipos escritorio, portátiles	M-	2	M	3	6
Ejecución de software malicioso -- Equipos de comunicaciones:HP, D-Link	M	3	M	3	9
Ejecución de software malicioso -- Equipos de seguridad perimetral:Firewall Fortinet	M	3	M	3	9
Ejecución de software malicioso -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M-	2	M-	2	4
Ejecución de software malicioso -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M	3	M-	2	6

Ejecución de software malicioso -- Bases de datos: SQL server 2008 estándar	M	3	M	3	9
Ejecución de software malicioso -- Correo electrónico: Exchange	M	3	M	3	9
Ejecución de software malicioso -- Antivirus: Symantec Endpoint	M	3	M-	2	6
Ejecución de software malicioso -- Webserver: IIS	M	3	M-	2	6
Ejecución de software malicioso -- Sistema de backups: Symantec System recovery, Cobian	M	3	M	3	9
Ejecución de software malicioso -- ERP: JDEdwards	M-	2	M+	4	8
Ejecución de software malicioso -- Sistemas SCADA	M-	2	M+	4	8
Ejecución de software malicioso -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M	3	M-	2	6
Ejecución de software malicioso -- Código fuente aplicaciones de planta y administrativas	M	3	M-	2	6
Ejecución de software malicioso -- Registros de operación: logs, informes y monitoreo	M	3	M-	2	6
Ejecución de software malicioso -- Bases de datos corporativas	M-	2	M	3	6
Ejecución de software malicioso -- Backups de usuarios corporativos	M-	2	M-	2	4
Ejecución de software malicioso -- Red de datos	M-	2	M+	4	8
Ejecución de software malicioso -- Red de telefonía	M-	2	M+	4	8
Ejecución de software malicioso -- acceso a Internet	M-	2	M	3	6
Ejecución de software malicioso -- Red de control e instrumentación	M-	2	M+	4	8
Ejecución de software malicioso -- Internet	M	3	M	3	9
Ejecución de software malicioso -- Intranet	A	5	M-	2	10
Ejecución de software malicioso -- Telefonía	M	3	M-	2	6
Ejecución de software malicioso -- Correo	M	3	M	3	9
Ejecución de software malicioso -- Discos duros de servidores y estaciones de trabajo	M-	2	M-	2	4
Ejecución de software malicioso -- Discos externos información de backups	M-	2	M-	2	4
Ejecución de software malicioso -- Unidades de CD , DVD y Memorias extraíbles	M	3	M-	2	6
Ataque aplicaciones -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M-	2	M	3	6
Ataque aplicaciones -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M	3	M	3	9
Ataque aplicaciones -- Bases de datos: SQL server 2008 estándar	M	3	M	3	9
Ataque aplicaciones -- Correo electrónico: Exchange	M	3	M	3	9
Ataque aplicaciones -- Antivirus: Symantec Endpoint	M	3	M-	2	6
Ataque aplicaciones -- Webserver: IIS	M	3	M-	2	6
Ataque aplicaciones -- Sistema de backups: Symantec System recovery, Cobian	M	3	M-	2	6
Ataque aplicaciones -- ERP: JDEdwards	M-	2	M	3	6
Ataque aplicaciones -- Sistemas SCADA	M	3	M+	4	12

Ataque aplicaciones -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M	3	M	3	9
Ataque aplicaciones -- Código fuente aplicaciones de planta y administrativas	M	3	M	3	9
Ataque aplicaciones -- Registros de operación: logs, informes y monitoreo	M	3	M	3	9
Ataque aplicaciones -- Bases de datos corporativas	M	3	M	3	9
Ataque aplicaciones -- Backups de usuarios corporativos	M+	4	M	3	12
Ataque infraestructura -- Servidores controladores de dominio	M+	4	M+	4	16
Ataque infraestructura -- Servidor web	M+	4	M+	4	16
Ataque infraestructura -- Servidores file server	M+	4	M+	4	16
Ataque infraestructura -- Servidores de correo electrónico	M+	4	M+	4	16
Ataque infraestructura -- Servidor de nomina	M+	4	M+	4	16
Ataque infraestructura -- Servidores ERP	M+	4	M+	4	16
Ataque infraestructura -- Servidores Base de datos	M+	4	M+	4	16
Ataque infraestructura -- Servidor de antivirus	M+	4	M+	4	16
Ataque infraestructura -- Servidor planta	M+	4	M+	4	16
Ataque infraestructura -- Servidor de impresión	M+	4	M+	4	16
Ataque infraestructura -- Servidor de Encripcion PGP	M+	4	M+	4	16
Ataque infraestructura -- Dispositivo almacenamientos NAS para Backups	M+	4	M+	4	16
Ataque infraestructura -- Servidor filtrado spam	M+	4	M+	4	16
Ataque infraestructura -- Equipos escritorio, portátiles	M+	4	M+	4	16
Ataque infraestructura -- Equipos de comunicaciones:HP, D-Link	M+	4	M+	4	16
Ataque infraestructura -- Equipos de seguridad perimetral:Firewall Fortinet	M+	4	M+	4	16
Ataque infraestructura -- Planta telefónica: Siemens	M+	4	M+	4	16
Ataque infraestructura -- Red de datos	M+	4	M+	4	16
Ataque infraestructura -- Red de telefonía	M+	4	M+	4	16
Ataque infraestructura -- acceso a Internet	M+	4	M+	4	16
Ataque infraestructura -- Red de control e instrumentación	M+	4	M+	4	16
Ataque infraestructura -- Discos duros de servidores y estaciones de trabajo	M+	4	M+	4	16
Ataque infraestructura -- Discos externos información de backups	M+	4	M+	4	16
Ataque infraestructura -- Unidades de CD , DVD y Memorias extraíbles	M	3	M+	4	12
falta de sistema de parches -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M	3	M-	2	6
falta de sistema de parches -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M	3	M-	2	6
falta de sistema de parches -- Bases de datos: SQL server 2008 estándar	M	3	M-	2	6
falta de sistema de parches -- Correo electrónico: Exchange	M	3	M-	2	6

falta de sistema de parches -- Antivirus: Symantec Endpoint	M	3	M-	2	6
falta de sistema de parches -- Webserver: IIS	M	3	M-	2	6
falta de sistema de parches -- ERP: JDEdwards	M+	4	M-	2	8
falta de sistema de parches -- Sistemas SCADA	M	3	M	3	9
falta de sistema de parches -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M	3	M-	2	6
falta de sistema de parches -- Bases de datos corporativas	M+	4	M-	2	8
Falta de software de control de versiones -- Bases de datos: SQL server 2008 estándar	M+	4	M	3	12
Falta de software de control de versiones -- ERP: JDEdwards	M+	4	M	3	12
Falta de software de control de versiones -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M	3	12
Robo de información -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M+	4	16
Robo de información -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M+	4	M+	4	16
Robo de información -- Bases de datos: SQL server 2008 estándar	M+	4	M+	4	16
Robo de información -- Correo electrónico: Exchange	M+	4	M+	4	16
Robo de información -- Antivirus: Symantec Endpoint	M+	4	M+	4	16
Robo de información -- Webserver: IIS	M+	4	M+	4	16
Robo de información -- Sistema de backups: Symantec System recovery, Cobian	M+	4	M+	4	16
Robo de información -- ERP: JDEdwards	M+	4	M+	4	16
Robo de información -- Sistemas SCADA	M+	4	M+	4	16
Robo de información -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M+	4	16
Robo de información -- Código fuente aplicaciones de planta y administrativas	M+	4	M+	4	16
Robo de información -- Registros de operación: logs, informes y monitoreo	M+	4	M+	4	16
Robo de información -- Bases de datos corporativas	M+	4	M+	4	16
Robo de información -- Backups de usuarios corporativos	M+	4	M+	4	16
Robo de información -- Red de datos	M+	4	M+	4	16
Robo de información -- Red de telefonía	M+	4	M+	4	16
Robo de información -- Red de control e instrumentación	M+	4	M+	4	16
Robo de información -- Internet	M+	4	M+	4	16
Robo de información -- Intranet	M+	4	M+	4	16
Robo de información -- Telefonía	M+	4	M+	4	16
Robo de información -- Correo	M+	4	M+	4	16
Robo de información -- Discos duros de servidores y estaciones de trabajo	M+	4	M+	4	16
Robo de información -- Discos externos información de backups	M+	4	M+	4	16
Robo de información -- Unidades de CD , DVD y Memorias extraíbles	A	5	M+	4	5
Ausencia de estándares en cableado estructurado	A	5	A	5	25

-- Red de datos					
Ausencia de estándares en cableado estructurado -- Red de telefonía	A	5	A	5	25
Ausencia de estándares en cableado estructurado -- acceso a Internet	A	5	A	5	25
Ausencia de estándares en cableado estructurado -- Red de control e instrumentación	A	5	A	5	25
Ausencia de estándares en cableado estructurado -- Telefonía	A	5	A	5	25
Ausencia de estándares en cableado estructurado -- Sistema de cableado datos: Sede alterna	A	5	A	5	25
Ausencia de estándares en cableado estructurado -- Sistema de cableado datos : Centro de datos principal	A	5	A	5	25
Ausencia de estándares en cableado estructurado -- Sistema de cableado datos: Centro de datos alterno	A	5	A	5	25
Uso de software no oficial -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M-	2	8
Uso de software no oficial -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M	3	M-	2	6
Uso de software no oficial -- Bases de datos: SQL server 2008 estándar	M	3	M-	2	6
Uso de software no oficial -- Correo electrónico: Exchange	M	3	M-	2	6
Uso de software no oficial -- Antivirus: Symantec Endpoint	M	3	M-	2	6
Uso de software no oficial -- Webserver: IIS	M	3	M-	2	6
Uso de software no oficial -- Sistema de backups: Symantec System recovery, Cobian	M	3	M-	2	6
Uso de software no oficial -- ERP: JDEdwards	M+	4	M-	2	8
Uso de software no oficial -- Sistemas SCADA	M+	4	M	3	12
Uso de software no oficial -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M	3	M-	2	6
Uso de software no oficial -- Bases de datos corporativas	M+	4	M-	2	8
Acceso no autorizado -- Servidores controladores de dominio	M+	4	M+	4	16
Acceso no autorizado -- Servidor web	M+	4	M+	4	16
Acceso no autorizado -- Servidores file server	M+	4	M+	4	16
Acceso no autorizado -- Servidores de correo electrónico	M+	4	M+	4	16
Acceso no autorizado -- Servidor de nomina	M+	4	M+	4	16
Acceso no autorizado -- Servidores ERP	M+	4	M+	4	16
Acceso no autorizado -- Servidores Base de datos	M+	4	M+	4	16
Acceso no autorizado -- Servidor de antivirus	M+	4	M+	4	16
Acceso no autorizado -- Servidor planta	M+	4	M+	4	16
Acceso no autorizado -- Servidor de impresión	M+	4	M+	4	16
Acceso no autorizado -- Servidor de Encripcion PGP	M+	4	M+	4	16
Acceso no autorizado -- Dispositivo almacenamientos NAS para Backups	M+	4	M+	4	16
Acceso no autorizado -- Servidor filtrado spam	M+	4	M+	4	16
Acceso no autorizado -- Equipos escritorio,	M+	4	M+	4	16

portátiles					
Acceso no autorizado -- Equipos de comunicaciones:HP, D-Link	M+	4	M+	4	16
Acceso no autorizado -- Equipos de seguridad perimetral:Firewall Fortinet	M+	4	M+	4	16
Acceso no autorizado -- Planta telefónica: Siemens	M+	4	M+	4	16
Acceso no autorizado -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M+	4	16
Acceso no autorizado -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M+	4	M+	4	16
Acceso no autorizado -- Bases de datos: SQL server 2008 estándar	M+	4	M+	4	16
Acceso no autorizado -- Correo electrónico: Exchange	M+	4	M+	4	16
Acceso no autorizado -- Antivirus: Symantec Endpoint	M+	4	M+	4	16
Acceso no autorizado -- Webserver: IIS	M+	4	M+	4	16
Acceso no autorizado -- Sistema de backups: Symantec System recovery, Cobian	M+	4	M+	4	16
Acceso no autorizado -- ERP: JDEdwards	M+	4	M+	4	16
Acceso no autorizado -- Sistemas SCADA	M+	4	M+	4	16
Acceso no autorizado -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M+	4	16
Acceso no autorizado -- Código fuente aplicaciones de planta y administrativas	M+	4	M+	4	16
Acceso no autorizado -- Registros de operación: logs, informes y monitoreo	M+	4	M+	4	16
Acceso no autorizado -- Bases de datos corporativas	M+	4	M+	4	16
Acceso no autorizado -- Backups de usuarios corporativos	M+	4	M+	4	16
Acceso no autorizado -- Red de datos	M+	4	M+	4	16
Acceso no autorizado -- Red de telefonía	M+	4	M+	4	16
Acceso no autorizado -- acceso a Internet	M+	4	M+	4	16
Acceso no autorizado -- Red de control e instrumentación	M+	4	M+	4	16
Acceso no autorizado -- Internet	M+	4	M+	4	16
Acceso no autorizado -- Intranet	M+	4	M+	4	16
Acceso no autorizado -- Telefonía	M+	4	M+	4	16
Acceso no autorizado -- Correo	M+	4	M+	4	16
Acceso no autorizado -- Discos duros de servidores y estaciones de trabajo	M+	4	M+	4	16
Acceso no autorizado -- Discos externos información de backups	M+	4	M+	4	16
Acceso no autorizado -- Unidades de CD , DVD y Memorias extraíbles	M	3	M+	4	12
Retiro personal -- Coordinador de TI	M	3	M	3	9
Retiro personal -- Administrador de base de datos	M	3	M	3	9
Retiro personal -- Analistas funcionales	M	3	M	3	9
Retiro personal -- Desarrolladores	M	3	M	3	9
Retiro personal -- técnicos de operación	M	3	M	3	9
Retiro personal -- Analista de seguridad de la información	M	3	M	3	9

Retiro personal -- Director de informática	M+	4	M	3	12
Incapacidad -- Coordinador de TI	M+	4	M-	2	8
Incapacidad -- Administrador de base de datos	M+	4	M-	2	8
Incapacidad -- Analistas funcionales	M+	4	M-	2	8
Incapacidad -- Desarrolladores	M+	4	M-	2	8
Incapacidad -- técnicos de operación	M+	4	M-	2	8
Incapacidad -- Analista de seguridad de la información	M+	4	M-	2	8
Incapacidad -- Director de informática	M	3	M-	2	6
Poca disponibilidad -- Servidores controladores de dominio	M	3	M	3	9
Poca disponibilidad -- Servidor web	M	3	M	3	9
Poca disponibilidad -- Servidores file server	M	3	M	3	9
Poca disponibilidad -- Servidores de correo electrónico	M	3	M	3	9
Poca disponibilidad -- Servidor de nomina	M	3	M	3	9
Poca disponibilidad -- Servidores ERP	M	3	M	3	9
Poca disponibilidad -- Servidores Base de datos	M	3	M	3	9
Poca disponibilidad -- Servidor de antivirus	M	3	M	3	9
Poca disponibilidad -- Servidor planta	M	3	M	3	9
Poca disponibilidad -- Servidor de impresión	M	3	M	3	9
Poca disponibilidad -- Servidor de Encripcion PGP	M	3	M	3	9
Poca disponibilidad -- Dispositivo almacenamientos NAS para Backups	M	3	M	3	9
Poca disponibilidad -- Servidor filtrado spam	M	3	M	3	9
Poca disponibilidad -- Planta telefónica: Siemens	M+	4	M	3	12
Copia no autorizada -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M+	4	16
Copia no autorizada -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M+	4	M+	4	16
Copia no autorizada -- Bases de datos: SQL server 2008 estándar	M+	4	M+	4	16
Copia no autorizada -- Correo electrónico: Exchange	M+	4	M+	4	16
Copia no autorizada -- Antivirus: Symantec Endpoint	M+	4	M+	4	16
Copia no autorizada -- Webserver: IIS	M+	4	M+	4	16
Copia no autorizada -- Sistema de backups: Symantec System recovery, Cobian	M+	4	M+	4	16
Copia no autorizada -- ERP: JDEdwards	M+	4	M+	4	16
Copia no autorizada -- Sistemas SCADA	M+	4	M+	4	16
Copia no autorizada -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M+	4	16
Copia no autorizada -- Código fuente aplicaciones de planta y administrativas	M+	4	M+	4	16
Copia no autorizada -- Registros de operación: logs, informes y monitoreo	M+	4	M+	4	16
Copia no autorizada -- Bases de datos corporativas	M+	4	M+	4	16
Copia no autorizada -- Backups de usuarios corporativos	M+	4	M+	4	16
Copia no autorizada -- Discos duros de servidores y estaciones de trabajo	M+	4	M+	4	16

Copia no autorizada -- Discos externos información de backups	M+	4	M+	4	16
Copia no autorizada -- Unidades de CD , DVD y Memorias extraíbles	M+	4	M+	4	16
Borrado y alteración -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M+	4	16
Borrado y alteración -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M+	4	M+	4	16
Borrado y alteración -- Bases de datos: SQL server 2008 estándar	M+	4	M+	4	16
Borrado y alteración -- Correo electrónico: Exchange	M+	4	M+	4	16
Borrado y alteración -- Antivirus: Symantec Endpoint	M+	4	M+	4	16
Borrado y alteración -- Webserver: IIS	M+	4	M+	4	16
Borrado y alteración -- Sistema de backups: Symantec System recovery, Cobian	M+	4	M+	4	16
Borrado y alteración -- ERP: JDEdwards	M+	4	M+	4	16
Borrado y alteración -- Sistemas SCADA	M+	4	M+	4	16
Borrado y alteración -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M+	4	16
Borrado y alteración -- Código fuente aplicaciones de planta y administrativas	M+	4	M+	4	16
Borrado y alteración -- Registros de operación: logs, informes y monitoreo	M+	4	M+	4	16
Borrado y alteración -- Bases de datos corporativas	M+	4	M+	4	16
Borrado y alteración -- Backups de usuarios corporativos	M+	4	M+	4	16
Borrado y alteración -- Discos duros de servidores y estaciones de trabajo	M+	4	M+	4	16
Borrado y alteración -- Discos externos información de backups	M+	4	M+	4	16
Borrado y alteración -- Unidades de CD , DVD y Memorias extraíbles	M+	4	M+	4	16
Incendio -- Centro de procesamiento de datos principal	B	1	A	5	5
Incendio -- Centro de procesamiento de datos alterno	B	1	A	5	5
Incendio -- Ubicación local de infraestructura y comunicaciones	B	1	A	5	5
Incendio -- sala eléctrica, ups, telecomunicaciones	B	1	A	5	5
Incendio -- Servidores controladores de dominio	B	1	A	5	5
Incendio -- Servidor web	B	1	A	5	5
Incendio -- Servidores file server	B	1	A	5	5
Incendio -- Servidores de correo electrónico	B	1	A	5	5
Incendio -- Servidor de nomina	B	1	A	5	5
Incendio -- Servidores ERP	B	1	A	5	5
Incendio -- Servidores Base de datos	B	1	A	5	5
Incendio -- Servidor de antivirus	B	1	A	5	5
Incendio -- Servidor planta	B	1	A	5	5
Incendio -- Servidor de impresión	B	1	A	5	5
Incendio -- Servidor de Encripcion PGP	B	1	A	5	5
Incendio -- Dispositivo almacenamientos NAS	B	1	A	5	5

para Backups					
Incendio -- Servidor filtrado spam	B	1	A	5	5
Incendio -- Equipos escritorio, portátiles	B	1	A	5	5
Incendio -- Equipos de comunicaciones:HP, D-Link	B	1	A	5	5
Incendio -- Equipos de seguridad perimetral:Firewall Fortinet	B	1	A	5	5
Incendio -- Planta telefónica: Siemens	B	1	A	5	5
Incendio -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	B	1	A	5	5
Incendio -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	B	1	A	5	5
Incendio -- Bases de datos: SQL server 2008 estándar	B	1	A	5	5
Incendio -- Correo electrónico: Exchange	B	1	A	5	5
Incendio -- Antivirus: Symantec Endpoint	B	1	A	5	5
Incendio -- Webserver: IIS	B	1	A	5	5
Incendio -- Sistema de backups: Symantec System recovery, Cobian	B	1	A	5	5
Incendio -- ERP: JDEdwards	B	1	A	5	5
Incendio -- Sistemas SCADA	B	1	A	5	5
Incendio -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	B	1	A	5	5
Incendio -- Código fuente aplicaciones de planta y administrativas	B	1	A	5	5
Incendio -- Registros de operación: logs, informes y monitoreo	B	1	A	5	5
Incendio -- Bases de datos corporativas	B	1	A	5	5
Incendio -- Backups de usuarios corporativos	B	1	A	5	5
Incendio -- Red de datos	B	1	A	5	5
Incendio -- Red de telefonía	B	1	A	5	5
Incendio -- acceso a Internet	B	1	A	5	5
Incendio -- Red de control e instrumentación	B	1	A	5	5
Incendio -- Internet	B	1	A	5	5
Incendio -- Intranet	B	1	A	5	5
Incendio -- Telefonía	B	1	A	5	5
Incendio -- Correo	B	1	A	5	5
Incendio -- Sistema de alimentación UPS	B	1	A	5	5
Incendio -- Generadores de energía	B	1	A	5	5
Incendio -- Sistema de aire acondicionado	B	1	A	5	5
Incendio -- Sistema de cableado Eléctrico: Centro de datos principal	B	1	A	5	5
Incendio -- Sistema de cableado Eléctrico: Centro de datos alterno	B	1	A	5	5
Incendio -- Sistema de cableado Eléctrico: Sede alterna	B	1	A	5	5
Incendio -- Sistema de cableado datos: Sede alterna	B	1	A	5	5
Incendio -- Sistema de cableado datos : Centro de datos principal	B	1	A	5	5
Incendio -- Sistema de cableado datos: Centro de datos alterno	B	1	A	5	5
Incendio -- Equipos de control de temperatura	B	1	A	5	5

Incendio -- Coordinador de TI	B	1	A	5	5
Incendio -- Administrador de base de datos	B	1	A	5	5
Incendio -- Analistas funcionales	B	1	A	5	5
Incendio -- Desarrolladores	B	1	A	5	5
Incendio -- técnicos de operación	B	1	A	5	5
Incendio -- Analista de seguridad de la información	B	1	A	5	5
Incendio -- Director de informática	B	1	A	5	5
Incendio -- Discos duros de servidores y estaciones de trabajo	B	1	A	5	5
Incendio -- Discos externos información de backups	B	1	A	5	5
Incendio -- Unidades de CD , DVD y Memorias extraíbles	B	1	A	5	5
Terremoto -- Centro de procesamiento de datos principal	B	1	A	5	5
Terremoto -- Centro de procesamiento de datos alterno	B	1	A	5	5
Terremoto -- Ubicación local de infraestructura y comunicaciones	B	1	A	5	5
Terremoto -- sala eléctrica, ups, telecomunicaciones	B	1	A	5	5
Terremoto -- Servidores controladores de dominio	B	1	A	5	5
Terremoto -- Servidor web	B	1	A	5	5
Terremoto -- Servidores file server	B	1	A	5	5
Terremoto -- Servidores de correo electrónico	B	1	A	5	5
Terremoto -- Servidor de nomina	B	1	A	5	5
Terremoto -- Servidores ERP	B	1	A	5	5
Terremoto -- Servidores Base de datos	B	1	A	5	5
Terremoto -- Servidor de antivirus	B	1	A	5	5
Terremoto -- Servidor planta	B	1	A	5	5
Terremoto -- Servidor de impresión	B	1	A	5	5
Terremoto -- Servidor de Encripcion PGP	B	1	A	5	5
Terremoto -- Dispositivo almacenamientos NAS para Backups	B	1	A	5	5
Terremoto -- Servidor filtrado spam	B	1	A	5	5
Terremoto -- Equipos escritorio, portátiles	B	1	A	5	5
Terremoto -- Equipos de comunicaciones:HP, D-Link	B	1	A	5	5
Terremoto -- Equipos de seguridad perimetral:Firewall Fortinet	B	1	A	5	5
Terremoto -- Planta telefónica: Siemens	B	1	A	5	5
Terremoto -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	B	1	A	5	5
Terremoto -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	B	1	A	5	5
Terremoto -- Bases de datos: SQL server 2008 estándar	B	1	A	5	5
Terremoto -- Correo electrónico: Exchange	B	1	A	5	5
Terremoto -- Antivirus: Symantec Endpoint	B	1	A	5	5
Terremoto -- Webserver: IIS	B	1	A	5	5
Terremoto -- Sistema de backups: Symantec System recovery, Cobian	B	1	A	5	5

Terremoto -- ERP: JDEdwards	B	1	A	5	5
Terremoto -- Sistemas SCADA	B	1	A	5	5
Terremoto -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	B	1	A	5	5
Terremoto -- Código fuente aplicaciones de planta y administrativas	B	1	A	5	5
Terremoto -- Registros de operación: logs, informes y monitoreo	B	1	A	5	5
Terremoto -- Bases de datos corporativas	B	1	A	5	5
Terremoto -- Backups de usuarios corporativos	B	1	A	5	5
Terremoto -- Red de datos	B	1	A	5	5
Terremoto -- Red de telefonía	B	1	A	5	5
Terremoto -- acceso a Internet	B	1	A	5	5
Terremoto -- Red de control e instrumentación	B	1	A	5	5
Terremoto -- Internet	B	1	A	5	5
Terremoto -- Intranet	B	1	A	5	5
Terremoto -- Telefonía	B	1	A	5	5
Terremoto -- Correo	B	1	A	5	5
Terremoto -- Sistema de alimentación UPS	B	1	A	5	5
Terremoto -- Generadores de energía	B	1	A	5	5
Terremoto -- Sistema de aire acondicionado	B	1	A	5	5
Terremoto -- Sistema de cableado Eléctrico: Centro de datos principal	B	1	A	5	5
Terremoto -- Sistema de cableado Eléctrico: Centro de datos alterno	B	1	A	5	5
Terremoto -- Sistema de cableado Eléctrico: Sede alterna	B	1	A	5	5
Terremoto -- Sistema de cableado datos: Sede alterna	B	1	A	5	5
Terremoto -- Sistema de cableado datos : Centro de datos principal	B	1	A	5	5
Terremoto -- Sistema de cableado datos: Centro de datos alterno	B	1	A	5	5
Terremoto -- Equipos de control de temperatura	B	1	A	5	5
Terremoto -- Coordinador de TI	B	1	A	5	5
Terremoto -- Administrador de base de datos	B	1	A	5	5
Terremoto -- Analistas funcionales	B	1	A	5	5
Terremoto -- Desarrolladores	B	1	A	5	5
Terremoto -- técnicos de operación	B	1	A	5	5
Terremoto -- Analista de seguridad de la información	B	1	A	5	5
Terremoto -- Director de informática	B	1	A	5	5
Terremoto -- Discos duros de servidores y estaciones de trabajo	B	1	A	5	5
Terremoto -- Discos externos información de backups	B	1	A	5	5
Terremoto -- Unidades de CD , DVD y Memorias extraíbles	B	1	A	5	5
Falla eléctrica -- Centro de procesamiento de datos principal	M	3	M	3	9
Falla eléctrica -- Centro de procesamiento de datos alterno	M	3	M	3	9
Falla eléctrica -- Ubicación local de infraestructura y comunicaciones	M	3	M	3	9
Falla eléctrica -- sala eléctrica, ups,	M	3	M	3	9

telecomunicaciones					
Falla eléctrica -- Servidores controladores de dominio	M	3	M	3	9
Falla eléctrica -- Servidor web	M	3	M	3	9
Falla eléctrica -- Servidores file server	M	3	M	3	9
Falla eléctrica -- Servidores de correo electrónico	M	3	M	3	9
Falla eléctrica -- Servidor de nomina	M	3	M	3	9
Falla eléctrica -- Servidores ERP	M	3	M	3	9
Falla eléctrica -- Servidores Base de datos	M	3	M	3	9
Falla eléctrica -- Servidor de antivirus	M	3	M	3	9
Falla eléctrica -- Servidor planta	M	3	M	3	9
Falla eléctrica -- Servidor de impresión	M	3	M	3	9
Falla eléctrica -- Servidor de Encripcion PGP	M	3	M	3	9
Falla eléctrica -- Dispositivo almacenamientos NAS para Backups	M	3	M	3	9
Falla eléctrica -- Servidor filtrado spam	M	3	M	3	9
Falla eléctrica -- Equipos escritorio, portátiles	M	3	M	3	9
Falla eléctrica -- Equipos de comunicaciones:HP, D-Link	M	3	M	3	9
Falla eléctrica -- Equipos de seguridad perimetral:Firewall Fortinet	M	3	M	3	9
Falla eléctrica -- Planta telefónica: Siemens	M	3	M	3	9
Falla eléctrica -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M	3	M	3	9
Falla eléctrica -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M	3	M	3	9
Falla eléctrica -- Bases de datos: SQL server 2008 estándar	M	3	M	3	9
Falla eléctrica -- Correo electrónico: Exchange	M	3	M	3	9
Falla eléctrica -- Antivirus: Symantec Endpoint	M	3	M	3	9
Falla eléctrica -- Webserver: IIS	M	3	M	3	9
Falla eléctrica -- Sistema de backups: Symantec System recovery, Cobian	M	3	M	3	9
Falla eléctrica -- ERP: JDEdwards	M	3	M	3	9
Falla eléctrica -- Sistemas SCADA	M	3	M	3	9
Falla eléctrica -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M	3	M	3	9
Falla eléctrica -- Código fuente aplicaciones de planta y administrativas	M	3	M	3	9
Falla eléctrica -- Registros de operación: logs, informes y monitoreo	M	3	M	3	9
Falla eléctrica -- Bases de datos corporativas	M	3	M	3	9
Falla eléctrica -- Backups de usuarios corporativos	M	3	M	3	9
Falla eléctrica -- Red de datos	M	3	M	3	9
Falla eléctrica -- Red de telefonía	M	3	M	3	9
Falla eléctrica -- acceso a Internet	M	3	M	3	9
Falla eléctrica -- Red de control e instrumentación	M	3	M	3	9
Falla eléctrica -- Internet	M	3	M	3	9
Falla eléctrica -- Intranet	M	3	M	3	9
Falla eléctrica -- Telefonía	M	3	M	3	9

Falla eléctrica -- Correo	M	3	M	3	9
Falla eléctrica -- Sistema de alimentación UPS	M	3	M	3	9
Falla eléctrica -- Generadores de energía	M	3	M	3	9
Falla eléctrica -- Sistema de aire acondicionado	M	3	M	3	9
Falla eléctrica -- Sistema de cableado Eléctrico: Centro de datos principal	M	3	M	3	9
Falla eléctrica -- Sistema de cableado Eléctrico: Centro de datos alterno	M	3	M	3	9
Falla eléctrica -- Sistema de cableado Eléctrico: Sede alterna	M	3	M	3	9
Falla eléctrica -- Sistema de cableado datos: Sede alterna	M	3	M	3	9
Falla eléctrica -- Sistema de cableado datos : Centro de datos principal	M	3	M	3	9
Falla eléctrica -- Sistema de cableado datos: Centro de datos alterno	M	3	M	3	9
Falla eléctrica -- Equipos de control de temperatura	M	3	M	3	9
Inundación -- Centro de procesamiento de datos principal	B	1	A	5	5
Inundación -- Centro de procesamiento de datos alterno	B	1	A	5	5
Inundación -- Ubicación local de infraestructura y comunicaciones	B	1	A	5	5
Inundación -- sala eléctrica, ups, telecomunicaciones	B	1	A	5	5
Inundación -- Servidores controladores de dominio	B	1	A	5	5
Inundación -- Servidor web	B	1	A	5	5
Inundación -- Servidores file server	B	1	A	5	5
Inundación -- Servidores de correo electrónico	B	1	A	5	5
Inundación -- Servidor de nomina	B	1	A	5	5
Inundación -- Servidores ERP	B	1	A	5	5
Inundación -- Servidores Base de datos	B	1	A	5	5
Inundación -- Servidor de antivirus	B	1	A	5	5
Inundación -- Servidor planta	B	1	A	5	5
Inundación -- Servidor de impresión	B	1	A	5	5
Inundación -- Servidor de Encripcion PGP	B	1	A	5	5
Inundación -- Dispositivo almacenamientos NAS para Backups	B	1	A	5	5
Inundación -- Servidor filtrado spam	B	1	A	5	5
Inundación -- Equipos escritorio, portátiles	B	1	A	5	5
Inundación -- Equipos de comunicaciones:HP, D-Link	B	1	A	5	5
Inundación -- Equipos de seguridad perimetral:Firewall Fortinet	B	1	A	5	5
Inundación -- Planta telefónica: Siemens	B	1	A	5	5
Inundación -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	B	1	A	5	5
Inundación -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	B	1	A	5	5
Inundación -- Bases de datos: SQL server 2008 estándar	B	1	A	5	5
Inundación -- Correo electrónico: Exchange	B	1	A	5	5

Inundación -- Antivirus: Symantec Endpoint	B	1	A	5	5
Inundación -- Webserver: IIS	B	1	A	5	5
Inundación -- Sistema de backups: Symantec System recovery, Cobian	B	1	A	5	5
Inundación -- ERP: JDEdwards	B	1	A	5	5
Inundación -- Sistemas SCADA	B	1	A	5	5
Inundación -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	B	1	A	5	5
Inundación -- Código fuente aplicaciones de planta y administrativas	B	1	A	5	5
Inundación -- Registros de operación: logs, informes y monitoreo	B	1	A	5	5
Inundación -- Bases de datos corporativas	B	1	A	5	5
Inundación -- Backups de usuarios corporativos	B	1	A	5	5
Inundación -- Red de datos	B	1	A	5	5
Inundación -- Red de telefonía	B	1	A	5	5
Inundación -- acceso a Internet	B	1	A	5	5
Inundación -- Red de control e instrumentación	B	1	A	5	5
Inundación -- Internet	B	1	A	5	5
Inundación -- Intranet	B	1	A	5	5
Inundación -- Telefonía	B	1	A	5	5
Inundación -- Correo	B	1	A	5	5
Inundación -- Sistema de alimentación UPS	B	1	A	5	5
Inundación -- Generadores de energía	B	1	A	5	5
Inundación -- Sistema de aire acondicionado	B	1	A	5	5
Inundación -- Sistema de cableado Eléctrico: Centro de datos principal	B	1	A	5	5
Inundación -- Sistema de cableado Eléctrico: Centro de datos alterno	B	1	A	5	5
Inundación -- Sistema de cableado Eléctrico: Sede alterna	B	1	A	5	5
Inundación -- Sistema de cableado datos: Sede alterna	B	1	A	5	5
Inundación -- Sistema de cableado datos : Centro de datos principal	B	1	A	5	5
Inundación -- Sistema de cableado datos: Centro de datos alterno	B	1	A	5	5
Inundación -- Equipos de control de temperatura	B	1	A	5	5
Inundación -- Coordinador de TI	B	1	A	5	5
Inundación -- Administrador de base de datos	B	1	A	5	5
Inundación -- Analistas funcionales	B	1	A	5	5
Inundación -- Desarrolladores	B	1	A	5	5
Inundación -- técnicos de operación	B	1	A	5	5
Inundación -- Analista de seguridad de la información	B	1	A	5	5
Inundación -- Director de informática	B	1	A	5	5
Inundación -- Discos duros de servidores y estaciones de trabajo	B	1	A	5	5
Inundación -- Discos externos información de backups	B	1	A	5	5
Inundación -- Unidades de CD , DVD y Memorias extraíbles	B	1	A	5	5
Terrorismo -- Centro de procesamiento de datos principal	B	1	A	5	5

Terrorismo -- Centro de procesamiento de datos alterno	B	1	A	5	5
Terrorismo -- Ubicación local de infraestructura y comunicaciones	B	1	A	5	5
Terrorismo -- sala eléctrica, ups, telecomunicaciones	B	1	A	5	5
Terrorismo -- Servidores controladores de dominio	B	1	A	5	5
Terrorismo -- Servidor web	B	1	A	5	5
Terrorismo -- Servidores file server	B	1	A	5	5
Terrorismo -- Servidores de correo electrónico	B	1	A	5	5
Terrorismo -- Servidor de nomina	B	1	A	5	5
Terrorismo -- Servidores ERP	B	1	A	5	5
Terrorismo -- Servidores Base de datos	B	1	A	5	5
Terrorismo -- Servidor de antivirus	B	1	A	5	5
Terrorismo -- Servidor planta	B	1	A	5	5
Terrorismo -- Servidor de impresión	B	1	A	5	5
Terrorismo -- Servidor de Encripcion PGP	B	1	A	5	5
Terrorismo -- Dispositivo almacenamientos NAS para Backups	B	1	A	5	5
Terrorismo -- Servidor filtrado spam	B	1	A	5	5
Terrorismo -- Equipos escritorio, portátiles	B	1	A	5	5
Terrorismo -- Equipos de comunicaciones:HP, D-Link	B	1	A	5	5
Terrorismo -- Equipos de seguridad perimetral:Firewall Fortinet	B	1	A	5	5
Terrorismo -- Planta telefónica: Siemens	B	1	A	5	5
Terrorismo -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	B	1	A	5	5
Terrorismo -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	B	1	A	5	5
Terrorismo -- Bases de datos: SQL server 2008 estándar	B	1	A	5	5
Terrorismo -- Correo electrónico: Exchange	B	1	A	5	5
Terrorismo -- Antivirus: Symantec Endpoint	B	1	A	5	5
Terrorismo -- Webserver: IIS	B	1	A	5	5
Terrorismo -- Sistema de backups: Symantec System recovery, Cobian	B	1	A	5	5
Terrorismo -- ERP: JDEdwards	B	1	A	5	5
Terrorismo -- Sistemas SCADA	B	1	A	5	5
Terrorismo -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	B	1	A	5	5
Terrorismo -- Código fuente aplicaciones de planta y administrativas	B	1	A	5	5
Terrorismo -- Registros de operación: logs, informes y monitoreo	B	1	A	5	5
Terrorismo -- Bases de datos corporativas	B	1	A	5	5
Terrorismo -- Backups de usuarios corporativos	B	1	A	5	5
Terrorismo -- Red de datos	B	1	A	5	5
Terrorismo -- Red de telefonía	B	1	A	5	5
Terrorismo -- acceso a Internet	B	1	A	5	5
Terrorismo -- Red de control e instrumentación	B	1	A	5	5
Terrorismo -- Internet	B	1	A	5	5

Terrorismo -- Intranet	B	1	A	5	5
Terrorismo -- Telefonía	B	1	A	5	5
Terrorismo -- Correo	B	1	A	5	5
Terrorismo -- Sistema de alimentación UPS	B	1	A	5	5
Terrorismo -- Generadores de energía	B	1	A	5	5
Terrorismo -- Sistema de aire acondicionado	B	1	A	5	5
Terrorismo -- Sistema de cableado Eléctrico: Centro de datos principal	B	1	A	5	5
Terrorismo -- Sistema de cableado Eléctrico: Centro de datos alterno	B	1	A	5	5
Terrorismo -- Sistema de cableado Eléctrico: Sede alterna	B	1	A	5	5
Terrorismo -- Sistema de cableado datos: Sede alterna	B	1	A	5	5
Terrorismo -- Sistema de cableado datos : Centro de datos principal	B	1	A	5	5
Terrorismo -- Sistema de cableado datos: Centro de datos alterno	B	1	A	5	5
Terrorismo -- Equipos de control de temperatura	B	1	A	5	5
Terrorismo -- Coordinador de TI	B	1	A	5	5
Terrorismo -- Administrador de base de datos	B	1	A	5	5
Terrorismo -- Analistas funcionales	B	1	A	5	5
Terrorismo -- Desarrolladores	B	1	A	5	5
Terrorismo -- técnicos de operación	B	1	A	5	5
Terrorismo -- Analista de seguridad de la información	B	1	A	5	5
Terrorismo -- Director de informática	B	1	A	5	5
Terrorismo -- Discos duros de servidores y estaciones de trabajo	B	1	A	5	5
Terrorismo -- Discos externos información de backups	B	1	A	5	5
Terrorismo -- Unidades de CD , DVD y Memorias extraíbles	B	1	A	5	5
Desmotivación -- Coordinador de TI	M+	4	M-	2	8
Desmotivación -- Administrador de base de datos	M+	4	M-	2	8
Desmotivación -- Analistas funcionales	M+	4	M-	2	8
Desmotivación -- Desarrolladores	M+	4	M-	2	8
Desmotivación -- técnicos de operación	M+	4	M-	2	8
Desmotivación -- Analista de seguridad de la información	M+	4	M-	2	8
Desmotivación -- Director de informática	M+	4	M-	2	8
Solo un especialista -- Servidores controladores de dominio	M+	4	M+	4	16
Solo un especialista -- Servidor web	M+	4	M+	4	16
Solo un especialista -- Servidores file server	M+	4	M+	4	16
Solo un especialista -- Servidores de correo electrónico	M+	4	M+	4	16
Solo un especialista -- Servidor de nomina	M+	4	M+	4	16
Solo un especialista -- Servidores ERP	M+	4	M+	4	16
Solo un especialista -- Servidores Base de datos	M+	4	M+	4	16
Solo un especialista -- Servidor de antivirus	M+	4	M+	4	16
Solo un especialista -- Servidor planta	M+	4	M+	4	16
Solo un especialista -- Servidor de impresión	M+	4	M+	4	16

Solo un especialista -- Servidor de Encripcion PGP	M+	4	M+	4	16
Solo un especialista -- Dispositivo almacenamientos NAS para Backups	M+	4	M+	4	16
Solo un especialista -- Servidor filtrado spam	M+	4	M+	4	16
Solo un especialista -- Equipos escritorio, portátiles	M+	4	M+	4	16
Solo un especialista -- Equipos de comunicaciones:HP, D-Link	M+	4	M+	4	16
Solo un especialista -- Equipos de seguridad perimetral:Firewall Fortinet	M+	4	M+	4	16
Solo un especialista -- Planta telefónica: Siemens	M+	4	M+	4	16
Solo un especialista -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M+	4	16
Solo un especialista -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M+	4	M+	4	16
Solo un especialista -- Bases de datos: SQL server 2008 estándar	M+	4	M+	4	16
Solo un especialista -- Correo electrónico: Exchange	M+	4	M+	4	16
Solo un especialista -- Antivirus: Symantec Endpoint	M+	4	M+	4	16
Solo un especialista -- Webserver: IIS	M+	4	M+	4	16
Solo un especialista -- Sistema de backups: Symantec System recovery, Cobian	M+	4	M+	4	16
Solo un especialista -- ERP: JDEdwards	M+	4	M+	4	16
Solo un especialista -- Sistemas SCADA	M+	4	M+	4	16
Solo un especialista -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M+	4	16
Solo un especialista -- Código fuente aplicaciones de planta y administrativas	M+	4	M+	4	16
Solo un especialista -- Registros de operación: logs, informes y monitoreo	M+	4	M+	4	16
Solo un especialista -- Bases de datos corporativas	M+	4	M+	4	16
Solo un especialista -- Backups de usuarios corporativos	M+	4	M+	4	16
Solo un especialista -- Red de datos	M+	4	M+	4	16
Solo un especialista -- Red de telefonía	M+	4	M+	4	16
Solo un especialista -- acceso a Internet	M+	4	M+	4	16
Solo un especialista -- Red de control e instrumentación	M+	4	M+	4	16
Solo un especialista -- Internet	M+	4	M+	4	16
Solo un especialista -- Intranet	M+	4	M+	4	16
Solo un especialista -- Telefonía	M+	4	M+	4	16
Solo un especialista -- Correo	M+	4	M+	4	16
Negligencia -- Coordinador de TI	B	1	M-	2	2
Negligencia -- Administrador de base de datos	B	1	M-	2	2
Negligencia -- Analistas funcionales	B	1	M-	2	2
Negligencia -- Desarrolladores	B	1	M-	2	2
Negligencia -- técnicos de operación	B	1	M-	2	2
Negligencia -- Analista de seguridad de la información	B	1	M-	2	2
Negligencia -- Director de informática	B	1	M-	2	2

Mal diseño de los procesos -- Bases de datos: SQL server 2008 estándar	M-	2	M	3	6
Mal diseño de los procesos -- ERP: JDEdwards	M-	2	M	3	6
Mal diseño de los procesos -- Sistemas SCADA	M-	2	M	3	6
Mal diseño de los procesos -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M-	2	M	3	6
Líder inexperto -- Servidores controladores de dominio	M-	2	M	3	6
Líder inexperto -- Servidor web	M-	2	M	3	6
Líder inexperto -- Servidores file server	M-	2	M	3	6
Líder inexperto -- Servidores de correo electrónico	M-	2	M	3	6
Líder inexperto -- Servidor de nomina	M-	2	M	3	6
Líder inexperto -- Servidores ERP	M-	2	M	3	6
Líder inexperto -- Servidores Base de datos	M-	2	M	3	6
Líder inexperto -- Servidor de antivirus	M-	2	M	3	6
Líder inexperto -- Servidor planta	M-	2	M	3	6
Líder inexperto -- Servidor de impresión	M-	2	M	3	6
Líder inexperto -- Servidor de Encripcion PGP	M-	2	M	3	6
Líder inexperto -- Dispositivo almacenamientos NAS para Backups	M-	2	M	3	6
Líder inexperto -- Servidor filtrado spam	M-	2	M	3	6
Líder inexperto -- Equipos escritorio, portátiles	M-	2	M	3	6
Líder inexperto -- Equipos de comunicaciones:HP, D-Link	M-	2	M	3	6
Líder inexperto -- Equipos de seguridad perimetral:Firewall Fortinet	M-	2	M	3	6
Líder inexperto -- Planta telefónica: Siemens	M-	2	M	3	6
Líder inexperto -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M-	2	M	3	6
Líder inexperto -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M-	2	M	3	6
Líder inexperto -- Bases de datos: SQL server 2008 estándar	M-	2	M	3	6
Líder inexperto -- Correo electrónico: Exchange	M-	2	M	3	6
Líder inexperto -- Antivirus: Symantec Endpoint	M-	2	M	3	6
Líder inexperto -- Webserver: IIS	M-	2	M	3	6
Líder inexperto -- Sistema de backups: Symantec System recovery, Cobian	M-	2	M	3	6
Líder inexperto -- ERP: JDEdwards	M-	2	M	3	6
Líder inexperto -- Sistemas SCADA	M-	2	M	3	6
Líder inexperto -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M-	2	M	3	6
Líder inexperto -- Código fuente aplicaciones de planta y administrativas	M-	2	M	3	6
Líder inexperto -- Registros de operación: logs, informes y monitoreo	M-	2	M	3	6
Líder inexperto -- Bases de datos corporativas	M-	2	M	3	6
Líder inexperto -- Backups de usuarios corporativos	M-	2	M	3	6
Líder inexperto -- Red de datos	M-	2	M	3	6
Líder inexperto -- Red de telefonía	M-	2	M	3	6
Líder inexperto -- acceso a Internet	M-	2	M	3	6

Líder inexperto -- Red de control e instrumentación	M-	2	M	3	6
Líder inexperto -- Internet	M-	2	M	3	6
Líder inexperto -- Intranet	M-	2	M	3	6
Líder inexperto -- Telefonía	M-	2	M	3	6
Líder inexperto -- Correo	M-	2	M	3	6
Analistas inexpertos -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M-	2	M	3	6
Analistas inexpertos -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M-	2	M	3	6
Analistas inexpertos -- Bases de datos: SQL server 2008 estándar	M-	2	M	3	6
Analistas inexpertos -- Correo electrónico: Exchange	M-	2	M	3	6
Analistas inexpertos -- Antivirus: Symantec Endpoint	M-	2	M	3	6
Analistas inexpertos -- Webserver: IIS	M-	2	M	3	6
Analistas inexpertos -- Sistema de backups: Symantec System recovery, Cobian	M-	2	M	3	6
Analistas inexpertos -- ERP: JDEdwards	M-	2	M	3	6
Analistas inexpertos -- Sistemas SCADA	M-	2	M	3	6
Analistas inexpertos -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M-	2	M	3	6
Falta de alcances claros -- Coordinador de TI	M-	2	M+	4	8
Falta de alcances claros -- Administrador de base de datos	M-	2	M+	4	8
Falta de alcances claros -- Analistas funcionales	M-	2	M+	4	8
Falta de alcances claros -- Desarrolladores	M-	2	M+	4	8
Falta de alcances claros -- técnicos de operación	M-	2	M+	4	8
Falta de alcances claros -- Analista de seguridad de la información	M-	2	M+	4	8
Falta de alcances claros -- Director de informática	M	3	M+	4	12
Robo de equipos -- Servidores controladores de dominio	M	3	M+	4	12
Robo de equipos -- Servidor web	M	3	M+	4	12
Robo de equipos -- Servidores file server	M	3	M+	4	12
Robo de equipos -- Servidores de correo electrónico	M	3	M+	4	12
Robo de equipos -- Servidor de nomina	M	3	M+	4	12
Robo de equipos -- Servidores ERP	M	3	M+	4	12
Robo de equipos -- Servidores Base de datos	M	3	M+	4	12
Robo de equipos -- Servidor de antivirus	M	3	M+	4	12
Robo de equipos -- Servidor planta	M	3	M+	4	12
Robo de equipos -- Servidor de impresión	M	3	M+	4	12
Robo de equipos -- Servidor de Encripcion PGP	M	3	M+	4	12
Robo de equipos -- Servidor filtrado spam	M	3	M+	4	12
Robo de equipos -- Equipos escritorio, portátiles	M	3	M+	4	12
Robo de equipos -- Equipos de comunicaciones:HP, D-Link	M	3	M+	4	12
Robo de equipos -- Equipos de seguridad perimetral:Firewall Fortinet	M	3	M+	4	12
Robo de equipos -- Planta telefónica: Siemens	M	3	M+	4	12

Robo de equipos -- Discos duros de servidores y estaciones de trabajo	M	3	M+	4	12
Robo de equipos -- Discos externos información de backups	M	3	M+	4	12
Robo de equipos -- Unidades de CD , DVD y Memorias extraíbles	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidores controladores de dominio	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor web	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidores file server	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidores de correo electrónico	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor de nomina	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidores ERP	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidores Base de datos	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor de antivirus	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor planta	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor de impresión	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor de Encripcion PGP	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Dispositivo almacenamientos NAS para Backups	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Servidor filtrado spam	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Sistemas Operativos Clientes :Windows 7, Windows 8, Windows 10	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Bases de datos: SQL server 2008 estándar	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Correo electrónico: Exchange	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Antivirus: Symantec Endpoint	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Webserver: IIS	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Sistema de backups: Symantec System recovery, Cobian	M+	4	M+	4	16
Pérdida de capacidad de servidores -- ERP: JDEdwards	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Sistemas SCADA	M+	4	M+	4	16
Pérdida de capacidad de servidores -- Aplicaciones de desarrollo :Visual studio .Net y SQl developer	M+	4	M+	4	16

Tabla 19. Calculo de Riesgo

3.8 NIVEL DE RIESGO ACEPTABLE Y RESIDUAL

Los criterios de aceptación de riesgo demandados por Textilera S.A, establece que riesgos de niveles “Alto” y “Medio Alto” se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios requeridos. Así mismo para los niveles Medio y bajo su tratamiento depende del aporte del control para mitigar riesgos, la relación costo/beneficio y la contribución que este aporte al cumplimiento de los objetivos del negocio.

Mejor Esfuerzo	Inaceptables
Bajo	Medio Alto
Medio	Alto

Tabla 20.Criterios de Aceptación

De acuerdo a nuestro cálculo de riesgo tenemos entonces:

CON CONTROL						
Probabilidad						
	valor	1	2	3	4	5
Muy Alto	5		software malicioso -- Intranet ||		informacion -- Unidades de CD , DVD y Memorias	estandares en cableado estructurado --
alto	4		falta de sistema de parches -- ERP: JDEdwards || falta de sistema	Ataque aplicaciones -- Backups de usuarios	Ataque infraestructura -- Servidores controladores	
Medio	3		Ejecucion de software malicioso -- Servidores	Ejecucion de software malicioso -- Servidores de	Ataque aplicaciones -- Sistemas SCADA || Ataque	
Bajo	2		software malicioso -- Servidor filtrado	software malicioso -- Equipos	software malicioso -- ERP: JDEdwards	
Menor	1		Coordinador de TI || Negligencia -- Administrador de			de procesamiento de datos principal || Incendio -- Centro

Tabla 21. Matriz Riesgos

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Bajo	1.716738197	12
Medio	13.018598	91
Medio-Alto	54.50643777	381
Altos	30.75822604	215

Tabla 22. Distribución Porcentual

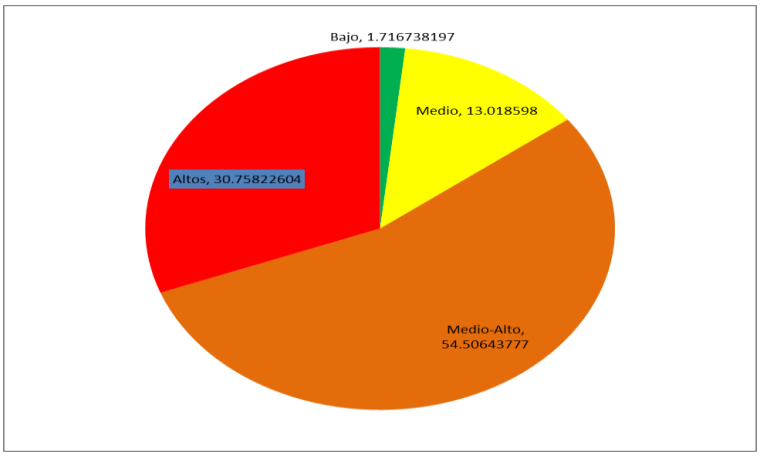


Ilustración 9. Distribucion porcentual

De acuerdo a los criterios de aceptación Los riesgos inaceptables que requieren tratamiento son:

- Robo de información
- Ataque de infraestructura
- Acceso no autorizado
- Copia no autorizada
- Borrado y alteración
- Solo un especialista
- Robo de equipos
- Pérdida de capacidad de servidores
- Ataque a aplicaciones –Sistemas SCADA
- Falta de sistema de parches-ERP-JDEdwars
- Incapacidad de servidores
- Falta de software control de versiones
- Ejecución de software malicioso
- Falta de alcances claros
- Inundación
- Terremoto
- Incendio
- Terrorismo
- Líder inexperto
- Retiro Personal

Para ver más detalle de los cálculos utilizados en la matriz de riesgos. Ver anexo: MatrizRiesgos.xlsx.

4.1 PLAN DE TRATAMIENTO DEL RIESGO

Una vez establecidos los niveles de riesgo para los diferentes activos, se debe establecer las medidas de protección, salvaguardas o contramedidas que se deben implementar para cada uno de los activos en función del impacto que pueda representar la materialización de la amenaza.

RIESGOS ALTOS	TRATAMIENTO				Plan de monitoreo	Responsable	Resultado Esperado
	Aceptarlo	Evitarlo	Mitigarlo	Transferirlo			
Acceso no autorizado		x			Diario - reportes vía mail de aplicativo gobierno de datos/Revisión de reporte alogin auditing motor de Base de datos/ Mensajes de correo, logs- configurados desde dispositivos/reportes vía mail política GPO mayor de intentos permitidos	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Ataque aplicaciones		x			Diario- Reportes vía mail de software de endpoint políticas de intrusión prevención	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Ataque infraestructura		x			Diario-mensaje de correo con logs de acceso y reporte de logs de IPS/Reportes vía mail de software de endpoint políticas de intrusión prevención/	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Falta de alcances claros		x			Documentación asociada a la Metodología y buenas prácticas en el desarrollo de software	Jefe de división informática	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Borrado y alteración		x			Diario - reportes vía mail de aplicativo gobierno de datos, Revisión de reporte alogin auditing motor de Base de datos	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Copia no autorizada		x			Diario- Reportes vía mail de software de endpoint políticas de intrusión prevención, reporte de control de periféricos de endpoint, reporte de políticas NAC	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad

					para equipos		
Robo de información		**x**			Diario- Reportes vía mail de software de endpoint políticas de intrusión prevención, reporte de control de periféricos de endpoint, reporte de políticas NAC para equipos, software IPS	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Falta de sistema de parches		**x**			semanal- Revisión y viabilidad de instalación de Actualizaciones y parches para instalar desde el WSUS/Mensual- Revisión y viabilidad de instalación de las actualizaciones de firmware en el fabricante /semanal reportes de actualización de otros software diferentes a Microsoft	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Incendio			**x**		Semestral- Evaluación al modelo de la ARP implementado, Mensual- evaluación al proceso de respaldo externo y ubicación externa	Jefe de división de recursos humanos	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Inundación			**x**		Semestral- Evaluación al modelo de la ARP implementado, Mensual- evaluación al proceso de respaldo externo y ubicación externa	Jefe de división de recursos humanos	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Líder inexperto		**x**			Cuando aplique cierre de proyecto- Evaluación al proyecto, Semestral - Evaluaciones de desempeño	Jefe de división informática	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Ejecución software malicioso		**x**			Diario- Reportes vía mail de software de endpoint amenazas recientes y logs de acciones tomadas	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Pérdida de capacidad de servidores		**x**			Diario- Reportes de estado de espacio de aplicativo supervisor de redes/Diario- reporte de operador después de chequeo de alarmas por espacio de menos de un 10%	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad

Retiro personal			x		Anual- auditoria interna en cuanto al proceso de bienestar y garantías del empleado	Jefe de división de recursos humanos	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Robo de equipos			x		Anual-auditoria interna evaluar estado de pólizas, mensual-Revisión reportes de accesos físicos al centro de cómputo, Mensual-Revisión de reporte de monitoreo de cámaras de vigilancia, Mensual- Revisión de las formas de prestación de llaves de racks y responsables	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Solo un especialista		x			Anual- auditoria interna al proceso de funciones y matriz de remplazos	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Terremoto			x		Semestral- Evaluación al modelo de la ARP implementado, Mensual- evaluación al proceso de respaldo externo y ubicación externa	Jefe de división de recursos humanos	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Terrorismo			x		Semestral- Evaluación al modelo de la ARP implementado, Mensual- evaluación al proceso de respaldo externo y ubicación externa	Jefe de división de recursos humanos	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
incapacidad de servidores		x			Semanal-Reporte de espacios en discos y estado de salud de los servidores	Coordinador de TI	Reducirlo a medio disminuyendo el impacto y/o la probabilidad
Falta de software control de versiones		x			Documentación asociada a la Metodología y buenas prácticas en el desarrollo de software	Jefes de departamento de soluciones planta y administrativa	Reducirlo a medio disminuyendo el impacto y/o la probabilidad

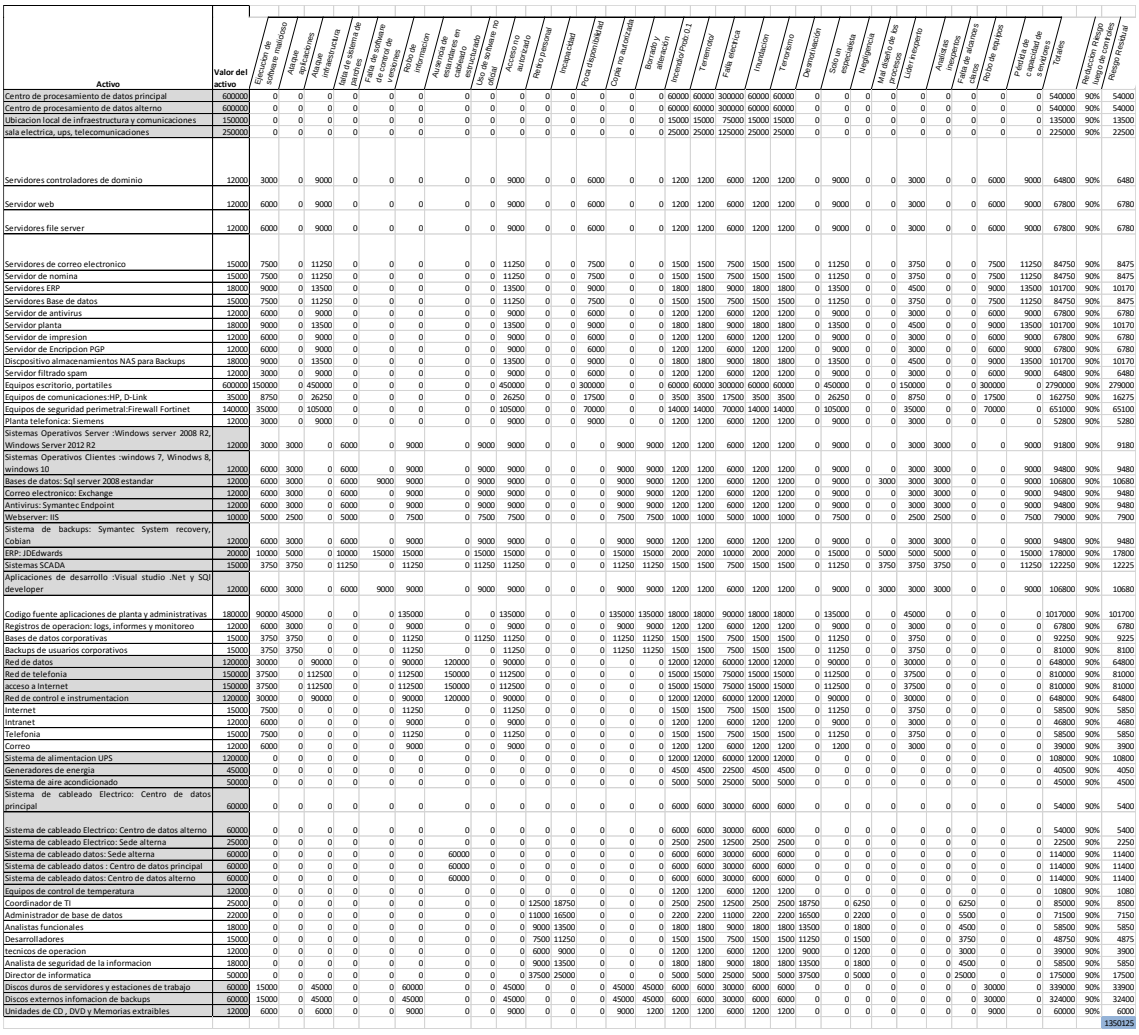
Tabla 23. Tratamiento al Riesgo

4.2 RIESGO RESIDUAL

EL riesgo residual, que son los riesgos remanentes que existes tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información, para ello la organización determina que la aplicación del mejor o mejores controles para mitigar un riesgo aporta una

disminución del mismo en un 90% en promedio, el valor restante deberá ser asumido por la organización en cada uno de los activos.
A continuación se anexa la tabla de los activos con los valores calculados de los riesgos y las amenazas y una columna en donde se calcula el porcentaje de reducción de los riesgos, el valor calculado nos da el riesgo residual por activo sobre el cual la organización deberá tomar las decisiones del caso.

Para calcular el Riesgo Residual se multiplica el valor del activo por la probabilidad.



Activo	Valor del activo	Ejecución de software malicioso	Ataque aplicaciones	Ataque infraestructura	Daño al sistema de jerarquía	Falla de software de control de versiones	Robo de información	Ausencia de estándares en cableado estructurado	Uso de software no oficial	Acceso no autorizado	Retiro personal	Incidentalidad	Pérdida disponibilidad	Copia no autorizada	Eliminación y alteración	Incendio/Pote.0.21	Terremoto	Falla eléctrica	Inundación	Terrorismo	Deshumedación	Sólo un especialista	Negligencia	Mal diseño de los procesos	Lider irresponsable	Ausencia incidentes	Falta de alarmas claras	Robo de equipos	Pérdida de capacidad de servidores	Totales	Reducción Riesgo Mayor control es	Riesgo Residual
Centro de procesamiento de datos principal	600000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	60000	60000	300000	60000	60000	0	0	0	0	0	0	0	0	0	540000	90%	54000
Centro de procesamiento de datos alterno	600000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	60000	60000	300000	60000	60000	0	0	0	0	0	0	0	0	0	540000	90%	54000
Ubicacion local de infraestructura y comunicaciones	150000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	15000	15000	75000	15000	15000	0	0	0	0	0	0	0	0	0	135000	90%	13500
sala electrica, ups, telecomunicaciones	250000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	25000	25000	125000	25000	25000	0	0	0	0	0	0	0	0	0	225000	90%	22500
Servidores controladores de dominio	12000	3000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	64800	90%	6480
Servidor web	12000	6000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	67800	90%	6780
Servidores file server	12000	6000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	67800	90%	6780
Servidores de correo electronico	15000	7500	0	11250	0	0	0	0	0	11250	0	0	7500	0	0	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	7500	11250	84750	90%	8475
Servidor de nomina	15000	7500	0	11250	0	0	0	0	0	11250	0	0	7500	0	0	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	7500	11250	84750	90%	8475
Servidores ERP	18000	9000	0	13500	0	0	0	0	0	13500	0	0	9000	0	0	1800	1800	9000	1800	1800	0	13500	0	0	4500	0	0	9000	13500	101700	90%	10170
Servidores Base de datos	15000	7500	0	11250	0	0	0	0	0	11250	0	0	7500	0	0	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	7500	11250	84750	90%	8475
Servidor de antivirus	12000	6000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	67800	90%	6780
Servidor planta	18000	9000	0	13500	0	0	0	0	0	13500	0	0	9000	0	0	1800	1800	9000	1800	1800	0	13500	0	0	4500	0	0	9000	13500	101700	90%	10170
Servidor de impresion	12000	6000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	67800	90%	6780
Servidor de Encripcion PGP	12000	6000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	67800	90%	6780
Discpositivo almacenamientos NAS para Backups	18000	9000	0	13500	0	0	0	0	0	13500	0	0	9000	0	0	1800	1800	9000	1800	1800	0	13500	0	0	4500	0	0	9000	13500	101700	90%	10170
Servidor filtrado spam	12000	3000	0	9000	0	0	0	0	0	9000	0	0	6000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	6000	9000	64800	90%	6480
Equipos escritorio, portatiles	600000	150000	0	450000	0	0	0	0	0	450000	0	0	300000	0	0	60000	60000	300000	60000	60000	0	450000	0	0	150000	0	0	300000	0	2790000	90%	279000
Equipos de comunicaciones:HP, D-Link	35000	8750	0	26250	0	0	0	0	0	26250	0	0	17500	0	0	3500	3500	17500	3500	3500	0	26250	0	0	8750	0	0	17500	0	162750	90%	16275
Equipos de seguridad perimetral:Firewall Fortinet	140000	35000	0	105000	0	0	0	0	0	105000	0	0	70000	0	0	14000	14000	70000	14000	14000	0	105000	0	0	35000	0	0	70000	0	651000	90%	65100
Planta telefonica: Siemens	12000	3000	0	9000	0	0	0	0	0	9000	0	0	9000	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	0	0	52800	90%	5280
Sistemas Operativos Server :Windows server 2008 R2, Windows Server 2012 R2	12000	3000	3000	0	6000	0	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	0	3000	3000	0	0	9000	91800	90%	9180
Sistemas Operativos Clientes :windows 7, Winodws 8, windows 10	12000	6000	3000	0	6000	0	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	0	3000	3000	0	0	9000	94800	90%	9480
Bases de datos: Sql server 2008 estandar	12000	6000	3000	0	6000	9000	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	3000	3000	3000	0	0	9000	106800	90%	10680
Correo electronico: Exchange	12000	6000	3000	0	6000	0	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	0	3000	3000	0	0	9000	94800	90%	9480
Antivirus: Symantec Endpoint	12000	6000	3000	0	6000	0	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	0	3000	3000	0	0	9000	94800	90%	9480
Webserver: IIS	10000	5000	2500	0	5000	0	7500	0	7500	7500	0	0	0	7500	7500	1000	1000	5000	1000	1000	0	7500	0	0	2500	2500	0	0	7500	79000	90%	7900
Sistema de backups: Symantec System recovery, Cobian	12000	6000	3000	0	6000	0	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	0	3000	3000	0	0	9000	94800	90%	9480
ERP: JDEdwards	20000	10000	5000	0	10000	15000	15000	0	15000	15000	0	0	0	15000	15000	2000	2000	10000	2000	2000	0	15000	0	5000	5000	5000	0	0	15000	178000	90%	17800
Sistemas SCADA	15000	3750	3750	0	11250	0	11250	0	11250	11250	0	0	0	11250	11250	1500	1500	7500	1500	1500	0	11250	0	3750	3750	3750	0	0	11250	122250	90%	12225
Aplicaciones de desarrollo :Visual studio .Net y SQJ developer	12000	6000	3000	0	6000	9000	9000	0	9000	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	3000	3000	3000	0	0	9000	106800	90%	10680
Codigo fuente aplicaciones de planta y administrativas	180000	90000	45000	0	0	0	135000	0	0	135000	0	0	0	135000	135000	18000	18000	90000	18000	18000	0	135000	0	0	45000	0	0	0	0	1017000	90%	101700
Registros de operacion: logs, informes y monitoreo	12000	6000	3000	0	0	0	9000	0	0	9000	0	0	0	9000	9000	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	0	0	67800	90%	6780
Bases de datos corporativas	15000	3750	3750	0	0	0	11250	0	11250	11250	0	0	0	11250	11250	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	0	0	92250	90%	9225
Backups de usuarios corporativos	15000	3750	3750	0	0	0	11250	0	0	11250	0	0	0	11250	11250	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	0	0	81000	90%	8100
Red de datos	120000	30000	0	90000	0	0	90000	120000	0	90000	0	0	0	0	0	12000	12000	60000	12000	12000	0	90000	0	0	30000	0	0	0	0	648000	90%	64800
Red de telefonia	150000	37500	0	112500	0	0	112500	150000	0	112500	0	0	0	0	0	15000	15000	75000	15000	15000	0	112500	0	0	37500	0	0	0	0	810000	90%	81000
acceso a Internet	150000	37500	0	112500	0	0	112500	150000	0	112500	0	0	0	0	0	15000	15000	75000	15000	15000	0	112500	0	0	37500	0	0	0	0	810000	90%	81000
Red de control e instrumentacion	120000	30000	0	90000	0	0	90000	120000	0	90000	0	0	0	0	0	12000	12000	60000	12000	12000	0	90000	0	0	30000	0	0	0	0	648000	90%	64800
Internet	15000	7500	0	0	0	0	11250	0	0	11250	0	0	0	0	0	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	0	0	58500	90%	5850
Intranet	12000	6000	0	0	0	0	9000	0	0	9000	0	0	0	0	0	1200	1200	6000	1200	1200	0	9000	0	0	3000	0	0	0	0	46800	90%	4680
Telefonia	15000	7500	0	0	0	0	11250	0	0	11250	0	0	0	0	0	1500	1500	7500	1500	1500	0	11250	0	0	3750	0	0	0	0	58500	90%	5850
Correo	12000	6000	0	0	0	0	9000	0	0	9000	0	0	0	0	0	1200	1200	6000	1200	1200	0	1200	0	0	3000	0	0	0	0	39000	90%	3900
Sistema de alimentacion UPS	120000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12000	12000	60000	12000	12000	0	0	0	0	0	0	0	0	0	108000	90%	10800
Generadores de energia	45000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4500	4500	22500	4500	4500	0	0	0	0	0	0	0	0	0	40500	90%	4050
Sistema de aire acondicionado	50000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5000	5000	25000	5000	5000	0	0	0	0	0	0	0	0	0	45000	90%	4500
Sistema de cableado Electrico: Centro de datos principal	60000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	0	0	54000	90%	5400
Sistema de cableado Electrico: Centro de datos alterno	60000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	0	0	54000	90%	5400
Sistema de cableado Electrico: Sede alterna	25000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2500	2500	12500	2500	2500	0	0	0	0	0	0	0	0	0	22500	90%	2250
Sistema de cableado datos: Sede alterna	60000	0	0	0	0	0	0	60000	0	0	0	0	0	0	0	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	0	0	114000	90%	11400
Sistema de cableado datos : Centro de datos principal	60000	0	0	0	0	0	0	60000	0	0	0	0	0	0	0	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	0	0	114000	90%	11400
Sistema de cableado datos: Centro de datos alterno	60000	0	0	0	0	0	0	60000	0	0	0	0	0	0	0	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	0	0	114000	90%	11400
Equipos de control de temperatura	12000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1200	1200	6000	1200	1200	0	0	0	0	0	0	0	0	0	10800	90%	1080
Coordinador de TI	25000	0	0	0	0	0	0	0	0	0	12500	18750	0	0	0	2500	2500	12500	2500	2500	18750	0	6250	0	0	0	6250	0	0	85000	90%	8500
Administrador de base de datos	22000	0	0	0	0	0	0	0	0	0	11000	16500	0	0	0	2200	2200	11000	2200	2200	16500	0	2200	0	0	0	5500	0	0	71500	90%	7150
Analistas funcionales	18000	0	0	0	0	0	0	0	0	0	9000	13500	0	0	0	1800	1800	9000	1800	1800	13500	0	1800	0	0	0	4500	0	0	58500	90%	5850
Desarrolladores	15000	0	0	0	0	0	0	0	0	0	7500	11250	0	0	0	1500	1500	7500	1500	1500	11250	0	1500	0	0	0	3750	0	0	48750	90%	4875
tecnicos de operacion	12000	0	0	0	0	0	0	0	0	0	6000	9000	0	0	0	1200	1200	6000	1200	1200	9000	0	1200	0	0	0	3000	0	0	39000	90%	3900
Analista de seguridad de la informacion	18000	0	0	0	0	0	0	0	0	0	9000	13500	0	0	0	1800	1800	9000	1800	1800	13500	0	1800	0	0	0	4500	0	0	58500	90%	5850
Director de informatica	50000	0	0	0	0	0	0	0	0	0	37500	25000	0	0	0	5000	5000	25000	5000	5000	37500	0	5000	0	0	0	25000	0	0	175000	90%	17500
Discos duros de servidores y estaciones de trabajo	60000	15000	0	45000	0	0	60000	0	0	45000	0	0	0	45000	45000	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	30000	0	339000	90%	33900
Discos externos infomacion de backups	60000	15000	0	45000	0	0	45000	0	0	45000	0	0	0	45000	45000	6000	6000	30000	6000	6000	0	0	0	0	0	0	0	30000	0	324000	90%	32400
Unidades de CD , DVD y Memorias extraibles	12000	6000	0	6000	0	0	9000	0	0	9000	0	0	0	9000	1200	1200	1200	6000	1200	1200	0	0	0	0	0	0	0	9000	0	60000	90%	6000
																																135012

Ilustración 10. Calculo de Riesgo Residual

Ver Anexo: Calculo Riesgo Residual.xlsx

4.3 PLANTEAMIENTO DE PROYECTOS

El objetivo de esta fase es plantear y detallar los proyectos a realizar para implementar las salvaguardas identificadas en el análisis de riesgos, basado en

el objetivo establecido de los controles de la norma, en nuestro caso tocaría los numerales:

- Numeral 5. Políticas de seguridad de la información.
- Numeral 6. Organización de la información.
- Numeral 7. Seguridad Ligada a los Recursos Humanos.
- Numeral 8. Gestión de Activos.
- Numeral 9. Control de Acceso.
- Numeral 10. Criptografía.
- Numeral 12. Seguridad en las operaciones.
- Numeral 13. Seguridad de las comunicaciones.
- Numeral 14. Adquisición, desarrollo y mantenimiento de sistemas de información.
- Numeral 15. Relación con proveedores.
- Numeral 16. Gestión de Incidentes de Seguridad.
- Numeral 17. Gestión continuidad del negocio.
- Numeral 18. Cumplimiento.

Los proyectos más significativos serían los siguientes:

- Proyecto Políticas de seguridad de la información.
- Proyecto Monitoreo SGSI.
- Proyecto Contratación legalidad.
- Proyecto control de acceso y seguridad física.
- Proyecto servicios de plataforma.
- Proyecto Desarrollo del software.
- Proyecto Clasificación/Gestión de Activos.
- Proyecto continuidad del negocio.
- Proyecto Análisis de Riesgos.
- Proyecto Criptografía.

Para cada uno de estos proyectos se deben cumplir básicamente los siguientes pasos:

- Investigación y selección de soluciones y/o herramientas

En este punto el personal del área de tecnología y en particular del área de seguridad informática se deben encargar de buscar soluciones y/o herramientas cuyas funciones cumplan con el propósito identificado, para ello se utilizan los reportes de Gartner o sitios web de evaluación de productos como guías y luego de identificar mínimo tres candidatos, se analizan en detalle y se generan cuadros comparativos con las principales características, incluyendo el valor comercial de las mismas.

- Pruebas de concepto de las soluciones y/o herramientas

  La realización de pruebas de concepto con las soluciones, implica de las soluciones y/o herramientas previamente identificadas, se contacta con los proveedores (dos o tres) y se solicita una prueba de concepto de la herramienta con el fin de evaluar de manera práctica su funcionalidad, apoyados en estas pruebas se termina el cuadro comparativo de las soluciones y se selecciona el producto /o herramienta más adecuado para cubrir la necesidad identificada.

- Elección de solución y/o herramienta

  Basados en la tabla comparativa de solución y/o herramientas la dirección de infraestructura selecciona la herramienta más adecuada basados en la relación costo / beneficio, genera una solicitud de compra de la misma, la presentación en primera instancia se le envía al jefe de la división del área justificando la necesidad de la misma.

- Proceso de Compra

  Si la aplicación es aprobada, se sube al sistema de compras en donde cursa los niveles de aprobación necesarios (incluyendo la vicepresidencia si la inversión es considerable) para que el departamento de compras finalmente emita correo con la solicitud de compra final al proveedor.

- Implementación de la Solución y/o producto comprado

  Una vez el producto y/o solución se compra, se formaliza con el proveedor un plan de trabajo para llevar a cabo la implementación del mismo, con el plan de trabajo se separan los recursos necesarios para acompañar al proveedor en la implementación y en cualquier caso se debe exigir unas actas de seguimiento del cronograma planteado.

- Estabilización de la Solución

  Luego de la fase de implementación sigue una fase de estabilización de la solución y/o producto, en donde se hace seguimiento junto con el proveedor del comportamiento del mismo y se hacen los ajustes necesarios para que su funcionamiento sea lo esperado por la organización, para el caso de los proyectos de tecnología además de

esta fase se debe incluir los procesos propios de administración y monitoreo de la solución.

4.4 PROYECTOS

Proyecto identificado	Riesgo
Políticas seguridad de la información	Robo de información, ataques de aplicaciones, ataques de infraestructura, falta de alcances claros, borrado y alteración, robo de equipos, copia no autorizada.
Monitoreo SGSI	Robo de información, falta sistema de parches, Ejecución software malicioso, pérdida de capacidad servidores, incapacidad de servidores, Ataque de aplicaciones, Ataque de infraestructura
Contratación legalidad	Robo de información, Retiro personal, líder inexperto, falta de alcances claros
Control de acceso y seguridad física	Copia no autorizada, robo de información, robo de equipos, ejecución software malicioso, borrado y alteración, ataque de infraestructura, ataque de aplicaciones, acceso no autorizado
Servicios de plataforma	Robo de información, ataque de infraestructura, ataque de aplicaciones, ejecución software malicioso, falta sistema de parches, incapacidad de servidores, pérdida de capacidad de servidores
Desarrollo de software	Ataque aplicaciones, falta de alcances claros, falta sistema de parches, solo un especialista, falta de control de versiones de software, líder inexperto
Clasificación / Gestión Activos	Robo de información, robo de equipos, incapacidad de servidores, robo de equipos, acceso no autorizado, ataque de infraestructura
Continuidad de negocio	Incendio, inundación, terremoto, terrorismo, ataque de infraestructura, borrado y alteración, robo de equipos, robo de información, acceso no autorizado
Análisis de riesgos	Ejecución de software malicioso, incapacidad de servidores, solo un especialista, líder inexperto, robo de equipos, robo de información
Criptografía	Acceso no autorizado, ataque de aplicaciones, borrado y alteración, copia no autorizada, robo de información.

Tabla 24. Proyectos

4.4.1 Proyecto Políticas de seguridad de la información

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a políticas de seguridad de la información.
Creando nuevas políticas necesarias que permitan fortalecer el sistema de información.
Modificando políticas existentes de manera que sean claras y abarquen el contenido necesario que permita a la organización crear un sistema de gestión de la información conforme a estándares y leyes.

Objetivo General

Actualizar el documento actual de políticas de seguridad de la información de Textilera S.A estableciendo controles y métodos de divulgación.

Objetivos Específicos

- Definir políticas de seguridad de acuerdo al análisis de la norma ISO 27001:2013 y Establecerlas en el documento políticas de seguridad de la información de Textilera S.A.
- Establecer controles de seguridad con el fin de velar el cumplimiento de las políticas de seguridad establecidas en el documento “políticas de seguridad de la información”.
- Establecer metodologías y estrategias de divulgación de las políticas de seguridad para que todas las personas que tengan acceso a la información la conozcan.
- Elaborar un plan de monitoreo para la revisión periódica de las políticas de seguridad de la información.

Para ver el detalle de la carta del proyecto:
Ver anexo: *ProyectoPoliticasSeguridad.docx*

4.4.2 Proyecto Monitoreo SGSI

Este proyecto pretende analizar los procesos actuales de revisión que se realizan al sistema de gestión de seguridad de la información identificando las falencias, sugiriendo nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013.

Objetivo General

Fortalecer dentro del sistema de gestión de la información los controles y procedimientos orientados a la revisión y monitoreo de los procesos y sistemas sensibles orientados al cumplimiento de la norma ISO 27001:2013

Objetivos Específicos

- Crear una “definición de cargo” para el responsable del Sistema de Gestión de seguridad de la información.
- Crear un proceso que apunte al manejo adecuado de recolección de evidencia informática forense.
- Crear un procedimiento que permita evaluar y hacer seguimiento a los proveedores relacionados con el sistema de gestión de seguridad de la información.
- Clasificar dentro del sistema de manejo de incidentes los directamente relacionados a seguridad de la información.
- Actualizar y complementar los procedimientos relacionados con las revisiones de seguridad de manera que involucren responsables, periodicidad, rutas de ubicación.
- Almacenar en los procesos de monitoreo las evidencias y registros de las actividades relacionadas al sistema de gestión de seguridad de la información.
- Establecer una directriz para cada uno de los procesos de monitoreo actuales en los servicios del sistema de información de manera que se defina un tiempo de monitoreo.
- Establecer un procedimiento para el control de cambios en equipos y servicios de plataforma.
- Crear una estrategia de comunicación y divulgación orientada hacia los proveedores de manera que tengan conocimiento del manejo de incidentes, como reportarlos, seguimiento y planes de acción.
- Crear un procedimiento que centralice las actividades de auditoria a todo el sistema de gestión de seguridad de la información.

Para ver el detalle de la carta del proyecto:
Ver anexo: ProyectoMonitoreoSGSI.docx

4.4.3 Proyecto Contratación legalidad

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a contratación y aspectos legales que den cumplimiento a lo que se recomienda en un sistema de gestión de seguridad de la información.
Fortaleciendo procesos ya existentes, creando nuevos y apoyándose en controles que puedan responder a un ciclo de creación, implementación, sensibilización y revisión.

Objetivo General

Incorporar dentro del esquema legal de la compañía los procesos legales conforme a la norma ISO 27001:2013 y las leyes colombianas que apliquen al manejo de la información.

Objetivos Específicos

- Incorporar dentro de las clausulas existentes de confidencialidad el tiempo de retención, el manejo adecuado y normalización de la información al finalizar un contrato ya sea a empleados, proveedores o contratistas.
- Incorporar en contratos con proveedores, contratistas las formas de tratamiento, retención y trasmisión de la información.
- Incorporar dentro del reglamento o convención colectiva de la compañía leyes aplicables en tema de seguridad de la información y las sanciones conforme a la norma.
- Clasificar la información conforme a ley colombiana del tratamiento y protección de datos.

Para ver el detalle de la carta del proyecto:

Ver Anexo: ProyectoContratacionLegalidad.docx

4.4.4 Proyecto control de acceso y seguridad física

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos y controles de la organización existentes orientados hacia los controles de acceso y seguridades físicas establecidas en el manejo de activos y sistemas de información

Objetivo general

Fortalecer y documentar los procesos que intervienen en las actividades de seguridad física y control de acceso a los sistemas de información.

Objetivos Específicos

- Crear y documentar un proceso centralizado que haga referencia a los procesos de revisión de seguridad actuales en plataforma ya que existe mucha información dispersa.
- Actualizar los procedimientos que hacen referencia al tratamiento de seguridad de la información para usuarios nuevos en su ingreso y para los retiros de empleados o contratistas de la compañía.
- Centralizar y definir para las diferentes formas y plantillas que se manejan actualmente en el manejo de seguridades del sistema de información responsables, periodicidad de actualización y hacerlos parte del proceso.

- Crear un procedimiento que permita realizar una trazabilidad del usuario en cuanto a las seguridades de acceso en los diferentes programas y servicios de los sistemas de información.
- Definir los tipos de acceso a la información según los perfiles.
- Complementar y estandarizar los procesos existentes que hacen referencia a las tareas de monitoreo actuales.
- Incorporar en la metodología de desarrollo de software las buenas prácticas en cuanto a los registros que se deben tener para cambios en el código, las seguridades de los usuarios, las ubicaciones y protección de los contenedores o sitios donde se depositan los fuentes y bases de conocimiento de cada software.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoControlAccesoySeguridaFisica.docx

4.4.5 Proyecto servicios de plataforma

Este proyecto pretende analizar los procesos actuales de plataforma y definir las necesidades conforme a la norma ISO 27001:2013 enfocados al cumplimiento y creación de controles.

Objetivo General

Fortalecer dentro del proceso de plataforma los controles y procedimientos ya existentes y crear los necesarios orientados al cumplimiento de la norma ISO 27001:2013

Objetivos Específicos

- Registrar los procesos de mantenimiento de todos los equipos que intervienen en la continuidad de los servicios de plataforma.
- Adecuar el sistema de cableado estructurado con las protecciones y estándares adecuados.
- Establecer los lineamientos técnicos en el proceso de eliminación segura de activos de información.
- Actualizar los procedimientos actuales y crear los que hagan falta en cuanto a la operación de la información, comunicaciones, revisión de seguridades y procesos de respaldo que se requieran.
- Fortalecer los controles de descarga e instalación de aplicativos desde medios extraíbles en especial a áreas administrativas.

- Incorporar las buenas prácticas que recomienda la norma en cuanto a la programación de pruebas de hacking ético a los servicios o aplicaciones que sean foco de atacantes.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoServiciosPlataforma.docx

4.4.6 Proyecto Desarrollo del software

Este proyecto pretende analizar los procesos actuales de desarrollo de software en el sistema de gestión de seguridad de la información que se aplican, identificando las falencias, sugiriendo nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013.

Objetivo General

Fortalecer dentro del sistema de gestión de la información los controles y procedimientos ya existentes en el proceso de desarrollo de software además de proponer la creación de nuevos que contribuyan al cumplimiento de la norma ISO 27001:2013.

Objetivos Específicos

- Definir dentro de la metodología actual de desarrollo de software el manejo y control de versiones además de implementar los controles de cambios.
- Definir y documentar dentro de la etapa de desarrollo como se realiza el desarrollo de las aplicaciones, las metodologías que se utilizan y las buenas practicas.
- Evidenciar en el proceso de desarrollo de software los seguimientos que se realizan en cuanto a los controles de calidad.
- Establecer la metodología de proyecto de desarrollo de software como un estándar para ambos departamentos soluciones administrativas y planta.
- Oficializar los formatos y registros existentes en el proceso de desarrollo de software relacionados al tema de seguridad que apliquen como un aporte de valor al sistema de gestión de seguridad de la información.
- Implementar una metodología de revisión de código indispensable en la calidad.
- Implementar y documentar una metodología de desarrollo seguro.

- Implementar dentro de la metodología el análisis de riesgos en el desarrollo de aplicaciones.
- Incorporar dentro del proceso de pruebas funcionales, pruebas de seguridad a las aplicaciones.
- Establecer y documentar un proceso dentro de la metodología de desarrollo de software que involucre la intervención del departamento de plataforma y se compacte el proceso.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoDesarrolloSoftware.docx

4.4.7 Proyecto Clasificación/Gestión de Activos

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a la clasificación y el manejo de activos en un sistema de gestión de seguridad de la información.
Fortaleciendo procesos ya existentes, creando nuevos y apoyándose en controles que puedan responder a un ciclo de clasificación, diferenciación, uso, dar de baja delos activos informáticos de la compañía.

Objetivo General

Fortalecer el proceso de identificación, clasificación y cuidados especiales de activos de información más relevantes de la compañía conforme al ciclo de vida del mismo.

Objetivos Específicos

- Documentar el proceso del retiro del personal de la compañía.
- Documentar el proceso de inventario de activos de información para contratistas dentro de la compañía.
- Emitir un documento de responsabilidad frente a los activos de información que se le entregan a cada empleado.
- Clasificar la información con marcas respectivas que permitan diferenciar entre información entre privada, pública, sensible.
- Crear y documentar el proceso de eliminación segura de activos de información.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoClasificacionGestion Activos.docx

4.4.8 Proyecto continuidad del negocio

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto al

modelo de continuidad de negocio analizando los procesos más críticos que se involucran en el soporte a la cadena de valor y a los sistemas.

Objetivo General

Implementar un modelo de continuidad de negocio que involucre los procesos críticos de la compañía y asegure frente a un evento externo o interno el sostenimiento de la misma.

Objetivos Específicos

- Integrar un proceso para las copias de seguridad en el sistema de información.
- Actualizar y complementar los actuales procedimientos que hacen referencia al proceso de continuidad del negocio.
- Crear un procedimiento que reúna toda la esfera de seguridad aplicada al sistema de gestión de seguridad de la información.
- Crear un comité de seguridad que vele por el cumplimiento y continuidad de los procesos.
- Documentar el plan y periodicidad de simulacros que se realizan para los servidores críticos.
- Registrar los resultados de los simulacros establecidos y sus planes de acción correspondientes.
- Documentar el plan de continuidad de negocio de los servidores redundantes y el tiempo de activación en caso de incidentes.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoContuinidadNegocio.docx

4.4.9 Proyecto Análisis de Riesgos

Este proyecto pretende analizar los procesos actuales orientados a las revisiones de vulnerabilidades al sistema de gestión de seguridad de la información identificando falencias, sugiriendo la creación de nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013.

Objetivo General

Analizar y documentar dentro del sistema de gestión de seguridad de la información los riesgos que afectan los activos de información con el fin de identificar amenazas, vulnerabilidades y fuentes y con estas generar salvaguardas y contingencias que ayuden a disminuir el impacto y la probabilidad de los mismos para dar cumplimiento de la norma ISO 27001:2013.

Objetivos Específicos

- Crear una matriz de riesgos para el sistema de gestión de seguridad de la información.
- Documentar el proceso de chequeo de vulnerabilidades que se lleva a cabo de manera periódica para los servidores.
- Actualizar los procesos actuales de seguridad que involucran tareas de revisión y pruebas de vulnerabilidades.
- Establecer un proceso y documentarlo del chequeo de vulnerabilidades orientado a los dispositivos de redes y comunicaciones.
- Establecer, implementar y documentar un proceso de revisión de vulnerabilidades para los equipos de usuarios.
- Identificar las amenazas y vulnerabilidades que puedan afectar a todos los activos de información dela compañía.
- Establecer y documentar controles para mitigar los riesgos identificados.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoAnalisisRiesgos.docx

4.4.10 Proyecto Criptografía

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a la necesidad de cifrar canales e información en los procesos más críticos de la compañía.

Objetivo General

Establecer dentro de los servicios controles criptográficos para los sistemas de información y activos de información que lo requieran.

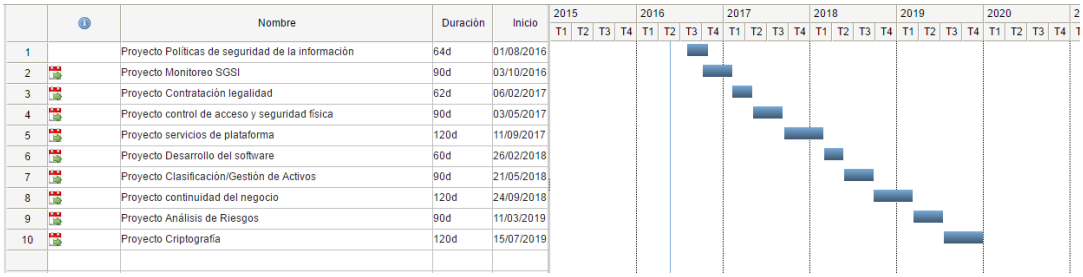
Objetivos Específicos

- Establecer metodologías o canales encriptados para el servicio de correo electrónico.
- Establecer una política de seguridad adecuada para el servicio actual de mensajería instantánea y la información que se maneja.

- Establecer códigos criptográficos, certificados, firmas digitales en las aplicaciones desarrolladas que manejan y trasmiten información sensible.
- Identificar los activos de información que requieran controles criptográficos y ampliarlos a que sean aplicables al proceso existente.

Para ver el detalle de la carta del proyecto:
Ver Anexo: ProyectoCriptografia.docx

A continuación, se detallan los proyectos de la organización, expresados mediante un diagrama de Gantt, para complementar la información presentada de cada proyecto.
La estimación de tiempos se realiza teniendo en cuenta las limitaciones de recursos en cuanto al personal responsable y que la mayoría deben participar en todos los proyectos.



	Nombre	Duración	Inicio
1	Proyecto Políticas de seguridad de la información	64d	01/08/2016
2	Proyecto Monitoreo SGSI	90d	03/10/2016
3	Proyecto Contratación legalidad	62d	06/02/2017
4	Proyecto control de acceso y seguridad física	90d	03/05/2017
5	Proyecto servicios de plataforma	120d	11/09/2017
6	Proyecto Desarrollo del software	60d	26/02/2018
7	Proyecto Clasificación/Gestión de Activos	90d	21/05/2018
8	Proyecto continuidad del negocio	120d	24/09/2018
9	Proyecto Análisis de Riesgos	90d	11/03/2019
10	Proyecto Criptografía	120d	15/07/2019

Ver anexo: Proyectos SGSI.pdf

FASE 5: AUDITORIA DE CUMPLIMIENTO

5.1 INTRODUCCIÓN

La presente sección registra un GAP_Anlysis(análisis de brecha) de seguridad para textilera S.A el cual consiste en identificar el nivel de eficiencia y eficacia de los controles existentes en la organización para proteger la integridad, confidencialidad y disponibilidad de sus activos de información.

5.2 METODOLOGÍA

Para ejecutar la auditoria de cumplimiento, se usará el modelo de madurez de la capacidad (CMM) como metodología para el análisis del grado de madurez en la implementación del SGSI (Sistema de Gestión De Seguridad de la Información) en la implementación de la norma ISO 27002:2013, que agrupa un total de 114 controles sobre las recomendaciones de buenas prácticas para la Gestión de la Seguridad de la Información que está organizado en 14 dominios y que cuenta con 35 objetivos de control.

Como base de Conocimiento para el análisis se tomaran las valoraciones siguientes:

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible No se ha reconocido siquiera que existe un problema a resolver
10%	L1	Inicial /Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoria de veces en el esfuerzo personal Los procesos son inexistentes o localizadaos en áreas concretas. No existen plantillas definidas a nivel corporativo
50%	L2	Repetible pero Intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al metodo No hay comunicación o entrenamiento Formal, las responsabilidades quedan a cargo de cada individuo Se depende del grado de conocimiento de cada individuo
90%	L3	Proceso Definido	La organización entera participa en el proceso Los procesos estan implantados, documentados y comunicados mediante entrenamiento
95%	L4	Gestionado y Medible	Se puede seguir con indicadores númericos y estadisticos la evolución de los procesos Se dispone de tecnología para automaticar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia
100%	L5	Optimizado	Los procesos están bajo constante mejora En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos

Ilustración 11. Valoraciones criterios de madurez CMM

5.3 EVALUACIÓN DE LA MADUREZ

El objetivo de esta fase es evaluar el nivel de madurez implementado en la seguridad en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la norma ISO 27002:2013.
De forma resumida, los dominios que deben analizarse son:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad en los recursos humanos.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de Sistemas de Información
- Gestión de incidentes.
- Gestión de continuidad de negocio Cumplimiento.

Para desarrollar este punto se realizó una auditoria y se evidenciaron por cada uno de los controles:

- Aspectos a verificar en cada auditoria los cuales corresponden a preguntas realizadas para enmarcar cada proceso.

- Hallazgos positivos y negativos lo que permitió realizar la estimación basada en el modelo de maduración de la capacidad (CMM) y su respectiva efectividad.
- Se creó una columna de cumplimento la cual se calificó basado en:

  Grado de Cumplimiento
  - **C**= Cumplido
  - **NC Mayor**= No Conformidad Mayor – Incumplimiento de un apartado completo de la norma.
  - **NC Menor=** No conformidad Menor – Incumplimiento de un punto de la norma
  - **RC=** Requiere corrección/Observación – No existe incumplimiento pero se requiere corrección; ya que si no se corrige en una futura auditoria se puede llegar a convertir en No conformidad.
  - **SFI=** Scope for improvement (Posibilidad de mejora)- Es una recomendación del equipo auditor basada en la experiencia, no existe un incumplimiento a la norma.
  - **PF=** punto fuerte – Reconocimiento del esfuerzo por parte de la organización que ha realizado para gestionar uno o más elementos en sus Sistema de Gestión de seguridad de la información

  En cuanto a la aplicabilidad todos aplican excepto un control el cual se especificó con NA para no aplica.

- Se agrega además una columna de hallazgos/cumplimiento donde se describe por qué el grado de cumplimiento.

- Además se asoció cada control al proyecto a considerar para lograr el nivel esperado.

El detalle del trabajo realizado se complementó desde la declaración de aplicabilidad que ya se había presentado como GAP, adicionando los ítems anteriormente descritos.

Ver detalle en el anexo: EvaluaciondeMadurez.xlsx

5.4 PRESENTACIÓN DE RESULTADOS

Si se evalúa por nivel de madurez, observamos que la mayoría de controles se encuentran en un nivel (L2) seguido de controles de procesos definidos (L3). Esto indica que hay en su mayoría procesos que están parcialmente definidos, que se evidencian buenas prácticas y seguimientos en muchos de los controles planteados en la ISO 27002 pero que carecen en su mayoría de documentación, entrenamiento, comunicación, consolidación de información, definición de responsables, caracterizaciones de proceso.

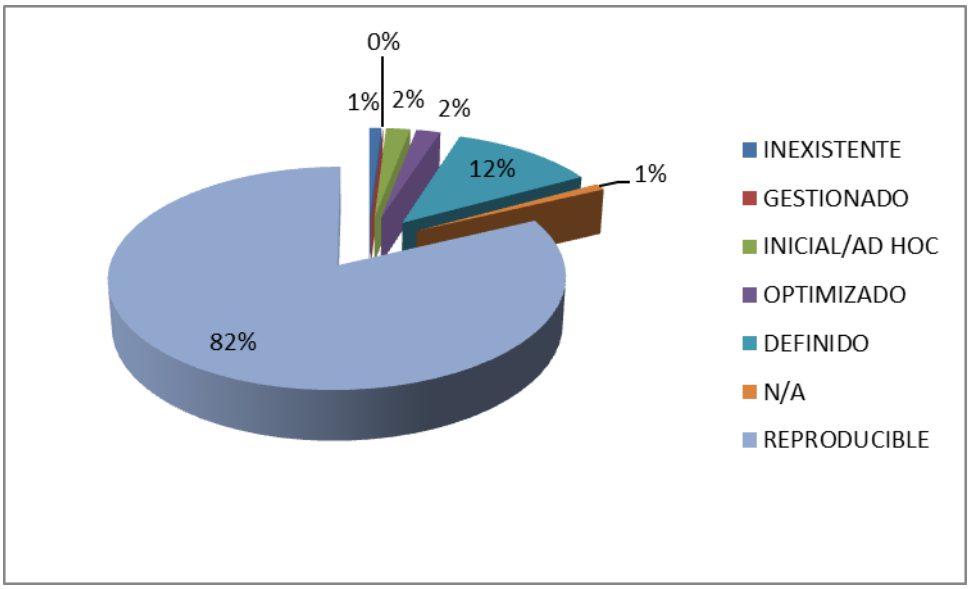


Ilustración 12. Madurez CMM de los controles ISO

A continuacion se presenta una vision mas detallada que mostrara el nivel de cumplimiento por capitulo ISO, Anticipandonos a las medidas, compara el estado actual con el estado deseado.
Las series1 al grado actual de madurez CMM%; la series2 corresponde al grado post-implementacion de madurez CMM %.
Para la organización el nivel deseado de los dominios es de un 90% en una etapa inicial e ir mostrando el proceso de mejora continua y optimizar hasta tener un cumplimiento de un 100%.

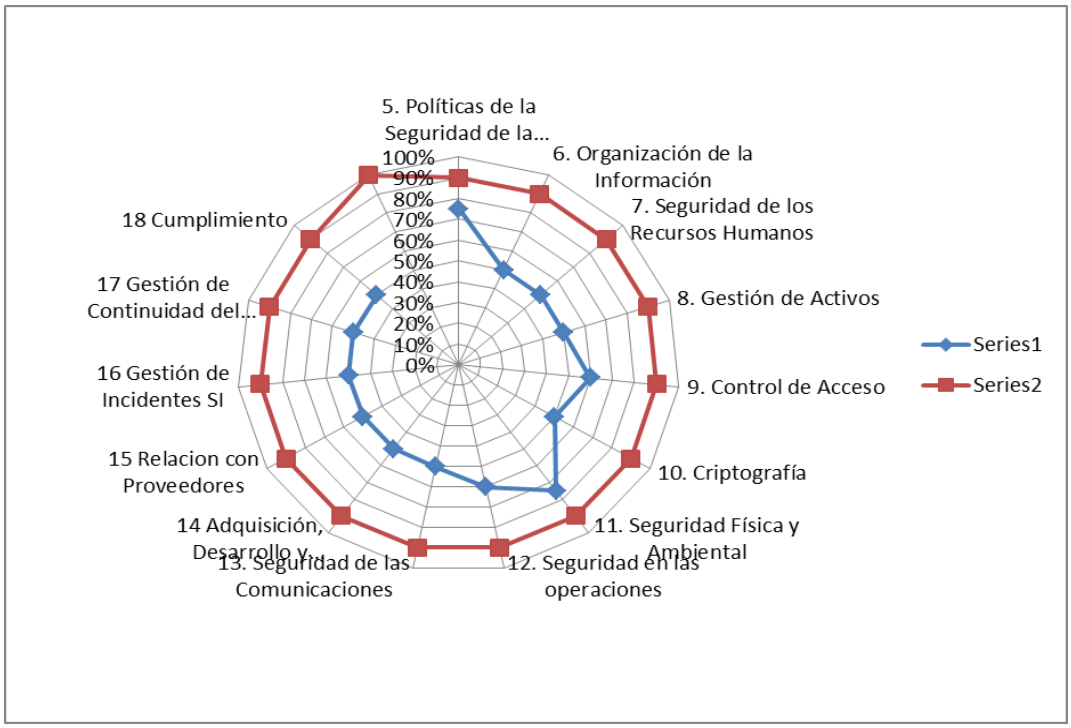


Ilustración 13. Diagrama comparativo el estado actual con el estado deseado controles ISO

5.5 RESUMEN DE HALLAZGOS DE LA AUDITORIA

El alcance de la auditoria ha sido realizado tomando en consideración lo dispuesto en la norma ISO 27001:2013, según la documentación suministrada como evidencia y fuente de información, abarcados en todos los sistemas de información asociados a los procesos.
A continuación se muestra una tabla resumen del grado de cumplimiento por cada dominio.

Sección	Descripción	Grado cumplimiento
5. Políticas de la Seguridad de la Información	**Orientación de la dirección para la gestión de la seguridad de la información**	
5. Política de Seguridad de la Información	Políticas para la seguridad de la información	NC - Menor
5. Política de Seguridad de la Información	Revisión de las políticas de seguridad de la información	NC- Mayor
6. Organización de la Información	**Organización Interna**	
6. Organización de la Seguridad de la Información	Funciones de seguridad de la Información y las responsabilidades	NC- Menor
6. Organización de la Seguridad de la Información	La segregación de funciones	RC
6. Organización de la Seguridad de la Información	Póngase en contacto con las autoridades	RC
6. Organización de la Seguridad de la Información	Póngase en contacto con los grupos de interés especial	NC- Menor
6. Organización de la Información	**Dispositivos móviles y teletrabajo**	
6. Organización de la Seguridad de la Información	Política de dispositivo móvil	NC- Mayor
6. Organización de la Seguridad de la Información	Teletrabajo	NC- Menor
7. Seguridad de los Recursos Humanos	**Antes de la contratación laboral**	
7. Seguridad de los Recursos Humanos	Proyección	NC-menor
7. Seguridad de los Recursos Humanos	Términos y condiciones de empleo	NC- Menor
7. Seguridad de los Recursos Humanos	**Durante la contratación laboral**	
7. Seguridad de los Recursos Humanos	Responsabilidades de gestión	NC-Menor
7. Seguridad de los Recursos Humanos	Concienciación sobre la seguridad de la información, la educación y la formación	NC- Menor
7. Seguridad de los Recursos Humanos	Proceso disciplinario	NC-Menor
7. Seguridad de los Recursos Humanos	**Durante la terminación o cambio del contrato**	
7. Seguridad de los Recursos Humanos	La terminación o el cambio de las responsabilidades laborales	NC- Menor

8. Gestión de Activos	**Responsabilidad por los Activos**	
8. Gestión de Activos	Inventario de activos	NC- Menor
8. Gestión de Activos	Propiedad de los bienes	NC- Menor
8. Gestión de Activos	Uso aceptable de los activos	NC-menor
8. Gestión de Activos	Retorno de los activos	RC
8. Gestión de Activos	**Clasificación de la Información**	
8. Gestión de Activos	Clasificación de la información	NC-Menor
8. Gestión de Activos	Etiquetado de la información	NC-Menor
8. Gestión de Activos	Manejo de activos	NC-Menor
8. Gestión de Activos	**Manipulación de Medios**	
8. Gestión de Activos	Gestión de soportes extraíbles	NC-Menor
8. Gestión de Activos	La eliminación de los medios de comunicación	NC- Menor
8. Gestión de Activos	Transferencia de medios físicos	NC- Mayor
9. Control de Acceso	**Control de Acceso de requerimientos del Negocio**	
9. Control de Acceso	Política de control de acceso	NC-Menor
9. Control de Acceso	El acceso a las redes y los servicios de red	NC-Menor
9. Control de Acceso	**Gestión de Acceso de Usuarios**	
9. Control de Acceso	Registro de usuarios y de la matrícula	RC
9. Control de Acceso	Provisión de acceso al usuario	SFI
9. Control de Acceso	Gestión de derechos de acceso privilegiado	NC-Menor
9. Control de Acceso	Gestión de la información de autenticación de secreto de los usuarios	NC-Menor
9. Control de Acceso	Revisión de los derechos de acceso de usuario	RC
9. Control de Acceso	**Responsabilidad de los usuarios**	
9. Control de Acceso	El uso de la información secreta de autenticación	NC-Menor
9. Control de Acceso	**Control de Acceso a Sistemas y aplicaciones**	
9. Control de Acceso	Restricción de acceso Información	NC-Menor
9. Control de Acceso	Procedimientos seguros de inicio de sesión	NC-Menor
9. Control de Acceso	Sistema de gestión de contraseñas	C
9. Control de Acceso	El uso de programas de utilidad privilegiados	RC
9. Control de Acceso	Control de acceso al código fuente del programa	RC
10. Criptografía	**Controles criptográficos**	

10. Criptografía	Política sobre el uso de controles criptográficos	NC-Menor
10. Criptografía	Gestión de claves	NC-menor
11. Seguridad Física y Ambiental	**Áreas Seguras**	
11. Seguridad física y del entorno	Perímetro de seguridad física	C
11. Seguridad física y del entorno	Controles de entrada físicas	NC-Menor
11. Seguridad física y del entorno	Asegurar oficinas, salas e instalaciones	NC-Menor
11. Seguridad física y del entorno	La protección contra amenazas externas y ambientales	C
11. Seguridad física y del entorno	Trabajar en zonas seguras	NC-Menor
11. Seguridad física y del entorno	Zonas de entrega y carga	NC-Menor
11. Seguridad Física y Ambiental	**Equipos**	
11. Seguridad física y del entorno	Emplazamiento y Protección del equipo	C
11. Seguridad física y del entorno	Apoyo a los servicios públicos	NC-Menor
11. Seguridad física y del entorno	Seguridad del cableado	NC-Mayor
11. Seguridad física y del entorno	El mantenimiento del equipo	RC
11. Seguridad física y del entorno	La eliminación de los activos	NC-Menor
11. Seguridad física y del entorno	Seguridad de los equipos y de los activos fuera del establecimiento	Nc-Menor
11. Seguridad física y del entorno	La eliminación segura o la reutilización de los equipos	Nc-Menor
11. Seguridad física y del entorno	Equipos de usuario desatendida	NC-Menor
11. Seguridad física y del entorno	Política de escritorio y pantalla clear Despejado	NC-Mayor
12. Seguridad en las operaciones	**12. Procedimientos Operacionales y Responsabilidades**	
12. Operaciones de Seguridad	Procedimientos operacionales, adecuadamente documentados	RC
12. Operaciones de Seguridad	Gestión del cambio	NC-Menor
12. Operaciones de Seguridad	Gestión de la capacidad	Nc-Menor
12. Operaciones de Seguridad	Separación de desarrollo, prueba y entornos operativos	NC-Menor
12. Seguridad en las operaciones	**Protección contra código malicioso**	
12. Operaciones de Seguridad	Controles contra mal-ware	NC-Menor
12. Seguridad en las operaciones	**Copias de Respaldo**	
12. Operaciones de Seguridad	Copia de seguridad de la información	RC
12. Seguridad en las operaciones	**Registro y Seguimiento**	
12. Operaciones de Seguridad	El registro de eventos	RC
12. Operaciones de Seguridad	Protección de la información de registro	NC-Menor
12. Operaciones de Seguridad	Registros de administrador y operador	RC

12. Operaciones de Seguridad	Sincronización de reloj	RC
12. Seguridad en las operaciones	**Control de Software Operacional**	
12. Operaciones de Seguridad	La instalación del software en los sistemas operativos	Nc-Menor
12. Seguridad en las operaciones	**Gestión de Vulnerabilidades técnicas**	
12. Operaciones de Seguridad	Gestión de vulnerabilidades técnicas	NC-Menor
12. Seguridad en las operaciones	**Consideraciones sobre auditorias de Sistemas de Información**	
12. Operaciones de Seguridad	Controles de auditoría de sistemas de información	NC-Menor
13. Seguridad de las Comunicaciones	**Gestión de la Seguridad de las redes**	
13. Seguridad en las Comunicaciones	Controles de red	NC-Menor
13. Seguridad en las Comunicaciones	Seguridad de los servicios de red	NC-Menor
13. Seguridad en las Comunicaciones	La segregación en las redes	SFI
13. Seguridad de las Comunicaciones	**Transferencia de Información**	
13. Seguridad en las Comunicaciones	Las políticas y los procedimientos de transferencia de información	NC-Menor
13. Seguridad en las Comunicaciones	Los acuerdos sobre la transferencia de información	NC-Menor
13. Seguridad en las Comunicaciones	La mensajería electrónica	NC-menor
13. Seguridad en las Comunicaciones	Los acuerdos de confidencialidad o de no divulgación	Nc-Menor
14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	**Requerimientos de seguridad de los SI**	
14. Sistema de adquisición, desarrollo y mantenimiento	Análisis de los requisitos de seguridad de la información y especificación	NC-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	Asegurar los servicios de aplicaciones en las redes públicas	NC-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	La protección de las transacciones de servicios de aplicación	NC-Mayor
14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	**Seguridad en desarrollo y procesos de soporte**	
14. Sistema de adquisición, desarrollo y mantenimiento	Politicas de desarrollo seguro	Nc-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	Procedimientos de control de cambios del sistema	NC-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	Revisión técnica de las aplicaciones después de operar cambios de plataforma	Nc-menor
14. Sistema de adquisición, desarrollo y mantenimiento	Restricciones en los cambios a los paquetes de software	Nc-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	Uso de principios de ingeniería en protección de sistemas	RC

14. Sistema de adquisición, desarrollo y mantenimiento	Seguridad en entornos de desarrollo	NC-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	Desarrollo Outsourced	NA
14. Sistema de adquisición, desarrollo y mantenimiento	Pruebas de funcionalidad durante el desarrollo de los sistemas	Nc-Menor
14. Sistema de adquisición, desarrollo y mantenimiento	Pruebas de aceptación del sistema	NC-Menor
14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	**Datos de prueba**	
14. Sistema de adquisición, desarrollo y mantenimiento	Protección de los datos de prueba	Nc-Menor
15 Relacion con Proveedores	**Seguridad de la Información en la relación con los proveedores**	
15. Relaciones con los proveedores	Política de seguridad de la información para las relaciones con proveedores	NC-Menor
15. Relaciones con los proveedores	Abordar la seguridad dentro de los acuerdos con proveedores	NC-Mayor
15 Relacion con Proveedores	**Gestión de la prestación de servicios del proveedor**	
15. Relaciones con los proveedores	El seguimiento y la revisión de los servicios de proveedores	NC-Menor
15. Relaciones con los proveedores	Gestión de cambios en los servicios de proveedores	Nc-Menor
16 Gestión de Incidentes SI	**Gestión de Incidentes y Mejoras en la SI**	
16. Gestión de Seguridad de la Información de Incidentes	Responsabilidades y procedimientos	Nc-Menor
16. Gestión de Seguridad de la Información de Incidentes	Informar sobre los eventos de seguridad de información	Nc-Menor
16. Gestión de Seguridad de la Información de Incidentes	Presentación de informes de información debilidades de seguridad	Nc-Menor
16. Gestión de Seguridad de la Información de Incidentes	Valoración de eventos de seguridad de la información y toma de decisiones	Nc-Menor
16. Gestión de Seguridad de la Información de Incidentes	Respuesta a incidentes de seguridad de la información	Nc-Menor
16. Gestión de Seguridad de la Información de Incidentes	Aprendiendo de los incidentes de seguridad de la información	Nc-Menor
16. Gestión de Seguridad de la Información de Incidentes	El acopio de pruebas	NC-Mayor
17 Gestión de Continuidad del Negocio	**Continuidad SI**	
17. Aspectos de seguridad de información de la gestión de continuidad del negocio	Información de planificación de continuidad de seguridad	NC-Menor
17. Aspectos de seguridad de información de la gestión de continuidad del negocio	Implantación de la continuidad de la seguridad de la información	Nc-Menor
17. Aspectos de seguridad de información de la gestión de continuidad del negocio	Verificar, revisar y evaluar la información de seguridad de continuidad	Nc-Menor
17 Gestión de Continuidad del Negocio	**Redundancias**	

17 Gestión de Continuidad del Negocio	Disponibilidad de instalaciones para el procesamiento de la informacion	NC-Menor
18 Cumplimiento	**información**	
18. Cumplimiento	Identificación de la legislación aplicable y los requisitos contractuales	Nc-Menor
18. Cumplimiento	Derechos de propiedad intelectual	Nc-Menor
18. Cumplimiento	Protección de los registros	Nc-Menor
18. Cumplimiento	Privacidad y protección de datos personales	NC-Menor
18. Cumplimiento	Regulación de los controles criptográficos	Nc-Menor
18 Cumplimiento	**Revisiones de SI**	
18. Cumplimiento	Revisión independiente de la seguridad de la información	NC-Menor
18. Cumplimiento	El cumplimiento de las políticas y normas de seguridad	Nc-Menor
18. Cumplimiento	Revisión de cumplimiento técnico	NC-Menor

Tabla 25. Tabla detallada grado de cumplimiento.

Resumen de resultados

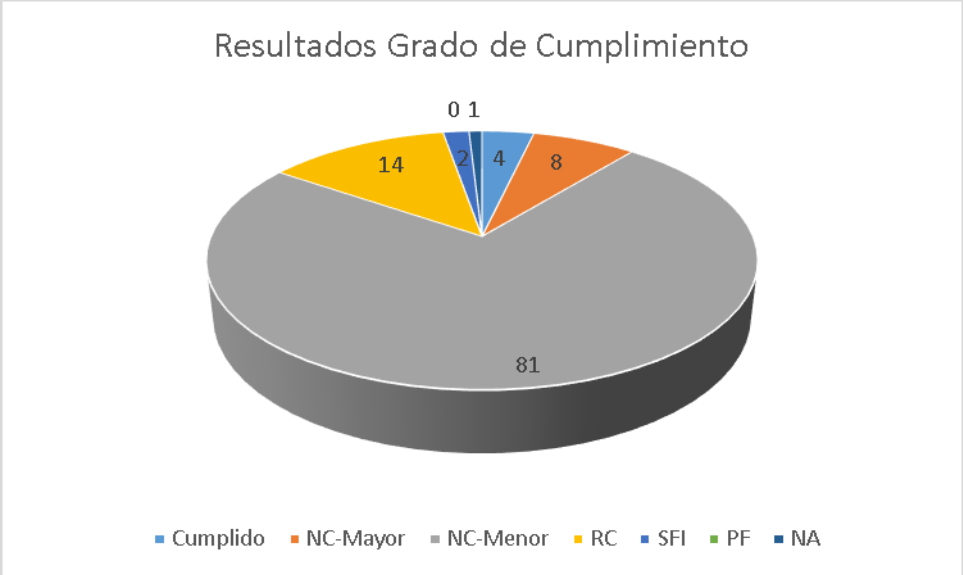


Ilustración 14. Resultados Grado de Cumplimiento

Cumplido (C) =4
Se da cumplido a lo requerido en el control.

No conformidades – Meyores (NC-Meyor)=8
Estas no conformidades es el incumplimiento de un apartado completo de la norma, en este caso el control.

No conformidades – Menores (NC-Menor)=81

Las no conformidades Menores en su mayoria corresponden a procesos que tienen evidencias y resgistros que dan cumplimiento al control pero no existe documentacion del proceso, ni difusion del mismo, por lo que se tiene un incumplimiento de un punto de la norma.

Requiere Correccion/Observacion (RC)= 14
No existe incumplimiento pero se requiere la revision en este caso de los procedimientos y documentacion facilitada, se encuentran incompletos y hay falta de detalle en el proceso.
Si no se corrige podria convertirse en una no confrormidad en una auditoria futura.

Posibilidad de Mejora (SFI)=2
Se muestra como una recomendación del auditor, no existe incumplimiento de la norma.

Punto Fuerte (PF)=0
Aun cuando se notan procesos de buenas practicas y un esfuerzo de mejora en el SGSI no se destaca ningun control.

No aplica (NA)=1
Solo un control se considera que no aplica para la organización.

3. Capítulo III. Conclusiones

- La implementación de un sistema de gestión de seguridad de la información SGSI, conformara un mecanismo de optimización de recursos, ahorro de costos y mejora continua que permitirá a Textilera S.A alcanzar los objetivos y metas planteadas.

- Las mejoras al sistema Gestión de seguridad de la información posibilitara alcanzar niveles de madurez fijados por la organización, al mismo tiempo que permitirá un mayor acercamiento para realizar la certificación del SGSI mediante la norma ISO 27001:2013.

- Un SGSI conlleva a cambios de procesos y estructuras pero hace que la integridad, confidencialidad y disponibilidad estén enmarcadas como uno de los mayores activos dentro de una compañía y para Textilera S.A esto es de vital importancia para su crecimiento.

- El análisis y la gestión de riesgos ha permitido la correcta identificación de los activos en riesgo, determinando sus dependencias y el impacto potencial de la materialización de las amenazas, desarrollando y cuantificando las medidas de protección, ya sean operativas, técnicas y humanas que permiten mitigar, aceptar o transferir los riesgos.

- Con las visitas realizadas a Textilera S.A se identificaron procesos no existentes a implementar al SGSI.

- Con las diferentes auditorías realizadas a los procesos y áreas existentes se logró identificar las evidencias, hallazgos positivos, negativos, grado de cumplimiento para cada uno de los controles aplicables a la norma ISO 27001:2013 en miras al fortalecimiento del SGSI.

- A través del análisis de riesgos de los activos más críticos de la empresa Textilera S.A se logró identificar los proyectos a desarrollarse en miras al cumplimiento de la norma ISO 27001:2013.

- Se presentaron las cartas de los diez proyectos resultantes como punto de partida de la gestión de proyectos necesarios para el cumplimiento de la norma ISO 27001:2013 en el fortalecimiento de SGSI.

- Es necesario dimensionar un presupuesto más amplio para las estrategias de seguridad de la información en la organización Textilera S.A.

- La Presentación de la asesoría realizada a Textilera S.A genero un impacto positivo al personal de TI y cumplió con las necesidades planteadas.

- El apoyo de la dirección es un factor clave para la madurez del sistema de gestión de seguridad de la información.

- Se deberá contar con estrategias y medios que permitan la sensibilización del SGSI permanente con los usuarios ya que ellos son los responsables del manejo adecuado de la información.

4. Capítulo IV. Glosario

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo, si sólo incluye una parte de la organización.

Alerta: Notificación formal de un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.

Lista de Chequeo: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Entidad de acreditación: Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina)...

Entidad de certificación: (Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27000, ISO 9000, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Evaluación de riesgos: Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO. Es certificable. Publicación 2013.

IT: Information technology, Tecnología de la Información

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Política de escritorio despejado: La política de la empresa que indica a los empleados que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

Requerimiento: Es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

SI: Seguridad de la información.

Trackit: Software mesa de ayuda para manejo de ingreso de incidentes

Tratamiento de riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

6. Capitulo V. Bibliografía

- Dayal E. (2.014). Plantilla Project charter –templater.docs-Eric-dayal-. Recuperado de: http://www.hitdocs.com/project-charter-template-docx, Marzo a Junio de 2016

- ISO/IEC 27001, Information Technology – Security Techineques – Information Security Management systems – Requirements –Pag. 1-22,Second Edition 2013-10-01,ISO/IEC 2013,Switzerland.

- ISO/IEC 27002, Information Technology – Security Techineques –Code of practice for information security controls–Pag. 2-78, Second Edition 2013-10-01,ISO/IEC 2013,Switzerland.

- Acosta Mira L.F (2012). *Los verdaderos obstáculos de la implantación de la seguridad de la información*. (Tesis de pregrado). Universidad Pontificia Bolivariana, Medellín.

- http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf, NIST Guide for Conducting Risk Assessments , Marzo a Junio de 2016.

- http://www.iso27002.es/, Portal de Soluciones técnicas y organizativas a los controles de la Norma Internacional ISO/IEC 27002, Marzo a Junio de 2016.

- http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html - .Uw5dlvR5NGI, Marzo a Junio de 2016.

6. Capítulo VI. Anexos

Fase de proyecto	Anexo Asociado
Fase 1: situación actual: contextualización y análisis diferencial.	hoja de verificación.xlsx
Fase 2: Sistema de Gestión Documental	*PW-15-007 Política de seguridad de la información .doc* PQ-01-171 .doc PQ-01-013.doc PQ-01-011.doc PQ-01-012.doc A1PQ01171.doc FQ-01-173.xls Declaración de aplicabilidad y hoja de verificacion.xlsx
Fase 3: Análisis de Riesgos	*Escenario del Riesgo.xlsx* *MatrizRiesgos.xlsx*
Fase 4: Propuestas de proyectos	*Calculo Riesgo Residual.xlsx* *ProyectoPoliticasSeguridad.docx* *ProyectoMonitoreoSGSI.docx* *ProyectoContratacionLegalidad.docx* *ProyectoControlAccesoySeguridaFisica.docx* *ProyectoServiciosPlataforma.docx* *ProyectoDesarrolloSoftware.docx* *ProyectoClasificacionGestion Activos.docx* *ProyectoContuinidadNegocio.docx* *ProyectoAnalisisRiesgos.docx* *ProyectoCriptografia.docx* *Proyectos SGSI.pdf*
Fase 5. Auditoria de Cumplimiento	EvaluaciondeMadurez.xlsx