Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 Para la empresa Pollos Pachito

IMPLEMENTACIÓN SGSI EMPRESA POLLOS PACHITO S.A

Descripción

La gran demanda de clientes que requieren que sus proveedores gestionen adecuadamente la información hace necesario la implementación de controles para protegerla, por lo anterior Pollos Pachito implementara un SGSI de acuerdo a la norma ISO 27001:2013

Robinson Ruiz Muñoz

Màster Interuniversitari en Seguretat

de les TIC (MISTIC)

Plan de Implementación de la ISO/IEC 27001:2013 Para la empresa Pollos Pachito S.A

Trabajo Final de Master

Trabajo escrito y presentado al tutor:

Carles Garriguez Olivella

Antonio Jose Segovia Henares

Asignatura: TFM-Sistemas de gestión de la seguridad de la información

ROBINSON RUIZ MUÑOZ

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Junio 10 de 2015

Dedicatoria

En primer lugar a DIOS que me permitió cursar este estudio; en segundo lugar a mi Madre Carmen Muñoz, quien me apoyo en este proceso, a mi esposa Merilin Legarda e hijo Johan Alejandro Ruiz, quienes me comprendieron y me dieron el espacio suficiente para dedicarme a este estudio aun cuando sacrificase tiempo de compartir con ellos, es por ellos que realizo este esfuerzo para poderles brindar una mejor calidad de vida

Robinson Ruiz Muñoz

Resumen

Pollos Pachito S.A, es una empresa ficticia del sector avícola colombiana, se encuentra ubicada en el departamento del valle del cauca, está dedicada a la producción y comercialización de carne de pollo, conscientes de que el mercado internacional requiere unos niveles de cumplimiento acerca del tratamiento de la seguridad de la información surge la necesidad de implementar un sistema para gestionar adecuadamente la información, con el objeto de permitir la implementación de un SGSI, pollos pachito S.A, de aquí en adelante como la empresa, permite que se valore su estado de seguridad actual, se establece un plan director que permite identificar que se requiere realmente con la implementación, se presenta el esquema documental se realiza el análisis de riegos se identificó el riesgo aceptable y el no aceptado por la organización, partiendo de este riesgo no aceptable se establecieron planes de seguridad los cuales se planearon y de su ejecución se espera minimizar el riesgo, para validar esto se estableció un programa de auditoria a los controles de la norma ISO/IEC 27002, con el objeto de valorar el estado de seguridad inicial y el estado de seguridad esperado posterior a la implementación de los planes de seguridad, dando como resultado un estado de madurez más alto que el inicialmente identificado.

.

Abstract

Chickens Pachito SA, is a fictional company for the Colombian poultry industry, is located in the department of Valle del Cauca, is dedicated to the production and marketing of chicken, aware that the international market requires a level of compliance regarding treatment Security of information the need to implement a system to properly manage information in order to allow the implementation of an ISMS, pachito chickens SA, hereinafter as the company allows its security status is assessed arises Current, a master plan that identifies who is actually required to implement the scheme document the risk analysis is performed acceptable risk identified and not accepted by the organization, based on this risk is not acceptable states settled Security plans which were planned and its implementation is expected to minimize risk, to validate this established an audit program controls the ISO / IEC 27002, in order to assess the initial state of security and rule safety expected after the implementation of security plans, resulting in a higher state of maturity than initially identified.

Tabla de Contenido

1 INTRODUCCION DEL PROYECTO

En la era actual donde el acceso a la información es menos restringido, donde las oportunidades de negocio están posterior a un clic, empresas como Pollos Pachito S.A, no pueden limitarse a un mercado local, pueden aspirar a extender sus horizontes y alcanzar nuevos mercados, pero llegar a estos nuevos mercados demanda por parte de los clientes el cumplimiento de normas de seguridad de la información a través de estándares reconocidos mundialmente, el propósito del siguiente Trabajo es presentar los pasos para la correcta implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/27001:2013.

La siguiente memoria está compuesta por fases donde se establece un proceso de la implementación, cada fase está relacionada con la anterior y depende el éxito de la fase actual de la asertividad que se tenga con la anterior, así mismo se tiene un grupo de archivos u anexos que apoyan cada una de las fases implementadas y sirven de evidencia de implementación del sistema de gestión de seguridad de la información.

1.1 DEFINICIONES:

Activos: Cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos

Amenaza: “Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización” (http://www.iso27000.es/glosario.html, s.f.)

Análisis de riesgos: Proceso que busca identificar los activos, amenazas, probabilidad de ocurrencia y el riesgo al cual está sometido el activo.

Control: Medios para gestionar el riesgo.

Degradación: “cuán perjudicado resultaría el valor del activo”. (Magerit Version 3.0 Metodología de Análisis y Gestión de Riesgos Libro 1 - Método)

Declaración de aplicabilidad: Documento que describe los controles aplicables y no aplicables en el Sistema de Gestión de seguridad de la empresa

Disponibilidad: Propiedad de los activos de ser accedidos por el personal autorizado cuando se requiera.

Integridad: Característica de los activos la cual indica que los activos no pueden ser modificados por personal no autorizado

Confidencialidad: Propiedad de los activos de ser accedidos solo por el personal autorizado.

Política: Intención o directriz expresada por la dirección

Riesgo: Es la probabilidad de que un incidente o evento adverso ocurra sobre un activo.

Vulnerabilidad: Falencia o debilidad que puede ser actividad de manera accidental o intencionalmente

Impacto: es la medida del daño que sufre un activo

Salvaguarda: Son medidas de protección

Mitigar el Riesgo: Acciones que se toman para disminuir la probabilidad, las consecuencias o las dos asociadas a un riesgo

Transferir Riesgo: Se transfiere o comparte el riesgo a terceros

Aceptar: No se hace nada

1.2 ÍNDICE DE ILUSTRACIONES

1.3 INDICE DE TABLAS

1.4 ÍNDICE DE ANEXOS

2 Fase 1: Situación actual Contextualización, Objetivos y Análisis Diferencial

2.1 INTRODUCCIÓN

El presente trabajo se centra sobre una empresa del sector avícola, Pollos Pachito es una empresa vallecaucana, fundada en 1984, está dedicada a la producción y comercialización de carne de pollo, actualmente consta de una planta de incubación, 6 granjas reproductoras, 23 granjas de engorde, una planta de alimentos una planta de sacrificio, para la comercialización del pollo cuenta con 5 distribuidoras las cuales cuentan con almacenes anexos a cada una de ellas. En la actualidad y como parte del proceso de expansión de la marca, Pollos Pachito ve en el mercado extranjero una oportunidad para alcanzar este objetivo. Estos nuevos clientes exigen que sus proveedores implementen procesos certificables para resguardar la información, por lo cual Pollos Pachito tiene como necesidad implementar un sistema de gestión de seguridad de la información de ahora en adelante SGSI, que permita la gestión eficiente de la seguridad de la información, para así brindar a sus clientes un alto de grado de confiabilidad en el tratamiento de sus datos sobre los cuales somos los responsables y hacer de esto un diferenciador competitivo en el mercado.

2.2 CONOCIENDO LA ISO 27001- 27002

Para alcanzar el objetivo de implementar un SGSI, la empresa ha decido adoptar y poner en funcionamiento lo indicado por la ISO /IEC 27001 como un conjunto de buenas prácticas concretadas bajo el anexo 27002, esta norma tiene como última actualización oficial la edición 2013, como características importantes se destaca que cuenta con un total de 14 dominios 35 objetivos de control y 114 controles, pero para llegar a lo que es actualmente la norma ISO 27001 y la 27002, cabe destacar que esta inicio como una norma británica la BS7799-1 de la British Standards Institución en el año de 1995, pero esta norma no permitía ni establecía un esquema de certificación, está en si era una guía de buenas prácticas, lo contrario se presentó con la publicación de la BS 779-2 en el año 1998, ya que esta norma si permitía la certificación, en esta se establecen los requisitos de un sistema de gestión de seguridad de la información, esta norma evoluciono en el año de 1999 posterior a la revisión de la parte 1 y 2, de esta revisión la BS 7799-1 fue adoptada por la ISO, en el 2000 se aprobó con el nombre ISO 17799:2000, mediante un proceso rápido no se presentaron grandes cambios, para el 2002 se realiza una revisión a la norma BS 7799-2, esta fue una especificación de un sistema de gestión de seguridad de la información, presento un acercamiento a la ISO 9001, ISO 14001, en si se adaptó la norma al esquema ISO de sistemas de gestión, para el año 2005 la BS 7799-2 fue publicada por la ISO como el estándar internacional ISO 27001, la ISO 17799 se actualizo y cambio de nombre a ISO 27002:2005, la BSI publico la BS 7799-3:2006 esta norma centra su contenido en la gestión del riesgo, esto se generó en el año 2006

2.3 SISTEMA DE INFORMACIÓN

Pollos pachito tiene diferentes sistemas de información para soportar sus diferentes procesos, en particular el sistema de información comercial, actualmente tiene dos tipos de procesos : la venta a mayoreo (clientes a los cuales se les distribuye desde la distribuidora) y ventas almacenes (ventas que se realizan en los almacenes), la venta mayoreo cuenta con una arquitectura cliente servidor donde los usuarios ingresan pedidos, registran facturas, controlan el inventario, registran los pagos, se utiliza otro sistema de información para la creación de clientes, el acceso a la minería de datos, creación y modificación de campañas comerciales, este último está conectado con un servidor pasarela telefónica el cual se comunica con la planta telefónica para el registro de las llamadas. Para la venta de almacenes la lógica, los datos y la interfaz se encuentran en un mismo equipo

2.4 ORGANIGRAMA FUNCIONAL

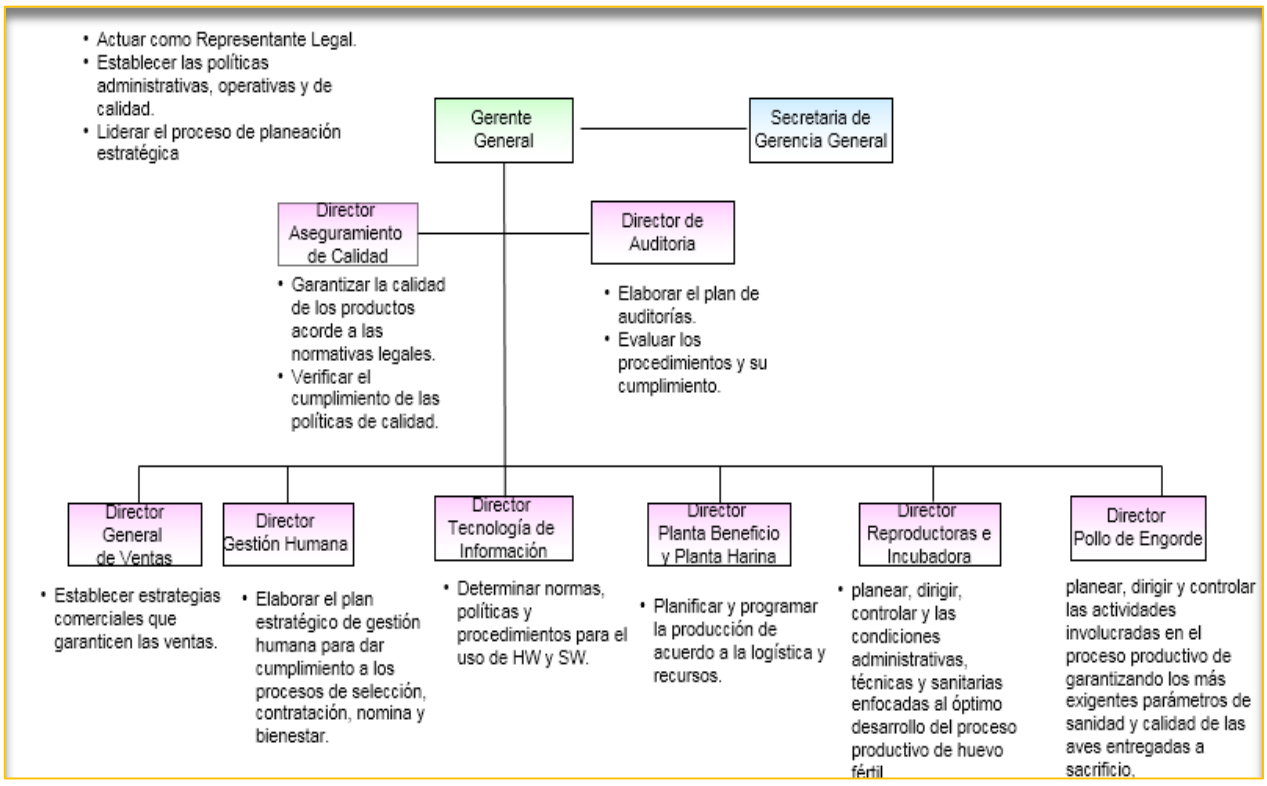


Ilustración 1 Organigrama Funcional

2.5 ALCANCE

El alcance es para todo los sistemas que soportan el proceso comercial de venta por mayoreo, se excluye la venta almacenes. (Ver Ilustración 2 Proceso comercial Mayoreo)

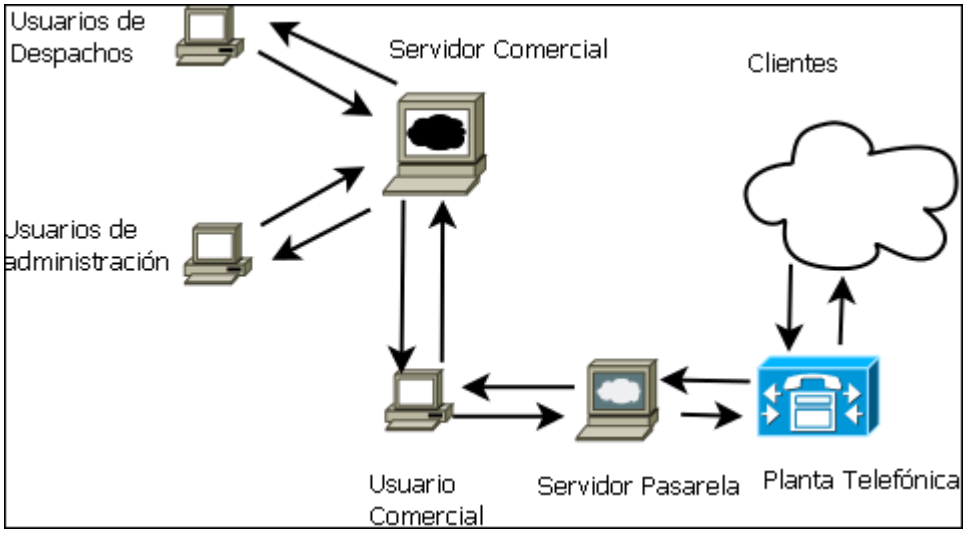


Ilustración 2Proceso Comercial Mayoreo

2.6 OBJETIVOS DEL PLAN DIRECTOR

Conscientes de la necesidad de cumplir con los requerimientos que demanda los clientes del mercado internacional la organización establece el siguiente objetivo en el plan director:

Implementar un sistema de gestión de seguridad de la información certificado, que permita brindar a los clientes nacionales y extranjeros confianza por el tratamiento de los datos que la empresa gestiona, cumpliendo con la legislación nacional e internacional vigente para la transferencia de datos y garantizando la implementación de controles eficientes que protejan la información. Buscando alcanzar de esta manera el objetivo misional de la empresa el cual es hacer presencia en el mercado internacional con productos de alta calidad.

2.7 ANÁLISIS DIFERENCIAL

Con el objeto de identificar el estado de seguridad en la empresa se hace necesario realizar un análisis diferencial con respecto a la ISO 27001:2013 y la ISO 27002, esta actividad se lleva a cabo evaluando una revisión de cada uno de los controles de las normas en referencia, para esto se realiza entrevistas a usuarios responsables de procesos de

diferentes áreas Auditoria – A, Recursos Humanos –R, Seguridad S, Jurídico J, Departamento de Tecnología D, para evaluar el estado de la seguridad, se califica el grado de cumplimiento al control presentado y el nivel de madurez, este último se pondera de acuerdo a la tabla 1.

Abr	Madurez	Cumplimiento
0	**No existente:** No cumple, no se hace.	No cumple
1	**Inicial / Ad hoc:** La actividad no se realiza por falta de recursos, no se ha considerado su ejecución.	Parcial
2	**Repetible pero intuitivo**: La actividad no está completamente entendida, se ha planificado la ejecución a futuro.	Parcial
3	**Proceso definido**: La actividad se realiza de forma incompleta y limitada en alcance.	Cumple
4	**Administrado y medible**: Se hace cubriendo todo el alcance de la actividad pero no de la forma más óptima, requiere mejoras.	Cumple
5	**Optimizado**: No requiere mejoras, está funcionando de acuerdo con lo requerido por el proceso y conforme a las mejores practicas	Cumple

Tabla 1 Modelo de Cumplimiento

2.8 ANÁLISIS DIFERENCIAL – EVALUACIÓN D ARTÍCULOS ISO 27001

Para determinar el grado de cumplimiento de los controles de la ISO 27001, se debe de tomar cada artículo de la norma y definir el grado de cumplimiento de acuerdo a la tabla 2 ver anexo 1 Análisis Diferencial ISO 27001

Valoración Nivel de Cumplimiento	
Si	Cumple
Parcial	Cumplimiento Parcial
No	No Cumple

Tabla 2 Nivel de Cumplimiento

2.9 ESTADÍSTICAS GENERALES-ESTADO DE SEGURIDAD NORMA ISO/IEC 27001:

El análisis nos permite identificar que la organización tiene un proceso ya iniciado con respecto a los requisitos de la norma ISO/IEC 27001, donde existe un cumplimiento parcial del 55%, pero que hay que mejorar el cumplimiento puesto que solo se cumple un 17% y

se detecta un incumplimiento del 28% (ver tabla 3 Análisis Cumplimiento Estado de Seguridad Según ISO 27001)

	Articulo	Cantidad Articulo	Cumple	Cumple Parcial	No Cumple
4	Contexto de la Organización	7	2	3	2
5	Liderazgo	19	2	4	13
6	Planificación	32	0	25	7
7	Soporte	23	3	17	3
8	Operación	8	2	6	0
9	Evaluación del Desempeño	26	0	15	11
10	Mejora	12	12	0	0
	Total	**127**	21	70	36
		%	**17%**	**55%**	**28%**

Tabla 3 Análisis Cumplimiento Estado de Seguridad Según ISO 27001

La ilustración 3 y 4 análisis de controles ISO 27001 permite visualizar el estado de la seguridad donde es notorio que en los requisitos de los apartados de planificación y evaluación del desempeño no existe un cumplimiento total de ninguno de los requisitos evaluados, existe un cumplimiento parcial

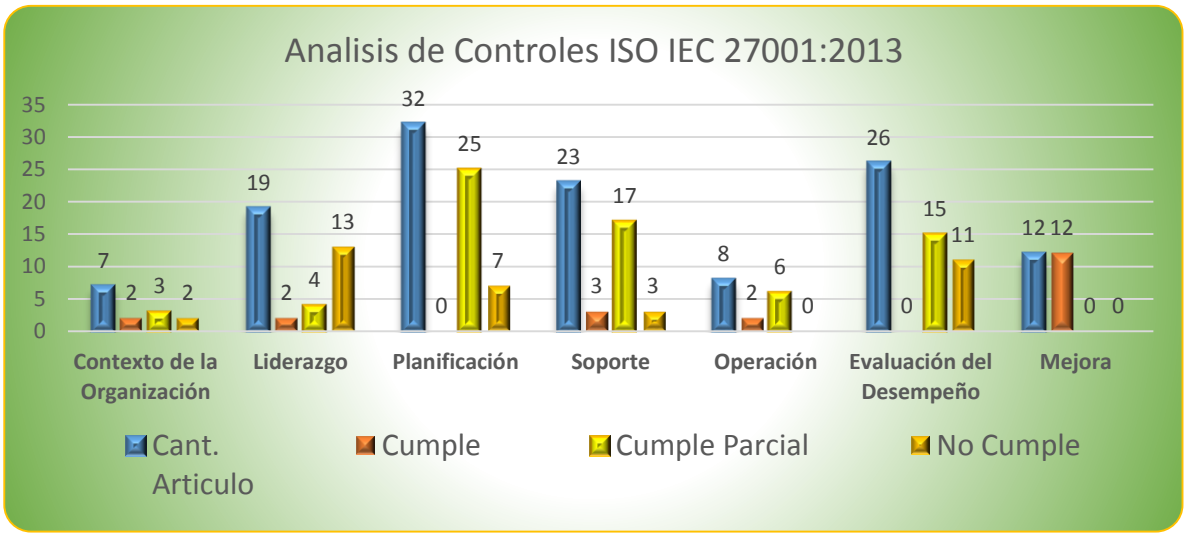


Ilustración 3 análisis de controles ISO 27001

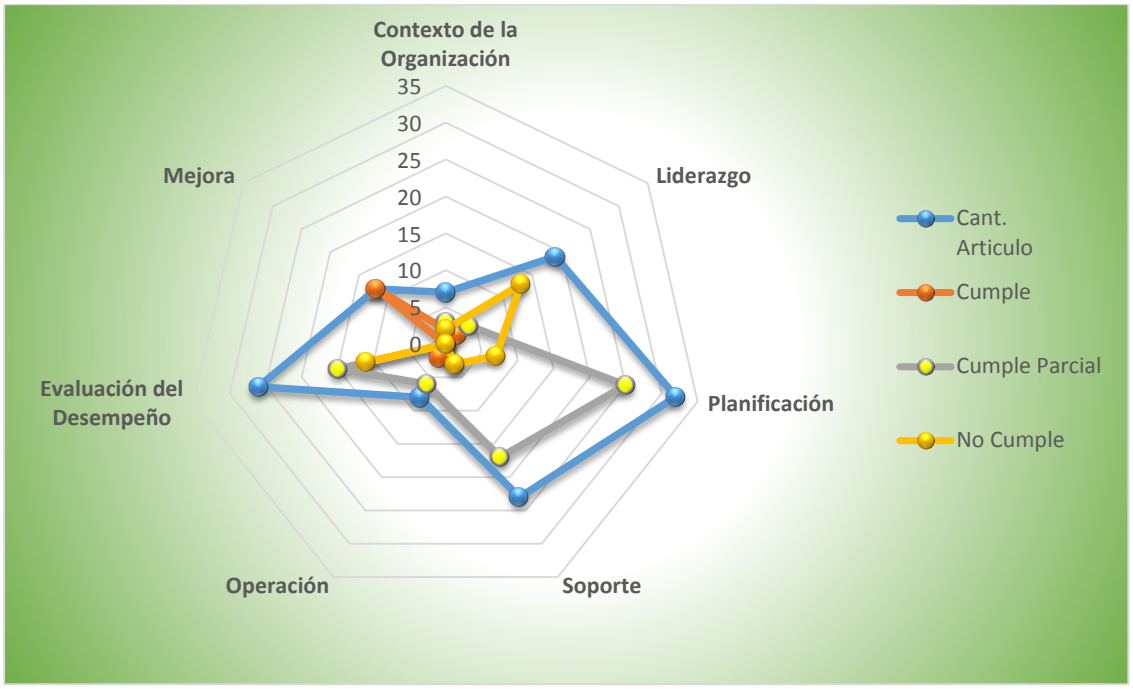


Ilustración 4 análisis de controles ISO 27001

2.10 Análisis Diferencial – Evaluación de Artículos ISO 27002

Para determinar el grado de cumplimiento de los controles de la ISO 27002, se debe de tomar cada control de la norma y definir el grado de cumplimiento de acuerdo a la tabla 2 y de manera similar calificar el grado de madures del control de acuerdo a lo descrito en la tabla 1 Modelo de Madurez, lo anterior se registra en anexo 2 Análisis Diferencial-ISO 27002

.

2.11 Estadísticas Generales-Estado de Seguridad Norma ISO/IEC 27002:

Se realiza un resumen por cada dominio del cumplimiento de la norma ISO 27002, este se esquematiza en la tabla 4 Análisis Cumplimiento Estado de Seguridad Según ISO 27002, donde se presenta el porcentaje de cumplimiento teniendo en cuenta las variables de cumplimiento: Cumple, Cumple parcialmente, No Cumple.

	Dominio	Cant. Secciones	Cumple	% Cumplimiento	Cumple Parcial	% Cumple Parcial	No Cumple	% No Cumple
A	Política de Seguridad	2	0	0%	2	100%	0	0%
B	Aspectos organizativos de la seguridad de la información	7	3	43%	3	43%	1	14%
C	Seguridad ligada a los Recursos Humanos	6	3	50%	3	50%	0	0%
D	Gestión de Activos	10	2	20%	6	60%	2	20%
E	Control de Accesos	14	13	93%	1	7%	0	0%
F	Criptografía	1	0	0%	0	0%	1	100%
G	Seguridad Fisica y ambiental	15	9	60%	4	27%	2	13%
H	Operaciones de Seguridad	14	8	57%	5	36%	1	7%
I	Seguridad en las Telecomunicaciones	7	2	29%	4	57%	1	14%
J	Sistema de Adquisición, desarrollo y mantenimiento	13	10	77%	2	15%	1	8%
K	Relaciones con Proveedores	5	0	0%	5	100%	0	0%
L	Gestión De lincidentes en la Seguridad de la Información	7	3	43%	4	57%	0	0%
M	Aspectos de Seguridad de la Información en la Gestión de	4	1	25%	3	75%	0	0%
N	Cumplimiento	8	2	25%	4	50%	2	25%
		113	56	50%	46	41%	11	10%

Tabla 4 Análisis Cumplimiento Estado de Seguridad Según ISO 27002

2.12 RESULTADOS

Los resultados que presenta la verificación del estado de seguridad de la organización Pollos Pachito referente a la norma ISO/27002, es que se tiene un grado de madurez del 50% se está cumpliendo con 56 controles, parcialmente se tiene un cumplimiento de 46 controles que equivalen al 41%, se identifica la carencia de controles en procesos importantes como es los controles criptográficos, en algunos controles como la gestión de activos existe un incumplimiento del 25%.

Se anexa la ilustración número 5 donde se muestra el estado de la seguridad de acuerdo a los controles

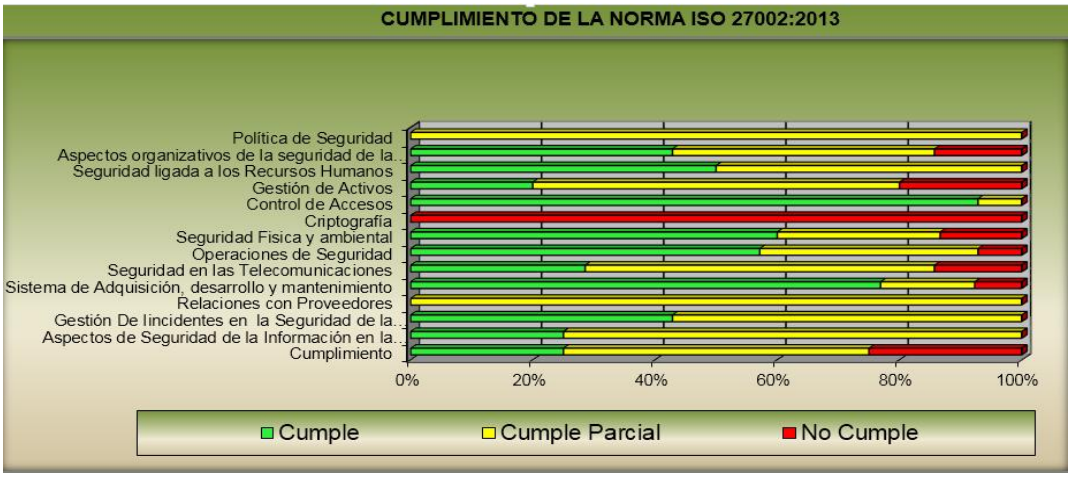


Ilustración 5 Análisis Estado de Seguridad Norma ISO 27002

3 Fase -2 Sistema de Gestión Documental

La fase de gestión documental comprende los documentos requeridos para la certificación del sistema este documento consta de las políticas por dominio, la declaración de la política, los procedimientos de auditorías internas, la gestión de indicadores, los procedimientos de revisión por la dirección, la gestión de roles y responsabilidades, la metodología de análisis de riesgos y la declaración de aplicabilidad.

3.1 POLÍTICA DE SEGURIDAD

Pollos Pachito S.A, dentro de su estructura organizacional establece un Comité de Seguridad de la Información, conformado por un grupo interdisciplinario de colaboradores, responsable de todas las acciones referidas a la seguridad de la información de la organización, controles y procedimientos según los requerimientos de la organización para detallar se dispone el anexo 3 manual de seguridad

3.2 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad consiste en definir los controles adecuados para el sistema de gestión de seguridad de información

Se anexa tabla con los controles bajo el anexo A de la norma ISO/IEC 27001:2013 que aplica y el estado actual del control Ver anexo 4 Declaración de aplicabilidad.

3.3 PROCEDIMIENTO DE AUDITORÍAS INTERNAS:

Se establece que el proceso de auditoria se llevara a cabo bajo las directrices:

Se establecerá el programa de auditoria el cual se basa bajo la norma NTC ISO 19011, en el cual se tiene en cuenta:

1. Establecer los objetivos del programa de auditoria
2. Definir el alcance para cada auditoria
3. Establecer los criterios para seleccionar el equipos auditor
    a. Validar las competencias de los auditores
    b. Aspectos como la honradez, observador, seguro, abierto a las diversidades culturales son cualidades necesarias para pertenecer al equipo de auditoria.
4. Identificar responsables, estos deben de tener las competencias, principios e independencia para llevar a cabo el proceso de auditoria
5. Identificar los riesgos que pueden afectar la ejecución de las auditorias

6. Identificar responsables, estos deben de tener las competencias, principios e independencia para llevar a cabo el proceso de auditoria

7. Se debe de presupuestar los recursos a utilizar (económicos, personal auditores como auditados, tiempo)

8. Se debe concertar las herramientas, procedimientos a utilizar en el proceso de auditoria

9. Se debe realizar los entregables donde se evidencien los resultados de la auditoria
10. La información debe de entregarse al cliente de la auditoria. en el plan de auditoria, se establece un proceso de auditoría y otro de verificación, tiene un periodo de duración estimado de tres años

Ver anexo 5 Formato de Auditoria.

Cronograma:

Fecha 1	Fecha 2	Dominio
Abril 20 2015	Feb 03 2017	Política de Seguridad de la Información
		Organización Interna
Mayo 30 2015	Jun 16 2017	Seguridad en los recursos humanos
		Gestión de Activos
		Requisitos de negocio para el control de acceso
Agosto 22 2015	Oct 18 2017	Controles criptográficos
		Seguridad Física y Ambiental
Nov 26 2015	Dic 07 2017	Seguridad Operativa
Feb 02 2016	Ene 18 2018	Gestión de la Seguridad en las redes
		Requisitos de seguridad de los sistemas de información.
		Seguridad de la información en las relaciones con suministradores
Julio 23 2016	Abril 15 2018	Gestión de incidentes de seguridad de la información y mejoras
		Continuidad de la Seguridad de la Información
Dic 07 2016		Cumplimiento de los requisitos legales y contractuales

Tabla 5 Cronograma de Auditorias

3.4 GESTIÓN DE INDICADORES

Se establecen los indicadores, los cuales se anexaron en el archivo Gestión Indicadores, con el objeto de medir la eficacia de los controles, esta tabla cuenta con una columna **control** indica el control a evaluar de la norma ISO/IEC 27002, la columna **descripción** hace una descripción de los que hace el indicador, la columna **Objetivo** indica el objeto de

mediad del indicador, el campo **Formula** indica los cálculos para obtener la medición se tiene en cuenta que la **frecuencia** de medición varía del control a evaluar, el **valor objetivo** permite definir el valor ideal, el **valor umbral** es el valor que cuando se está por debajo de él se debe de activar la alarmas para su revisión. Ver anexo 5 Gestión de indicadores

Ver anexo 6 Gestión de Indicadores

3.5 PROCEDIMIENTO REVISIÓN POR DIRECCIÓN:

La dirección de la organización se compromete a realizar revisiones del SGSI una vez al año, cuando existan cambios significativos en la organización que afecten la implementación del SGSI o cuando se presente algún incidente de seguridad de la información

1. Se debe de realizar mediante lo establecido en el proceso de auditorías internas, estas revisiones pueden ser parciales (procedimiento crítico) o totales
2. Se debe de realizar cuando exista algún cambio que afecte al Sistema de gestión de seguridad de información.
3. Se debe de especificar en la revisión:
4. La identificación de no conformidades
5. Seguimiento a las mediciones
6. Cambios en el contexto legal que rige el proceso involucrado en el alcance del SGSI
7. Se debe de generar un documento como evidencia de la revisión este debe de contener:
8. Proceso revisado
9. Resultados de la auditoria
10. En caso de encontrar no conformidades se debe de establecer acciones correctivas
11. Oportunidades de mejora del proceso evaluado

3.6 GESTIÓN DE ROLES Y RESPONSABILIDADES:

Las responsabilidades del sistema de gestión documental están a cargo de:

Gerencia General: Ser consultado en la elaboración dela política y realizar las revisiones a la misma.

Comité Directivo SGSI: Es un grupo compuesto por los líderes de áreas, el cual como función principal es la de redactar las políticas para la seguridad de la información, está encargado de dar apoyo a actividades como la definición de acuerdo de confidencialidad, aprobar revisiones externas a la seguridad de la información-

Propietarios de Activos: El la persona encargada del activo de información, la cual tiene como función principal resguardar los activos de información independiente en que medio se encuentre o como se reproduzca.

Dirección De Recursos Humanos: El líder del área de recursos humanos es responsable de las actividades concernientes a la gestión del talento humano antes, durante y después de la contratación

Dirección Jurídica: El departamento Jurídico es responsable de garantizar que la empresa cumple con las obligaciones legales y vigentes de acuerdo a lo dispuesto en el anexo A 18 de la norma ISO/IEC 27001:2013

Dirección de Auditoria: La dirección de auditoria es responsable de gestionar adecuadamente el acceso a los sistemas de información de la empresa.

Administrador Seguridad Información: Es la persona responsable de realizar la revisión a la política de seguridad de la información, tiene a cargo

Dirección de Compras: Es encargada de realizar los procesos de compras y debe de garantizar el tratamiento de la seguridad de la información que se establece con los proveedores.

Dirección de DTI: Esta encargada de hacer cumplir los controles relacionados con el desarrollo seguro, la gestión de cambios, los controles de las redes parte de los roles que desempeña revisar la ejecución de las copias se seguridad, atender las solicitudes para la gestión de accesos de los usuarios.

3.7 MATRIZ RACSI

Para definir los roles y responsabilidades de manera más específica se usa la matriz Racsi contra los controles del anexo A de la ISO 27001:2013, ver Anexo 7 Matriz Racsi

Variables:

R: Encargado: Es el encargado de rendir cuentas

A: Responsable: Es el responsable de realizar las actividades

C: Consultado: Participa en el sistema a través de aportes, orientación

I: Informado: Recibe información sobre la ejecución de los procesos y la calidad de estos

S: Soporte: Permite dar apoyo a los procesos

3.8 METODOLOGÍA DE ANÁLISIS DE RIESGOS

El objetivo de aplicar una metodología para el análisis de riesgos es identificar y valorar los riesgos a los cuales están expuestos los activos de información del proceso comercial de

Pollos Pachito, para llevar a cabo este análisis se va a utilizar la metodología de Magerit, la cual cuenta con las siguientes directrices:

1. Realizar inventarios de activos (Instalaciones, Hardware, Aplicación, Datos, Red, Servicios, Equipamiento Auxiliar)
2. Identificar dependencias de los activos
3. Valorar los activos, se debe definir las escalas de valoración.
4. Valoración de los activos sobre las dimensiones de seguridad (C: confidencialidad, I Integridad, Disponibilidad, A Autenticidad, T Trazabilidad)
5. Identificación de las amenazas que afectan los activos de información
6. Valorar las amenazas
7. Identificar el impacto potencial
8. Identificar el riesgo aceptable
9. Identificar el riego residual

4 Fase 3: Análisis de Riesgos

4.1 INTRODUCCIÓN

El análisis de riesgos permite identificar los activos de información con los cuales cuenta la organización a sí mismo a que amenazas están expuestos y determinar la eficacia de las controles buscando estimar el riesgo al cual está sometido el activo

4.2 ACTIVOS:

Los activos de información a analizar se agruparan de acuerdo a la metodología Magerit 3.0

4.3 TIPOS DE ACTIVOS:

De acuerdo a Magerit, existen diferentes tipos de activos, los cuales se relacionan a continuación:

Hardware: Equipos físicos que soportan directa o indirectamente la ejecución los servicios de la organización.

[SW] Aplicación: Procesos que han sido automatizados para optimizar el desempeño de tareas

[D] Datos: Información de la organización

[COM] Redes de comunicación: Medios de transporte de los datos

[S] Servicios: Servicio que cumple un requerimiento de los usuarios

[Media] Soporte de Almacenamiento: Dispositivos físicos que permiten el almacenamiento información

[AUX] Equipamiento auxiliar: Equipos que sirven de soporte al sistema de información pero no tienen relación directa con los datos

[P] Personal: Personas que están relacionadas con el sistema de información

Las anteriores definiciones se tomaron de “2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8.pdf”

Se identifican los activos y se registra en el anexo 9 análisis de riesgos hoja **activos**

VALORACIÓN	
MA	**MUY ALTO**
A	**ALTO**

4.4 VALORACIÓN DE ACTIVOS:

El valor de los activos se asigna de acuerdo a la premisa cuánto vale el activo para la organización si este no se encontrara en funcionamiento, para esto se califica de manera cualitativa según la directriz de Magerit 3.0 punto 2.1, la cual indica una escala con los siguientes valores según **tabla 6 Valoración de activos:**

M	**MEDIO**
B	**BAJO**
MB	**MUY BAJO**

Tabla 6 Valoración Activos

4.5 DEPENDENCIA ENTRE ACTIVOS

La dependencia de los activos es una manera jerárquica donde los activos que se encuentran en las partes superiores dependen de los activos que se encuentran por debajo de ellos, en línea con esta apreciación se puede decir que los riesgos de un activo puede aumentar de acuerdo a las dependencias que este tenga con otros

Se anexa la **Tabla 7 dependencia entre Activos**

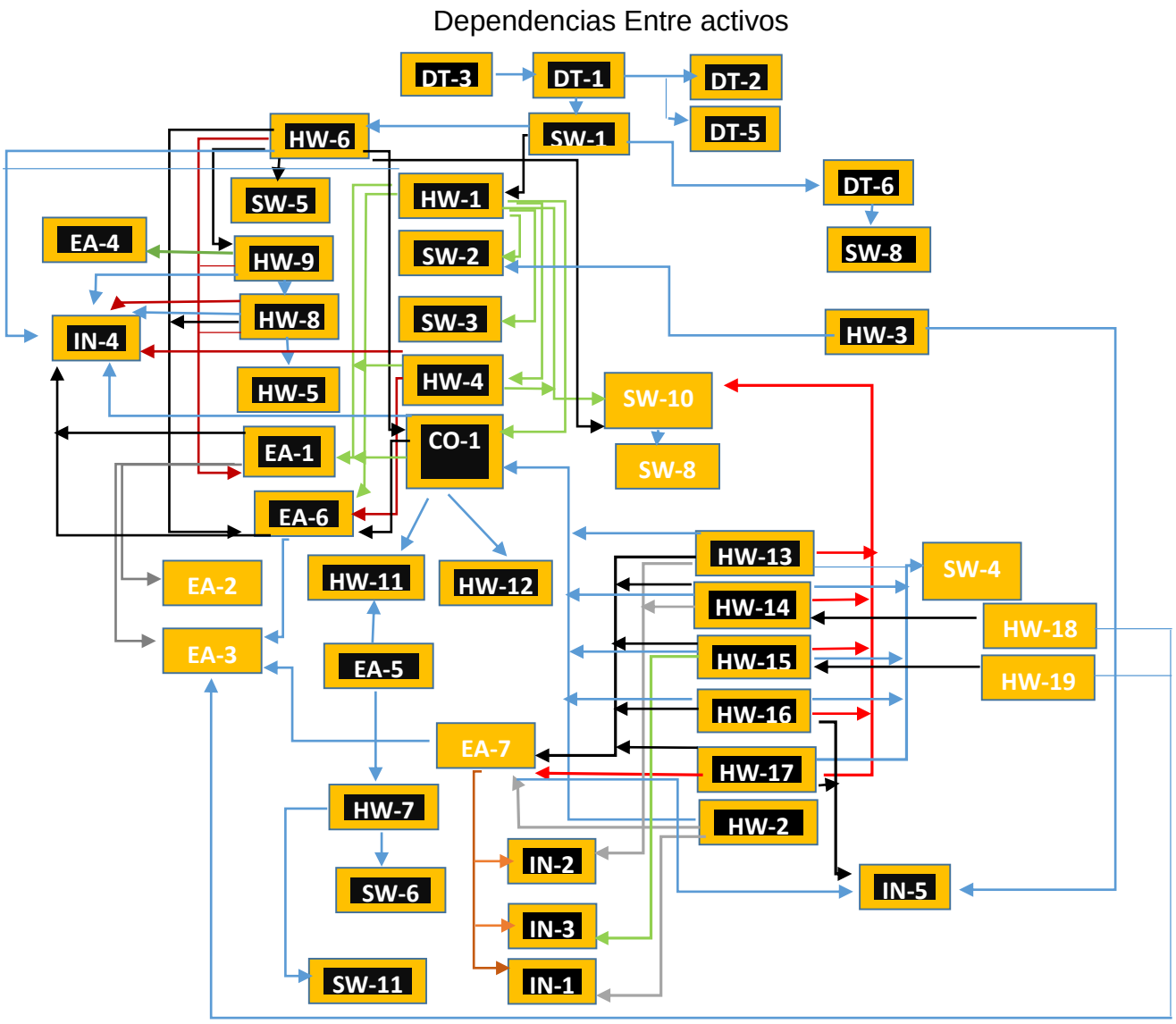


Tabla 7 dependencia entre Activos

4.6 DIMENSIONES DE SEGURIDAD

El valor de los activos se da de acuerdo a la valoración de las 5 dimensiones de seguridad de la información, busca identificar el valor de degradación del activo en cada una de sus dimensiones cuando una amenaza se materialice sobre el activo, las dimensiones son:

Disponibilidad: Propiedad de los activos de ser accedidos por el personal autorizado cuando se requiera.

Integridad: Característica de los activos la cual indica que los activos no pueden ser modificados por personal no autorizado

Confidencialidad: Propiedad de los activos de ser accedidos solo por el personal autorizado.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos

Trazabilidad: Forma de determina en cualquier momento quién hizo qué y en qué momento.

La valoración de las dimensiones de la seguridad de un activo se trata en valores, donde 5 es la degradación más alta, lo anterior de acuerdo a la tabla 8 degradaciones de activos

VALOR	CRITERIO
5	Degradación muy grave
4	Degradación grave
3	Degradación importante
2	Degradación menor
1	Sin Degradación o irrelevante

Tabla 8 Degradación de Activos

4.7 VALORACIÓN DE ACTIVOS SOBRE SUS DIMENSIONES

La valoración de los activos en cuanto al grado de degradación de las dimensiones de la seguridad se debe de realizar asignando a cada activo el impacto que sufriría el activo sobre la dimensión si este se expusiera a algún riesgo, para asignar un valor se toma los valores de la tabla 12, y se relaciona este valor a cada activo. Ver el anexo 10 análisis de riesgos hoja **Valoración Activos**

4.8 FRECUENCIA

Los activos están expuestos a amenazas estas se pueden presentar 1 o más veces en el año, este tiempo es la frecuencia, para valorar las amenazas se debe determinar la frecuencia de ocurrencia en que se puede presentar la amenaza, esta información es suministrada por los dueños de los activos y valorada según la tabla de frecuencias

Nro. Veces	Valor	Descripción
1 vez cada 1 semana	5	Muy Alta
1 Vez cada mes	4	Media
1 Vez cada trimestre	3	Baja
1 Vez Cada semestre	2	Muy Baja
1 Vez cada año	1	Insignificante

Tabla 9 Frecuencia

4.9 GESTIÓN DEL RIESGO

Para la valoración del riesgo se usa la tabla de Valoración de Activos sobre sus Dimensiones, pero a esta se le asigna la frecuencia, se promedia el impacto (Autenticidad, Confidencialidad, integridad, disponibilidad, trazabilidad) y se multiplica por la frecuencia, se toma los mayores impactos identificados así como la máxima frecuencia con que se pueda presentar un evento que pueda afectar al activo, posterior se asocia el valor del riesgo a una escala (ver tabla escala valoración del riesgo) para determinar la prioridad de su tratamiento

Prioridad	Descripción	Valor
MA	Muy Alta	>=16
A	Alta	>=9<16
M	Media	>=4<9
B	Baja	>=2<4
MB	Muy Baja	=1

Tabla 10 Valor del Riesgo

4.10 ANÁLISIS DE AMENAZAS

De acuerdo con la metodología de acuerdo al tipo de activo se valoran las amenazas, es decir los activos cuyo ámbito sean datos tienen asociadas las mismas amenazas, se califica el impacto que tiene al materializarse sobre el activo en cada una de las dimensionas de seguridad (Autenticidad, Confidencialidad, integridad, Disponibilidad, trazabilidad) ver anexo 11 análisis de riesgos hoja **amenazas**

4.11 RIESGO INTRÍNSECO

Con el objeto de identificar el riesgo intrínseco al cual está expuesto los activos de información, tomo los activos ya identificados, la frecuencia de ocurrencia y el impacto, con estos valores identifico el riesgo, en este caso riesgo intrínseco porque no se tiene en cuenta ninguna salvaguarda que minimice el impacto de ocurrencia y/o de degradación sobre las dimensiones de seguridad

Riesgo = Frecuencia X Impacto

Donde el impacto es el promedio de los impactos valorados en cada una de las dimensiones

El registró para la valoración del riesgo se realiza en el anexo 12 análisis de riesgos hoja **Intrínseco**

4.12 REPRESENTACIÓN DEL RIESGO INTRÍNSECO

Se anexa imágenes donde se evidencia el riesgo al que se encuentran expuestos los activos por tipo, donde se obtienen las siguientes conclusiones:

Para el tipo de activos Datos, la información almacenada en la base de datos requiere la implementación de controles debido a que la afectación de este activo implica un daño muy grave para la organización.

La ilustración 6, permite visualizar el riesgo intrínseco al tipo de activo Datos, en este se puede observar que el activo Información almacenada en base de datos es el que mayor riesgo genera para este tipo de activo, de la misma manera se representa a través de un mapa de calor (ver ilustración 7 Mapa de Calor Riesgo Intrínseco DATOS) este indica que los activos están expuestos a un riesgo muy critico

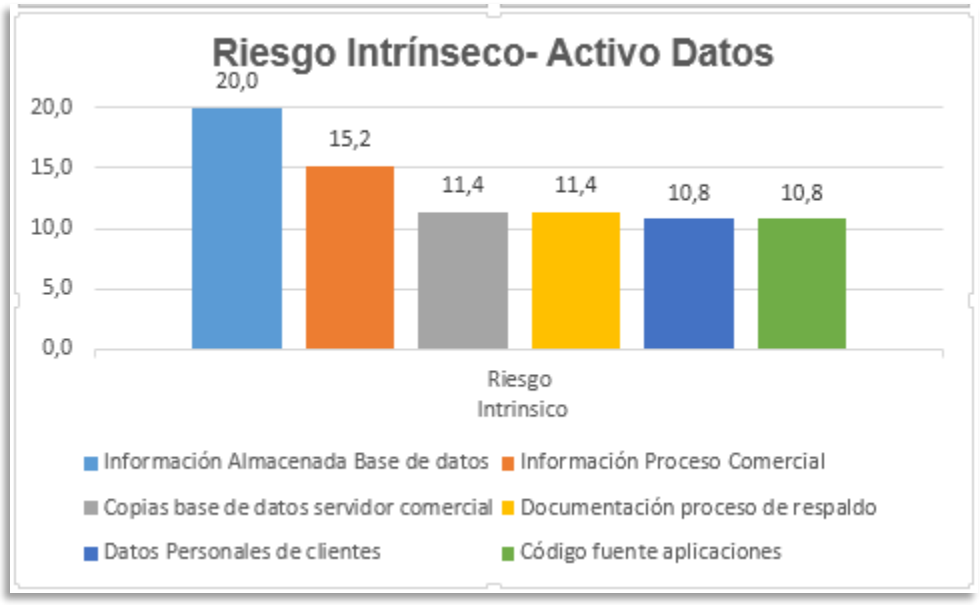


Ilustración 6 Riesgo Intrínseco DATOS

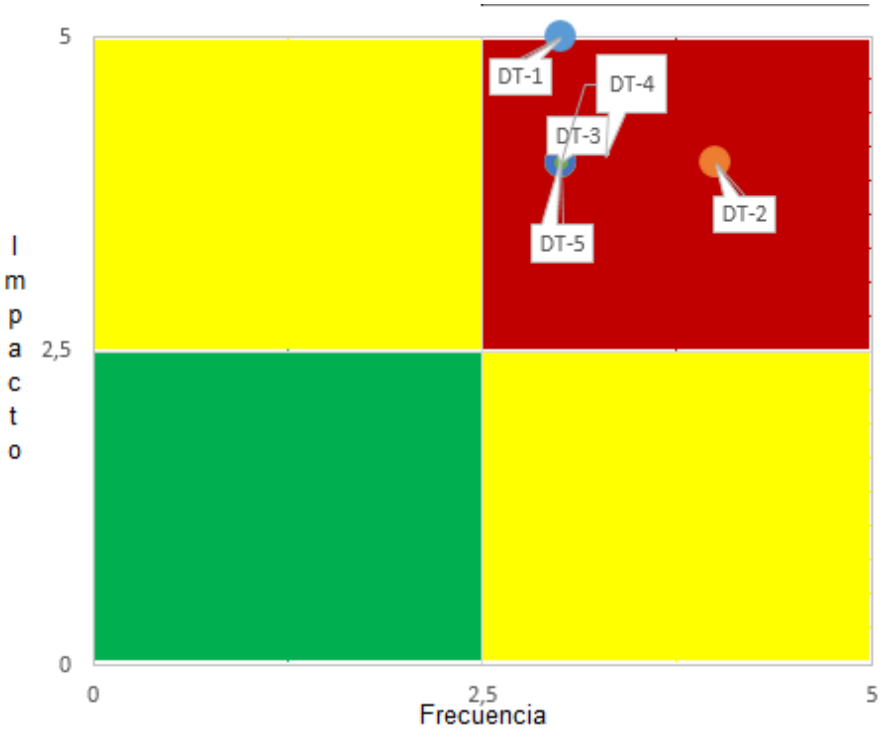


Ilustración 7 Mapa de Calor Riesgo Intrínseco DATOS

Para el tipo de activos equipamiento Auxiliar, el activo Suministro eléctrico es el activo más representativo.

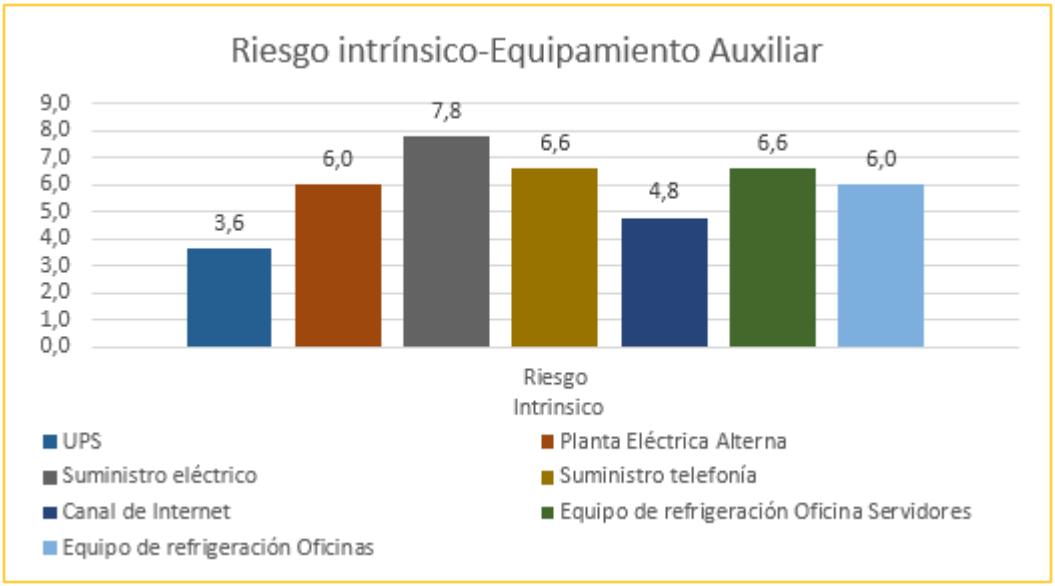


Ilustración 8 Riesgo Intrínseco EQUIPAMIENTO AUXILIAR

A través de un mapa de calor (ver ilustración 9 Mapa de Calor Riesgo Intrínseco Equipamiento Auxiliar) este indica que los activos están expuestos a un riesgo medio, que el servicio de suministro eléctrico es el único que entra en un estado critico

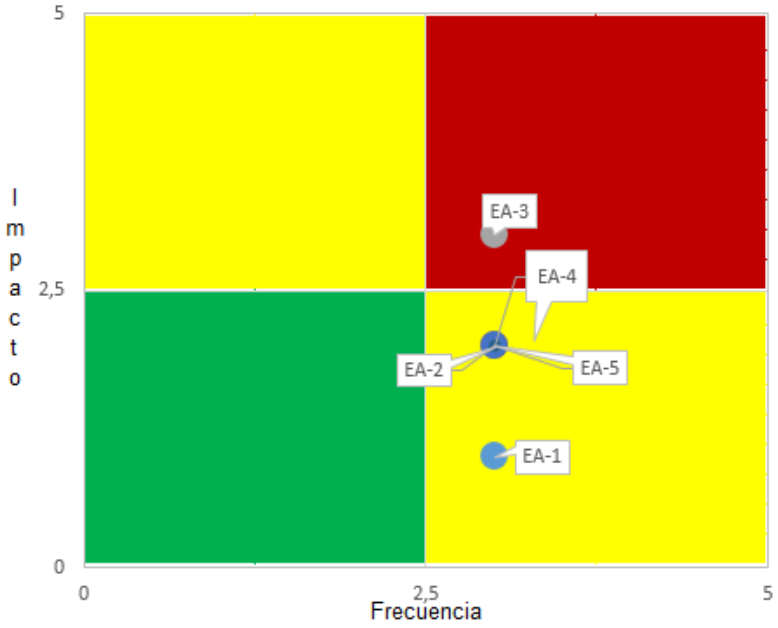


Ilustración 9 Mapa de Calor Riesgo Intrínseco EQUIPAMIENTO AUXILIAR

Para el tipo de activos Hardware, existen varios activos los cuales su afectación pueden ocasionar parálisis en los procesos los cuales soporta, como ejemplo están: El servidor comercial, los computadores del área de muelles, servidor de desarrollo, los cuales están por encima de la valoración Media y alta. Ver ilustración 10, de la misma manera, el mapa de calor (ver grafica 9) indica que gran porcentaje de los activos están en un riesgo crítico

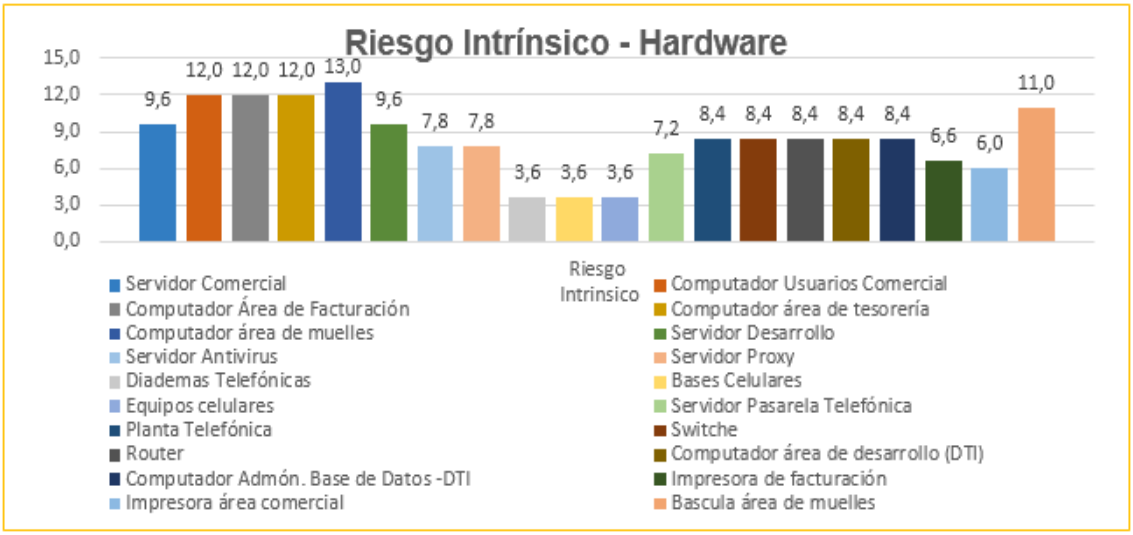


Ilustración 10 Riesgo Intrínseco HARDWARE

Grafica 8 Riesgo Intrínseco HARDWARE

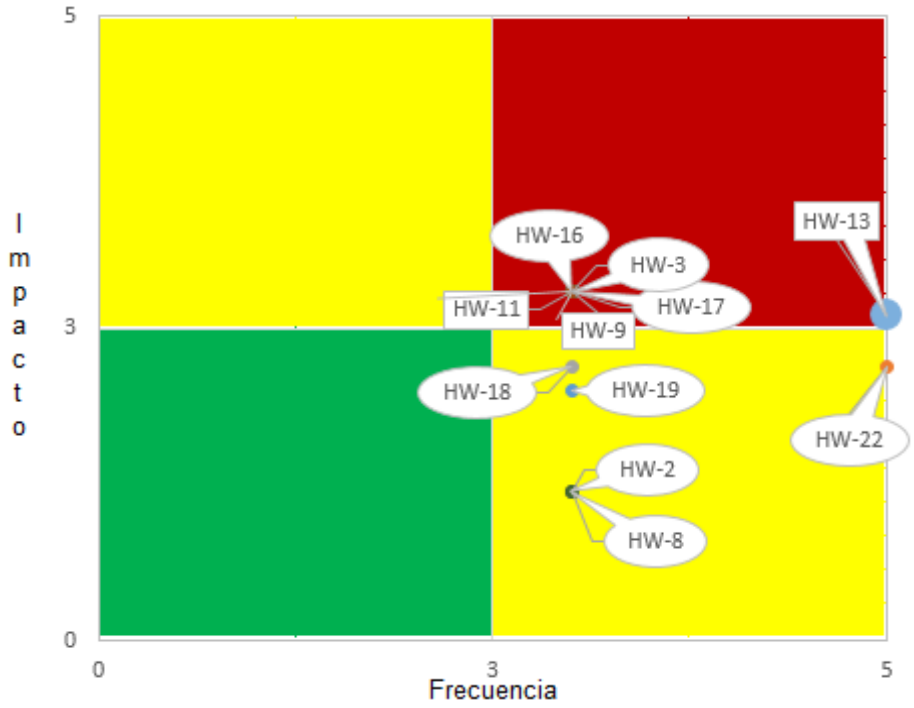


Ilustración 11Mapa de Calor Riesgo Intrínseco HARDWARE

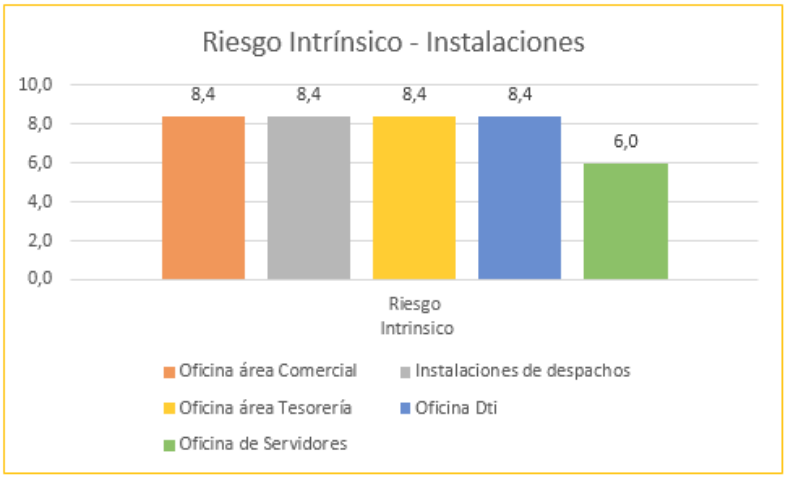


Ilustración 12 Riesgo Intrínseco INSTALACIONES

Para el tipo de activos Software, la aplicación comercial requiere de controles para su protección ya que la valoración de este da 10,2

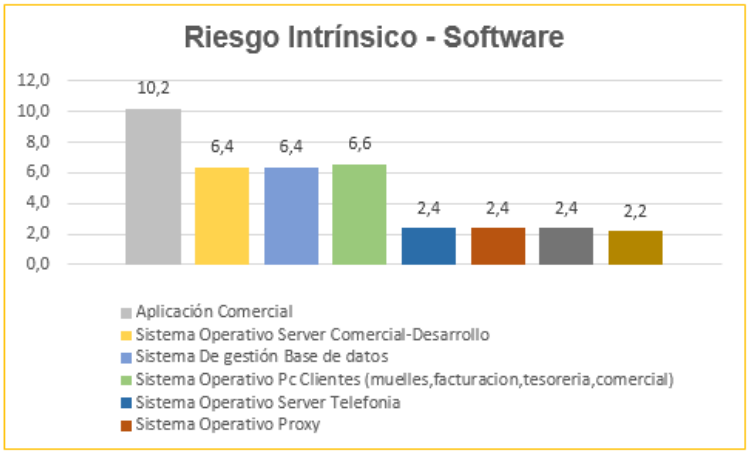


Ilustración 13 Riesgo Intrínseco SOFTWARE

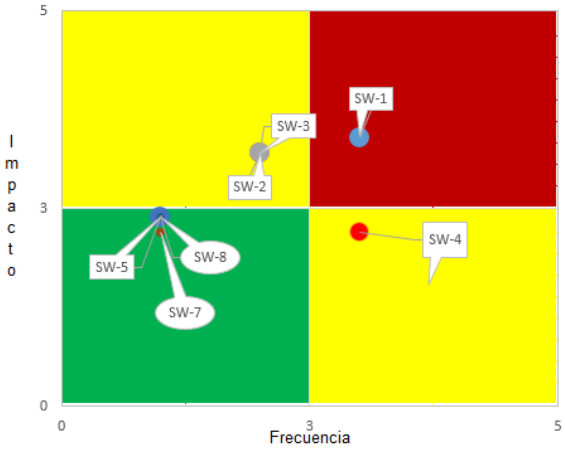


Ilustración 14 Mapa de Calor Riesgo Intrínseco SOFTWARE

4.13 SALVAGUARDAS

Las salvaguardas son las medidas que buscan proteger los activos de las amenazas,

4.14 EFICACIA DE SALVAGUARDAS

Para estimar el grado de eficacia de las amenazas se va a se estima la eficacia de acuerdo a la tabla 11 eficacia de las salvaguardas

Valor	Nivel	Significado
5	L1	Inexistente
4	L2	Inicial, es Reproducible pero Intuitivo
3	L3	Proceso definido, los procesos no son claros
2	L4	Gestionado y medible, existen procedimientos claros
1	L5	Optimizado, existen procedimientos claros el personal se encuentra capacitado y concientizado

Tabla 11 Eficacia de las salvaguardas

4.15 RIESGO RESIDUAL

El riesgo residual se define como la disminución del riesgo potencial sobre un activo a través de las salvaguardas, para el análisis se recalcula el riesgo a través del nuevo impacto y probabilidad de ocurrencia.

4.16 RIESGO ACEPTABLE

La empresa con el objeto de priorizar los planes de seguridad sobre los activos que están más expuestos opta por definir como riesgo aceptable a cada activo cuya nivel de valoración este como medio, bajo o muy bajo, todo activo cuya nivel de riesgo sea alta o muy alta, debe de establecer controles para su mitigación (ver Tabla 12 Criterio Riesgo Aceptable)

Valor Riesgo	Criterio	Aceptable (S/N)
1	Muy Bajo	S
4	Bajo	S
9	Medio	S
16	Alto	N
25	Muy Alto	N

Tabla 12 Criterio Riesgo Aceptable

El resultado de la valoración se resume en la siguiente tabla

Ver anexo 13 Análisis de riesgo aceptable

Act	Control	Frecuencia Nueva	Eficacia	Impacto Nuevo	Riesgo Residual	Criterio	Riesgo Aceptable
DT-1	**S DT-1 - Copias de Seguridad**	**4**	**L4**	**2**	**8,0**	M	SI
DT-2	S DT-2 - Acuerdos de Confidencialidad	**4**	**L3**	**3**	**12,0**	A	NO
DT-3	S DT-3 Proceso de Verificación y retiro de la copia	**3**	**L3**	**3**	**9,0**	A	NO
DT-4	DT-4 Documentación proceso de respaldo	**3**	**L5**	**1**	**3,0**	B	SI
DT-5	S DT-5 acuerdos de confidencialidad	**3**	**L3**	**3**	**9,0**	M	SI
DT-6	Sin Salvaguarda	**3**	**L5**	**1**	**3,0**	B	SI
EA-1	S EA-1 Filtros eléctricos	**3**	**L5**	**1**	**3,0**	B	SI
EA-2	S EA-2 Mantenimiento preventivo	**3**	**L4**	**2**	**6,0**	M	SI
EA-3	Sin Salvaguarda	**3**	**L5**	**1**	**3,0**	B	SI
EA-4	S EA-3 Uso de celulares	**3**	**L4**	**2**	**6,0**	M	SI
EA-5	Sin Salvaguarda	**4**	**L4**	**2**	**7,2**	M	SI
EA-6	Sin Salvaguarda	**3**	**L4**	**2**	**6,6**	M	SI
EA-7	EA-7 Equipo de refrigeración Oficinas	**3**	**L4**	**2**	**6,0**	M	SI
IN-1	IN-1 Oficina área Comercial	**3**	**L3**	**3**	**8,4**	M	SI
IN-2	IN-2 Instalaciones de despachos	**3**	**L3**	**3**	**8,4**	M	SI
IN-3	IN-3 Oficina área Tesorería	**3**	**L3**	**3**	**8,4**	M	SI
IN-4	IN-5 Oficina Dti	**3**	**L3**	**3**	**8,4**	M	SI
IN-5	IN-4 Oficina de Servidores	**2**	**L3**	**3**	**6,0**	M	SI
HW-1	S HW-1 Servidor Contingencia	**3**	**L2**	**4**	**12,0**	A	NO
HW-2	S HW-2 Computador de contingencia	**5**	**I4**	**2**	**10,0**	A	NO
HW-14	S HW-3 Computador de contingencia	**5**	**I4**	**2**	**10,0**	A	NO
HW-15	S HW-4 Computador área de Contingencia	**5**	**I4**	**2**	**10,0**	A	NO
HW-13	HW-13 Computador área de muelles	**5**	**L4**	**2**	**10,0**	A	NO
HW-3	HW-3 Servidor Desarrollo	**4**	**L3**	**3**	**12,0**	A	NO
HW-4	HW-4 Servidor Antivirus	**3**	**L3**	**3**	**7,8**	M	SI
HW-22	HW-22 Servidor Proxy	**3**	**L3**	**3**	**7,8**	M	SI
HW-5	S HW-5 Teléfonos	**3**	**L5**	**1**	**3,0**	B	SI
HW-8	S HW-8 Celulares	**3**	**L5**	**1**	**3,0**	B	SI
HW-2	S HW-2 Equipos celulares Contingencia	**3**	**L5**	**1**	**3,0**	B	SI
HW-6	HW-6 Servidor Pasarela Telefónica	**3**	**L3**	**3**	**10,2**	A	NO
HW-9	HW-9 Planta Telefónica	**3**	**L2**	**4**	**12,0**	A	NO
HW-11	HW-11 Switche	**3**	**L3**	**3**	**8,4**	M	SI
HW-3	HW-3 Router	**3**	**L3**	**3**	**8,4**	M	SI
HW-16	HW-16 Computador área de desarrollo (DTI)	**3**	**L3**	**3**	**8,4**	M	SI
HW-17	HW-17 Computador Admón. Base de Datos -DTI	**3**	**L3**	**3**	**8,4**	M	SI
HW-18	S HW-18 Impresora de facturación	**3**	**L4**	**2**	**6,0**	M	SI
HW-19	HW-19 Impresora área comercial	**3**	**L5**	**1**	**3,0**	B	SI
HW-22	HW-2 Bascula área de muelles	**5**	**L5**	**1**	**5,0**	M	SI
SW-1	S SW-1 Copia de Aplicación Comercial	**3**	**L4**	**2**	**6,0**	M	SI
SW-2	S SW-2 Medios disponibles	**2**	**L3**	**3**	**6,0**	M	SI
SW-3	S SW-3 Medios disponibles	**2**	**L3**	**3**	**6,0**	M	SI
SW-4	S SW-4 Medios disponibles	**3**	**L5**	**1**	**3,0**	B	SI
SW-5	SW-5 Sistema Operativo Server Telefonía	**1**	**L5**	**1**	**2,4**	B	SI

SW-6	S SW-6 Imagen disponible	**1**	**I4**	**2**	**2,0**	B	SI
SW-8	SW-8 Sistema Operativo Antivirus	**1**	**L1**	**1**	**2,4**	B	SI
SW-7	S SW-7 Medios disponibles	**1**	**L4**	**2**	**2,0**	B	SI
ME-1	ME-1 Disco duro externo para copias de servidores	**1**	**L5**	**1**	**1,0**	MB	SI
CO-1	CO-1 Red Lan	**4**	**L4**	**2**	**8**	M	NO
PE-1	PE-1 Personal de backup	**4**	**L5**	**1**	**4,0**	B	SI
PE-2	PE-2 Personal de backup	3	L5	1	3,0	B	SI
PE-3	PE-3 Administrador Base de datos -DTI	**3**	**L5**	**1**	**3,0**	B	SI
PE-4	PE-4 Personal Área comunicaciones -DTI	**1**	**L5**	**1**	**1,0**	MB	SI
PE-6	PE-6 Personal Soporte Informática- DTI	**1**	**L5**	**1**	**1,0**	MB	SI
PE-5	PE-5 Matriz de Proveedores	**1**	**L5**	**1**	**1,0**	MB	SI

Tabla 13 Valoración del riesgo

4.17 CONCLUSIONES:

Para determinar una comparación entre el riesgo intrínseco y el riesgo residual se toma el activo Información almacenada Base de datos se puede evidenciar que el riesgo sin salvaguardas tomo un valor de 20 (Muy alto), pero con salvaguardas tomo un valor de 8 (Medio)

Cod	Activo	Frecuencia	A	C	I	D	T	Impacto	Riesgo Intrínseco
DT-1	Información Almacenada Base de datos	4	5	5	5	5	5	5	20,0
DT-2	Información Proceso Comercial	4	4	4	4	4	3	3,8	15,2

Tipo	Act	Control	Frecuencia Nueva	Eficac	Impacto Nuevo	Riesgo Residual	Criter	Riesgo Acept
Datos	DT-1	S DT-1 - Copias de Seguridad	4	L4	2	8,0	M	SI

Tabla 14Comparación Riesgo Intrínseco vs Residual Activo DT-1

4.18 REPRESENTACIÓN DEL RIESGO INTRÍNSECO VS RESIDUAL

A través de la ilustración 15 se puede observar que los controles minimizan el impacto que generan las amenazas sobre las vulnerabilidades, ejemplo el riesgo inicial para el activo Información almacenada en base de datos tenía una riesgo de 20 al implementar controles su nuevo riesgo (riesgo residual) quedo en 12

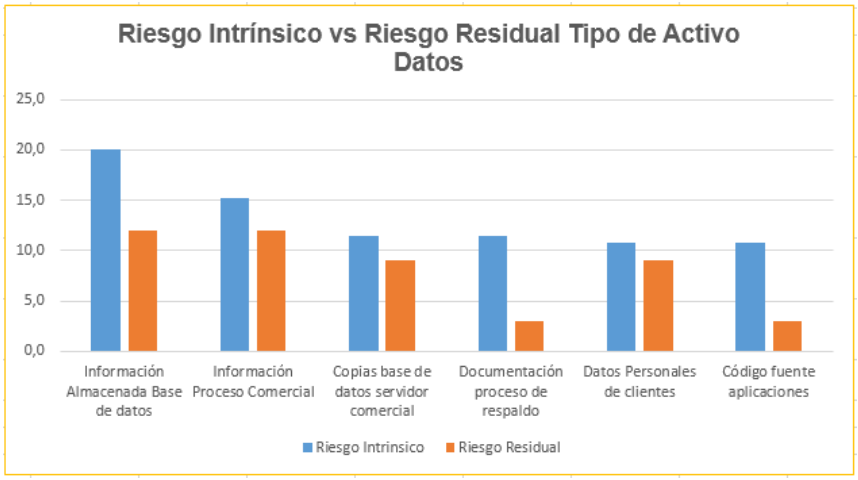


Ilustración 15 Riesgo Intrínseco VS Riesgo Residual ACTIVO DATOS

La ilustración 28 permite visualizar un activo (suministro eléctrico) con una disminución representativa, pero los demás activos no representan una disminución representativa.

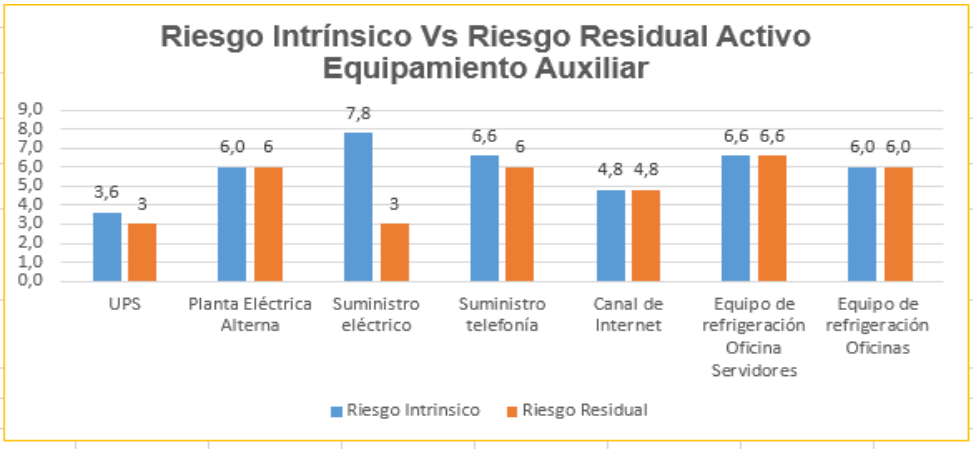


Ilustración 16 Riesgo Intrínseco VS Riesgo Residual EQUPAMIENTO AUXILIAR

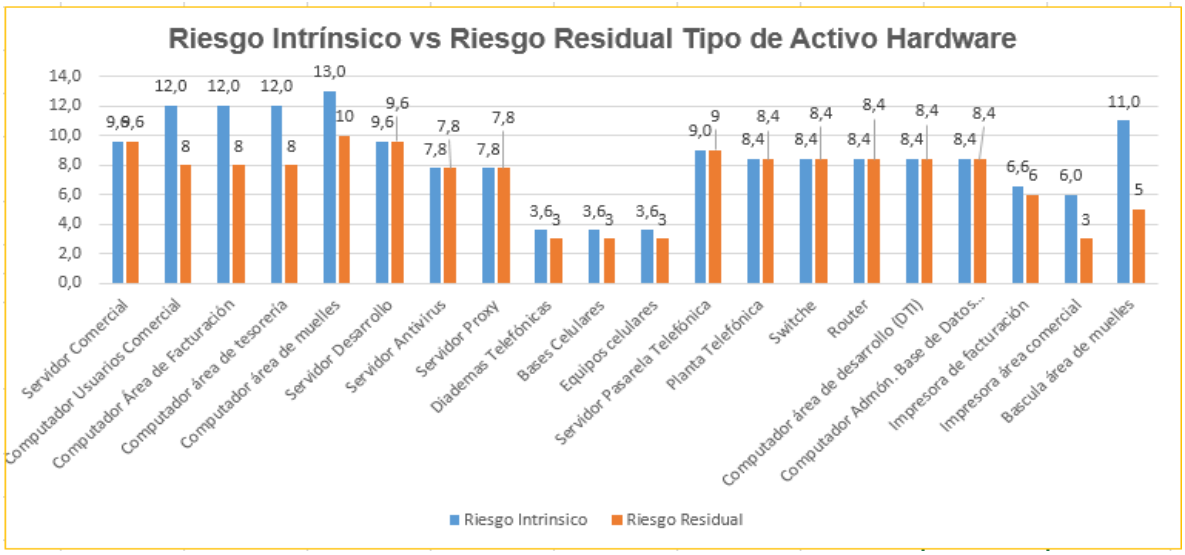


Ilustración 17 Riesgo Intrínseco VS Riesgo Residual HARDWARE

5 Propuestas

5.1 INTRODUCCIÓN

Las propuestas o planes de seguridad, es el proceso a seguir posterior a la identificación del riesgo residual y con el objeto tratar los riesgos como no aceptables, esta fase cuenta con tres pasos en línea de acuerdo a las directrices de la Versión 3 de Magerit Metodología de análisis y gestión de riesgos de los sistemas de información, estos pasos son:

1. Identificación de proyectos de seguridad
2. Plan de ejecución
3. Ejecución

5.2 IDENTIFICACIÓN DE PROYECTOS DE SEGURIDAD

Como objeto tiene implementar o aumentar la eficacia de las salvaguardas existentes a través de un programa de seguridad, este es en sí una agrupación de tareas que tienen un objetivo común, el programa tiene en cuenta los costes estimados de adquisición de productos, contratación de servicios, capacitación, tiempos de ejecución, para obtener el listado de proyectos a implementar es necesario identificar los activos cuyo riesgo no es aceptable (ver Tabla 14 Valoración del riesgo Riesgo Aceptable) para de acuerdo a estos se identifiquen los planes de seguridad a implementar o reforzar (Tabla 15 Proyectos de seguridad)

Act	Control	Frecuencia Nueva	Eficacia	Impacto Nuevo	Riesgo Residual	Criterio	Riesgo Aceptable
HW-1	S HW-1 Servidor Contingencia	3	L2	4	12,0	A	NO
HW-2	S HW-2 Computador de contingencia	5	I4	2	10,0	A	NO
HW-14	S HW-3 Computador de contingencia	5	I4	2	10,0	A	NO
HW-15	S HW-4 Computador área de Contingencia	5	I4	2	10,0	A	NO
HW-13	HW-13 Computador área de muelles	5	L4	2	10,0	A	NO
HW-3	HW-3 Servidor Desarrollo	4	L3	3	12,0	A	NO
HW-6	HW-6 Servidor Pasarela Telefónica	3	L3	3	10,2	A	NO
HW-9	HW-9 Planta Telefónica	3	L2	4	12,0	A	NO
DT-2	S DT-2 - Acuerdos de Confidencialidad	4	L3	3	12,0	A	NO

Tabla 15 Valoración del riesgo Aceptable

Cód. Salvaguarda	Descripción	Activo Protege
PS-1	Server Contingencia Proceso Comercial-Desarrollo	HW-1 Servidor Comercial HW-3 Servidor Desarrollo
PS-2	Server Pasarela Telefónica	HW-6 Servidor Pasarela Telefónica
PS-3	Computador Backup	HW-2 Computador Usuarios Comercial HW-14 Computador Área de Facturación HW-15 Computador área de tesorería HW-13 Computador área de muelles
PS-4	Tarjeta de Planta Telefónica	HW-9 Planta Telefónica
PS-5	Acuerdos De Confidencialidad	DT-2 Información Proceso Comercial
PS--6	Sistema de Cifrado	DT-1 Información Almacenada Base de datos
PS--7	Concientización importancia revisión de políticas	Proceso de implementación SGSI -Políticas

Tabla 16 Proyectos de Seguridad

Se anexa las siguientes tablas, las cuales presentan el programa de implementación de cada proyecto de seguridad, está organizado de la siguiente manera:

El campo objetivo indica a que activo o control se le va a establecer el plan de seguridad

El campo nuevo impacto, es el impacto estimado si se materializan las amenazas sobre el activo posterior a la implementación de la salvaguarda.

El campo valor riesgo esperado, es el nuevo valor que se espera que tenga activo a proteger o el control a cumplir

El campo indicador: permite el cumplimiento del programa de seguridad

El campo valor: indica el costo que vale implementar la salvaguarda

Se destinó un campo para actividades donde se encuentra la actividad, la fecha de compromiso y el responsable.

Salvaguarda		PS-1			
Descripción - Objetivo		Server Contingencia para los procesos de Comercial-Desarrollo			
Activos a proteger	HW-1 Servidor Comercial HW-3 Servidor Desarrollo	Indicador	Cumplimiento=Ejecución de actividades / Nro. de Actividades		
Valor	$5000000	Nuevo Impacto	2.0	Valor Riesgo Esperado	6 8

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Adquirir Equipo de Respaldo	18/05/15	21/05/15	3	Dirección DTI
Presentación de cotizaciones (equipo, licencia Sist...	18/05/15	19/05/15	1	Oficial de Seguridad
Viabilización de orden de compra	19/05/15	20/05/15	1	Dirección DTI
Adquisición Equipo	20/05/15	21/05/15	1	Dirección DTI
Configuracion y Pruebas	21/05/15	26/05/15	3	Oficial de Seguridad
Configuración de equipo	21/05/15	22/05/15	1	Oficial de Seguridad
Coordinar Pruebas	22/05/15	23/05/15	1	Oficial de Seguridad
Pruebas	25/05/15	26/05/15	1	Oficial de Seguridad
Simulaciones	25/05/15	26/05/15	1	Oficial de Seguridad
Socializar Contingencia	26/05/15	1/06/15	4	Oficial de Seguridad
Elaboración de Manual proceso de restauración	26/05/15	27/05/15	1	Oficial de Seguridad
Revisión de Manual por Dirección de DTI	27/05/15	28/05/15	1	Dirección DTI
Socialización Contingencia	29/05/15	1/06/15	1	Dirección DTI

Tabla 17 Proyectos de Seguridad PS-1

Salvaguarda		PS-2			
Descripción - Objetivo		Server Pasarela Telefónica			
Activos a proteger	HW-6 Servidor Pasarela Telefónica	Indicador	Cumplimiento=Ejecución de actividades / Nro. de Actividades		
Valor	$3200000	Nuevo Impacto	1.0	Valor Riesgo Esperado	3.0

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Adquirir Equipo de Respaldo	18/05/15	21/05/15	3	Dirección DTI
Presentación de cotizaciones (equipo, licencias)	18/05/15	19/05/15	1	Auxiliar Administrativo
Viabilización de orden de compra	19/05/15	20/05/15	1	Dirección DTI
Adquisición Equipo	20/05/15	21/05/15	1	Dirección DTI
Configuracion y Pruebas	21/05/15	26/05/15	3	Servidor, Coordinador de Redes
Configuración de equipo	21/05/15	22/05/15	1	Oficial de Seguridad
Coordinar Pruebas	22/05/15	23/05/15	1	Coordinador de Redes
Pruebas	25/05/15	26/05/15	1	Coordinador de Redes
Simulaciones	25/05/15	26/05/15	1	Coordinador de Redes
Socializar Contingencia	1/05/15	29/05/15	20	Oficial de Seguridad
Elaboración de Manual proceso de restauración	27/05/15	29/05/15	2	Coordinador de Redes
Revisión de Manual por Dirección de DTI	1/05/15	2/05/15	1	Dirección DTI
Socialización Contingencia	4/05/15	5/05/15	1	Coordinador de Redes

Tabla 18 Proyectos de Seguridad PS-2

Salvaguarda		PS-3			
Descripción - Objetivo		Computador Contingencia Procesos Usuarios			
Activos a proteger	HW-2 Computador Usuarios Comercial HW-14 Computador Área de Facturación HW-15 Computador área de tesorería HW-13 Computador área de muelles	Indicador	Cumplimiento=Ejecución de actividades / Nro. de Actividades		
Valor	$1.300.000	Nuevo Impacto	1.0	Valor riesgo esperado	5.0

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Adquirir Equipo de Respaldo	2/06/15	9/06/15	5	Dirección DTI
Presentación de cotizaciones (equipo, licencias)	2/06/15	3/06/15	1	Auxiliar Administrativo
Viabilización de orden de compra	3/06/15	4/06/15	1	Dirección DTI
Adquisición Equipo	8/06/15	9/06/15	1	Dirección DTI
Configuracion y Pruebas	10/06/15	24/06/15	10	Oficial de Seguridad
Configuración de equipo	10/06/15	11/06/15	1	Oficial de Seguridad
Coordinar Pruebas	16/06/15	17/06/15	1	Oficial de Seguridad
Realizar Pruebas	17/06/15	24/06/15	5	Oficial de Seguridad
Simulaciones	17/06/15	18/06/15	1	Oficial de Seguridad
Socializar Contingencia	29/06/15	4/07/15	5	Oficial de Seguridad
Elaboración de Manual proceso de restauración	29/06/15	30/06/15	1	Oficial de Seguridad
Revisión de Manual por Dirección de DTI	1/07/15	2/07/15	1	Dirección DTI
Socialización Contingencia	3/07/15	4/07/15	1	Oficial de Seguridad

Tabla 19 Proyectos de Seguridad PS

Salvaguarda		PS-4			
Descripción - Objetivo		Repuesto Contingencia Tarjeta de Planta Telefónica			
Activos a proteger	HW-9 Planta Telefónica	Indicador	Cumplimiento=Ejecución de actividades / Nro. de Actividades		
Valor	$1.300.000	Nuevo Impacto	2.0	Valor riesgo esperado	6

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Adquirir Tarjeta de Respaldo	8/06/15	11/06/15	3	Coordinador de Redes
Presentación de cotizaciones	8/06/15	9/06/15	1	Auxiliar Administrativo
Viabilización de orden de compra	9/06/15	10/06/15	1	Dirección DTI
Adquisición Equipo	10/06/15	11/06/15	1	Dirección DTI
Configuracion y Pruebas	15/06/15	25/06/15	8	Coordinador de Redes
Configuración de Tarjeta en planta	15/06/15	17/06/15	2	Coordinador de Redes
Coordinar Pruebas	17/06/15	18/06/15	1	Coordinador de Redes
Realizar Pruebas	18/06/15	25/06/15	5	Coordinador de Redes
Simulaciones	18/06/15	19/06/15	1	Coordinador de Redes
Socializar Contingencia	25/06/15	27/06/15	2	Coordinador de Redes
Elaboración de Manual proceso de restauración	25/06/15	26/06/15	1	Coordinador de Redes
Revisión de Manual por Dirección de DTI	26/06/15	27/06/15	1	Dirección DTI
Socialización Contingencia	26/06/15	27/06/15	1	Coordinador de Redes

Tabla 20 Proyectos de Seguridad PS-4

Salvaguarda		PS-5	
Descripción - Objetivo		Buscar medidas legales para evitar la fuga de información	
Activos a proteger	DT-2 Información Proceso Comercial	Indicador	Cumplimiento=Ejecución de actividades / Nro. de Actividades
Valor	$3000.000	Nuevo Impacto	3.0

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Revisión acuerdos de confidencialidad	1/07/15	23/07/15	16	Dirección Juridico
Identificar normatividad vigente	1/07/15	3/07/15	2	Dirección Juridico
Revisión procedimientos disciplinarios	3/07/15	4/07/15	1	Dirección Juridico
Definir nuevos procedimientos disciplinarios	6/07/15	7/07/15	1	Dirección DTI
Aprobación por la gerencia	15/07/15	16/07/15	1	Gerente
Publicación de nueva normatividad	17/07/15	18/07/15	1	Dirección Juridico
Socialización de la nueva normatividad	22/07/15	23/07/15	1	Dirección Juridico

Tabla 21 Proyectos de Seguridad PS-5

Salvaguarda		PS-6			
Descripción - Objetivo		Sistema de Cifrado			
Activos a proteger	Cumplimiento Anexo A 10.1.1, 10.1.2 Controles criptográficos	Indicador	Nro. Sistemas con cifrado de datos/ Nro. de sistemas		
Valor	$6000.000	Nuevo Impacto	1.0	Madurez esperada	Administrado

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Implementación Sistema de Cifrado	18/05/15	26/05/15	6	Dirección DTI
Identificación de sistema de cifrado	18/05/15	20/05/15	2	Coordinador de Desarrollo
Selección de metodo de cifrado	20/05/15	21/05/15	1	Coordinador de Desarrollo
Pruebas para validar fortaleza de cifrado	21/05/15	22/05/15	1	Coordinador de Desarrollo
Pruebas para implementación en codigo fuente	22/05/15	23/05/15	1	Coordinador de Desarrollo
Implementación	25/05/15	26/05/15	1	Coordinador de Desarrollo

Tabla 22 Proyectos de Seguridad PS-6

Salvaguarda		PS-7			
Descripción - Objetivo		Garantizar apoyo en la revisión de las políticas			
Activos a proteger	Cumplimiento Anexo A 5.1.2 Revisión de la política de seguridad de la información	Indicador	Cumplimiento=Nro. De políticas revisadas/ Nro. de políticas existentes		
Valor	$600.000	Nuevo Impacto	1.0	Madurez esperada	Administrado

Nombre	Fecha de inicio	Fecha de fin	Duración	Coordinador
Revisión Políticas SI	18/05/15	26/05/15	6	Dirección DTI
Presentar Analisis de riesgos a alta Gerencia	18/05/15	20/05/15	2	Oficial de Seguridad, Dirección DTI
Exponer necesidades por lo que se requiere la revisión	20/05/15	21/05/15	1	Oficial de Seguridad
Definir interalos de revisión	21/05/15	22/05/15	1	Dirección Juridico
Capacitar a la altra gerencia	22/05/15	23/05/15	1	Oficial de Seguridad
Aprobación por la gerencia	25/05/15	26/05/15	1	Gerente

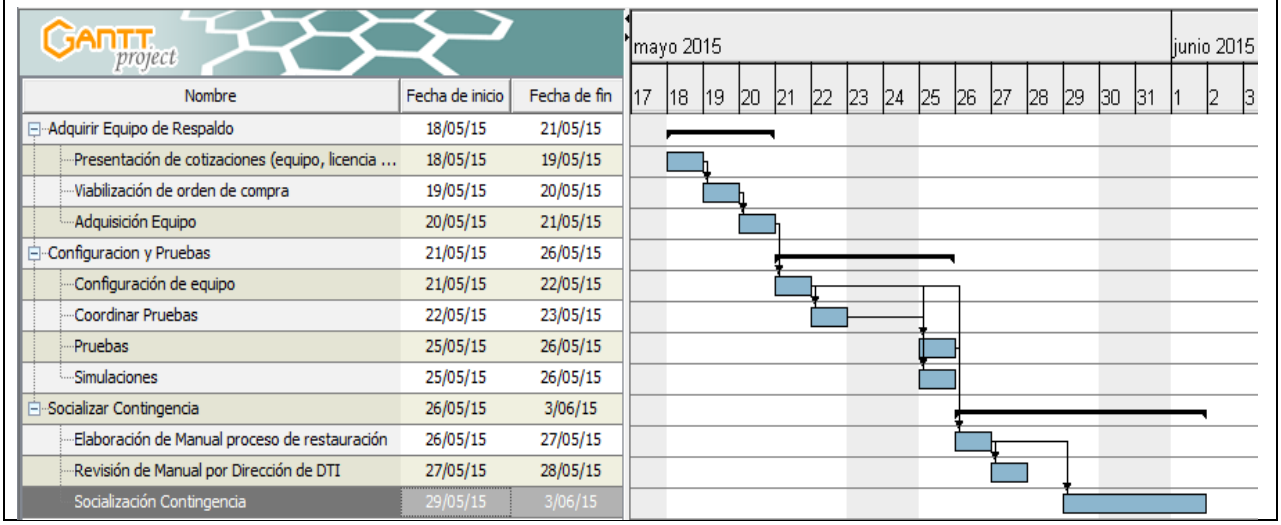
Tabla 23 Proyectos de Seguridad PS-5

5.3 PLAN DE EJECUCIÓN

El objetivo es determinar la prioridad para ejecutar los planes de seguridad, como el activo HW-1 Servidor Comercial HW-3 Servidor Desarrollo, tiene un alto riesgo y de este depende el proceso comercial, por lo anterior se debe de comenzar con establecer controles para mitigar el riesgo de este activo.

Se establece los siguientes diagramas para determinar las programaciones de los diferentes planes de seguridad establecidos

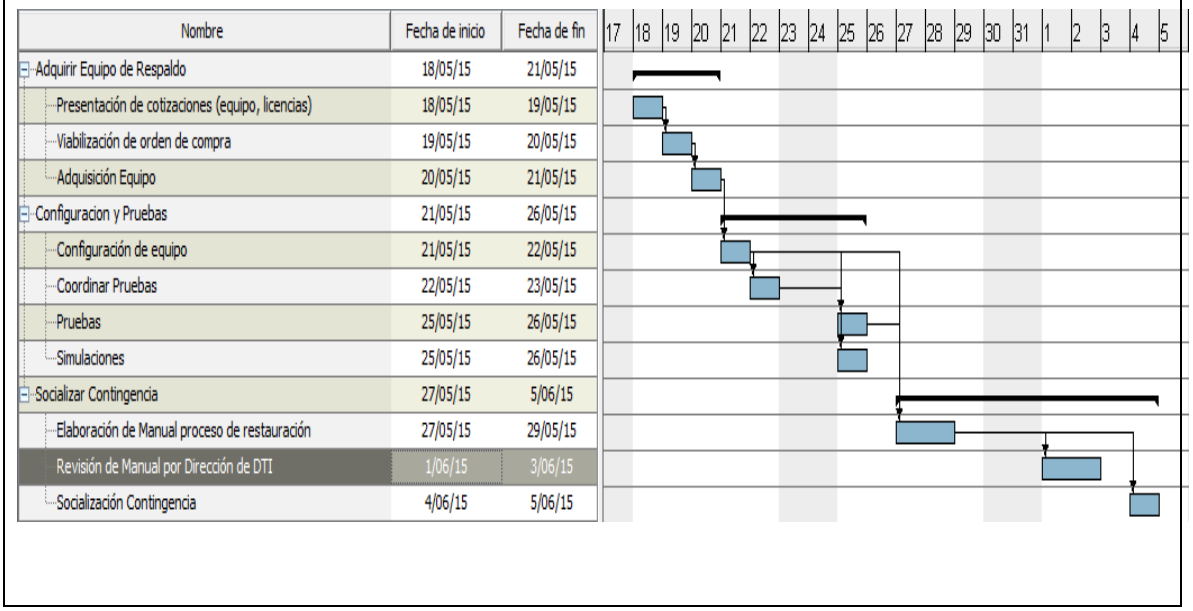
Salvaguarda	PS-1
Descripción - Objetivo	Server Contingencia para los procesos de Comercial-Desarrollo



Nombre	Fecha de inicio	Fecha de fin
Adquirir Equipo de Respaldo	18/05/15	21/05/15
Presentación de cotizaciones (equipo, licencia ...	18/05/15	19/05/15
Viabilización de orden de compra	19/05/15	20/05/15
Adquisición Equipo	20/05/15	21/05/15
Configuracion y Pruebas	21/05/15	26/05/15
Configuración de equipo	21/05/15	22/05/15
Coordinar Pruebas	22/05/15	23/05/15
Pruebas	25/05/15	26/05/15
Simulaciones	25/05/15	26/05/15
Socializar Contingencia	26/05/15	3/06/15
Elaboración de Manual proceso de restauración	26/05/15	27/05/15
Revisión de Manual por Dirección de DTI	27/05/15	28/05/15
Socialización Contingencia	29/05/15	3/06/15

Tabla 24 Diagrama de Gantt PS-1

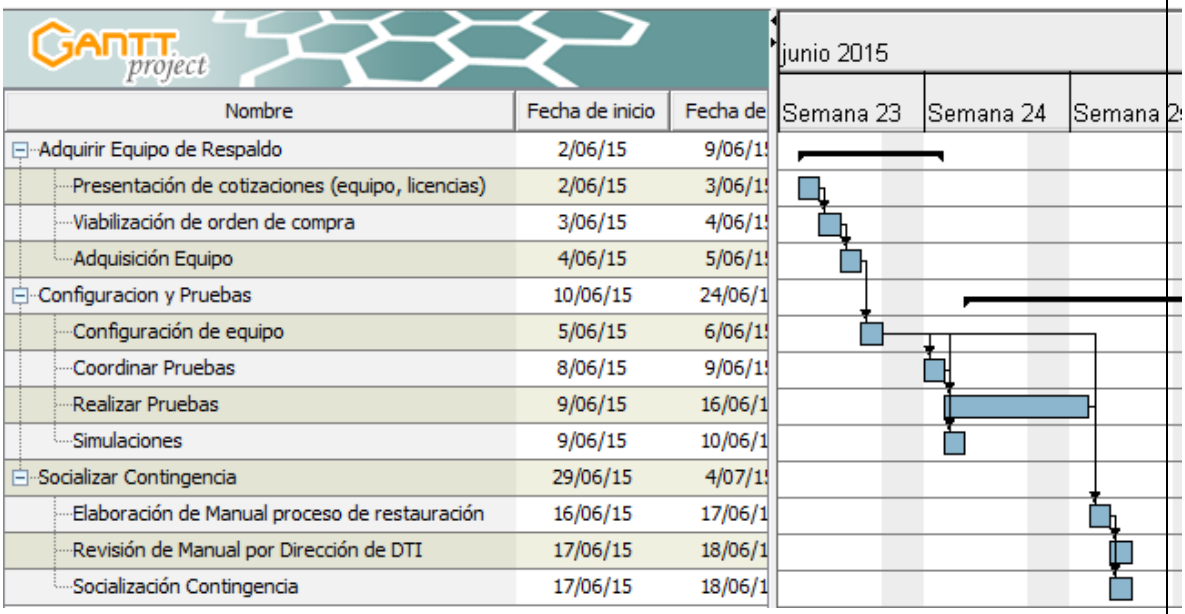
Salvaguarda	PS-2
Descripción - Objetivo	Server Pasarela Telefónica



Nombre	Fecha de inicio	Fecha de fin
Adquirir Equipo de Respaldo	18/05/15	21/05/15
Presentación de cotizaciones (equipo, licencias)	18/05/15	19/05/15
Viabilización de orden de compra	19/05/15	20/05/15
Adquisición Equipo	20/05/15	21/05/15
Configuracion y Pruebas	21/05/15	26/05/15
Configuración de equipo	21/05/15	22/05/15
Coordinar Pruebas	22/05/15	23/05/15
Pruebas	25/05/15	26/05/15
Simulaciones	25/05/15	26/05/15
Socializar Contingencia	27/05/15	5/06/15
Elaboración de Manual proceso de restauración	27/05/15	29/05/15
Revisión de Manual por Dirección de DTI	1/06/15	3/06/15
Socialización Contingencia	4/06/15	5/06/15

Tabla 25 Diagrama de Gantt PS-2

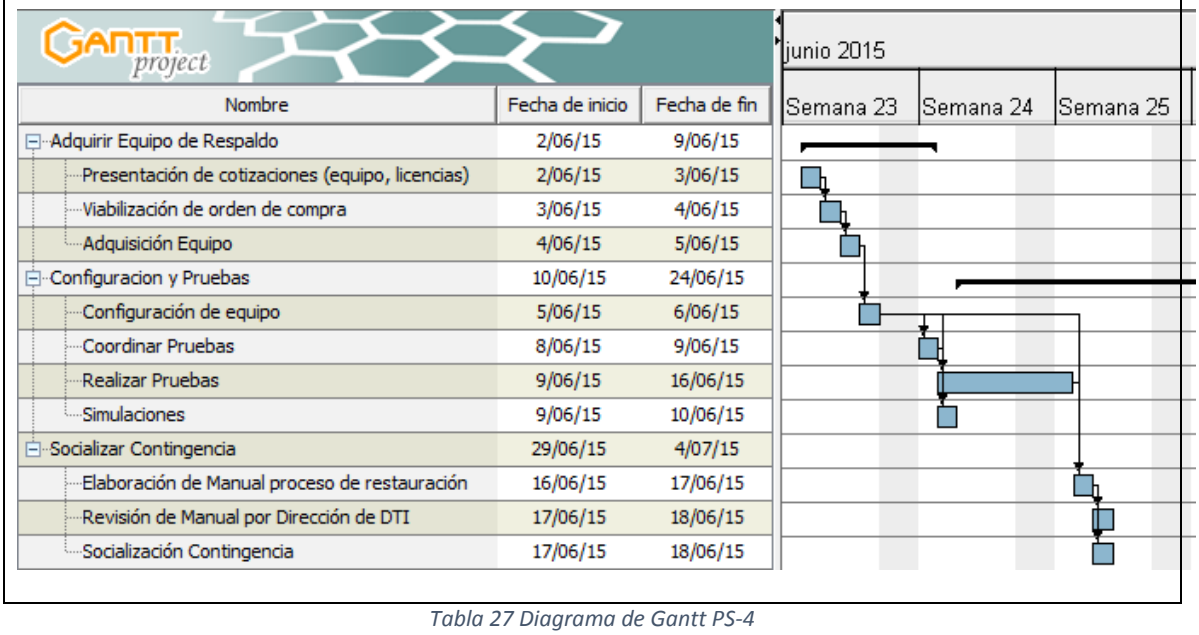
Salvaguarda	PS-3
Descripción - Objetivo	Computador Contingencia Procesos Usuarios



Nombre	Fecha de inicio	Fecha de
Adquirir Equipo de Respaldo	2/06/15	9/06/15
Presentación de cotizaciones (equipo, licencias)	2/06/15	3/06/15
Viabilización de orden de compra	3/06/15	4/06/15
Adquisición Equipo	4/06/15	5/06/15
Configuracion y Pruebas	10/06/15	24/06/1
Configuración de equipo	5/06/15	6/06/15
Coordinar Pruebas	8/06/15	9/06/15
Realizar Pruebas	9/06/15	16/06/1
Simulaciones	9/06/15	10/06/1
Socializar Contingencia	29/06/15	4/07/15
Elaboración de Manual proceso de restauración	16/06/15	17/06/1
Revisión de Manual por Dirección de DTI	17/06/15	18/06/1
Socialización Contingencia	17/06/15	18/06/1

Tabla 26 Diagrama de Gantt PS-3

Salvaguarda	PS-4
Descripción - Objetivo	Repuesto Contingencia Tarjeta de Planta Telefónica



Nombre	Fecha de inicio	Fecha de fin
Adquirir Equipo de Respaldo	2/06/15	9/06/15
Presentación de cotizaciones (equipo, licencias)	2/06/15	3/06/15
Viabilización de orden de compra	3/06/15	4/06/15
Adquisición Equipo	4/06/15	5/06/15
Configuracion y Pruebas	10/06/15	24/06/15
Configuración de equipo	5/06/15	6/06/15
Coordinar Pruebas	8/06/15	9/06/15
Realizar Pruebas	9/06/15	16/06/15
Simulaciones	9/06/15	10/06/15
Socializar Contingencia	29/06/15	4/07/15
Elaboración de Manual proceso de restauración	16/06/15	17/06/15
Revisión de Manual por Dirección de DTI	17/06/15	18/06/15
Socialización Contingencia	17/06/15	18/06/15

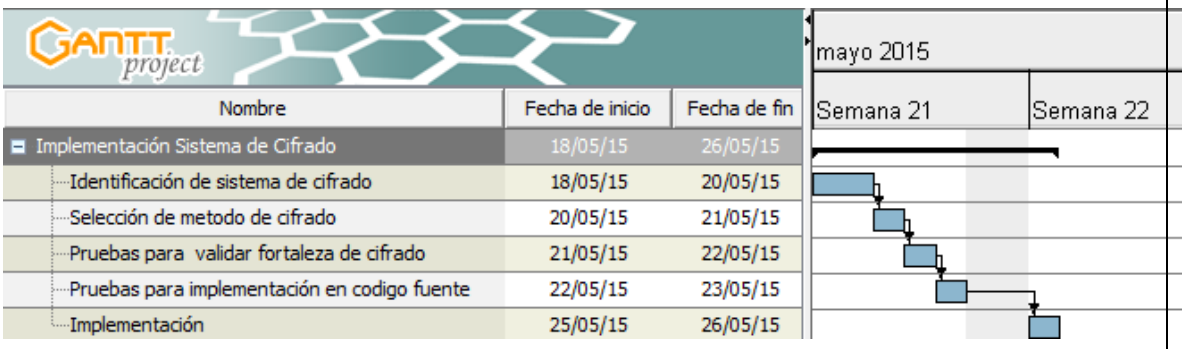
Tabla 27 Diagrama de Gantt PS-4

Salvaguarda	PS-5
Descripción - Objetivo	Buscar medidas legales para evitar la fuga de información

Nombre	Fecha de inicio	Fecha de fin
Revisión acuerdos de confidencialidad	1/07/15	10/07/15
Identificar normatividad vigente	1/07/15	3/07/15
Revisión procedimientos disciplinarios	3/07/15	4/07/15
Definir nuevos procedimientos disciplinarios	6/07/15	7/07/15
Aprobación por la gerencia	7/07/15	8/07/15
Publicación de nueva normatividad	8/07/15	9/07/15
Socialización de la nueva normatividad	9/07/15	10/07/15

Tabla 28 Diagrama de Gantt PS-5

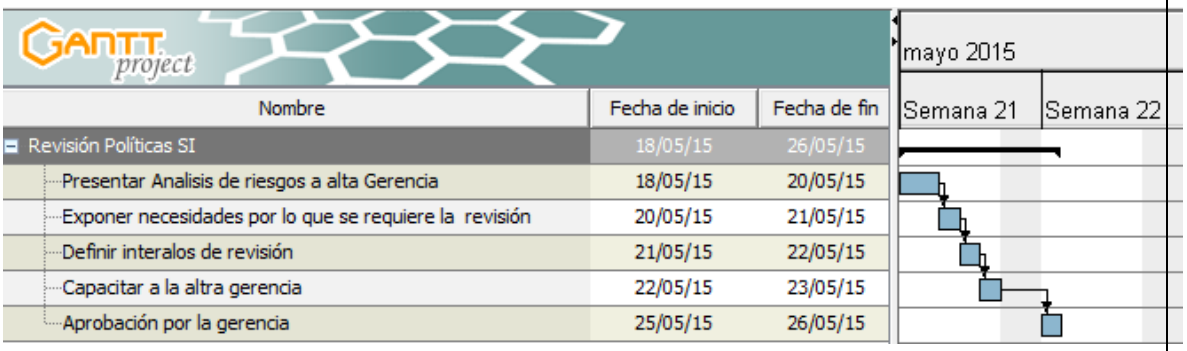
Salvaguarda	PS-6
Descripción - Objetivo	Sistema de Cifrado



Nombre	Fecha de inicio	Fecha de fin
Implementación Sistema de Cifrado	18/05/15	26/05/15
Identificación de sistema de cifrado	18/05/15	20/05/15
Selección de metodo de cifrado	20/05/15	21/05/15
Pruebas para validar fortaleza de cifrado	21/05/15	22/05/15
Pruebas para implementación en codigo fuente	22/05/15	23/05/15
Implementación	25/05/15	26/05/15

Tabla 29 Diagrama de Gantt PS-6

Salvaguarda	PS-7
Descripción - Objetivo	Garantizar apoyo en la revisión de las políticas



Nombre	Fecha de inicio	Fecha de fin
Revisión Políticas SI	18/05/15	26/05/15
Presentar Analisis de riesgos a alta Gerencia	18/05/15	20/05/15
Exponer necesidades por lo que se requiere la revisión	20/05/15	21/05/15
Definir interalos de revisión	21/05/15	22/05/15
Capacitar a la altra gerencia	22/05/15	23/05/15
Aprobación por la gerencia	25/05/15	26/05/15

Tabla 30 Diagrama de Gantt PS-7

5.4 EJECUCIÓN

El propósito es cumplir con los objetivos establecidos en los programas de seguridad, posterior se actualiza el estado del riesgo, evaluando nuevamente con las nuevas frecuencias/ impactos el nuevo riegos, para este trabajo el resultado esperado es un riesgo aceptable, sobre los activos

Activo	Control	Frecuencia Nueva	Eficacia	Impacto Nuevo	Riesgo Residual	Criterio	Riesgo Aceptable
HW-1	S HW-1 Servidor Contingencia	**3**	**L4**	**2**	**6,0**	B	SI
HW-2	S HW-2 Computador de contingencia	**5**	**L5**	**1**	**5,0**	B	SI
HW-14	S HW-3 Computador de contingencia	**5**	**L5**	**1**	**5,0**	B	SI
HW-15	S HW-4 Computador área de Contingencia	**5**	**L5**	**1**	**5,0**	B	SI
HW-13	HW-13 Computador área de muelles	**5**	**L5**	**1**	**5,0**	B	SI
HW-3	HW-3 Servidor Desarrollo	**4**	**L4**	**2**	**6,0**	B	SI
HW-6	HW-6 Servidor Pasarela Telefónica	**3**	**L3**	**3**	**9,0**	B	SI
HW-9	HW-9 Planta Telefónica	**3**	**L3**	**3**	**9,0**	B	SI
DT-2	S DT-2 - Acuerdos de Confidencialidad	**3**	**L3**	**3**	**9,0**	B	SI

Tabla 31 Riesgo aceptable

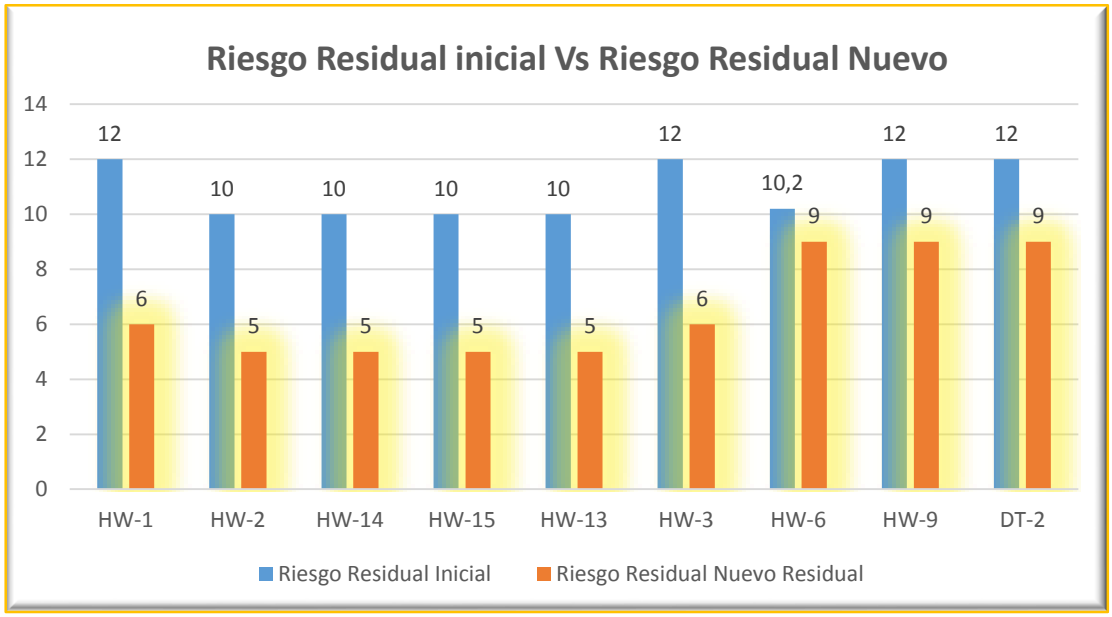


Ilustración 18 Riesgo inicial vs Nuevo Riesgo

5.5 AUDITORIA DE CUMPLIMIENTO

5.6 INTRODUCCION

Se procede a realizar una auditoría de los controles definidos en la declaración de aplicabilidad teniendo en cuenta la madurez de los mismos a partir Modelo de Madurez de la Capacidad (CMM). Para esto se establece una valoración para cada nivel de madurez (ver Tabla 31 Modelo de Madurez)

La evaluación se encuentra en el anexo 14 Auditoria

Ilustración 19 Auditoria

CMM	EFECTIVIDAD	SIGNIFICADO	DESCRIPCIÓN
L0	0%	Inexistente	No cumple, no se hace.
L1	10%	Inicial / Ad hoc	La actividad no se realiza por falta de recursos, no se ha considerado su ejecución.
L2	50%	Reproducible	La actividad no está completamente entendida, se ha planificado la ejecución a futuro. Depende del conocimiento del individuo
L3	90%	Proceso Definido	Los procesos están implementados y documentados
L4	95%	Gestionado	Se hace cubriendo todo el alcance de la actividad pero no de la forma más óptima, requiere mejoras
L5	100%	Optimizado	No requiere mejoras, está funcionando de acuerdo con lo requerido y conforme a las mejores practicas

Tabla 32 Modelo de Madurez

5.7 DESVIACIONES, OBSERVACIONES Y CONFORMIDADES

Se identifican las diferentes desviaciones (No conformidad mayor, NO conformidad leve) para aquellos controles que no cumplen con un nivel de madurez suficiente, se emiten observaciones para aquellos controles que requieren documentación, no son claros los procedimientos, pero que no afecta la implementación de la salvaguarda, aquellos controles que indican conformidad es porque se encuentran documentados, son medibles y en el caso ideal no requieren mejoras, para detallar la evaluación de los controles se dispone de la tabla Evaluación de Cumplimiento.

Abr	AREA	Criterios	Cumplimiento
L0	**No existente**	Si Madurez de control es =0%	No Conformidad Mayor
L1	**Inicial / Ad hoc**	Si Madurez de control es > 0% y <=10%	No Conformidad Mayor
L2	**Repetible pero intuitivo**.	Si Madurez de control >10% y <= 50	No Conformidad Leve
L3	**Proceso definido**	Si Madurez de control > 50% y <=90%	Observación

L4	**Administrado y medible**	Si Madurez de control > 90% y <=95%	Conforme
L5	**Optimizado**	Si Madurez de control, >95%	Conforme

Tabla 33 Evaluación de Cumplimiento

Se realiza una verificación control por control de acuerdo a los controles que se encuentran en la declaración de aplicabilidad, se valora el nivel de madurez y se calcula el estado de conformidad.

		0%	10%	50%	90%	95%	100%	Evaluación	
Dominio	Cant. Controles	Inexistente	Inicial	Repetible	Definido	Administrado	Optimizado	Madurez esperada	Resultado Auditoria
Política de Seguridad	2	0	0	0	2	0	0	90%	Observación
Aspectos organizativos de la seguridad de la información	7	0	1	0	1	5	0	82%	Observación
Seguridad ligada a los Recursos Humanos	6	0	0	3	0	2	1	73%	Observación
Gestión de Activos	10	0	2	1	4	3	0	72%	Observación
Control de Accesos	14	0	0	0	2	11	1	95%	Conforme
Criptografía	2	0	0	0	0	2	0	95%	Conforme
Seguridad Fisica y ambiental	15	1	1	2	7	3	1	75%	Observación
Operaciones de Seguridad	14	0	2	2	4	6	0	75%	Observación
Seguridad en las Telecomunicaciones	7	0	0	4	3	0	0	67%	Observación
Sistema de Adquisición, desarrollo y mantenimiento	12	0	0	8	4	0	0	63%	Observación
Relaciones con Proveedores	5	0	2	2	0	1	0	43%	No Conformidad Leve
Gestión De lincidentes en la Seguridad de la Información	7	0	0	0	7	0	0	90%	Observación
Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio	4	0	0	0	0	4	0	95%	Conforme
Cumplimiento	8	0	2	2	1	3	0	62%	Observación
	113	1	10	24	35	40	3		

Ilustración 20 Auditoria Estado de Seguridad ISO 27002

5.8 RESULTADOS

Se identifica las desviaciones con respecto a la norma ISO 27002 de dos maneras:

1. Evaluación Individual por control.
2. Evaluación de dominio.

Evaluación Individual por control.

Se identifica que de los 112 controles evaluados existen 11 controles con evaluación **No Conformidad Mayor**, 27 controles son **No conformidad leve**, existen 33 con **observación** los cuales pueden convertirse en **No conformidad leve,** anexo tabla de resumen de Evaluación individual de Controles así como la gráfica.

Estado de los controles Evaluados	Cant
No Conformidad Mayor	11
No conformidad leve	24
Observación	35
Conforme	43

Tabla 34 Resumen De evaluación Individual de controles

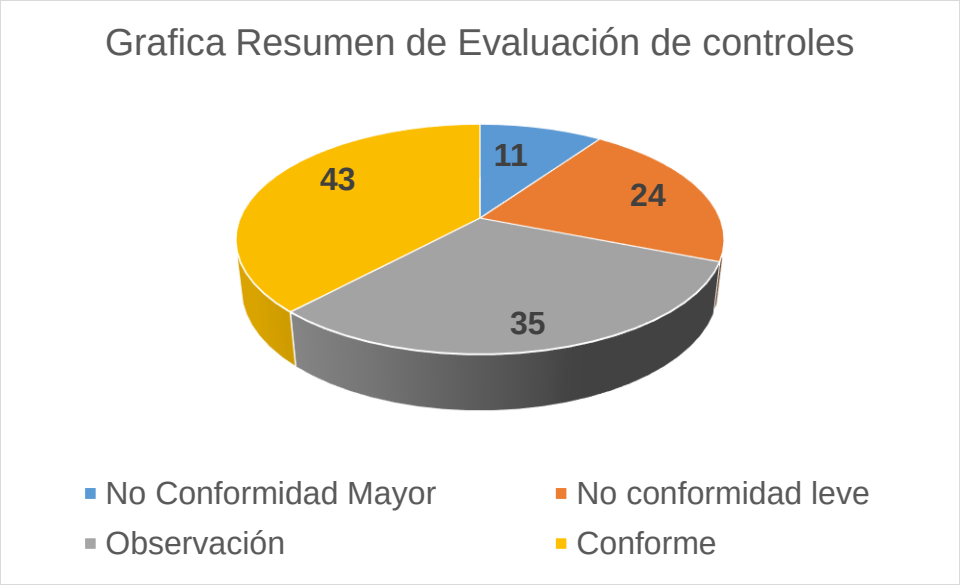


Ilustración 21 Estado De Evaluación De Controles ISO 27002

Resumen de controles cuya evaluación indica **No conformidad Mayor**

Nro.	Control
6.2.1	Política de uso de dispositivos para movilidad
8.3.1	Gestión de soportes extraíbles
8.3.3	Soportes físicos en transito
11.2.5	Salida de los equipos fuera de la empresa
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones
12.4.3	Registros de actividad del administrador y operador del sistema
12.6.1	Gestión de Vulnerabilidades Técnicas
15.1.1	Política de seguridad de la información para suministradores
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores
18.1.5	Regulación de los controles criptográficos
18.2.1	Revisión independiente de la seguridad de la información

Tabla 35 Controles con No Conformidad Mayor

Evaluación por dominio.

Se identifica que existe un dominio “Relaciones con Proveedores” con una desviación de tipo **No conformidad leve,** esto es de prestar atención porque puede convertirse en una No conformidad Mayor si no se atiende y establecen correctivos

6 Conclusiones.

Pollos pachito, es una empresa la cual tiene un grado inicial de concientización en lo referente a la seguridad de la información, se refleja que la dirección no está apoyando el proceso, estos se evidencio en la revisión de los requisitos de la norma ISO 27001:2013, posterior a la presentación de las propuestas se espera que en la implementación el riesgo que inicialmente se consideraba No aceptable cambie de estado, al revisar la auditoria se identificó que el dominio **Relaciones con Proveedores**, tiene **una No conformidad leve**, esto se debe que en el planteamiento de los planes de seguridad no se tuvo en cuenta y este conservo los mismos valores que traía desde la primera revisión, lo contrario se puede observar que el domino **criptografía** el cual no se cumplía ningún control en la primera fase en esta nueva revisión ya se encuentra en un nivel de madurez **95%,** de manera similar al dominio de la **política de seguridad al 90%.**

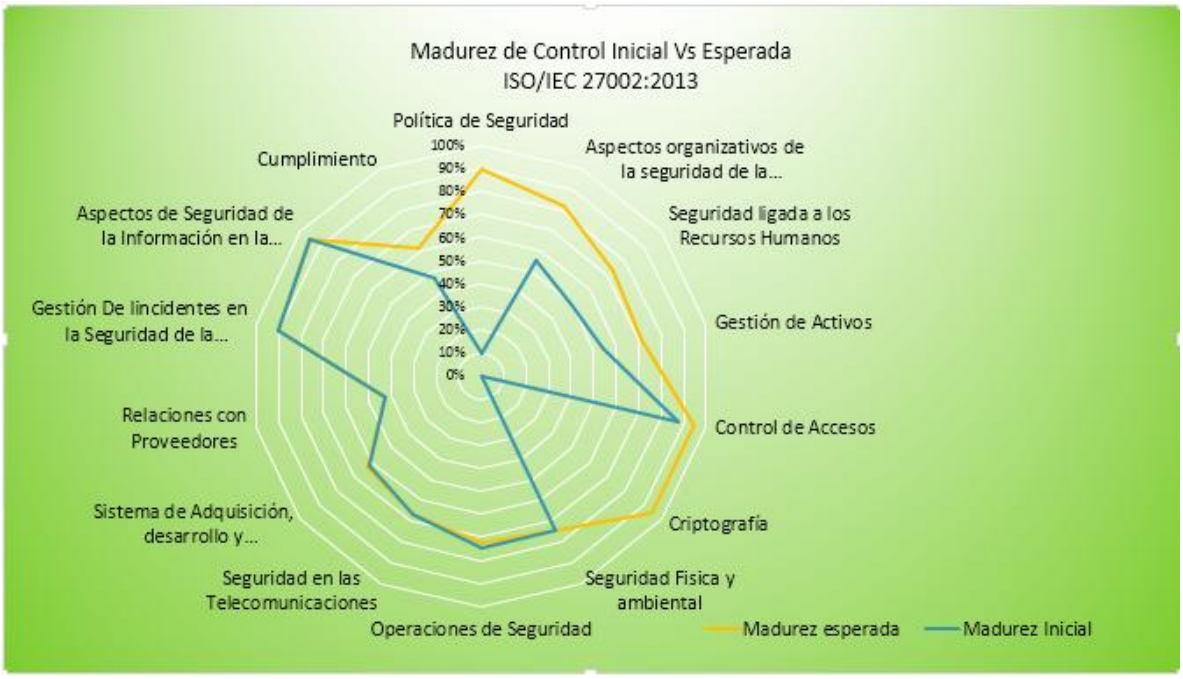


Ilustración 22 Estado de Madurez – Auditoria de controles ISO 27002

7 Bibliografía

Libro_II_Catalogo_de_Elementos-Magerit.pdf

2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8.pdf

http://almiropi.blogspot.com/

http://www.iso27000.es/glosario.html#section10a

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VR1ABOG2pZo

https://www.microsoft.com/spain/technet/recursos/articulos/srappb.mspx

http://aplica.uptc.edu.co/Procesos/Documentos/Inventario%20y%20Clasificaci%C3%B3n%20de%20Activos%20de%20Informaci%C3%B3n.pdf

https://www.ccn-cert.cni.es/publico/herramientas/pilar-5.3.1/help/html/magerit_dependencies.html

http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3233_impacto_potencial.html

http://urtanta.com/metodo-para-el-analisis-de-riesgos-de-seguridad/

http://urtanta.com/los-cambios-de-la-ultima-version-magerit-analisis-de-riesgos/

https://www.ccn-cert.cni.es/publico/herramientas/pilar5/exs/ejemplo.pdf

http://www.seguridadinformacion.net/los-10-tipos-de-activos-en-la-seguridad-de-la-informacion-que-son-y-como-valorarlos/

http://www.iso27001security.com/html/iso27k_toolkit.html

http://www.iso27001standard.com/es/blog/2011/04/18/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/

http://www.gesconsultor.com/ens/analisis-diferencial.html

http://www.iso27000.es/

http://cdigital.udem.edu.co/TESIS/CD-ROM45282008/12.Capitulo6.pdf

http://www.gerencie.com/graficos-excel-grafico-de-dispersion-mapa-de-calor-parte-1.html

http://blogs.gestion.pe/riesgosfinancieros/2014/06/una-reflexion-sobre-las-matrices-de-riesgo-operacional.html

https://seguridadinformaticaufps.wikispaces.com/MAGERIT