METODOLOGIA PARA IMPLEMETAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001 PARA LA COMPAÑÍA ALURA ANIMAL HEALTH NUTRITION SAS

OSCAR JAVIER VALERO RODRÍGUEZ

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
GRUPO DE INVESTIGACIÓN FICB-PG

Bogotá

2018

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
GRUPO DE INVESTIGACIÓN FICB-PG

METODOLOGIA PARA IMPLEMETAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001 PARA LA COMPAÑÍA ALURA ANIMAL HEALTH NUTRITION SAS

Proyecto de grado para obtener el título de Especialista en seguridad de la información.
Institución Universitaria Politécnico Grancolombiano

ASESOR TEMÁTICO:
Msc. Wilmar Jaimes Fernández

Oscar Javier Valero Rodriguez.
Bogotá, 2018.

Tabla de Contenidos

Índice de tablas

Índice de figuras

1. Resumen

En la actualidad la información de una organización están expuesta a ataques más complejas constituyendo un peligro sobre el core del negocio; ya que se considera como un activo critico dentro de los sistemas de Información Este proyecto explica un conjunto de procedimientos para proveer SGSI para la compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS ya que en la actualidad no cuentan con estos procedimientos y se busca a futuro obtener la certificación ISO/IEC 27001.

Abstract

Nowadays the information of an organization is exposed to more complex attacks constituting a danger on the core business, since it is considered as a critical asset within the information systems. This project explain a set of procedures to provide ISMS (ISMS) within the pharmaceutical company ALURA ANIMAL HEALTH NUTRITION SAS since they do not currently have these procedures and they are looking to obtain ISO / IEC 27001 certification in the future.

2. Palabras Clave

SGSI (Sistema de gestión de seguridad de la información), PHVA, diseño, riesgos, amenazas, salvaguardas, ALURA ANIMAL HEALTH NUTRITION SAS, activos, reservado, integridad, recurso, seguridad de la información,

Key words

SGSI (Information Security Management System), PCDA, design, risks, threats, safeguards, ALURA ANIMAL HEALTH NUTRITION SAS, assets, reserved, integrity, resource, information security,

3. Introducción

La compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS en la actualidad no cuenta con un plan para la continuidad del negocio; por lo cual se hace pertinente analizar una estrategia para poder implementar dentro de su organización políticas basadas en la norma ISO/TEC 27001, que permita que en una catástrofe (natural, informático o por terceros), conservar la integridad de la información.

En la actualidad se evidencia que las Pymes afrontan problemas graves debido a que la mayoría no destinan dentro de su presupuesto un rublo para afrontar las fallas de seguridad y prevenir los riesgos de sus activos de información.

Se planteará un modelo basados en estándares y normas internacionales como ISO/IEC 27001, el cual busca evitar, disminuir y prevenir ataques y/o desastres informáticos, antes de que éstos ocurran. Se dará inicio a un proceso de análisis de la situación actual de la empresa, posteriormente se realizará el inventario de activos y ya con esta información se llevará a cabo la definición del análisis de riesgos, para un posterior diseño de políticas, procesos y procedimientos que permitirán determinar y establecer los controles de seguridad que ayuden a gestionar los riesgos identificados.

4. Justificación.

Para la Empresa farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., el activo más importante el cual debe preservar es la información, más en esta época de avances tecnológicos el cual ha llevado a cambios radicales en la competitividad del mercado. Las malas prácticas por parte de los usuarios, los virus que se propagan por medio de la internet u otros medios, ataque de Hackers, hace que se afecte la continuidad del negocio; surge la necesidad de realizar procedimientos y controles que ayude a minimizar los riesgos presentes.

El control de los recursos tecnológicos constituye una fuente importante de seguridad sobre los activos de información; sin embargo al consultar a los actores implicados queda en evidencia que los equipos en su mayoría no se encuentran registrados en el inventario de los activos de la compañía. Tal situación deja en evidencia un grave problema que puede traer consigo perdidas económicas.

Sólo el personal autorizado tiene acceso a la información confidencial de la compañía cuando se necesite; es necesario implementar medidas para evitar accesos no autorizados; modificación no controlada de la información o consulta de la misma.

La compañía en la actualidad no cuenta con un DRP para dar continuidad al negocio, generan así intranquilidad dentro de las áreas implicadas puesto que en una caída del sistema no sabrían cómo actuar.

5. Objetivos.

Diseñar una metodología para implementar un sistema de gestión de seguridad de la información bajo el ciclo de mejora continua para la empresa ALURA ANIMAL HEALTH NUTRITION SAS, basado en la ISO 27001.

5.1. Objetivos específicos.

- Revisar la situación actual de la empresa ALURA ANIMAL HEALTH NUTRITION SAS con relación a la GSI.
- Diseñar una metodología para el mantenimiento de la norma ISO 27001 que involucre el PHVA.
- Realizar un estudio de los riesgos y vulnerabilidades presentes en la empresa ALURA ANIMAL HEALTH NUTRITION SAS, con el fin de poder minimizarlas.

6. Análisis desde el modelo de planeación estratégica situacional.

6.1. Descripción de la situación de interés

6.1.1. Antecedentes del Problema.

En la actualidad la compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., no cuenta con ningún método que permita identificar vulnerabilidades, riesgos y ataques en un momento de crisis; tampoco cuenta con un sistema de sistema de gestión documental que permita solventar las deficiencias, colocando en riesgo los activos de la compañía.

6.1.2. Formulación del Problema.

¿Cuenta la compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., con un plan que ayude a la realización de un análisis para implementar un SGSI?

6.1.3. Descripción del Problema.

La compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., desea tener una propuesta que le permita gestionar los riesgos a los que se encuentran expuestos, contando con un modelo de SGSI que permita identificar y luego mitigar los riesgos.

La propuesta podría generar un impacto en la compañía ya que no tiene definidas políticas que involucren la seguridad de la información, no cuentan con normas en materia de desastres de origen natural, informáticos o de terceros que puedan afectar los activos de la empresa; entre los problemas detectados se encuentra el uso inadecuado de los recursos tecnológicos, falta de control en navegación y uso del correo electrónico.

Con el propósito de identificar las causas del problema anteriormente mencionado, se procedió a ejecutar entrevistas al interior de la compañía involucrando a todos los actores relevantes.

- Presidencia.
- Gerencia de talento Humano.
- Gerencia de TI.
- Gerencia Financiera y Administrativo.
- Gerencia de Operaciones.
- Gerencia de HESQ.
- Gerencia de negocios.
- Gerencia de Marketing

Los actores relevantes expusieron las causas, como la inexistencia de documentación que permita tener control sobre los procesos internos de la compañía, inexistencia de políticas, procedimientos y/o formatos, fallas de tipo operativo, falta de capacitación, también expresan la falta de recursos asignados hacia la mejora de procesos y procedimientos.

6.1.4. Situación Problema.

Mediante la realización de auditorías internas dentro de la compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., se identificaron una lista de fallas en la seguridad de la información; las cuales traerán como consecuencias riesgos de tipo tecnológico, por lo cual a compañía tendrá que asumir pérdidas económicas.

Con el resultado de las auditorias se tomara 3 puntos relevantes que son:

i. Administración De Recursos Tecnológicos (Software, Hardware, comunicaciones). Durante la revisión de la auditoria, se identificó que la compañía farmacéutica no cuenta con el inventario actualizado de los equipos de cómputos, comunicación y de software, materializando el riesgo de pérdidas económicas. También se identificó fallas en la adecuada administración de los usuarios y roles del sistema (DIRECTORIO ACTIVO, CRM, ERP, Otros), ya que se encontró usuarios activos y con conexiones externas que fueron desvinculados de la compañía.

ii. Sistemas de respaldo de información y seguridad. Las auditorias encontraron que no se cuenta con copias de seguridad, políticas de respaldo y registros de planes de restauración de la información más relevante de la compañía farmacéutica (financiera, contable y del negocio). También Se evidencio que no se están controlando la conexión de medios para la extracción de información en los equipos de cómputo que manejan información sensible; en especial la información financiera, contable y del negocio para la compañía Farmacéutica, fallas que puede generar un riesgo de fuga de información.

iii. Plan de Recuperación de Desastres "DRP[1]: para finalizar la auditoria, se evidencio de la compañía farmacéutica no cuenta con estrategias de recuperación tales como un análisis de riesgo, análisis de impacto del negocio o tiempos para la restauración a partir de puntos de recuperación o información total.

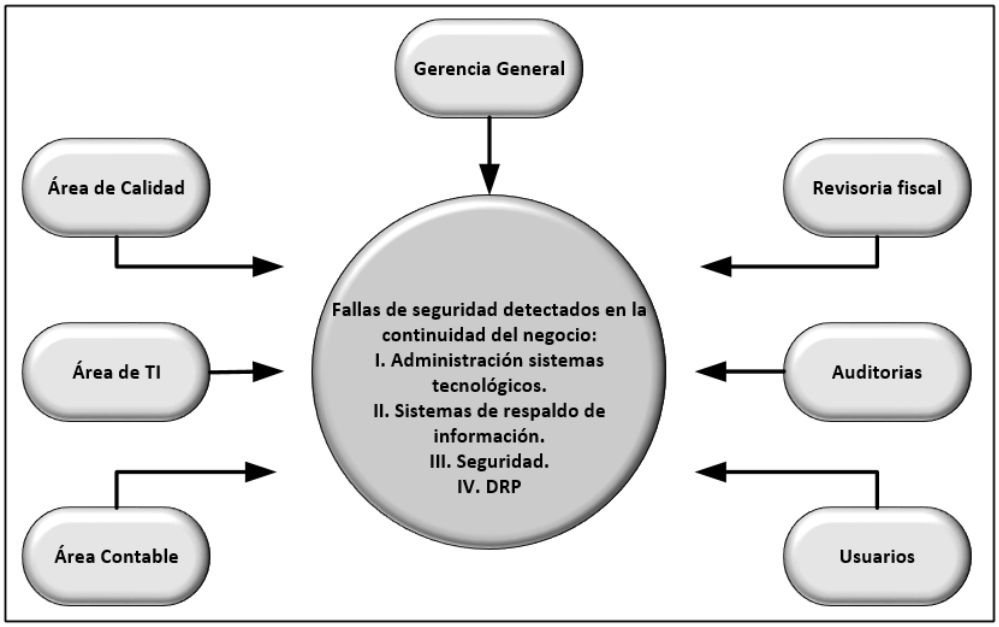
1 DRP: Data Recovery Disaster Recovery

6.2. Red de actores relevantes.

6.2.1. Identificación de los actores relevantes.

Los actores Relevantes, constituyen partes internas y externas a la compañía farmacéutica ya como se observa en el siguiente diagrama: En la gráfica se observa los actores más relevantes con la situación del problema planteado.

Ilustración 1. Identificación de los actores relevantes



6.2.2. Causas de la situación problema según los actores relevantes.

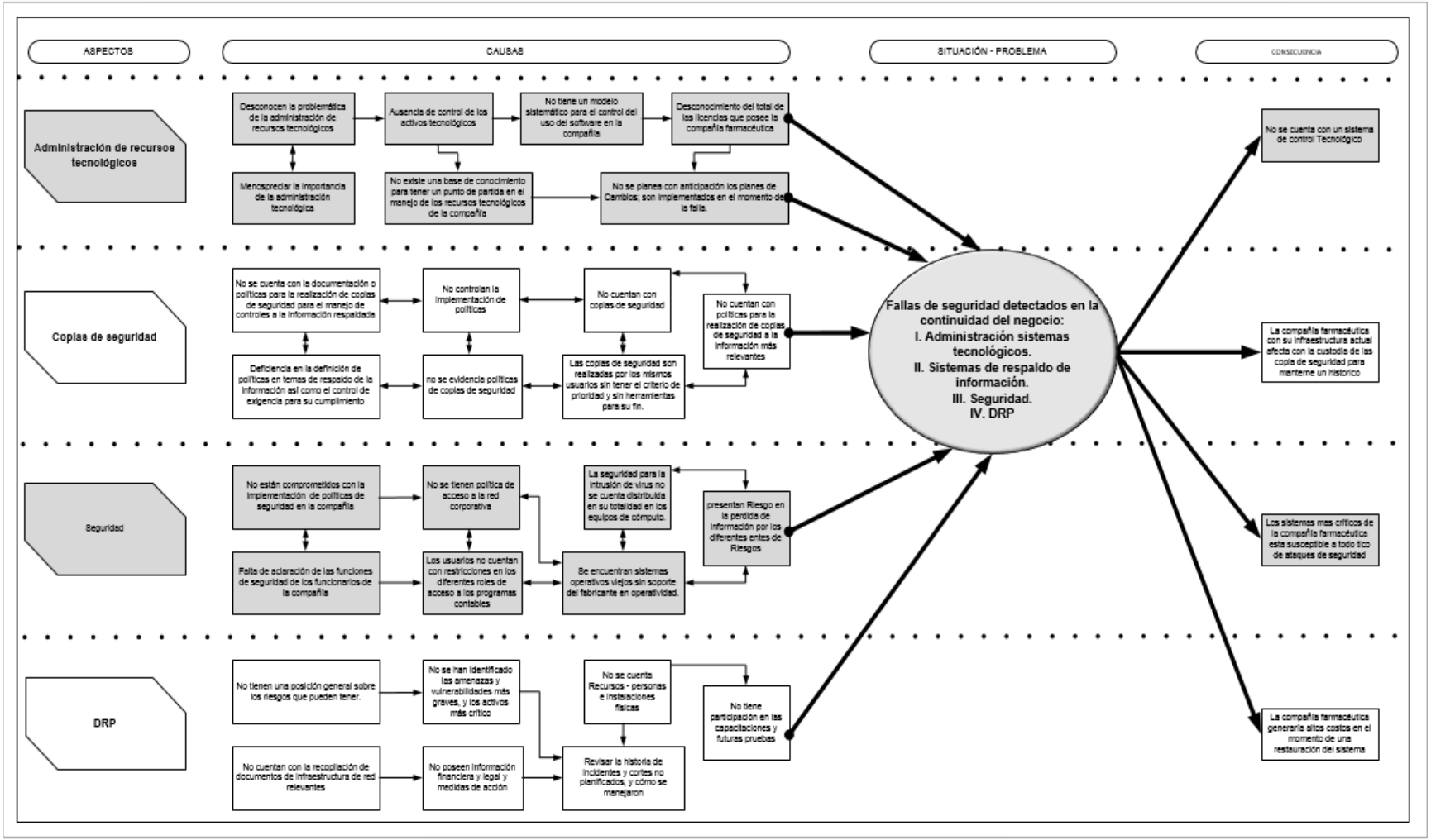
Tabla 1. Causas de la situación problema según los actores relevantes

PARTES INTERESADAS	ASPECTO	CAUSA
Gerencia general	**Administración de recursos tecnológicos**	Desconocen la problemática de la administración de recursos tecnológicos
	Copias de seguridad	No controlan la implementación de políticas
	Seguridad	No están comprometidos con la implementación de políticas de seguridad en la compañía
	DRP	No tienen una posición general sobre los riesgos que pueden tener.
Área de calidad	**Administración de recursos tecnológicos**	Menospreciar la importancia de la administración tecnológica
	Copias de seguridad	Deficiencia en la definición de políticas en temas de respaldo de la información así como el control de exigencia para su cumplimiento
	Seguridad	Falta de aclaración de las funciones de seguridad de los funcionarios de la compañía
	DRP	No cuentan con la recopilación de documentos de infraestructura de red relevantes
Área de TI	**Administración de recursos tecnológicos**	No se planea con anticipación los planes de Cambios; son implementados en el momento de la falla.
	Copias de seguridad	No cuentan con copias de seguridad
	Seguridad	No se tienen política de acceso a la red corporativa
	DRP	No se han Identificar las amenazas y vulnerabilidades más graves, y los activos más crítico
Área contable	**Administración de recursos tecnológicos**	No tiene un modelo sistemático para el control del uso del software en la compañía
	Copias de seguridad	No cuentan con políticas para la realización de copias de seguridad a la información más relevantes
	Seguridad	Los usuarios no cuentan con restricciones en los diferentes roles de acceso a los programas contables
	DRP	No poseen información financiera y legal y medidas de acción
Revisoría fiscal	**Administración de recursos tecnológicos**	Ausencia de control de los activos tecnológicos

	Copias de seguridad	No se cuenta con la documentación o políticas para la realización de copias de seguridad para el manejo de controles a la información respaldada
	Seguridad	La seguridad para la intrusión de virus no se cuenta distribuida en su totalidad en los equipos de cómputo.
	DRP	No se cuenta Recursos - personas e instalaciones físicas
Auditorias	**Administración de recursos tecnológicos**	Desconocimiento del total de las licencias que posee la compañía farmacéutica
	Copias de seguridad	no se evidencia políticas de copias de seguridad
	Seguridad	Se encuentran sistemas operativos viejos sin soporte del fabricante en operatividad.
	DRP	Revisar la historia de incidentes y cortes no planificados, y cómo se manejaron
Usuarios	**Administración de recursos tecnológicos**	No existe una base de conocimiento para tener un punto de partida en el manejo de los recursos tecnológicos de la compañía
	Copias de seguridad	Las copias de seguridad son realizadas por los mismos usuarios sin tener el criterio de prioridad y sin herramientas para su fin.
	Seguridad	presentan Riesgo en la perdida de información por los diferentes entes de Riesgos
	DRP	No tiene participación en las capacitaciones y futuras pruebas

6.3. Flujograma Explicativo.

Ilustración 2. Flujograma cadenas casuales



6.4. Tabla de indicadores

6.4.1. Identificador del estado actual de la situación Problema.

El cuadro a continuación explicará la compilación de indicadores adecuados que nos permite identificar el estado actual de la Situación – Problema.

Tabla 2. Estado actual de la Situación – Problema.

Indicador	Descripción	Análisis de la muestra	observaciones
1	Disponibilidad del Servicio	99,90%	Medición mensual de disponibilidad del sistema tecnológico para el manejo de la información Contable, financiera y del negocio
2	Porcentaje de servidores con solución antivirus instalada.	70,00%	Durante la inspección física realizada, no se identificó una solución de antivirus instalada en los servidores de criticidad media y baja.
3	Estado de asignación de licencias sobre el software de la compañía	40%	Se identificó que la distribución de licencias para software se encuentra mal distribuida ya que los programas con licencias nominales y concurrente son iguales, generando incremento en la legalización de software
4	Porcentaje de equipos de cómputo no registrados en inventario de activos.	28,00%	Al validar el Kartex de inventario de cómputo versus la revisión de los equipos físicos dentro de la compañía, logro evidenciar: * Equipos sin actualizaciones de seguridad. * Equipos sin registro de inventario. * Equipos con hardware distintos.
5	Porcentaje de instalación de antivirus global	19%	En revisión de la solución de antivirus con que actualmente cuenta la compañía, fue posible identificar en el servidor de administración de Antivirus que solo se tiene configurado para administrar el total de las estaciones de trabajo.
6	Cambios Planeados	% según cambio planeados	Planeados Porcentaje de cambios planeados
7	Detección de virus	% de virus identificados	Reporte de virus según la consola de administración

6.5. Formulación de la situación deseada.

6.5.1. Análisis de prospectiva.

Para el análisis de prospectiva se plantearán los siguientes escenarios:

- Optimista,
- Tendencial
- Pesimista

Con una proyección de 2 años, planteando las acciones hacia las causas más relevantes.

6.5.1.1. Escenario Optimista.

Administración de sistemas tecnológicos.

- La Gerencia General, asigna los recursos económicos que se necesitan para la implementación de herramientas de gestión tecnológicas para la administración del sistema corporativo (Software, hardware, comunicaciones).
- El área de TI gestionará la elaboración del inventario actualizado para la iniciación del proceso de los sistemas de gestión eficientemente.
- Al realizar la implantación de la herramienta de gestión de inventario automatizados mejorarán el control de los activos actuales, brindando mayor seguridad a la información recopilada; también ofrecerá reportes en tiempo real de las posibles alertas que se detecten (Cambios tecnológicos).
- La compañía farmacéutica se acopla a nuevas y mejores prácticas sobre la realización de inventarios automatizados.
- Todos los instructivos, procedimientos y políticas, son revisados y actualizados con el fin de garantizar calidad en el servicio.

Sistema de Respaldo de Información:

- Implementación de política de respaldo de la información más relevante con recursos asignados.
- Instalación de herramientas de copias de seguridad en los equipos clientes - servidor, con el fin de evitar la reproducción de copias sin ningún control por parte de los usuarios y administradores.
- Plan de copias de respaldo real según las tablas de retención documental exigidas en la organización.
- Implantación de ambientes QAS para la realización de pruebas de restauración de la información para ejecutar el plan de restauración de copias de seguridad.
- Desarrollo de Instructivos para la creación e inhabilitación de cuentas de usuario documentado, actualizado y en operación.

Seguridad:

- Políticas de seguridad factibles para el despliegue de actualizaciones; instalación de la consola de antivirus actualizada y activa obteniendo métricas de infección por virus en estaciones de trabajo y servidores.
- Implementación de políticas de roles y privilegios sobre los recursos compartidos, directorio activo, aplicativos y herramientas tecnológicas, como medio de protección de accesos no autorizados a información confidencial.
- Actualización de sistemas operativos actualizados para servidores con versiones soportadas por fábrica.

- Instructivos, procedimientos y políticas detallando las funciones del coordinador de TI, facilitando la compresión y responsabilidad sobre las actividades a ejecutar.

DRP

- Involucrar a la gerencia ya que son los responsables de coordinar y asegurar la efectividad de un plan de recuperación de desastre.
- La gerencia General debe involucrar a todos los departamentos de la organización para la participación de la definición del plan.
- A partir del análisis de riesgo, se debe establecer una lista con de probables desastres naturales o causados por errores humanos; una vez definidas los departamentos debe analizar las posibles consecuencias y el impacto relacionado con cada tipo de desastre.
- El personal de TI a partir de las necesidades definidas por cada departamento, asigna una prioridad con una cantidad máxima de tiempo para determinar un grado de orden según la importancia.

6.5.1.2. Escenario Tendencial.

Administración de sistemas tecnológicos

- La alta gerencia ha concientizado en asignar recursos económicos, para la implementación de sistemas tecnológicos con el objetivo de optimizar los tiempos en la administración de inventarios computacionales.
- La actualización de los inventarios se está realizando de forma manual con procesos de gestión de TI; generando retrasos en los proceso de implementación.

- La organización se adapta a un marco de referencia de mejores prácticas sobre gestión de configuración.
- Se realiza implementación de una herramienta de gestión de inventario automatizado, lo cual agrega procesos para la actualización al área de TI, la asignación de equipos de cómputo a los responsables, con la posibilidad de obtener alertas ante posibles cambios de hardware.
- Se agregan instructivos, procedimientos y política con el fin de garantizar la actualización de los cambios tecnológicos planeados.

Sistema de Respaldo de información:

- A partir de los recursos existentes, se implementará la política de respaldo de información.
- Se buscará herramientas de bajo costo para ejecutar respaldos de seguridad con la finalidad de disminuir el impacto económico sobre la implementación.
- La realización de copias de seguridad es corta al no disponer de espacio suficiente en los medios disponibles para tal fin.
- Los instructivos para la creación e inactivación de cuentas de usuario es aprobado por la gerencia, para mantenerse actualizado y en operación.

Seguridad:

- Se mantienen las políticas de seguridad efectivas para el despliegue de actualizaciones, también se mantiene la consola de antivirus actualizada con el fin de obtener métricas de infección por virus en equipos de cómputo como en servidores.
- Los roles y privilegios ya actualizados, se conservarán, se implementarán sobre directorio activo, aplicativos, los recursos compartidos y herramientas tecnológicas.

- Los instructivos, procedimientos y política, son actualizados detallando las funciones del coordinador de TI, facilitando el entrenamiento y responsabilidad sobre las actividades a ejecutar.

DRP

- Actualizar a la gerencia general teniendo en cuenta las responsabilidades para lograr efectividad en la puesta en marcha de un plan de recuperación de desastre.
- Capacitar a todos los departamentos involucrados de la organización para la asertiva participación de la definición del plan de recuperación de desastre.
- Evidenciar la importancia de la mitigación de riesgo al tener en cuenta el plan de riesgo analizados previamente con sus probables consecuencias.
- La asignación de prioridades a partir de los acuerdos de niveles de servicio adquiridos se podrá gestionar con el cumplimiento de los tiempos; generando así calidad en el servicio.

6.5.1.3. Escenario Pesimista.

Administración de sistemas tecnológicos

- La gerencia general no asigna recursos económicos para la implementación de recursos tecnológicos para la compañía farmacéutica.
- Se mantiene el inventario tecnológico desactualizados; por lo cual no sería confiable para la realización de informes de gestión.
- No se tendría el control de los cambios informáticos realizados en los equipos de cómputo perdiendo así la administración del mismo.

- La compañía Farmacéutica se mantendría sin los instructivos, procedimientos y política para la calidad de los servicios de TI.

Sistemas Respaldo de información

- La gerencia general no asigno recursos para la puesta en práctica de una política de respaldo, causando pérdidas de información.
- Las herramientas de copias de seguridad en usuarios finales no son instaladas, por lo cual se corre riesgo en la perdida de información.
- La información de la compañía no es respaldada, por lo anterior no es posible la restauración a partir de una memoria institucional.
- No se implementan ambientes de QAS.

Seguridad Informática.

- No se realiza gestión sobre las políticas de seguridad, consola de antivirus, el cual hace ineficiente la creación de métricas de infiltración de seguridad en los usuarios como en los servidores.
- Al no tener definidos los roles y privilegios sobre los recursos compartidos, directorio activo, aplicativos y herramientas tecnológicas, no se garantizara la confidencialidad de la información.
- Sin la definición de instructivos, procedimientos y política, las funciones del coordinador de TI, son confusas aumentando solicitudes de soporte informal.

DRP

- Sin la implementación de un plan de recuperación de desastre, la compañía farmacéutica no deja espacio para nuevas tecnologías e infraestructuras. Esto no sólo perjudica a la organización durante un desastre, si no que en todo momento; Un almacenamiento menos eficiente, siempre se traducen al empeoramiento del mantenimiento y la seguridad de los datos digitales.
- Al no tener plan de recuperación de desastres no se podrá realizar copias de seguridad y restauración al momento de una catástrofe generando interrupción del servicio tanto a los usuarios como a los clientes. Esto podría significar la diferencia entre permanecer en el negocio o no, ya que muchas empresas no sobrevivirán más de dos años después de una interrupción importante en relación con la pérdida de datos.
- Sin un plan de DRP que obligue a depurar la información en la compañía farmacéutica generaría una gran cantidad de datos de una múltiple variedad de fuentes, almacenada en un número de diferentes departamentos; generando almacenaje de toda la información obsoleta.

6.6. Matriz de valores estratégica.

Tabla 3. Matriz de valores estratégica

Aspectos	Causa del flujograma	Acción (variable de prospectiva)	Valoración de gobernabilidad		Valoración de impacto		Valoración de pertinencia	
Administración de sistemas tecnológicos	Falta de importancia de la administración de los recursos de software, hardware y comunicaciones por parte de la alta gerencia	Asignación de recursos económicos.	5	Los recursos económicos son asignados por la gerencia general de la compañía y se considera un facto infalible para la implementación del proyecto.	5	Con la implantación de herramientas de administración de inventarios, se asegura el domino sobre activos tecnológicos.	5	La asignación de recursos es una prioridad debió al impacto de la acción frente a la solución de la situación problema.
	se evidencia una falta de control sobre las licencias del software de la compañía	Realización de inventarios de los activos tecnológicos.	4	El área de TI no cuenta con las herramientas para garantizar el control del uso de las herramientas tecnológicas de la compañía.	3	Con el levantamiento de inventario objetivo se puede garantizar la confiabilidad de la información.	4	El levantamiento de información es una de las principales fuentes para la creación de actividades posteriores.
	Ausencia software para el control de los inventarios de los activos tecnológicos.	Implementación de unas herramientas para la gestión de inventarios.	3	Para implantar el programa de gestión de inventario, depende de la inversión por parte de la gerencia general.	3	Permitirá un mayor control en la realización de reportes de inventario de los activos tecnológicos.	3	La implementación de herramientas de gestión dependerá de actividades previas.
Sistemas Respaldo de información	No se tiene una política para las copias seguridad en la Compañía.	implementación de políticas de respaldo	5	Disponer con los equipos tecnológicos para la realización de copias de respaldo a partir de los recursos tecnológicos que existen.	5	La política determinara los lineamientos necesarios para la correcta ejecución de las copias.	5	La creación de la política depende de la disponibilidad de del personal y las herramientas a utilizar.

	Los usuarios realizan las copias de seguridad al no contar con una herramienta que les permita la realización de una copia.	Instalación de programas de copiado de seguridad de la información.	5	El área de TI puede determinar las herramientas a utilizar, considerando herramientas de bajo costo.	5	El respaldo de información de usuarios finales alimenta la construcción de memoria institucional.	5	No existen restricciones frente a la utilización de herramientas de backup gratuitas.
	Es evidente la falta de un ambiente QAS para validar la veracidad de las copias de seguridad realizadas.	Creación de un ambiente QAS disponible.	4	El área de TI cuenta en la actualidad con los recursos de virtualización para implementar escenarios de QAS.	3	Los escenarios de QAS aseguran la veracidad de las copias de respaldo ejecutadas.	4	Los escenarios de QAS son indispensables y se cuenta con las herramientas necesarias.
Seguridad	El programa de antivirus no está instalado en todo el parque informático de la compañía.	Configuración de la consola de antivirus.	4	La consola de antivirus se encuentra implementada.	4	La administración de la consola del antivirus, mitiga la infección por virus	4	Debido a la facilidad de implementación y los pocos recursos requeridos se considera pertinente.
	En la actualidad se cuenta con S.O. obsoletos que no cuenta con soporte de fabrica	Actualización y soporte del sistema Operativo.	5	Con la asignación de nuevos recurso se procederá a la actualización de sistemas operativos con nuevas versiones.	5	con las nuevas versiones se disminuye el riesgo de seguridad	5	Con la llegada de nuevas tecnologías la criticidad respecto a seguridad informática se considera urgente.
	No se tiene una política de control de acceso para los diferentes perfiles y roles de usuarios	Instructivos, procedimientos y política actualizados y en operación.	4	Dependen de la gerencia, la aprobación y difusión de los instructivos, procedimientos y política y cumplimiento del mismo	3	Con el cumplimiento de las políticas, se asegura que la información sea accedida únicamente por el personal autorizado.	2	En la creación de la política depende de las implementaciones a realizar.

DRP	A partir del análisis de riesgo, se debe establecer una lista con de probables desastres naturales o causados por errores humanos.	Personal de TI capacitado.	4	El área de TI puede reportar las brechas de conocimiento con el fin de solicitar capacitación en temas específicos.	3	La capacitación mejora la calidad y oportunidad del servicio.	2	Las necesidades de capacitación dependen en gran medida de los cambios realizados en la infraestructura y aplicaciones.
	El personal de TI, a partir de las necesidades encontradas debe asignar prioridades con un orden según la importancia.	Instructivos de operación sobre las necesidades encontradas actualizados y en operación	4	El área de TI está en capacidad de documentar los instructivos necesarios para asegurar la operación.	4	Con la correcta administración de los riesgos permitirá poder llevar el control de las mismas	4	Las herramientas y recursos para la creación de instructivos de operación están dadas.
	La gerencia general debe involucrar a todos los departamentos para la participación en la definición del plan.	Concientizar sobre la necesidad de tener políticas de desastres	3	Con la asignación de nuevos recurso se procederá a la capacitación del personal de la compañía.	3	Con las capacitaciones se debe busca solucionar cualquier tipo de riesgo ya encontrados.	3	Las herramientas y recursos para la creación de instructivos de operación están dadas.

7. Marco referencial.

7.1. Marco Teórico.

En estos tiempos modernos donde el activo más importante de una organización es la información, se necesita llevar a cabo estrategias, no solo a la altura del software, como ampliar la protección hacia las bases de almacenamiento de datos como los programas de gestión de archivos, si no que se debe ampliar al nivel físico y contratando personal con amplios conocimientos y ética.

7.1.1. Vulnerabilidades.

Al revisar las debilidades que actualmente cuneta el sistema informático en la compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS y al volverse susceptibles a una potencial amenaza, puede ser utilizado para causar daño.

Las vulnerabilidades pueden aparecer en cualquier elemento de la compañía (internas o externas), pero al aplicar controles apropiados, se puede disminuir la probabilidad de que estas se presenten.

Las vulnerabilidades detectadas son:

- **Física:** Referente al entorno físico; como lo son equipos de cómputo y servidores, Evitando que alguna conexión haya vulnerado los accesos a la información confidencial de manera contundente para ser sustraída, modificada o borrada.
- **Naturales:** ocasionadas por eventos naturales o accidental en el medio ambiente, ocasionando daños. como ejemplos descargas eléctricas, desbordamiento (por encontrarse a las alamedas del Rio Bogotá), terremotos, y todos aquellos desastres naturales.

- **TI**
    a. **Hardware:** hace referencia al desgaste propio el uso por descuido de terceros, en las piezas físicas y/o dispositivos provocando fallas, provocando que se deje desamparado los equipos computacionales.
    b. **Software:** también conocidos como bug del sistema, generando que personas mal intencionadas puedan acceder a la información, por medios de programas o mal diseño en la aplicación o puertos abiertos para acceder y captura la información.
- **Humanas:** Estas vulnerabilidades se ubica en la falta de capacitación por parte de la organización para proteger la información; también al no tener definidas políticas de autenticación y cambios de pasword.

7.1.2. Amenazas.

Este tipo de amenaza, los podemos clasificar en:

- **Origen criminal:** Acciones en las que se violan las leyes y nomas por parte de un individuo.
- **Origen físico:** Eventos proporcionados naturalmente por el factor humano.
- **Origen negligente:** ocasionadas por la ignorancia o acciones de personas con falta de conocimiento y sin ética moral sobre los sistemas de almacenamiento de información.

En la actualidad, los sistemas se encuentran a la merced de ataques informáticos cada vez que interactúa con la información; a partir de la utilización de medios de almacenamientos, accesos web dentro de la organización. Entre otros tipos de amenazas están:

- **Generación:** ocurre cuando se inyecta información directa en los programas de gestión documental, base de dato y programas de gestión de información, causando destrucción interna como externa en los equipos de cómputo y prestación del servicio, ya que incrusta

mensajes no autorizados en cada una de las líneas de los registros y datos requeridos para que funcione correctamente.

- **Modificación:** sucede en el momento que un grupo de usuarios modifican sin previo aviso los archivos para provocar daño en la información, problemas en el funcionamiento de los ordenadores y aplicativos o inyectar procesos de cambios en las secuencias de la información en las bases de datos.
- **Interrupción:** ocurre cuando se satura los sistemas de información por medio de querys transaccionales de código SQL, ya sea por código malicioso, virus, y aquellas aplicaciones que ocasionan lentitud al sistema generando un mal funcionamiento.
- **Intercepción:** son aquellas donde un grupo de usuarios acceden al sistema sin previa autorización para revisar, copiar o eliminar documentación fundamenta de la organización.

  Amenazas Involuntarias: Se generan por la falta d conocimiento y / o capacitación del personal sobre las políticas de seguridad al momento de utilizar cualquier tipo de información.

7.1.3. Riesgos.

Son condiciones, que afecta tanto a los ordenadores como a sistemas de gestión documenta, si no se cuenta con normas para proteger la información. Estos riesgos los podemos clasificar en:

- **Integridad:** Todas aquellas aplicaciones de reportes donde sé que valida el acceso a las aplicaciones de la organización. Estas se encuentran en:
  a. Interacción del usuario.
  b. Manipulación de errores.
  c. Control de cambios.
  d. Comunicación.
- **Relación:** Es referentes a la acción de tomar una decisión a partir de la información almacenada de manera oportuna.
- **Riesgos de acceso:** se encuentra enfocado al acceso de los sistemas de gestión de información donde no se tienen medidas pertinentes para proteger la fiabilidad y confidencialidad de la información. Estos datos pueden estar comprometidos al acceso de cualquier persona que pertenezca a una estructura jerárquica en la organización. ; podemos mencionar:
  a. Procesos de negocio.
  b. Aplicación.
  c. Administración de la información.
  d. Entorno de procesamiento.
  e. Redes
  f. Nivel físico

- **Riesgos operacionales:** Los riesgos de operación se orienta a 3 factores, :
  - **a.** Backup y/o planes de contingencia.
  - **b.** Procedimientos de recuperación del sistema al momento de una caída.
  - **c.** Acompañamiento en los posibles fallos en el entorno de la información.
- **Riesgo de infraestructura:** son estructuras que no poseen una tecnología para enfrentar una contingencia dentro de su sistema de información; dentro de los elementos operacionales de tecnología se puede diagnosticar a partir de:
  - **a.** Una proyección gerencial.
  - **b.** Explicación de las aplicaciones utilizadas por la organización.
  - **c.** Gestión de seguridad.
  - **d.** Procedimiento de comunicaciones y de computación.
  - **e.** Gestión dentro los sistemas de bases de datos.
  - **f.** Gestión del negocio.
  - **g.** Riesgos físicos en general.
  - **h.** Riesgos Eléctricos.
  - **i.** Riesgos de fuego.
  - **j.** Riesgos mecánicos
  - **k.** Riesgos Químicos.

8. Propuesta.

8.1. Alcance

Elaborar el planteamiento de la situación problema implementando la metodología de planeación estratégica situacional, como una herramienta que permita identifica problemas, también el desarrollo de escenarios que permitan realizar los cambios que se necesiten para tratar el problema planteado.

En la ejecución del proyecto se tendrá en cuenta la entrega de la documentación para establecer los lineamientos requeridos respecto a políticas y procedimientos destinados a solucionar los aspectos específicos que se relacionan con el problema evidenciado. Es así como se podrán brindar herramientas que implementen los controles de seguridad de la información para que sea menor el riesgo de pérdida de la información o incumplimientos legales.

El presente proyecto no llevara a cabo la entrega de políticas, procedimientos implementados, prototipos, escenarios de pruebas, ni resultados específicos de la implementación de los controles.

8.2. Plan de trabajo.

Para el presente proyecto se contara con el siguiente plan de trabajo:

i. Fase de diagnóstico.
ii. Fase de preparación.
iii. Fase de planificación.
iv. Fase de tratamiento de riesgo.
v. Resultados y discusiones.

En cada fase, se realizara los pasos que permitirán avanzar en la búsqueda de soluciones al problema evidenciado.

8.3. Estructura Organizacional ALURA ANIMAL HEALTH NUTRITION SAS.

8.3.1. Visión.

Traer las soluciones del mañana, para apoyar la alimentación segura del mundo actual.

8.3.2. Misión.

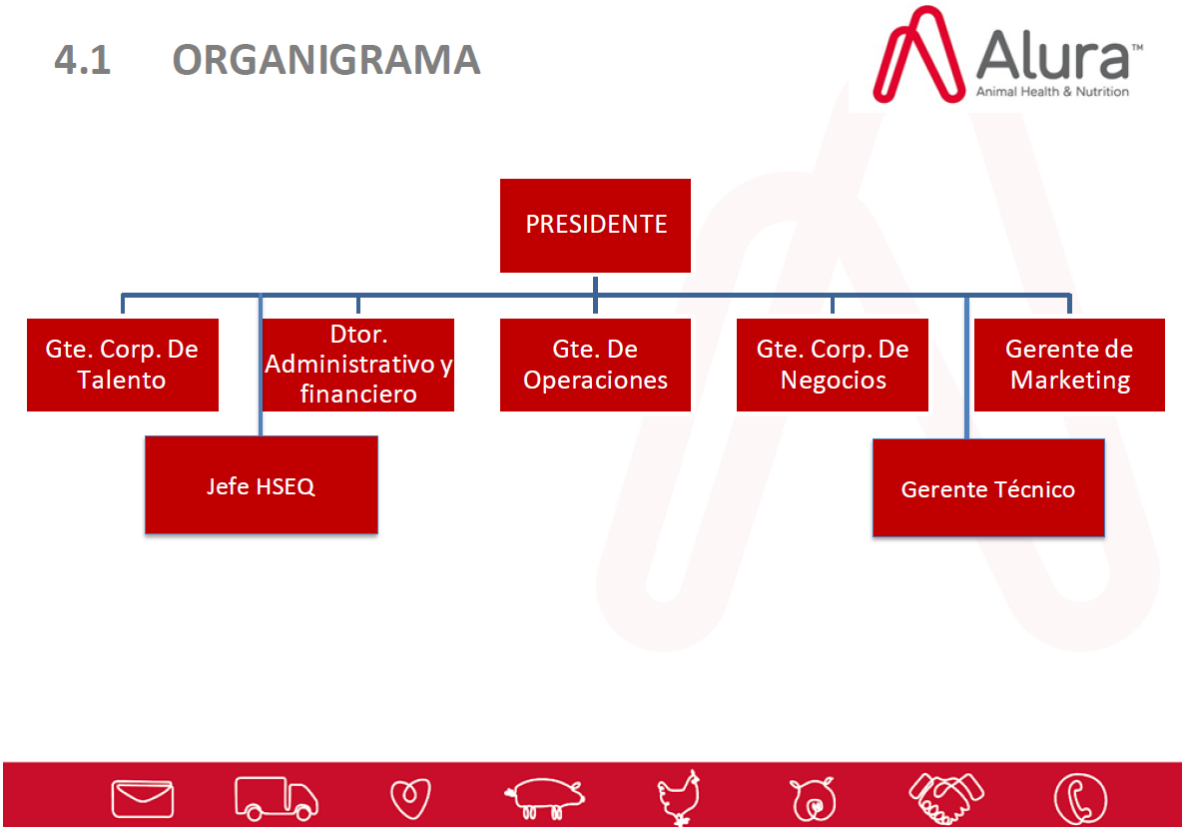
Ser una empresa capaz de proveer soluciones eficientes y competitivas que permitan incrementar la productividad de nuestros clientes a través de un equipo competente, generando valor en la cadena alimenticia

8.3.3. Propósito Corporativo.

Incrementar la productividad y generar valor a nuestros Clientes a través de soluciones eficientes y competitivas, apoyadas por el mejor talento humano.

8.3.4. Organigrama.

Ilustración 3. Organigrama Institucional.



9. Procedimientos para la implementación Del SGSI, ALURA ANIMAL HEALTH NUTRITION SAS

ALURA ANIMAL HEALTH NUTRITION SAS., como empresa debe poseer unas características para la implementación de un SGSI; ISO 27001 impulsa el acogimiento del ciclo de mejora continua PDCA; con la finalidad de definir los pasos relacionados en el Sistema de gestión de la seguridad de la información. Dentro del proyecto, no se toma como alcance encausar por procesos internos; se realizaran sugerencias que le ayudaran a los implicados determinar los procesos que se va a intervenir en el Sistema de gestión de la seguridad de la información.

Al establecer unos procedimientos para la implementación de la ISO27001 en ALURA ANIMAL HEALTH NUTRITION SAS, seguiremos los procesos del Planear, Hacer, Verificar y Actuar en la que se explicará cada una de las etapas para su implementación.

9.1. Definición.

El ciclo PHVA (o PDCA en inglés) es una herramienta de la mejora continua, diseñada por el Dr. Walter Shewhart en 1.920 y presentada por Deming a partir del año 1950, la cual se basa en un ciclo de 4 pasos: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act).[2]

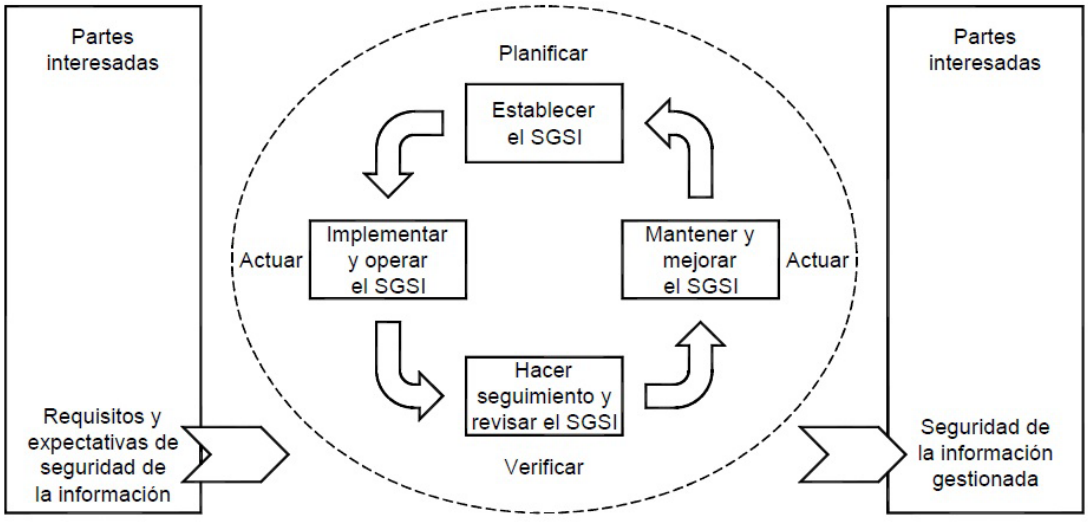
Esta metodología en la implementación de un sistema de gestión, la probabilidad de triunfo sea mayor; ya que permite aplicarla en política, objetivos y redes de proceso. Se puede aplicar a

[2] Plantilla para aplicar el ciclo PHVA. Tomado de: http://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html

todos los procesos la metodología a partir del PHVA “Planificar- Hacer-Verificar-Actuar”; a continuación se hará una explicación de cada uno:

- **Planear:** establecer los alcances, objetivos y procesos conforme a los términos del negocio y las políticas de la organización, para alcanzar los resultados de acuerdo con los requisitos del cliente.
- **Hacer**: Corresponde a la implementación de los objetivos del negocio.
- **Verificar:** supervisar el cumplimiento de los objetivos establecidos por la organización con el fin de que se cumplan.
- **Actuar:** busca la mejora continua de las prestaciones de la gestión de servicio a partir del desempeño de los procesos.

Ilustración 4. Modelo PHVA aplicado a los procesos de SGSI; Fuente https://ticcolombia.webnode.com.co/news/iso-9001/



9.2. Ciclo de Mejora Continua para el Sistema de Gestión de la Información.

Este trabajo se basó en el método de mejora continua bajo la norma 27001 para los sistemas de gestión de la información, con el fin de diseñar dicha metodología, para cada etapa. En la figura que a continuación se observa, tienen un esquema general de la metodología

expuesta, ayudando al cliente entender y desarrollar instrumentos para el cumplimiento que exige la ISO 27001.

Ilustración 5. Ciclo de Deming; fuente:https://image.slidesharecdn.com/sisemana11iso27001v011-160630153654/95/si-semana11-iso27001v011-46-638.jpg?cb=1467301033

A continuación conforme a los capítulos que se encuentran en la normas ISO 27001 y 27002; en las metodologías que se le planteo a la empresa farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS, con el fin de poderla Entender.

Tabla 4. Conexión Familia ISO27000

Metodología	**ISO 27001 (requisitos del SGSI) Sección**	**ISO 27002 (Código de buenas prácticas) Sección**
Salida del proyecto	5.1 y 5.2.1	
P	4.2.1	
H	4.2.2 y 5.2.2.	5.a 15
V	4.2.3., 6 y 7	
A	4.2.3 y 8	

Definición	3	
Documentación	4.3.	

9.3. Arranque del Proyecto.

A partir del apoyo adquirido por las gerencias de la farmacéutica para iniciar con la metodología de implementar el Sistema de Gestión de la seguridad de la información; cuyo cambio de cultura debe coexistir con la dirección ya que necesita estímulos constante, la ISO 27001 establece compromisos por parte de toda la organización para su correcto funcionamiento.

Las obligaciones por parte de la gerencia se demuestran mediante asentamiento de políticas, planes y objetivos del Sistema de Gestión de la Seguridad de la Información. Se debe instaurar funciones y responsabilidades de seguridad de la información; también se debe notificar a la compañía, la consideración de la ejecución de lo acordado, brindando los medios indispensables conforme con los niveles de aceptación de riesgos.

Las gerencias deben dirección debe suministrar los recursos que se necesiten para el despliegue del ciclo de mejora continua del sistema de gestión de la seguridad de la información; asegurando que los procedimientos, apoyen las condiciones del negocio, identificando las clausulas reglamentarias, así como los compromisos contractuales adquiridos.

9.4. Planear.

En esta etapa de la metodología, definimos el alcance del sistema de Gestión de Seguridad de la Información dentro de la organización teniendo en cuenta las políticas y directrices sobre lo que se va a desarrollar; también se muestran instrumentos para la evaluación y análisis de riesgos.

9.4.1. ALCANCE DEL SGSI.

La farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., determina el alcance del Sistema de Gestión de Seguridad en la Información “SGSI”; debe estar en misión del Core business, se recomienda limitar el alcance en el que comprometan los el negocio o que contenga información que pueda afectar el negocio; sin olvidar los activos y tecnologías. Es esencial disponer de los mapas de proceso e identificar los que va hacer parte del alcance.

Se debe tener en cuenta a los terceros y su peso dentro de la ISO 27001, al momento de establecer los alcances y los requisitos contractuales respecto a la seguridad de la información, se deben apreciar dentro del alcance del sistema. Al establecer planos de tecnología (comunicación y sistemas), se debe determinar las ubicaciones físicas y disponer de diagramas organizativos, donde facilite con claridad el alcance del SGSI.

Si la organización desea incluir cualquier otro proceso dentro del Sistema de Gestión de la Seguridad de la Información es válido, Se recomienda que al momento de incluir otros procesos sea bajo un análisis que proponga la importancia de incluirlo; no se busca que el SGSI sea muy

robusta y que sea poco efectiva. Al estar más compacta, refleja una buena práctica aún más cuando la organización no cuenta con estos procesos.

9.4.2. Política.

Dentro de los objetivos del proyecto no se incluye planeaciones estratégicas, por el contrario, se espera la empresa farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS tenga establecido dicho plan.

La política del SGSI, se debe centrar con los objetivos organización; las gerencias debe establecer un marco de referencia para fijar los objetivos específicos de control por cada proceso de la organización, los cual se deben instaurar con el líder de cada proceso.

Es importante durante la implementación del SGSI la publicación de la política a toda la Organización; buscando que las gerencias estén siempre alineadas con las decisiones de los otros niveles. Finalmente la política debe considerar la metodología y el criterio con respecto a la estimación del riesgo, en donde se debe tener en cuenta:

- Definir los procedimientos para la clasificación de los riesgos y el valor con el que impactan la seguridad de la información.
- Determinar las amenazas.
- Analizar y evaluar las amenazas detectadas.
- Determinar los objetivos para el tratamiento del control del riesgo.

9.4.3. Planificación del SGSI.

9.4.3.1 Evaluación de Riesgo.

Para el análisis de Riesgo de La compañía farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS, se utilizara la metodología MARGERIT, el cual permite medir y cuantificar los activos que posee la compañía.

9.4.3.2 Desarrollo de la Evaluación de Riesgo.

Para el desarrollo de la evaluación de riesgo a partir de la metodología MAGERIT, se utilizara la herramienta EAR/PILAR[3]; el cual incorpora los elementos de MAGERIT.

9.4.3.3 valoración de activos.

Con la valoración de los equipos, se busca tener una claridad de cuáles son los de mayor valor en la compañía y por tanto debe protegerse.

9.4.3.4 Identificación de activos.

Al identificar dentro del inventario facilitado por la Dirección de Tecnológico con el fin de poder determinar a qué área pertenece cada activo; a continuación identificamos las áreas y sus activos

[3] Aplicación de gestión de riesgo, descarga en http://www.ar-tools.com/es/index.html

Tabla 5. Identificación de activo

TIPO	NOMBRE DEL ACTIVO
INFORMACION	1. Servidor Principal 2. Servidor Laboratorio 3. Equipos PLC 4. Formulas Maestras 5. BD Sistema de Gestión 6. BD Microlab 7. Disco Duro Backups
SERVICIOS	8. Análisis de Muestras 9. Resultado de Análisis
APLICACIONES	10. Herramientas de ofimática 11. Antivirus 12. Sistema Operativo 13. Plataforma Sistema de Gestión
EQUIPAMIENTO INFORMATICO	14. Computadoras 15. Impresoras 16. Firewall 17. Switch
REDES DE COMUNICACIONES	18. Router Wifi 19. Red LAN 20. Telefonía 21. Internet
EQUIPAMIENTO AUXILIAR	22. UPS 23. Sistema de Vigilancia
INSTALACIONES	24. Cloud 25. Empresa
PERSONAL	26. Presidente 27. Director HSEQ 28. Director de Talento Humano 29. Asesor ext. Tecnología 30. Director de Operaciones 31. Director de Negocios 32. Director de Marketing 33. Director Financiero y administrativo

9.4.3.5 Valoración de activos.

Para la valoración de los activos de toma la información a partir de la metodología MAGERIT, con la siguiente nomenclatura:

- Disponibilidad [D].
- Integridad de los datos [I].
- Confidencialidad de la información [C].
- Autenticidad [A].
- Trazabilidad [T]

Al tener un valor cuantitativo se procede a calcular:

Tabla 6. Valoración Cuantitativo

Evaluación cualitativo	**Escala cuantitativo expresado en millon**	**Valor**
Muy Alto	Mayor $ 100	$ 100.000.000
Alto	Entre 100 y 50	$ 50.000.000
Medio	Entre 50 y 30	$ 30.000.000
Bajo	Entre 30 y 10	$ 10.000.000
Muy bajo	Entre 10 y 5	$ 5.000.000

Luego se procede a escalar la valoración del activo:

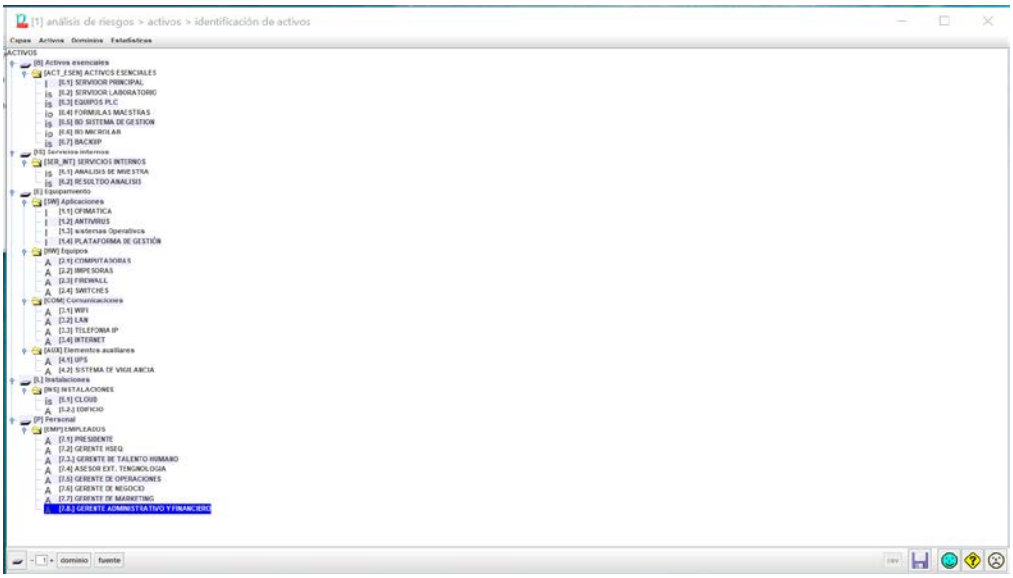
Tabla 7. Escala de valoración de activos

VALOR		**CRITERIO**
10	MA	Detrimento muy grave a la organización.
7 - 9	A	Detrimento grave a la organización.
4 - 6	M	Detrimento importante a la organización.
1 - 3	B	Detrimento menor a la organización.
0	D	Intrascendente en la organización

Con las tablas anteriores y con la ayuda de EAR/PILAR, se procederá a la valoración de los activos con la siguiente clasificación:

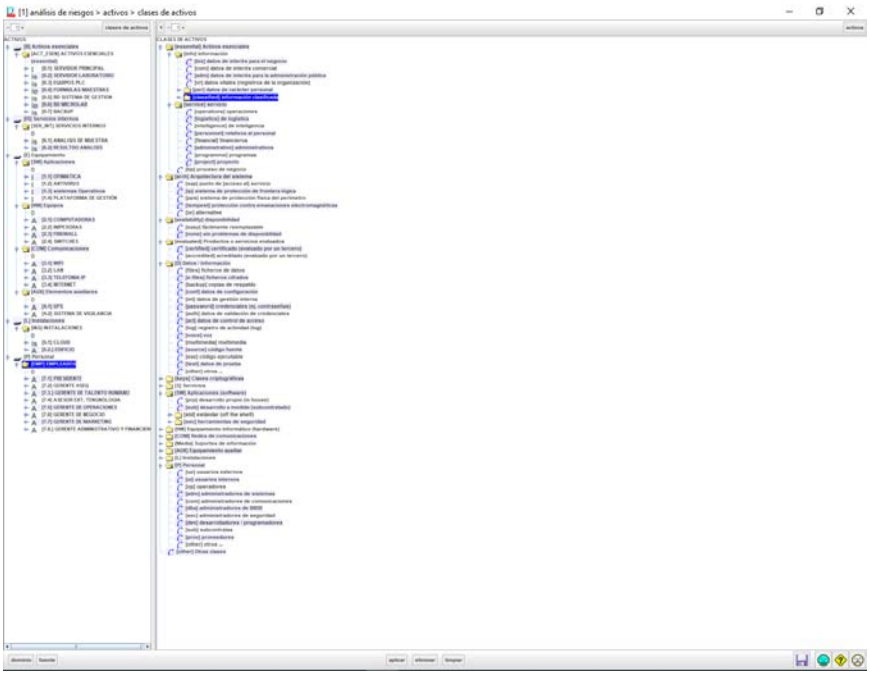
- Definición de activos

Ilustración 6. Definición de activos EAR/PILAR



- Clase de activos

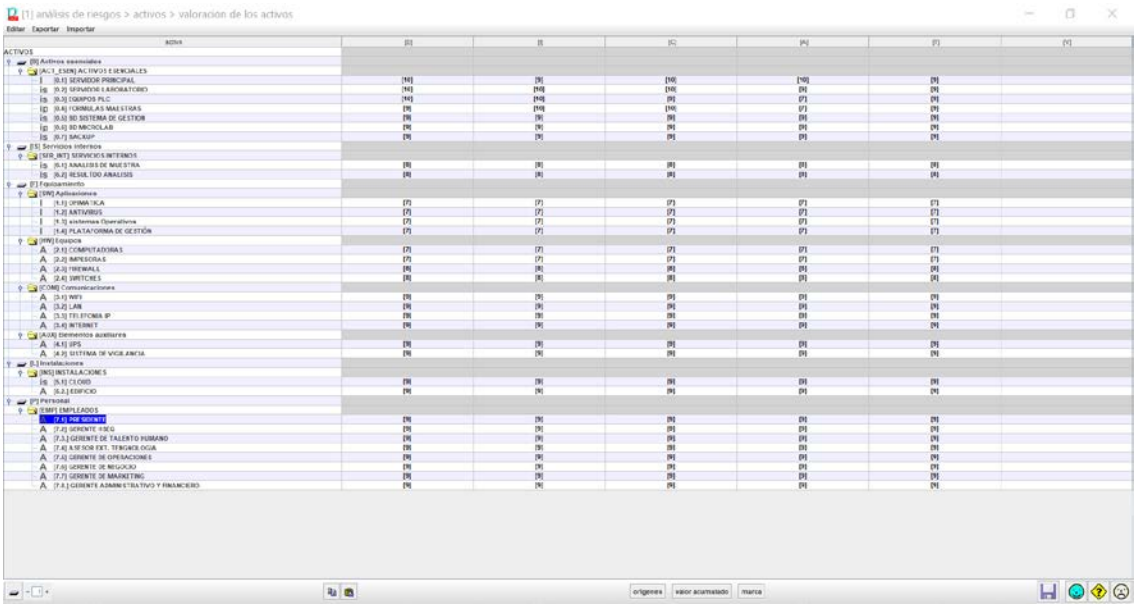
Ilustración 7.Clase de activos EAR/PILA



Dentro del EAR/PILAR, se tomó la siguiente escala para su desarrollo:

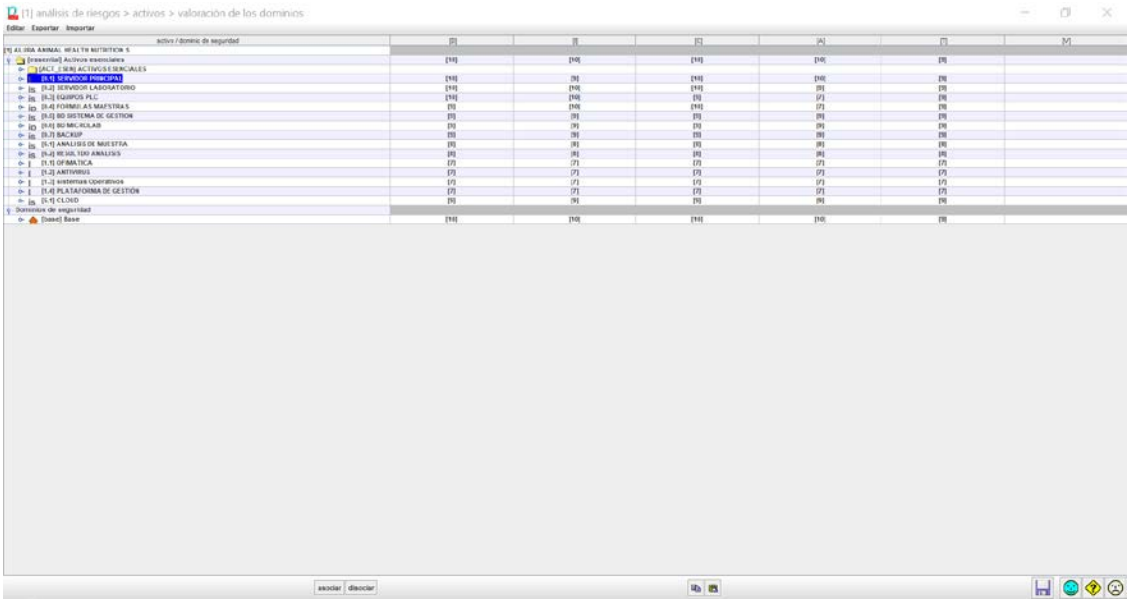
- Valoración de activos.

Ilustración 8. Valoración activos EAR/PILAR



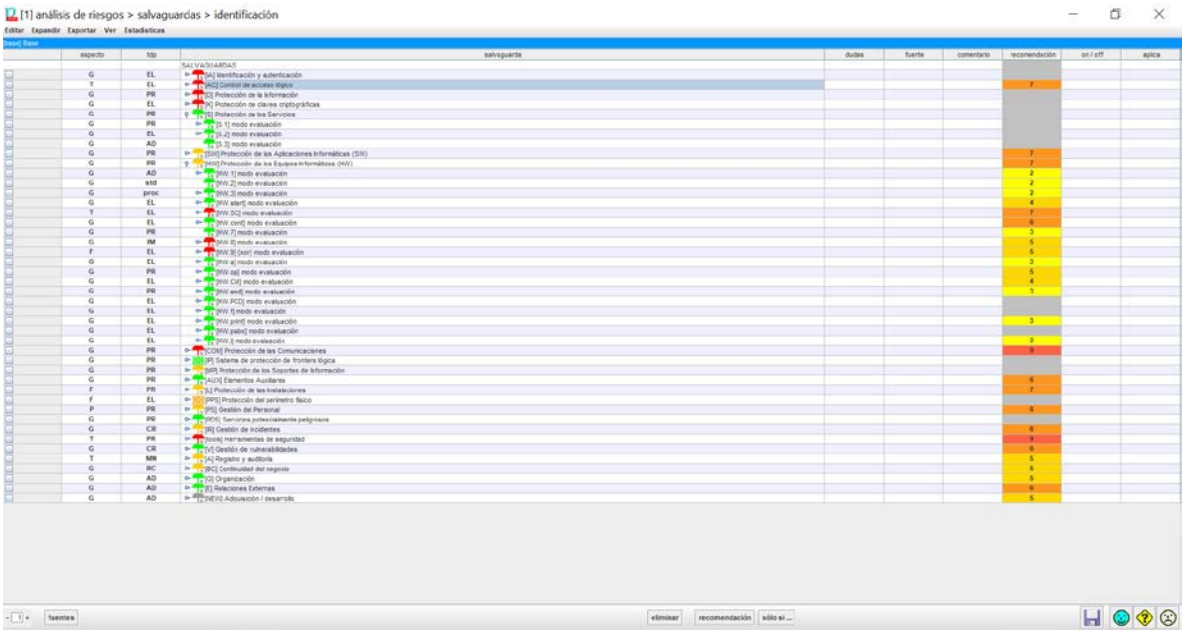
- Valoración de Dominio.

Ilustración 9. Valoración del dominio EAR/PILAR



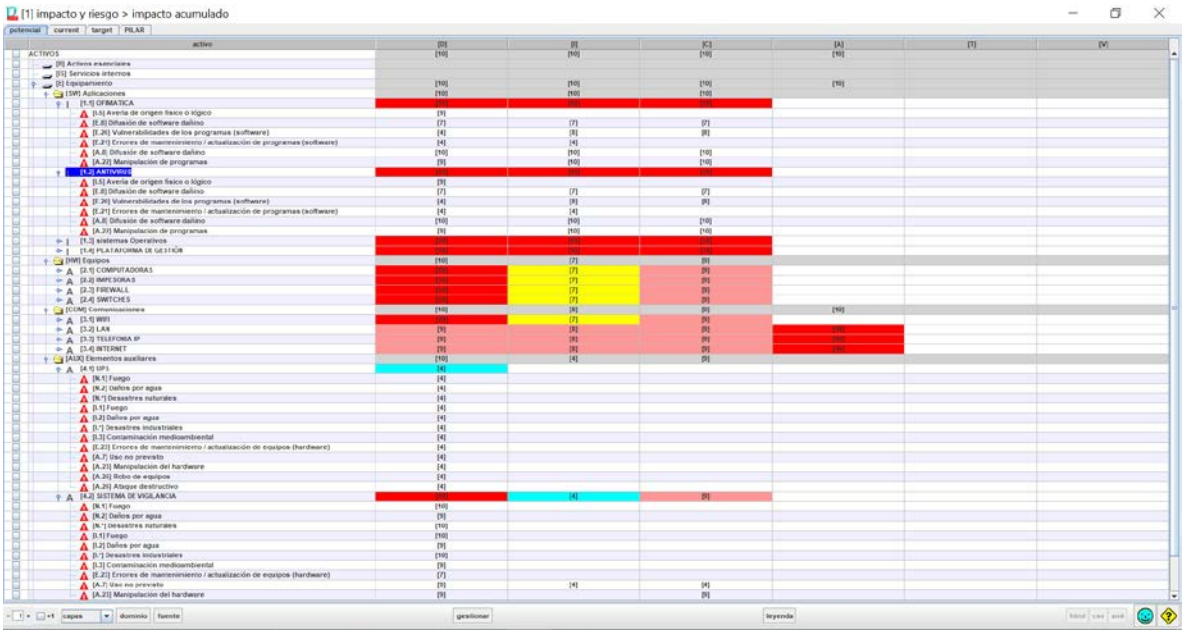
- Salvaguardias

Ilustración 10. Salvaguardias EAR/PILAR



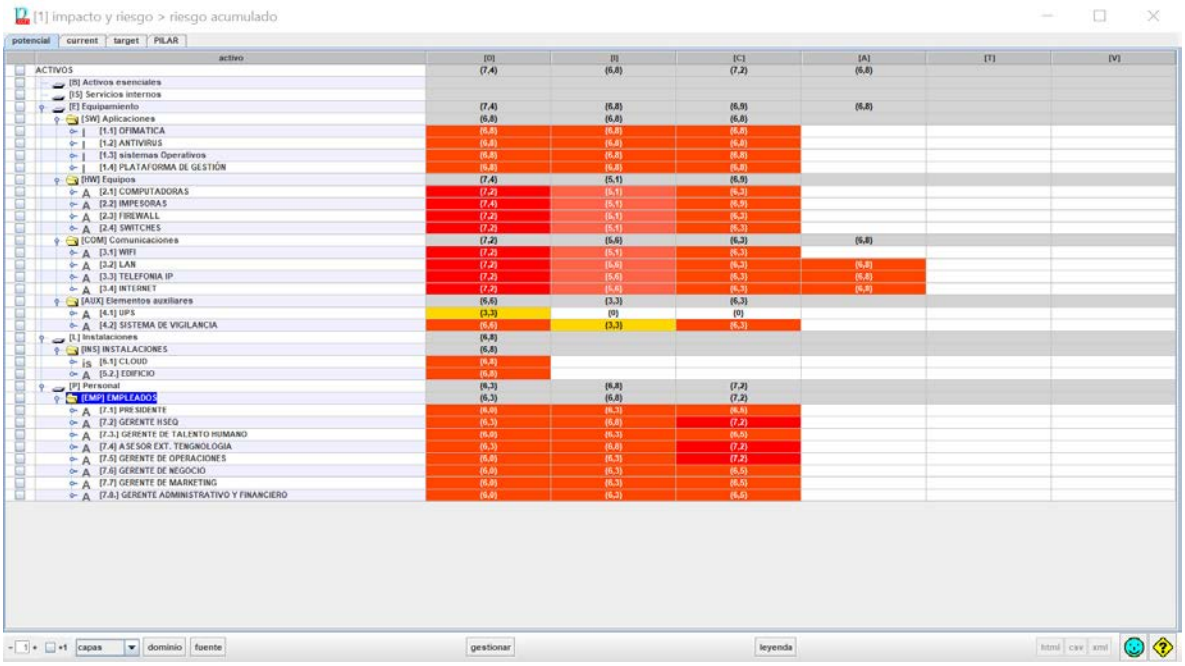
- Impacto del riesgo

Ilustración 11. Impacto de riesgo EAR/PILAR



- Riesgo acumulado

Ilustración 12. Riesgo acumulado EAR/PILAR



9.5. Hacer.

9.5.1. Controles, Implementación e indicadores para ALURA ANIMAL HEALTH NUTRITION SAS

En el proyecto se procede a relacionar algunas medidas de seguridad que se encuentran dentro de la norma 17799:2005 relacionadas con el objetivo del proyecto con la finalidad de tomar los controles y su implementación, tomando como base la norma ISO/IEC 27001[4]. (Ver Anexo 1).

[4] Tomado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

La ISO 27001 establece que la organización dentro de sus gerencias debe garantizar que todo el personal con responsabilidades en la seguridad de la información se encuentren capacitados con la finalidad de que pueda cumplir con sus obligaciones dentro de las políticas de la compañía ALURA ANIMAL HEALTH NUTRITION SAS., se debe definir sus habilidades; realizando formaciones y o contratando personal de ser necesario con el fin de evaluar las acciones que se están realizando y llevando actas de las actividades realizadas. La organización debe confirmar que todos los cooperantes tome conciencia de la importancia de sus labores dentro de los objetivos SGSI.

La Norma determina que toda acción que se realice para gestionar el riesgo debe estar incluidas dentro del plan de tratamiento, con el fin de ser parte de las mejoras continuas; esta se debe evaluar a partir de los objetivos.

9.6. Verificar.

Una vez en curso el SGSI, es esencial realizar los correspondientes seguimientos para validar el funcionamiento y su evolución dentro del sistema, buscando así poder corregir algún distanciamiento sobre lo que se planteó; también en búsqueda de oportunidad de mejora

Una de las condiciones de la Norma, es la revisión por parte de las gerencias implicadas con una regularidad de un año al Sistema de Gestión de Seguridad de la Información. Con esta verificación se busca asegurar que el SGSI este adecuada para los objetivos de la organización formando así parte del estado de verificación que se encuentra dentro de la mejora continua.

En este estado es factible llevar a cabo instrumentos de verificación del SGSI; que pueda facilitar la realización del seguimiento y poder determinar el cumplimiento de los acuerdos a la norma conforme a la metodología que se propuso a la empresa ALURA ANIMAL HEALTH NUTRITION SAS.,

De un modo practico, al verificar permite determinar riesgos que no se están tratando de forma correcta dentro del SGSI por diversas causas y o variables; Por lo tanto proporciona información para la toma de decisiones y poder acordar acciones de prevención o correctivas.

9.7. Actuar.

La implementación del SGSI debe ser una evolución dinámica, en esta etapa se debe tener claridad la misión del SGSI el cual es posicionar la seguridad de la información al mismo nivel que cualquier otro objetivo del negocio, y como tal, debe tener mejoras continuas. Es en esta fase donde se debe poner en funcionamiento las acciones correctivas, resultado de las comprobaciones, busca sacar la mayor ventaja SGSI. En esta etapa se debe tener en cuenta:

- Determinar las no conformidades del SGSI encontradas.
- Analizar las causas que lo generaron.
- Establecer acciones de corrección y prevención.
- Conseguir de la Dirección la aprobación y los recursos para llevar a cabo los cambios.
- Publicar las acciones y mejoras a toda la organización.

9.7.1. Entradas de progreso de las acciones:

- Reporte de las Auditoría interna.

- Reporte de las no conformidades de cada proceso.
- Reporte de conclusiones
- Reporte de PQR durante el proceso de revisión.
- Acciones de mejora a partir de las gerencias de la organización.

9.7.2. Personal Asignado:

- Personal de planeación: responsable de hacer las recomendaciones de mejora que se puede obtener y así realizar una valoración de los recursos que se necesitarían.
- Gerencia: Responsable en la autorización delos cambios, cuando este sea de un impacto al core del negocio o al requerir un presupuesto.

9.7.3. Salida del proceso a producción:

Se realizara un reporte donde explique los programas de mejoras haciendo mención de las conclusiones generadas durante la etapa de revisión del cumplimiento de los objetivos. Se debe revisar el impacto que generaría os cambios y las personas que van a estar involucradas, así como la programación para su ejecución.

Todo plan de mejora debe ser coordinado por las gerencias de tal forma que pueda causar molestias en la operatividad de la organización para evitar intromisión en los procesos.

10. Conclusiones

- La instauración de un SGSI en la farmacéutica ALURA ANIMAL HEALTH NUTRITION SAS., es de gran utilidad al proporcionarnos la adecuada metodología con el fin de respaldar la confidencialidad disponibilidad e integridad de los activos para mantener el Core del negocio.
- Los procesos y procedimiento de son importantes dentro del diseño de una organización con la finalidad de poder desplegar cualquier actividad que tenga el negocio conforme a lo indicado en el SGSI.
- El Diseño de la metodología debe ser adaptable para los cambios y mejoras a partir del ciclo de mejora continua PHVA. El planteamiento metódico propuesto por la norma, permite el siguiente desenlace:
    a. Determinar las acciones sobre la seguridad en los activos críticos, a partir dela investigación y desarrollo del análisis de riesgos.
    b. Encaminar los procesos a la mejora continua, por medo de procesos preventivos y correctivo.
    c. Contribuye a la mejora de la imagen corporativa y mantener la confianza de los colaboradores.
- Mitigar el impacto al diseñar un método de evaluación de riesgos, el cual nos permitirá afrontarlo de una forma coordinada.
- Es importante la precisión de los controles de seguridad con el fin de controlar el acompañamiento de los planes de acción, que se han integrado los cuales son centrados y con la posibilidad de cuantificar durante su ejecución

11. Bibliografía.

I. Disaster recovery plan (DRP) [En Línea]; https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan

II. ISO 27001: Planes de contingencia y la continuidad de negocio [En Línea]; https://www.pmg-ssi.com/2015/06/iso-27001-planes-de-contingencia-y-la-continuidad-de-negocio/

III. La importancia de un SGSI [En Línea]; https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

IV. ¿Por qué implantar un SGSI basado en la norma ISO 27001? [En Línea]; https://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/

V. Modelo PHVA aplicado a los procesos de SGSI; [En Línea]; https://ticcolombia.webnode.com.co/news/iso-9001/

VI. Ciclo de Deming [En Línea]; https://image.slidesharecdn.com/sisemana11iso27001v011-160630153654/95/si-semana11-iso27001v011-46-638.jpg?cb=1467301033

VII. Matriz de análisis de Riesgo [En Línea]; http://www.egambpm.com/wiki/index.php?title=Matriz_Analisis_de_Riesgos

VIII. Normas técnicas 27001 [En Línea]; http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

12. Anexos.

Anexo 1.

OBJETIVOS DE CONTROL Y CONTROLES

A.5 POLÍTICA DE SEGURIDAD			
A.5.1 Política de seguridad de la información Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.			
A.5.1.1	Documento de la política de seguridad de la información.	Control La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	
A.5.1.2	Revisión de la política de seguridad de la información.	Control La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 Organización interna Objetivo: gestionar la seguridad de la información dentro de la organización.			
A.6.1.1	Compromiso de la dirección con la seguridad de la información.	La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.	
A.6.1.2	Coordinación de la seguridad de la información.	Control Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.	
A.6.1.3	Asignación de responsabilidades para la seguridad de la información.	Control Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.	

Continúa

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Control Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.	
A.6.1.5	Acuerdos sobre confidencialidad	Control Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	
A.6.1.6	Contacto con las autoridades	Control Se deben mantener contactos apropiados con las autoridades pertinentes.	
A.6.1.7	Contacto con grupos de interés especiales	Control Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.	
A.6.1.8	Revisión independiente de la seguridad de la información.	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.	
A.6.2 Partes externas Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.			
A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	Control Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.	
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Control Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización	
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Control Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad	

A.7 GESTIÓN DE ACTIVOS			
A.7.1 Responsabilidad por los activos Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.			
A.7.1.1	Inventario de activos	Control Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.	
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad"[3] de una parte designada de la organización	
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	
A.7.2 Clasificación de la información Objetivo: asegurar que la información recibe el nivel de protección adecuado.			
A.7.2.1	Directrices de clasificación	Control La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	
A.7.2.2	Etiquetado y manejo de información	Control Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización	
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.1 Antes de la contratación laboral [4] Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.			
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	

3) El término "propietario" identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

4) Explicación: La palabra "contratación laboral" cubre todas las siguientes situaciones: empleo de personas (temporal o a término indefinido), asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos, y la terminación de cualquiera de estos acuerdos

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.1.2	Selección	Control Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos	
A.8.1.3	Términos y condiciones laborales.	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	
A.8.2 Durante la vigencia de la contratación laboral Objetivo: asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.			
A.8.2.1	Responsabilidades de la dirección	Control La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.	
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.8.3 Terminación o cambio del contratación laboral Objetivo: asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada..			
A.8.3.1	Responsabilidades en la terminación	Control Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.	
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	
A.8.3.3	Retiro de los derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio.	
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.1 Áreas seguras Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.			
A.9.1.1	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información	
A.9.1.2	Controles de acceso físico.	Control Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	Control Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	
A.9.1.4	Protección contra amenazas externas y ambientales.	Control Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	
A.9.1.5	Trabajo en áreas seguras.	Control Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.	

A.9 SEGURIDAD FÍSICA Y DEL ENTORNO			
A.9.2 Seguridad de los equipos Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.			
A.9.2.1	Ubicación y protección de los equipos.	Control Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado	
A.9.2.2	Servicios de suministro	Control Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	
A.9.2.3	Seguridad del cableado.	Control El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.	
A.9.2.4	Mantenimiento de los equipos.	Control Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	
A.9.2.5	Seguridad de los equipos fuera de las instalaciones.	Control Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos.	Control Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	
A.9.2.7	Retiro de activos	Control Ningún equipo, información ni software se deben retirar sin autorización previa.	
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.1 Procedimientos operacionales y responsabilidades Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.			
A.10.1.1	Documentación de los procedimientos de operación	Control Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	
A.10.1.2	Gestión del cambio.	Control Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.1.3	Distribución de funciones.	Control Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.	
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Control Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	
A.10.2 Gestión de la prestación del servicio por terceras partes Objetivo: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.			
A.10.2.1	Prestación del servicio	Control Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.	
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Control Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares.	
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	Control Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	
A.10.3 Planificación y aceptación del sistema Objetivo: minimizar el riesgo de fallas de los sistemas.			
A.10.3.1	Gestión de la capacidad.	Control Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.	
A.10.3.2	Aceptación del sistema.	Control Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.4 Protección contra códigos maliciosos y móviles Objetivo: proteger la integridad del software y de la información.			
A.10.4.1	Controles contra códigos maliciosos.	Control Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.	
A.10.5 Respaldo Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de linformación.			
A.10.5.1	Respaldo de la información.	Control Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.	
A.10.6 Gestión de la seguridad de las redes Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.			
A.10.6.1	Controles de las redes.	Control Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	
A.10.6.2	Seguridad de los servicios de la red.	Control En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.	
A.10.7 Manejo de los medios Objetivo: evitar la divulgación , modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.			
A.10.7.1	Gestión de los medios removibles	Control Se deben establecer procedimientos para la gestión de los medios removibles	
A.10.7.2	Eliminación de los medios.	Control Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.7.3	Procedimientos para el manejo de la información.	Control Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.	
A.10.7.4	Seguridad de la documentación del sistema.	Control La documentación del sistema debe estar protegida contra el acceso no autorizado.	
A.10.8 Intercambio de la información Objetivo: mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.			
A.10.8.1	Políticas y procedimientos para el intercambio de información	Control Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	
A.10.8.2	Acuerdos para el intercambio	Control Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.	
A.10.8.3	Medios físicos en tránsito.	Control Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.	
A.10.8.4	Mensajería electrónica.	Control La información contenida en la mensajería electrónica debe tener la protección adecuada	
A.10.8.5	Sistemas de información del negocio.	Control Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.	
A.10.9 Servicios de comercio electrónico Objetivo: garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura.			
A.10.9.1	Comercio electrónico	Control La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.	
A.10.9.2	Transacciones en línea	Control La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración , divulgación , duplicación o repetición no autorizada del mensaje.	

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES			
A.10.9.3	Información disponible al público	Control La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.	
A.10.10 Monitoreo Objetivo: detectar actividades de procesamiento de la información no autorizadas.			
A.10.10.1	Registro de auditorías	Control Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	
A.10.10.2	Monitoreo del uso del sistema	Control Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad	
A.10.10.3	Protección de la información del registro	Control Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.	
A.10.10.4	Registros del administrador y del operador	Control Se deben registrar las actividades tanto del operador como del administrador del sistema..	
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	
A.10.10.6	Sincronización de relojes	Control Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	
A.11 CONTROL DE ACCESO			
A.11.1 Requisito del negocio para el control de acceso Objetivo: controlar el acceso a la información.			
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	
A.11.2 Gestión del acceso de usuarios Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.			

A.11 CONTROL DE ACCESO			
A.11.2.1	Registro de usuarios.	Control Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	
A.11.2.2	Gestión de privilegios.	Control Se debe restringir y controlar la asignación y uso de privilegios.	
A.11.2.3	Gestión de contraseñas para usuarios.	Control La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	Control La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	
A.11.3 Responsabilidades de los usuarios Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.			
A.11.3.1	Uso de contraseñas.	Control Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	
A.11.3.2	Equipo de usuario desatendido.	Control Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	
A.11.3.3	Política de escritorio despejado y de pantalla despejada	Control Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	
A.11.4 Control de acceso a las redes Objetivo: evitar el acceso no autorizado a servicios en red.			
A.11.4.1	Política de uso de los servicios de red.	Control Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	
A.11.4.2	Autenticación de usuarios para conexiones externas.	Control Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	
A.11.4.3	Identificación de los equipos en las redes.	Control La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	

A.11 CONTROL DE ACCESO			
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	Control El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado	
A.11.4.5	Separación en las redes.	Control En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	
A.11.4.6	Control de conexión a las redes.	Control Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio (véase el numeral 11.1).	
A.11.4.7	Control de enrutamiento en la red.	Control Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.	
A.11.5 Control de acceso al sistema operativo			
Objetivo: evitar el acceso no autorizado a los sistemas operativos.			
A.11.5.1	Procedimientos de ingreso seguros	Control El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	
A.11.5.2	Identificación y autenticación de usuarios.	Control Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	
A.11.5.3	Sistema de gestión de contraseñas.	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	
A.11.5.4	Uso de las utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	
A.11.5.5	Tiempo de inactividad de la sesión	Control Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.	
A.11.5.6	Limitación del tiempo de conexión.	Control Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	

A.11 CONTROL DE ACCESO			
A.11.6 Control de acceso a las aplicaciones y a la información Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.			
A.11.6.1	Restricción de acceso a la información.	Control Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	
A.11.6.2	Aislamiento de sistemas sensibles.	Control Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	
A.11.7 Computación móvil y trabajo remoto Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.			
A.11.7.1	Computación y comunicaciones móviles.	Control Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.	
A.11.7.2	Trabajo remoto.	Control Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.1 Requisitos de seguridad de los sistemas de información Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.			
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Control Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.			
A.12.2.1	Validación de los datos de entrada.	Control Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados	
A.12.2.2	Control de procesamiento interno.	Control Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.	

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.2.3	Integridad del mensaje.	Control Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.	
A.12.2.4	Validación de los datos de salida.	Control Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias	
A.12.3 Controles criptográficos Objetivo: proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.			
A.12.3.1	Política sobre el uso de controles criptográficos.	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	
A.12.3.2	Gestión de llaves.	Control Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	
A.12.4 Seguridad de los archivos del sistema Objetivo: garantizar la seguridad de los archivos del sistema.			
A.12.4.1	Control del software operativo.	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	
A.12.4.2	Protección de los datos de prueba del sistema.	Control Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse	
A.12.4.3	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.	
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.			
A.12.5.1	Procedimientos de control de cambios.	Control Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Control Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Control Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	
A.12.5.4	Fuga de información	Control Se deben evitar las oportunidades para que se produzca fuga de información.	
A.12.5.5	Desarrollo de software contratado externamente	Control La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.			
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	
A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN			
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.			
A.13.1.1	Reporte sobre los eventos de seguridad de la información	Control Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	
A.13.1.2	Reporte sobre las debilidades de la seguridad	Control Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.			
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Control Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	

A.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.13.2.3	Recolección de evidencia	Control Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.	
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.			
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Control Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	
A.14.1.2	continuidad del negocio y evaluación de riesgos	Control Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.	
A.14.1.4	Estructura para la planificación de la continuidad del negocio	Control Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Control Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	

A.15 CUMPLIMIENTO			
A.15.1 Cumplimiento de los requisitos legales Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.			
A.15.1.1	Identificación de la legislación aplicable.	Control Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización	
A.15.1.2	Derechos de propiedad intelectual (DPI).	Control Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	
A.1.5.1.3	Protección de los registros de la organización.	Control Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	
A.15.1.4	Protección de los datos y privacidad de la información personal.	Control Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información.	Control Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	
A.15.1.6	Reglamentación de los controles criptográficos.	Control Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	
A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico Objetivo: asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización..			
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	Control Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.	
A.15.2.2	Verificación del cumplimiento técnico.	Control Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.	

A.15 CUMPLIMIENTO			
A.15.3 Consideraciones de la auditoría de los sistemas de información Objetivo: maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.			
A.15.3.1	Controles de auditoría de los sistemas de información.	Control Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Control Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.	