DISEÑO DE UN SGSI (SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION) BASADO EN ISO27001 PARA LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.

JORGE LEONARDO RODRÍGUEZ CORREA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ
2017

DISEÑO DE UN SGSI (SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION) BASADO EN ISO27001 PARA LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.

JORGE LEONARDO RODRÍGUEZ CORREA

Monografía para optar al título de Especialista en seguridad Informática

Asesor
John Freddy Quintero Tamayo
Ingeniero de Sistemas
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D. C. Abril 22 de 2017

DEDICATORIA

Dedico este proyecto a mis padres Luz Esthela Correa Pineda y José Guillermo Rodríguez Echeverry que desde el cielo me acompaña, por su constante apoyo, paciencia y compañía incondicional a lo largo de mi vida.

AGRADECIMIENTOS

El autor de este proyecto de grado desea expresar su agradecimiento a las siguientes personas que colaboraron durante todo el proceso de elaboración, revisión y culminación de este trabajo:

A Dios y a mi familia que me apoyaron incondicionalmente durante todo mi proceso de formación y en los momentos más difíciles de mi vida, además de acompañarme también en los mejores momentos.

A mis amigos, hermanos y compañeros por brindarme apoyo en cada fase del proyecto, compartir su conocimiento y mejores experiencias en pro del proyecto. Igualmente a la Universidad Nacional Abierta y a Distancia UNAD y a los tutores Jorge Enrique Ramírez y John Freddy Quintero Tamayo, por brindarme todos los conocimientos para formarme y crecer como profesional.

A LABORATORIOS SFC LTDA., por brindarme toda la información necesaria y recibirme amablemente durante la realización del proyecto.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

El sistema de gestión de seguridad de la información basada en ISO27001 para LABORATORIOS SFC LTDA, pretende ser un sistema de gestión integral que se pueda articular con cualquier sistema de gestión con el fin de asegurar los 3 (tres) pilares más importantes de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

El diseño de un SGSI en LABORATORIOS SFC LTDA implica una labor de compromiso por parte de la alta dirección, ya que es esta quien se encarga de aprobarla y proveer todos los recursos necesarios para su desarrollo, mantenimiento y mejora continua.

La metodología empleada para el diseño del SGSI fue el ciclo PHVA (Planear – Hacer – Verificar - Actuar), un enfoque basado en procesos el cual permite establecer, implementar, operar, hacer seguimiento, mantener y mejorar un sistema de gestión.

PALABRAS CLAVES - sistema de gestión, PHVA, diseño, riesgos, SGSI, planear, amenazas, salvaguardas, SFC, seguridad de la información, activos, confidencialidad, integridad, disponibilidad, sistema de gestión de seguridad de la información.

INTRODUCCION

La información constituye el activo más importante para las organizaciones y su proceso de negocio, por lo cual se busca preservar la confidencialidad, integridad y disponibilidad de la misma.

Todas las organizaciones están expuestas a vulnerabilidades y amenazas, las cuales deben ser detectadas, evaluadas y mitigadas para evitar que puedan afectar el proceso de negocio.

El diseño de un Sistema de Gestión de Seguridad de la Información debe estar directamente relacionado con los objetivos y las necesidades de la organización, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

LABORATORIOS SFC LTDA., es un laboratorio farmacéutico veterinario referente en el mercado del sector farmacéutico; entre su amplia gama de servicios presta los servicios de análisis fisicoquímico y microbiológico. El laboratorio de análisis microbiológico es la línea de negocio más importante para LABORATORIOS SFC LTDA ya que posee los clientes más importantes del sector farmacéutico (tanto para humanos como veterinarios).

El laboratorio se encuentra certificado en BPM y BPL, siendo esta última certificación la más representativa para la prestación de los servicios de análisis microbiológicos.

Como prestador de servicios de análisis microbiológicos el laboratorio, se encarga diariamente de emitir certificados de análisis para cada uno de sus clientes. La recepción, tratamiento, análisis y emisión de resultados de la muestras deben cumplir con estándares de seguridad adecuados que permitan asegurar la confidencialidad, integridad y disponibilidad tanto de la muestra como del resultado del ensayo. Esto se convierte tanto en un requerimiento de cada uno de sus clientes como de los organismos certificadores.

Existen muchos procesos y áreas críticas de la organización que no poseen controles o medidas de seguridad mínimas desde el punto de vista de la seguridad de la información, y que por la naturaleza de sus procesos deberían estar

implementadas. Los departamentos más críticos de la organización son: departamento de control de calidad, departamento de aseguramiento, departamento técnico y el departamento de talento humano / HSE.

Para el diseño del Sistema de Gestión de Seguridad de la Información al interior de LABORATORIOS SFC LTDA., se tuvieron en cuenta los requerimientos y controles del anexo A especificados en la norma NTC-ISO/IEC 27001 en su versión 2013.

1. DESCRIPCIÓN DEL PROBLEMA

LABORATORIOS SFC LTDA es un laboratorio farmacéutico veterinario que presta los servicios de maquila, análisis fisicoquímico, análisis microbiológico y validación de productos, la información que se maneja es de carácter confidencial pero aun así no posee el nivel adecuado de seguridad y procedimientos definidos que garanticen la confidencialidad de la misma. La información confidencial como certificados de análisis microbiológicos o procedimientos se encuentran en un estado crítico, ya que su protección es mínima y los riesgos a los que están expuestos no se han identificado claramente.

Al no contar con un sistema o procedimientos claros y definidos que permitan articular adecuadamente los procedimientos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información, se hace necesario el diseño de un SGSI (sistema de gestión de seguridad de la información) para proteger, minimizar los riesgos y darle el tratamiento adecuado a la información que posee la organización.

El riesgo que presenta la organización al no contar con adecuados controles en la información que maneja es la inminente pérdida de información, afectando la confidencialidad e integridad de las fórmulas maestras y certificados de análisis para la preparación de medicamentos veterinarios que hacen parte de su know how (conocimientos técnicos y administrativos).

1.1. FORMULACIÓN DEL PROBLEMA

¿De qué manera un enfoque basado en procesos permite diseñar el SGSI (Sistema de Gestión de Seguridad de la Información) para garantizar la confidencialidad, integridad y disponibilidad de la información en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA?

2. JUSTIFICACIÓN

En la actualidad la información se ha convertido en el activo más importante a proteger para todas las empresas, ya sea por fallos presentes en los equipos electrónicos, malas prácticas de usuarios, códigos maliciosos o hackers que afectan en muchos aspectos la continuidad del negocio; debido a esto surge la necesidad de seleccionar e implementar controles o procedimientos de seguridad que ayuden a las organizaciones a minimizar los riesgos presentes en sus labores diarias.

Para LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA la información es considerada un activo de valor estratégico y confidencial, por esta razón se deben implementar los mecanismos necesarios que garanticen un adecuado tratamiento en el ciclo de vida de la información, especialmente para aquellos casos que requieren mantener la disponibilidad de la misma.

Es indispensable preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad y disponibilidad de la información de la empresa y sus clientes.

Actualmente LABORATORIOS SFC LTDA se encuentra en proceso de renovación de registro ICA y en el proceso de certificación para ISO/IEC 17025, un SGSI adecuadamente estructurado permitiría cumplir con los requerimientos de seguridad exigidos por este conjunto de normas.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO27001 mediante el Ciclo PHVA que permita preservar la integridad, confidencialidad y disponibilidad de la información en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA – SFC.

3.2. OBJETIVOS ESPECÍFICOS

- Clasificar los activos informáticos existentes en la empresa LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.
- Realizar un análisis de las vulnerabilidades, amenazas y riesgos presentes en la organización con el fin de seleccionar las salvaguardas más adecuadas que ayuden a reducir los riesgos detectados.
- Determinar los controles existentes de acuerdo a la norma ISO/IEC 27001 e ISO/IEC 27002.
- Elaborar un manual para la implementación del SGSI en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.

4. DISEÑO METODOLÓGICO

4.1. DISEÑO METODOLÓGICO

Tabla 1. Modelo PHVA de un SGSI.

Planificar (establecer el SGSI)	Durante esta etapa debe establecerse la política, objetivos, procesos y procedimientos de seguridad que permitan gestionar el riesgo y mejorar la seguridad de la información.
Hacer (implementar y operar el SGSI)	Durante esta etapa se implementa y opera la política, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Esta etapa permite evaluar y medir el desempeño de la política y los objetivos de seguridad. Los resultados obtenidos se deben reportar a la dirección para su revisión.
Actuar (mantener y mejorar el SGSI)	Con el fin de lograr la mejora continua del SGSI se deben emprender acciones correctivas y preventivas con base a los resultados de las auditorías internas.

Fuente: NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS. Consultado el 22 de agosto de 2015 en: http://www.bogotaturismo.gov.co/sites/ intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Para el diseño del SGSI es necesario adoptar un enfoque basado en procesos que permita establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Sistema de Gestión adoptado por la organización[1].

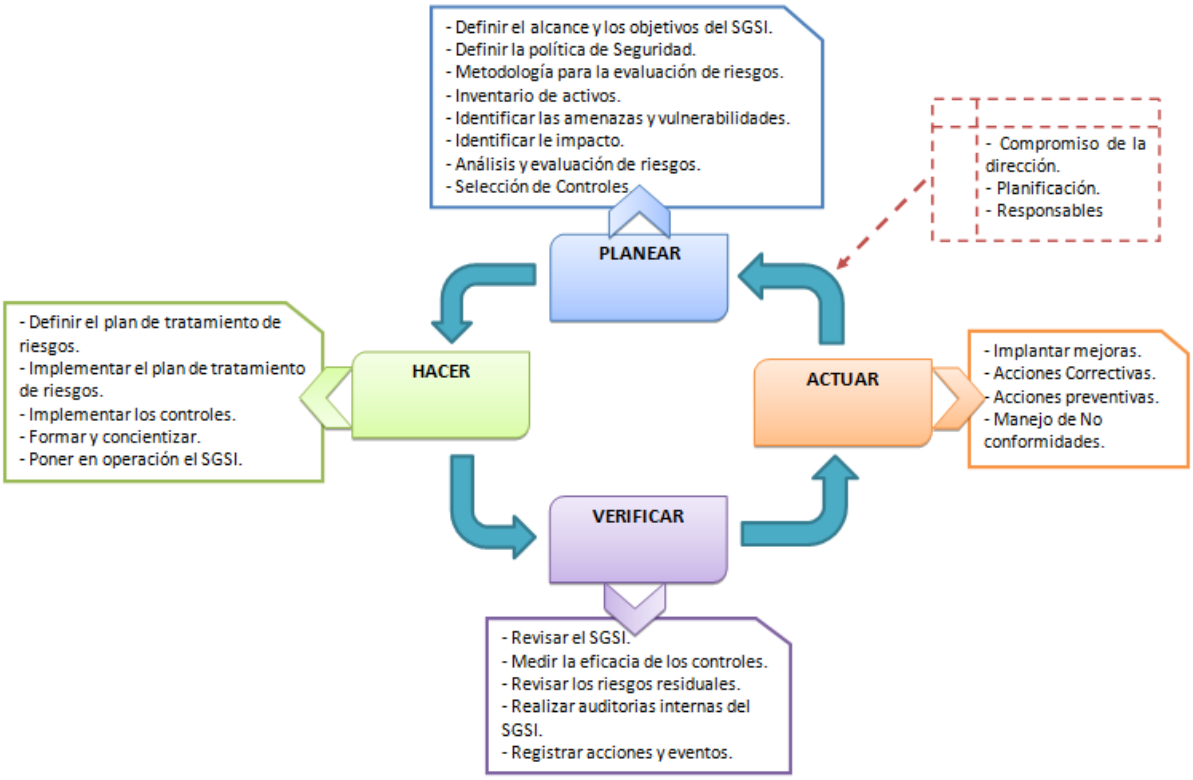
Según la norma ISO9001 “puede aplicarse a todos los procesos la metodología conocida como "Planificar - Hacer – Verificar - Actuar" (PHVA)”, respecto a lo

[1] NORMA INTERNACIONAL ISO 9001. *Sistemas de gestión de la calidad – Requisitos*. Consultado el 22 de agosto de 2015 en: http://farmacia.unmsm.edu.pe/noticias/2012/documentos/ ISO-9001.pdf

anterior con el fin de poder establecer una metodología general que permita implementar los procesos de la norma ISO27001:2013 para LABORATORIOS SFC LTDA, se adopta como metodología el ciclo PHVA (Planear – Hacer – Verificar – Actuar).

4.1.1. Ciclo PHVA para implantar el SGSI. En la figura 7 se puede observar un resumen del desarrollo de dicha metodología y cada entregable para tener en cuenta durante sus diferentes sus ciclos todo esto con el fin de conocer su desarrollo durante el proyecto.

Figura 1. Ciclo PHVA y desarrollo.



Fuente: El Autor.

El diseño metodológico adoptado para el diseño del SGSI en LABORATORIOS SFC LTDA está basado en el ciclo PHVA de la Norma ISO27001:2013 en la cual se contextualiza cada uno de sus ciclos y como se desarrollan.

Antes de empezar a describir el ciclo, es necesario que en la Organización se cuente con la identificación del punto en el cual la organización toma la decisión

de adoptar un sistema de gestión por fases, incluyendo los sistemas de calidad, de gestión de seguridad de la información, de las normas que regulan el negocio. Por lo general, esta fase se inicia como una decisión estratégica de la organización (se conoce como fase de concepción o direccionamiento estratégico), es decir, la alta dirección encuentra los beneficios de la implementación de un sistema (puede ser integrado) y otorga el direccionamiento del mismo a uno o varios responsables, así mismo, se plantean algunos retos puntuales en diferentes plazos y a partir de dicha decisión.

Algunas organizaciones, realizan "reservas presupuestales" o prevén la consecución de recursos económicos para que sean formulados proyectos concretos que faciliten el desarrollo de los mismos.

Una vez se definen los lineamientos generales, se puede mencionar que realmente se inicia con la fase del PLANEAR.

En la planificación del SGSI, se debe hacer un reconocimiento de los requisitos de la norma que se usa como guía de implementación (para este caso la Norma ISO 27001 en su versión 2013), especialmente para los numerales comprendidos entre el numeral 4 hasta el numeral 7.

Los numerales que se abarcan son:

- Numeral 4. Contexto de la Organización
- Numeral 5. Liderazgo
- Numeral 6. Planificación
- Numeral 7. Soporte

A partir del requisito 8 de la norma se empieza a desarrollar la fase del HACER del ciclo Deming. El requisito 9 de la norma, es el punto en donde las auditorias, mediciones y revisiones hacen la VERIFICACIÓN del funcionamiento del sistema de gestión. Para finalizar, el requisito 10 de la norma, abarca la fase del ACTUAR, pues permite que sean consolidados todos los resultados y la alta dirección valide la efectividad del sistema y avale la continuidad de operación del mismo.

4.2. MUESTRA POBLACIONAL

El grupo experimental tomado fueron 4 áreas de la organización que corresponden a las más críticas de LABORATORIOS SFC LTDA, en las cuales se aplicó una encuesta para determinar el problema actual en una determinada muestra. El nivel de confianza que se quiere obtener en las encuestas es del 75% y el margen de error es de 5%.

Figura 2. Fórmula Muestra población.

$$n = \frac{k^2 * p * q * N}{e^2 * (n-1) + k^2 * p * q}$$

Fuente: FEEDBACK. Calcular la muestra correcta.

Figura 3. Los valores k más utilizados y sus niveles de confianza.

K	1,15	1,28	1,44	1,65	1,96	2	2,58
Nivel de confianza	75%	80%	85%	90%	95%	95,5%	99%

Fuente: FEEDBACK. Calcular la muestra correcta.

k: es una constante que depende del nivel de confianza que se asigne. El nivel de confianza indica la probabilidad de que los resultados de nuestra investigación sean verdaderos o falsos.

e: Es el error muestral deseado, es la diferencia que puede haber entre el resultado obtenido entre la muestra poblacional y el total de la muestra.

p: Es la proporción de individuos que poseen la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5.

q: Es la proporción de individuos que no poseen esa característica.

n: Es el tamaño de la muestra (número de encuestas que se van a hacer)[2].

[2] FEEDBACK NETWORKS. Calcular la muestra correcta. Consultado el 10 Junio de 2015 en: http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

Se reemplazan los valores.

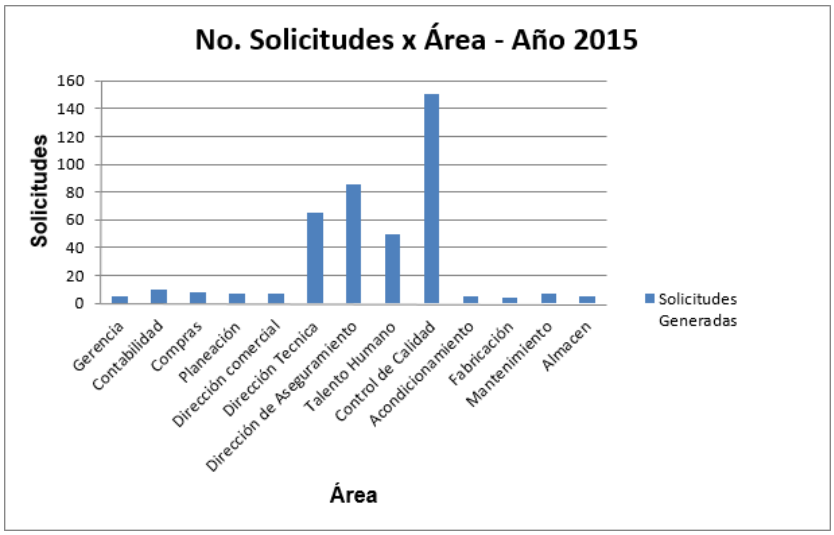
Figura 4. Calculando Muestra poblacional.

$$n = \frac{1.15^{2} * 0.05 * 0.95 * 4}{0.05^{2} * (4-1) + 1.15^{2} * 0.05 * 0.95} = \frac{0.25127500}{0.07031875} = 3.57337126$$

Fuente: El Autor.

La muestra poblacional nos da como resultado 4 personas / jefes de las áreas más críticas de la empresa.

Figura 5. Áreas más críticas de LABORATORIOS SFC LTDA.



Fuente: El Autor.

Actualmente LABORATORIOS SFC LTDA cuenta con 50 empleados y se encuentra dividida en 13 áreas de trabajo, de las cuales se tomaron como muestra poblacional las 4 áreas más críticas de la organización de acuerdo al número de solicitudes de servicio generadas.

4.3. INSTRUMENTOS

Se elaboró una encuesta la cual se aplicó a una muestra poblacional de 4 jefes de las áreas más críticas de LABORATORIOS SFC LTDA.

Tabla 2. Muestra Poblacional.

Área	Solicitudes Generadas
Gerencia	5
Contabilidad	10
Compras	8
Planeación	7
Dirección comercial	7
Dirección Técnica	65
Dirección de Aseguramiento	85
Talento Humano	50
Control de Calidad	150
Acondicionamiento	5
Fabricación	4
Mantenimiento	7
Almacén	5

Fuente: LABORATORIOS SFC LTDA.

4.3.1. Aplicación del instrumento. Las encuestas se aplicaron del 19 de junio al 29 de Octubre de 2015, se realizó a los jefes de las 4 áreas más críticas de la organización, se tomó un horario entre las 8:00 a.m. a 10:00 a.m. para la aplicación del instrumento.

5. MARCO DE REFERENCIA

5.1. MARCO TEORICO

5.1.1. Sistema de Gestión de la Calidad. Un sistema de gestión de calidad puede entenderse como un conjunto de los diferentes métodos, personas, recursos, estrategias, documentos, procedimiento e insumos que articulados generan resultados asociados al uso racional de recursos; además tiene como propósito la satisfacción de los clientes y los resultados deseados por la organización[3].

En pro de la satisfacción de sus clientes y resultados deseados, las organizaciones deben determinar, controlar y mejorar continuamente sus actividades. Este proceso se cubre muchas veces con la implementación de sistemas de gestión los cuales logran organización definidas y estructuradas en cada una de sus actividades. Los requisitos establecidos por los sistemas de gestión proporcionan una herramienta que permite a las organizaciones estructurar su trabajo y desarrollar metodologías que permitan medir su desempeño y actúen proactivamente frente a las oportunidades de mejora.

5.1.2. Seguridad de la Información. Considerando que la información representa valor para las organizaciones, esta debe clasificarse como un activo esencial para el negocio y velar por asegurar su protección[4].

Toda organización debe buscar preservar los 3 principios básicos de seguridad de la información, dichos principios se definen como[5]:

---

[3] Castro, T., & Cardona, L. (2014). DISEÑO DE UN SISTEMA DE GESTIÓN INTEGRADO PARA LA EMPRESA DE PINTURAS AUTOMOTRICES E INDUSTRIALES CARALZ LTDA. (Tesis de Especialización). Universidad Pontificia Bolivariana, Medellín, Colombia. Recuperado de: http://repository.upb.edu.co:8080/jspui/bitstream/123456789/1903/1/Dise%C3%B1o%20SGI%20CARALZ%20Ltda-Tahina%20Castro%20y%20Luz%20Dary%20Cardona.pdf

[4] García, W. (2012). POLÍTICAS, PLANES Y PROCEDIMIENTOS DE SEGURIDAD PARA ELECTROSOFTSYSTEM. Universidad Francisco de Paula Santander. Consultado el 23 de mayo de 2015 en: https://seguridadinformaticaufps.wikispaces.com/file/view/politicasDeSeguridadElectrosoftsystem.doc.

[5] UM. SEGURIDAD DE LA INFORMACIÓN. Consultado el 23 de mayo de 2015 en: http://www.um.edu.ar/catedras/claroline/backends/download.php?url=L0xpYy5fUm9sYW5kb19Db2

Confidencialidad: esta propiedad consiste en prevenir o asegurar la no divulgación de información a sistemas o personas no autorizadas.

Integridad: esta propiedad busca mantener y proteger los datos de cualquier modificación no autorizada.

Disponibilidad: esta propiedad busca que la información se encuentre únicamente a disposición de quienes lo requiera o se encuentren autorizados.

5.1.3. Norma ISO 27001. La norma ISO 27001 emitida por la ISO, (Organización internacional de Normalización) establece los requisitos para gestionar la seguridad de la información en una empresa.

La norma ISO 27001 puede ser implementada en cualquier tipo de organización, sin importar su actividad económica o el tamaño de la empresa (pequeña o grande). Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización[6].

5.1.4. Sistema de Gestión de Seguridad de la Información (SGSI). Un SGSI o Sistema de Gestión de Seguridad de la Información es un conjunto de políticas y procedimientos para la administración y gestión eficaz de la seguridad de la información.

Según la ISO 27001, la seguridad de la información consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información, así como cada uno de los sistemas implicados dentro de una organización para su gestión y tratamiento[7].

5kZS8xLjRfU2VndXJpZGFkX2RlX2xhX2luZm9ybWFjafNuLmRvYw%3D%3D&cidReset=true&cidReq=II020

[6] ADVISERA. ¿Qué es norma ISO 27001?. Consultado el 23 de Octubre de 2015 en: http://advisera.com/27001academy/es/que-es-iso-27001/

[7] ISO27000. ¿Qué es un SGSI?. Consultado el 23 de Octubre de 2015 en: http://www.iso27000.es/sgsi.html

5.1.5. Ciclo PHVA. Para monitorear y adoptar el proceso de planeación de un sistema de gestión se usa el modelo P.H.V.A. (planear, hacer, verificar y actuar), el cual permite planear, tomar acciones, verificar los resultados y actuar sobre los resultados esperados.

El ciclo PHVA consiste básicamente en:

- Planear: Definen las metas y los métodos para alcanzarla.
- Hacer: Después de haber realizado un proceso de formación se ejecutan y recogen todos los datos.
- Verificar: Se evalúan los resultados e identifican los problemas no resueltos.
- Actuar: Se toman las medidas correctivas necesarias para el cumplimiento de las metas.

A lo largo de todo este proceso, se encuentran presentes los indicadores e índices de gestión los cuales son usados para medir la efectividad de los objetivos estratégicos propuestos[8].

5.1.6. MAGERIT. MAGERIT permite saber cuánto valor está en juego y ayuda a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista[9].

Esta metodología está dividida en cuatro etapas:

- Planificación (definir lo que se va a cumplir).
- Análisis de Riesgos.
- Gestión de riesgos.

[8] UNIVERSIDAD NACIONAL DE COLOMBIA. CICLO DE CONTROL P.H.V.A. Consultado el 23 de Octubre de 2015 en: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4010014/Contenidos/Capitulo1/Pages/1.4/148Ciclo_Control_PHVA.htm

[9] PAE. MAGERIT v.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 12 de Agosto de 2015 en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VfRuntJ_Oko

- Seleccionar las salvaguardas.

La versión 3.0 de MAGERIT - Metodología de Análisis y Gestión de Riesgos Informáticos (Libro 1), que determina lo siguiente:

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

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

MAGERIT busca ofrecer un método sistemático para analizar los riesgos, concientizar a los responsables de los sistemas de información de la existencia de los riesgos y la necesidad de tratarlos a tiempo y planificar las medidas más adecuadas para tratar los riesgos y mantenerlos bajo control o minimizar su impacto[10].

Esta metodología además permite realizar una cuantificación y calcular el valor del activo de acuerdo al nivel de impacto que su daño o perdida pueda provocar en la empresa si se materializa. Esta valoración puede realizarse de manera cuantitativa o cualitativa de acuerdo a la siguiente escala:

- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (b)

[10] GÓMEZ, C. (s.f). METODOLOGIAS DE GESTION DE RIESGOS (OCTAVE, MAGERIT, DAFP). UNIVERSIDAD DE CALDAS. Consultado el 01 de octubre de 2015 en: http://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

- Muy bajo (MB)[11]

Es una metodología robusta, gratuita y que permite a los responsables en sistemas de información realizar un análisis y gestión de riesgos profundo, clasificar los activos, identificar las amenazas asociados a los activos, su nivel de impacto en la organización y seleccionar las salvaguardas más adecuadas para tratar y minimizar los riesgos y amenazas detectados previamente.

5.1.7. EAR / PILAR. PILAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos[12]. Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT[13].

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Para deducir el riesgo al que está expuesto el sistema se debe estimar la frecuencia con que se materializan las amenazas. PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son[14]:

- ISO/IEC 27002 (2005, 2013)- Código de buenas prácticas para la Gestión de la Seguridad de la Información
- ENS - Esquema Nacional de Seguridad

[11] UNAD. 3.2.2 VALORACIÓN DE LOS ACTIVOS. Consultado el 01 de octubre de 2015 en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-enlinea/322__paso_2_valoracin_de_los_activos.html

[12] PAE. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Consultado el 30 de octubre de 2015 en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VjuzWNIrLGg

[13] CCN. Análisis de Riesgos. Consultado el 30 de octubre de 2015 en: https://www.ccn.cni.es/index.php?option=com_content&view=article&id=7&Itemid=10&lang=es

[14] EAR. Entorno de análisis de riesgos. Consultado el 30 de octubre de 2015 en: http://www.ar-tools.com/es/index.html

5.2. MARCO CONCEPTUAL

5.2.1. Seguridad de la información. Tiene como finalidad proteger los sistemas de información y la información del uso, acceso, divulgación, destrucción o interrupción no autorizada[15].

5.2.2. Vulnerabilidades. Es un elemento o punto débil de un sistema informático el cual puede ser aprovechado por un atacante vulnerando la seguridad de la organización y causando daños a los sistemas informáticos[16].

5.2.3. Política de seguridad de la información. Es un conjunto de normas o prácticas para regular la forma en que se usa, protege y distribuye la información y los sistemas de información con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma[17].

5.2.4. Actividad de negocio. Proceso o conjunto de procesos establecidos por una organización para producir sus productos o servicios[20].

5.2.5. Activo. Son todos aquellos recursos con los que cuenta una empresa y que dan soporte a las actividades de negocio (Hardware y Software) [20].

5.2.6. Amenaza. Todo tipo de eventos que pueden desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos. Dentro de eventos se consideran tanto acciones, como interrupciones o falta de acción[18].

---

[15] AEC. SEGURIDAD DE LA INFORMACIÓN. Consultado el 25 de octubre de 2015 en: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

[16] UNAM. AMENAZAS Y VULNERABILIDADES. Consultado el 25 de octubre de 2015 en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

[17] ISMS. ¿Qué es una política de seguridad y cómo me afecta?. Consultado el 25 de octubre de 2016 en: http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=6&id_tema=56

[18] UNAL. GLOSARIO. Consultado el 25 de octubre de 2015 en: http://www.virtual.unal.edu.co/cursos/economicas/2006838/pdf/documentos/glosario.doc

5.2.7. Contingencia. Forma alterna de realizar alguna labor en caso de que no poder ejecutarla como normalmente se haría[19].

5.2.8. Desastre. Problema o evento no planificado, cuya consecuencia es la interrupción de los procesos de negocio durante un periodo de tiempo. Este tiempo de paralización de los procesos es superior a lo que la organización puede soportar sin sufrir perjuicios considerables para el negocio[20].

5.2.9. Disponibilidad. Característica o condición de un proceso de negocio/activo/recurso de encontrarse a disposición de la organización[20].

5.2.10. Impacto. Consecuencia evaluada de una interrupción[20].

5.2.11. Incidente. Se considera un incidente cualquier evento que no forma parte de la operación normal de un servicio y pueda causar una interrupción o reducción de la calidad de ese servicio[20].

5.2.12. Plan de continuidad del Negocio o Business Continuity Plan. Es un conjunto de criterios, normas de actuación y herramientas organizativas que, ante la ocurrencia de una contingencia, permiten la recuperación de la operatividad en el menor tiempo posible[20].

5.2.13. Copias de Seguridad. Son todas aquellas copias o respaldo de la información almacenadas en medios magnéticos.

5.3. MARCO LEGAL

- USP–NF: Es una combinación de dos compendios: la Farmacopea de Estados Unidos (USP) y el Formulario Nacional (NF). Contiene normas para medicamentos, formas farmacéuticas, fármacos, excipientes, productos

[19] SUGEF. PLAN DE CONTINUIDAD DEL NEGOCIO DE LA SUGEF. Consultado el 25 de octubre de 2015 en: http://www.sugef.fi.cr/manuales/plan_de_continuidad/documentos/P-CN-015.pdf

[20] INTECO. Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio. Consultado el 25 de octubre de 2015 en: https://www.incibe.es/file/t2sHW92KsAV506ZWcHTKRg

biológicos, preparaciones farmacéuticas, dispositivos médicos, suplementos dietéticos y otros tratamientos[21].

- Resolución 003619 de 17 de Septiembre de 2013: Manual de Buenas Prácticas de Laboratorio de control de Calidad de Productos Farmacéuticos[22].
- Resolución No. 03826 (22 Dic. 2003): cumplimiento de las Buenas Prácticas de Manufactura para las empresas productoras por contrato de medicamentos veterinarios[23].
- Resolución N° 003823 de 2013: requisitos para el reconocimiento de los laboratorios del sector agropecuario, los requisitos para acceder a las convocatorias del ICA como laboratorios autorizados y conformar la red nacional de laboratorios de ensayo/prueba y/o diagnóstico[24].
- Resolución 1056 (17 Abril 1996): disposiciones sobre el control técnico de los Insumos Pecuarios[25].
- Resolución 339 (24/01/2014): aclarar el procedimiento y las actividades que deben cumplir los laboratorios del sector agropecuario para la modificación de los registros como laboratorios reconocidos, y de igual manera el periodo transitorio para la articulación con la Resolución 3823 de 2013[26].
- Resolución Número 3028 de 2008 (13 de Agosto): áreas técnicas de producción de los establecimientos farmacéuticos[27].
- Informe 32 OMS: Especificaciones para las preparaciones farmacéuticas[28].

---

[21] USP. USP–NF. The United States Pharmacopeial Convention. Consultado el 31 de octubre de 2015 en: http://www.usp.org/es/tienda/productos-y-servicios/usp-nf

[22] INVIMA. Resolución 003619 de 17 de Septiembre de 2013. Consultado el 30 de octubre de 2015 en: https://www.invima.gov.co/index.php?option=com_content&view=article&id=3293:resolucion-003619-de-17-de-septiembre-de-2013&catid=147:resoluciones-medicamentos-&Itemid=203

[23] ICA. Resolución No. 03826. Consultado el 30 de octubre de 2015 en: http://www.ica.gov.co/getattachment/3c7a52a9-8696-4d9b-b6e8-f23cbbac110d/3826.aspx

[24] ICA. Resolución 003823. Consultado el 30 de octubre de 2015 en: http://www.ica.gov.co/Normatividad/Normas-Ica/Resoluciones/2013.aspx

[25] ICA. Resolución 1056 Consultado el 30 de octubre de 2015 en: http://www.ica.gov.co/getattachment/498ca7d0-65d6-4f6d-bb03-bc905c0a22d7/1056.aspx

[26] ICA. Resolución 000339. Consultado el 30 de octubre de 2015 en: http://www.ica.gov.co/getattachment/bb11751b-6ef7-4132-a86b-951586d38f4d/2014R00339.aspx

[27] MINSALUD. Resolución número 3028 de 2008. Consultado el 30 de octubre de 2015 en: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%203028%20DE%202008.pdf

[28] INVIMA. Serie de Informes Técnicos de la OMS. Consultado el 30 de octubre de 2015 en: https://www.invima.gov.co/images/pdf/medicamentos/informes/informe32delaOMScompleto.pdf

- Informe 441 OMS “Buenas prácticas de la OMS para laboratorios de control de calidad de productos farmacéuticos”[29].
- Decreto 4741 de 2005 (Diciembre 30): prevención y el manejo de los residuos o desechos peligrosos generados en el marco de la gestión integral[30].
- Ley 603 de 2000 (Julio 27): Protección de los derechos de autor en Colombia[31].
- Ley estatutaria 1266 de 2008 (Diciembre 31): disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países[32].
- Ley 1273 de 2009 (Enero 05): la protección de la información y de los datos - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones[33].
- Ley 1341 de 2009 (Julio 30): principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro[34].
- Ley estatutaria 1581 de 2012 (Octubre 17): se dictan disposiciones generales para la protección de datos personales[35].
- Decreto 1377 de 2013 (Junio 27): Protección de Datos, decreto por el cual se reglamenta la Ley 1581 de 2012[36].

[29] APPS. Buenas prácticas de la OMS para laboratorios de control de calidad de productos farmacéuticos. Consultado el 30 de octubre de 2015 en: http://apps.who.int/prequal/info_general/documents/TRS957/TRS957_annex1_SPANISH.pdf

[30] ALCALDIABOGOTA. DECRETO 4741 DE 2005. Consultado el 30 de octubre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18718

[31] ALCALDIABOGOTA. LEY 603 DE 2000. Consultado el 04 de Noviembre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960

[32] ALCALDIABOGOTA. LEY ESTATUTARIA 1266 DE 2008. Consultado el 04 de Noviembre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

[33] ALCALDIABOGOTA. LEY 1273 DE 2009. Consultado el 04 de Noviembre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[34] ALCALDIABOGOTA. LEY 1341 DE 2009. Consultado el 04 de Noviembre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

[35] ALCALDIABOGOTA. LEY ESTATUTARIA 1581 DE 2012. Consultado el 04 de Noviembre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[36] ALCALDIABOGOTA. DECRETO 1377 DE 2013. Consultado el 04 de Noviembre de 2015 en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

6. DESARROLLO DEL PROYECTO

6.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO

6.1.1. Estructura Organizacional.

Figura 6. Logo de la empresa.

Fuente: LABORATORIOS SFC LTDA.

- Identificación: Nit 830.001.242-1
- La empresa: LABORATORIOS SERVICIOS FARMACÉUTICOS DE CALIDAD S.F.C LTDA.
- Ciudad: Bogotá D.C.
- Dirección: Cra. 106 No. 15 A – 25 Mz 4 Interior 38 B Bodega 1
- Teléfono: 4395155
- Código de la actividad económica No. 2100 (Según Decreto 1607 del 31 de Julio de 2002 del Ministerio de Protección Social y Resolución 139 de 2012 de la DIAN)
- Tipo de Sector económico: Privado

Ubicados en la Zona Franca de Bogotá desde el año 2004, Laboratorios SFC LTDA., es un laboratorio farmacéutico veterinario con experiencia de 17 años en el mercado, prestando servicios de maquila, análisis fisicoquímico, microbiológico y validación de productos; cumpliendo con los más altos estándares de calidad y exigencias del mercado. Cuenta con una planta adecuada para ofrecer a sus clientes externos y proveedores la mejor atención.

Laboratorios S.F.C LTDA., es una empresa dedicada a la producción de medicamento de uso farmacéutico veterinario de excelente calidad, cuyo principal propósito es colaborar con el desarrollo de la salud animal, a través del mejoramiento continuo de sus procesos. A continuación se relacionan los servicios prestados por Laboratorios SFC Ltda.:

- Fisicoquímico: HPLC, Espectrofotometría y caracterización.
- Microbiológico: Recuentos, Esterilidad y Endotoxinas.
- Validación de desinfectantes.
- Pruebas de Estabilidad Natural y Acelerada.
- Diseño y evaluación de productos.

6.1.2. Misión. Velar por la salud animal y por el bienestar de nuestro personal, empleados, socios y clientes, a través de la fabricación de productos farmacéuticos de uso veterinario de excelente calidad, bajo la normatividad de las buenas prácticas de manufactura y de la reglamentación vigente[37].

6.1.3. Visión. Mejoramiento continuo para mantenerse como un laboratorio fabricante de medicamentos veterinarios reconocido entre los mejores por su calidad en los procesos de fabricación, y destacado por el cumplimiento en las entregas a nuestros clientes[37].

6.1.4. Política de calidad. En laboratorios S.F.C. LTDA nos dedicamos a la fabricación de medicamentos de uso veterinario de la más alta calidad, comprometidos con el cumplimiento de las BPMv (Buenas Prácticas de Manufactura vigentes) y la reglamentación vigente, buscando la satisfacción de nuestros clientes y del consumidor final mediante la mejora continua de nuestros procesos[37].

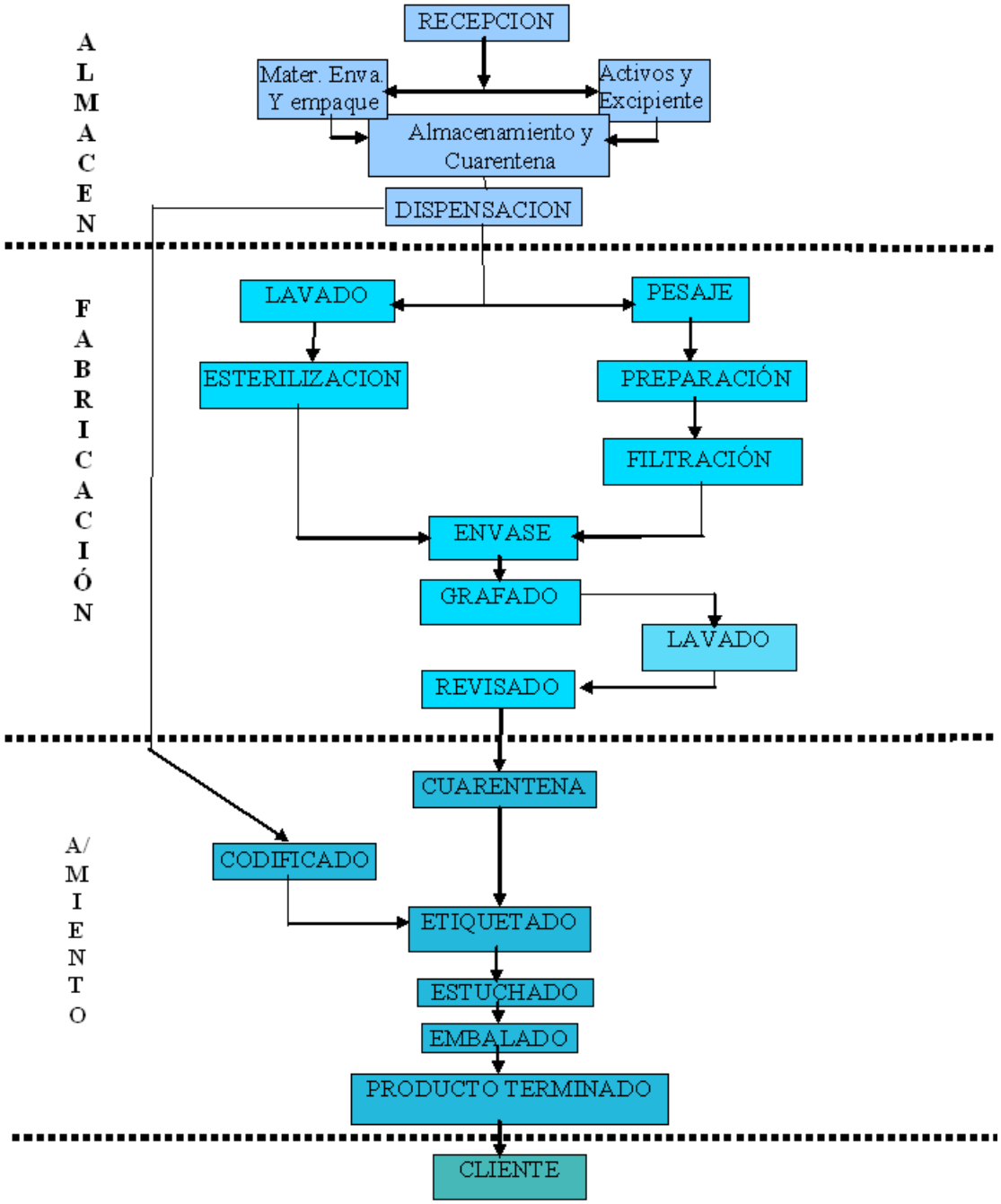
6.1.5. Actividad económica. Empresas dedicadas a la fabricación de productos farmacéutico, incluye solamente fabricación de algodón, gasas, vendas y similares, fabricación de productos farmacéuticos, medicamento.

6.1.6. Organigrama de la empresa. …Véase el Anexo B...

[37] LABORATORIOSSFC. NOSOTROS. Consultado el 04 de Noviembre de 2015 en: http://laboratoriossfc.com.co/?page_id=25

6.1.7. Descripción de los procesos desarrollados.

Figura 7. Diagrama de procesos.



Fuente: LABORATORIOS SFC LTDA.

6.2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Tabla 3. Descripción partes interesadas.

Identificación	Requisito	Requisito de obligatorio cumplimiento y reglamentación	Obligaciones Contractuales
Entes gubernamentales	Cumplimiento con la legislación vigente • Procedimiento: responsable, programación	• Protección de Datos Personales. • Contratación de Bienes Informáticos y Servicios Telemáticos. • Políticas Laborales y Prestación de Servicios por Terceros. • Servicios de Comercio Electrónico. • Propiedad Intelectual.	No Aplica
Cliente	Protección de las fórmulas maestras (maquila) Protección de resultados (Control de calidad)	• Protección de datos personales. • 27001: confidencialidad, integridad y disponibilidad, autenticidad.	Confidencialidad

Identificación	Requisito	Requisito de obligatorio cumplimiento y reglamentación	Obligaciones Contractuales
Trabajadores	Protección y manejo adecuado de la información personal	• Protección de datos personales.	Cláusulas de confidencialidad en los contratos
Junta de socios a través de la alta dirección	Continuidad del negocio	• Certificado de cámara y comercio.	No Aplica
Proveedores	Uso adecuado de la información de los proveedores	• Protección de datos personales.	
Contratistas	Controlar planilla de pago de seguridad social	• Protección de datos personales.	Seguridad de la información incluyendo tecnología.
SGI	Confidencial Disponibilidad Integridad Trazabilidad	• 27001 • 17025 • 9001 • Informe 32 BPM • Informe 44 / 45 BPL	Los contenidos en los contratos de los clientes

Fuente: LABORATORIOS SFC LTDA.

7. ALCANCE

La organización necesita definir los límites del SGSI para decidir qué información quiere proteger. La organización entiende que la información debe ser protegida independientemente del tipo de dato, medio de almacenamiento, método de procesamiento o protocolos de transferencia aplicados, dentro o fuera del alcance del SGSI.

Ante el hecho de que un conjunto determinado de información esté fuera del alcance del SGSI, no significa que no se le aplicarán las medidas de seguridad identificadas; por el contrario, esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad será transferida a un tercero que administre dicha información.

Los procesos que hacen parte del alcance inicial del Sistema de Gestión de Seguridad de la Información (SGSI) son:

- Procesos de Cadena de Valor: Forman parte del alcance inicial las áreas de Microbiología y Fisicoquímico.
- Procesos de Dirección: Forman parte del alcance inicial las áreas de Dirección Técnica y Aseguramiento de Calidad.
- Procesos de Soporte: Forma parte del alcance inicial el área de Recursos Humanos / HSE.

Estos procesos y áreas se desarrollan al interior de la sede principal de los LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA., ubicada en la carrera 106 Número 15 A – 25, Manzana 4, Interior 38 B, Bodega 1, de la Zona Franca de la ciudad de Bogotá D.C. – Colombia.

Igualmente, el alcance del SGSI cubrirá los activos de información identificados para dichos procesos y áreas tales como son las base de datos, ficheros de datos, documentación del sistema, manuales de usuario, material de capacitaciones, políticas, instructivos, procedimientos, formatos, planes de continuidad y de recuperación, formulas maestras, datos confidenciales de los clientes, certificados de análisis microbiológicos (internos y externos), documentos en papel que corresponden a contratos y documentación de la compañía, activos de software que corresponden a aplicaciones de software, herramientas de desarrollo y

utilidades y activos físicos que corresponden equipos de comunicaciones, redes, discos extraíbles y computadoras.

Por último, NO forman parte del alcance inicial del SGSI y por tanto quedarán excluidas las siguientes áreas y procesos:

Procesos:

- Gestión de la Dirección
- Gestión del aseguramiento de la calidad
- Gestión de Dirección Técnica
- Gestión de Investigación Científica
- Productos propios
- Maquila
- Gestión de mantenimiento y metrología
- Gestión Administrativa
- Gestión Comercial
- Gestión de Planeación
- Gestión del Talento Humano y HSE
- Gestión Contable
- Gestión de Sistemas de Información

Áreas:

- Almacén.
- Contabilidad.
- Fabricación.
- Acondicionamiento.
- Planeación.
- Mantenimiento.

En la siguiente revisión del SGSI se evaluarán las áreas que no fueron incluidas en el alcance inicial.

Este alcance será la guía para el diseño del SGSI en su primera fase, y podrá ser revisado y actualizado según lo indiquen las directivas de la entidad y/o en la revisión por parte de la dirección al concluir dicha fase.

7.1. ENTREGABLES

- Inventario de activos.
- Metodología de análisis y gestión de riesgos.
- Declaración de aplicabilidad.
- Política del Sistema de Gestión de Seguridad de la Información.
- Manual de seguridad de la información.

8. PLANIFICACIÓN DEL SGSI

8.1. METODOLOGÍA DE EVALUACIÓN DE RIESGOS

Para el análisis de riesgos de LABORATORIOS SFC LTDA se utilizará la metodología MAGERIT, la cual permite determinar las medidas apropiadas para cuantificar y dar el tratamiento adecuado a los activos que posee la empresa.

8.2. DESARROLLO DE LA METODOLOGÍA

Como apoyo al desarrollo de esta metodología se utilizará la herramienta EAR/PILAR, la cual es una herramienta de análisis de riesgos que incorpora todos los elementos de la metodología MAGERIT en su 3ra versión.

8.3. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

8.3.1. Identificación de activos. Para realizar la identificación de los activos se utilizará el inventario proporcionado por la Gerencia y se determinara el tipo de activo al que pertenece de las áreas seleccionadas en el alcance, los cuales son:

Tabla 4. Identificación de Activos.

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACION	1. [SRV_PPAL] Servidor Principal
	2. [SRV_MICRO] Servidor Microbiología
	3. [HPLC] Equipos HPLC
	4. [FORM_MTRAS] Formulas Maestras
	5. [BD_SG] BD Sistema de Gestión
	6. [BD_MICRO] BD MICROLAB
	7. [HD_BKP] Disco Duro Backups
SERVICIOS	8. [ANAL_MTRAS] Análisis de Muestras
	9. [RTDO_ANAL] Resultado de Análisis
APLICACIONES	10. [PGN_WEB] Página web
	11. [HER_OFI] Herramientas de ofimática
	12. [ANT_VIR] Antivirus
	13. [SO] Sistema Operativo

TIPO	NOMBRE DEL ACTIVO
	14. [PLAT_SG] Plataforma Sistema de Gestión
	15. [MICROLAB] Plataforma MICROLAB 1.0
EQUIPAMIENTO INFORMATICO	16. [PC] Computadoras
	17. [IMP] Impresoras
	18. [FIREWALL] Firewall
	19. [SWT] Switch
REDES DE COMUNICACIONES	20. [WIFI] Router Wifi
	21. [LAN_SFC] Red LAN
	22. [TEL] Telefonía
	23. [IE] Internet
EQUIPAMIENTO AUXILIAR	24. [UPS] UPS
	25. [SIS_VIG] Sistema de Vigilancia
INSTALACIONES	26. [CPD] CPD
	27. [SFC] Empresa
PERSONAL	28. [DIR_CALIDAD] Directora Aseguramiento de Calidad
	29. [RRHH] Director de Talento Humano/HSE
	30. [DT] Directora técnica
	31. [ASIST_DIR_CALID] Asistente Dirección de Aseguramiento de Calidad
	32. [AN_FQ] Analista de Fisicoquímico
	33. [JF_CC] Jefe de Control de Calidad
	34. [AUX_MICRO] Auxiliar de Microbiología
	35. [JF_MICRO] Jefe de Microbiología
	36. [AN_STM] Analista de sistemas

Fuente: EAR/PILAR 5.4.5. Identificación de Activos. LABORATORIOS SFC LTDA.

8.3.2. Valoración de activos. Para valorar los activos se tomaran las siguientes dimensiones de seguridad de la metodología MAGERIT:

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

Tabla 5. Valoración Cualitativa.

Valoración cualitativa	Escala de valor cuantitativo expresado en millones	Valor cuantitativo
Muy Alto (MA)	> $ 100	$ 100.000
Alto (A)	100 <valor> 50	$ 50.000
Medio (M)	50 <valor> 30.000	$ 30.000
Bajo (b)	30.000 <valor> 10.000	$ 10.000
Muy bajo (MB)	10.000 <valor> 5.000	$ 5.000

Fuente: El Autor.

Tabla 6. Escala de valoración de activos.

VALOR		CRITERIO
10	Muy alto	Daño muy grave a la organización.
7 - 9	Alto	Daño grave a la organización.
4 - 6	Medio	Daño importante a la organización.
1 - 3	Bajo	Daño menor a la organización.
0	Despreciable	Irrelevante a efectos prácticos.

Fuente: EAR/PILAR 5.4.5. Escala de valoración.

A continuación se valoran los activos con la siguiente clasificación: **[VALOR] [ESCALA_ESTANDAR] [ESCALA_ESTANDAR]…**Véase la Tabla 7…

Tabla 7. Valoración de Activos por Tipo: Datos / Información.

Activo	Dimensiones de Seguridad				
	[D]	**[I]**	**[C]**	**[A]**	**[T]**
ACTIVOS ESENCIALES					
1. [SRV_PPAL] Servidor Principal	[10] [da-9.da] [lg-9.lg(a,b)]		[10] [adm-9.adm] [lg-9.lg(a,b)]	[10] [si-10.si]	[10] [olm-10.olm]
2. [SRV_MICRO] Servidor Microbiología	[10] [da-9.da] [lg-9.lg(a,b)]		[10] [adm-9.adm] [lg-9.lg(a,b)]	[10] [si-10.si]	[10] [olm-10.olm]
3. [HPLC] Equipos HPLC	[9] [da-9.da] [lg-9.lg(a,b)]		[9] [adm-9.adm] [lg-9.lg(a,b)]	[9] [si-9.si]	[9] [olm-9.olm]
4. [FORM_MTRAS] Formulas Maestras		[9] [da-9.da] [lg-9.lg(a,b)]	[9] [adm-9.adm] [lg-9.lg(a,b)]	[9] [si-9.si]	[9] [olm-9.olm]
5. [BD_SG] BD		[9] [da-	[9] [adm-	[9] [si-	[9] [olm-

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
Sistema de Gestión		9.da] [lg-9.lg(a,b)]	9.adm] [lg-9.lg(a,b)]	9.si]	9.olm]
6. [BD_MICRO] BD MICROLAB		[9] [da-9.da] [lg-9.lg(a,b)]	[9] [adm-9.adm] [lg-9.lg(a,b)]	[9] [si-9.si]	[9] [olm-9.olm]
7. [HD_BKP] Disco Duro Backups		[9] [da-9.da] [lg-9.lg(a,b)]	[9] [adm-9.adm] [lg-9.lg(a,b)]	[9] [si-9.si]	[9] [olm-9.olm]
SERVICIOS INTERNOS					
8. [ANAL_MTRAS] Análisis de Muestras	[10] [da-9.da] [lg-9.lg(a,b)]	[10] [da-9.da] [lg-9.lg(a,b)]	[10] [adm-9.adm] [lg-9.lg(a,b)]	[10] [si-10.si]	[10] [olm-10.olm]
9. [RTDO_ANAL] Resultado de Análisis	[10] [da-9.da] [lg-9.lg(a,b)]	[10] [da-9.da] [lg-9.lg(a,b)]	[10] [adm-9.adm] [lg-9.lg(a,b)]	[10] [si-10.si]	[10] [olm-10.olm]
APLICACIONES					
10. [PGN_WEB] Página web		[7] [da-7.da2] [lg-7.lg(a,b)]	[7] [adm-.7adm] [lg-7.lg(a,b)]	[7] [si-7.si]	
11. [HER_OFI] Herramientas de ofimática					[5] [da-5.da]
12. [ANT_VIR] Antivirus					[5] [da-5.da]
13. [SO] Sistema Operativo					[5] [da-5.da]
14. [PLAT_SG] Plataforma Sistema de Gestión		[7] [da-7.da2] [lg-7.lg(a,b)]	[7] [adm-7.adm] [lg-7.lg(a,b)]	[7] [si-7.si]	[7] [olm-7.olm]
15. [MICROLAB] Plataforma MICROLAB 1.0		[9] [da-9.da] [lg-9.lg(a,b)]	[9] [adm-9.adm] [lg-9.lg(a,b)]	[9] [si-9.si]	[9] [olm-9.olm]
EQUIPOS					
16. [PC] Computadoras			[9] [adm-9.adm] [lg-9.lg(a,b)]		[8] [olm-9.olm]

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
17. [IMP] Impresoras					[7] [olm-7.olm]
18. [FIREWALL] Firewall			[7] [adm-7.adm]		[8] [olm-9.olm]
19. [SWT] Switch					[8] [olm-9.olm]
COMUNICACIONES					
20. [WIFI] Router Wifi		[5] [da-5.da]			
21. [LAN_SFC] Red LAN	[8] [da-7.da]				[8] [olm-9.olm]
22. [TEL] Telefonía		[7] [da-7.da]			
23. [IE] Internet		[7] [da-7.da]	[7] [adm-7.adm] [lg-7.lg(a,b)]		
ELEMENTOS AUXILIARES					
24. [UPS] UPS	[7] [da-7.da]				
25. [SIS_VIG] Sistema de Vigilancia	[7] [da-7.da]				
INSTALACIONES					
26. [CPD] CPD			[9] [adm-9.adm] [lg-9.lg(a,b)]		[9] [olm-9.olm]
27. [SFC] Empresa			[9] [adm-9.adm] [lg-9.lg(a,b)]		[9] [olm-9.olm]
PERSONAL					
28. [DIR_CALIDAD] Directora Aseguramiento de Calidad			[9] [adm-9.adm] [lg-9.lg(a,b)]		
29. [RRHH] Director de Talento Humano/HSE			[9] [adm-9.adm] [lg-		

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
			9.lg(a,b)]		
30. [DT] Directora técnica			[9] [adm-9.adm] [lg-9.lg(a,b)]		
31. [ASIST_DIR_CALID] Asistente Dirección de Aseguramiento de Calidad			[7] [adm-7.adm] [lg-7.lg(a,b)]		
32. [AN_FQ] Analista de Fisicoquímico			[7] [adm-7.adm] [lg-7.lg(a,b)]		
33. [JF_CC] Jefe de Control de Calidad			[9] [adm-9.adm] [lg-9.lg(a,b)]		
34. [AUX_MICRO] Auxiliar de Microbiología			[7] [adm-7.adm] [lg-7.lg(a,b)]		
35. [JF_MICRO] Jefe de Microbiología			[9] [adm-9.adm] [lg-9.lg(a,b)]		
36. [AN_STM] Analista de sistemas			[9] [adm-9.adm] [lg-9.lg(a,b)]		

Fuente: EAR/PILAR 5.4.5. Valoración Activos SFC.

Tabla 8. Escalas estándar seleccionadas.

ESCALAS ESTANDAR SELECCIONADAS.		
[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o

ESCALAS ESTANDAR SELECCIONADAS.		
		dificulte la investigación de incidentes graves
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general

Fuente: EAR/PILAR 5.4.5.

8.4. CARACTERIZACIÓN DE LAS AMENAZAS

La metodología MAGERIT define 4 grupos de amenazas:

- [N] Desastres naturales.
- [I] De origen industrial.
- [E] Errores y fallos no intencionados.
- [A] Ataques intencionados.

Esta fase consta de 2 actividades:

- Identificación de las amenazas.
- Valoración de las amenazas.

8.4.1. Identificación de las amenazas. Durante esta tarea se deben identificar las amenazas más relevantes sobre cada uno de los activos…Véase Tabla 9...

Tabla 9. Identificación de Amenazas.

ACTIVOS	AMENAZAS
ACTIVOS ESENCIALES	
1. [SRV_PPAL] Servidor Principal	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos
2. [SRV_MICRO] Servidor Microbiología	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos
3. [HPLC] Equipos HPLC	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos

ACTIVOS	AMENAZAS
4. [FORM_MTRAS] Formulas Maestras	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.19] Fugas de información [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información
5. [BD_SG] BD Sistema de Gestión	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.19] Fugas de información [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información
6. [BD_MICRO] BD MICROLAB	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.19] Fugas de información [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información

ACTIVOS	AMENAZAS
7. [HD_BKP] Disco Duro Backups	[I.11] Emanaciones electromagnéticas [E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.19] Fugas de información [E.25] Pérdida de equipos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.23] Manipulación del hardware [A.25] Robo de equipos
SERVICIOS INTERNOS	
8. [ANAL_MTRAS] Análisis de Muestras	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.24] Denegación de servicio
9. [RTDO_ANAL] Resultado de Análisis	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.15] Alteración de la información [E.18] Destrucción de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.13] Repudio (negación de actuaciones) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.24] Denegación de servicio

ACTIVOS	AMENAZAS
APLICACIONES	
10. [PGN_WEB] Página web	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas
11. [HER_OFI] Herramientas de ofimática	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas
12. [ANT_VIR] Antivirus	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas

ACTIVOS	AMENAZAS
13. [SO] Sistema Operativo	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas
14. [PLAT_SG] Plataforma Sistema de Gestión	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas
15. [MICROLAB] Plataforma MICROLAB 1.0	[E.1] Errores de los usuarios [E.2] Errores del administrador del sistema / de la seguridad [E.8] Difusión de software dañino [E.15] Alteración de la información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.19] Revelación de información [A.22] Manipulación de programas

ACTIVOS	AMENAZAS
EQUIPOS	
16. [PC] Computadoras	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos
17. [IMP] Impresoras	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos
18. [FIREWALL] Firewall	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos
19. [SWT] Switch	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.25] Pérdida de equipos [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.23] Manipulación del hardware [A.25] Robo de equipos

ACTIVOS	AMENAZAS
COMUNICACIONES	
20. [WIFI] Router Wifi	[I.11] Emanaciones electromagnéticas [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.25] Pérdida de equipos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.19] Revelación de información [A.23] Manipulación del hardware [A.25] Robo de equipos
21. [LAN_SFC] Red LAN	[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.18] Destrucción de la información [A.19] Revelación de información [A.24] Denegación de servicio

ACTIVOS	AMENAZAS
22. [TEL] Telefonía	[E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.19] Revelación de información
23. [IE] Internet	[E.2] Errores del administrador del sistema / de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación de la información [A.19] Revelación de información
ELEMENTOS AUXILIARES	
24. [UPS] UPS	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.7] Uso no previsto [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo

ACTIVOS	AMENAZAS
25. [SIS_VIG] Sistema de Vigilancia	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.2] Daños por agua [I.*] Desastres industriales [I.3] Contaminación medioambiental [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.7] Uso no previsto [A.23] Manipulación del hardware [A.25] Robo de equipos [A.26] Ataque destructivo
INSTALACIONES	
26. [CPD] CPD	[I.11] Emanaciones electromagnéticas [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.27] Ocupación enemiga
27. [SFC] Empresa	[I.11] Emanaciones electromagnéticas [A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.11] Acceso no autorizado [A.27] Ocupación enemiga
PERSONAL	
28. [DIR_CALIDAD] Directora Aseguramiento de Calidad	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
29. [RRHH] Director de Talento Humano/HSE	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)

ACTIVOS	AMENAZAS
30. [DT] Directora técnica	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
31. [ASIST_DIR_CALID] Asistente Dirección de Aseguramiento de Calidad	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
32. [AN_FQ] Analista de Fisicoquímico	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
33. [JF_CC] Jefe de Control de Calidad	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
34. [AUX_MICRO] Auxiliar de Microbiología	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
35. [JF_MICRO] Jefe de Microbiología	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)
36. [AN_STM] Analista de sistemas	[E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Fuente: EAR/PILAR 5.4.5. Valoración Activos SFC.

8.4.2. Valoración de las amenazas. Durante esta tarea se planea evaluar la probabilidad de ocurrencia de cada amenaza y estimar la degradación que causaría la amenaza si llegara a materializarse.

Tabla 10. Valoración de las amenazas.

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
[SRV_PPAL] Servidor Principal	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P	1%				
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P	20%	20%			
	[E.25] PÉRDIDA DE EQUIPOS	P			100 %		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		100 %	100 %		
	[A.7] USO NO PREVISTO	P		10%	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		100 %	100 %		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	PP			100 %		
[SRV_MICRO] Servidor Microbiología	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.25] PÉRDIDA DE EQUIPOS	P			100 %		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.7] USO NO PREVISTO	P		1%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE	P			100		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	EQUIPOS				%		
[HPLC] Equipos HPLC	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.25] PÉRDIDA DE EQUIPOS	P			50%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.7] USO NO PREVISTO	P		1%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	P			50%		
[FORM_MTRAS] Formulas Maestras	[E.1] ERRORES DE LOS USUARIOS	MA		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	MA		10%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	MA		10%	50%		
	[A.11] ACCESO NO AUTORIZADO	CS		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	MA		100 %			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			100 %		
[BD_SG]	[E.1] ERRORES DE LOS	MA		10%	10%		

Activos	Amenazas	Proba bilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
BD Sistema de Gestión	USUARIOS						
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	MA		10%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	MA		10%	50%		
	[A.11] ACCESO NO AUTORIZADO	CS		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	MA		100 %			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			100 %		
[BD_MICRO] BD MICROLAB	[E.1] ERRORES DE LOS USUARIOS	MA		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	MA		10%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	MA		10%	50%		
	[A.11] ACCESO NO AUTORIZADO	CS		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	MA		100 %			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			100 %		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
[HD_BKP] Disco Duro Backups	[I.11] EMANACIONES ELECTROMAGNÉTICAS	O			1%		
	[E.1] ERRORES DE LOS USUARIOS	MA		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.25] PÉRDIDA DE EQUIPOS	P			100 %		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	MA		10%	50%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		100 %	100 %		
	[A.7] USO NO PREVISTO	P		10%	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		100 %	100 %		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	MA		100 %			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			100 %		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	P			100 %		
[ANAL_MTRAS] Análisis de Muestras	[E.1] ERRORES DE LOS USUARIOS	P	10%	10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P	20%	20%	20%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	P	10%				
	[E.19] FUGAS DE	P			10%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	INFORMACIÓN						
	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	MA	50%				
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P	1%	10%	10%	100 %	
	[A.7] USO NO PREVISTO	P	1%	10%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%	100 %	
	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	MA					100 %
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	MA		50%			
	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	P	50%				
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.24] DENEGACIÓN DE SERVICIO	MA	50%				
[RTDO_ANAL] Resultado de Análisis	[E.1] ERRORES DE LOS USUARIOS	P	10%	10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P	20%	20%	20%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	P	10%				
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	MA	50%				
	[A.5] SUPLANTACIÓN DE	P		50%	50%	100	

Activos	Amenazas	Proba bilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	IDENTIDAD					%	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P	1%	10%	10%	100 %	
	[A.7] USO NO PREVISTO	P	1%	10%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%	100 %	
	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	MA					100 %
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	MA		50%			
	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	P	50%				
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.24] DENEGACIÓN DE SERVICIO	MA	50%				
[PGN_WEB] Página web	[E.1] ERRORES DE LOS USUARIOS	P		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		10%	10%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	P		20%	20%		
	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	MA		1%			
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	10%		
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		100 %	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.22] MANIPULACIÓN DE PROGRAMAS	P		100 %	100 %		
[HER_OFI] Herramientas de ofimática	[E.1] ERRORES DE LOS USUARIOS	P		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		10%	10%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	P		20%	20%		
	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	MA		1%			
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	10%		
	[A.7] USO NO PREVISTO	P		10%	10%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		100 %	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.22] MANIPULACIÓN DE PROGRAMAS	P		100 %	100 %		
[ANT_VIR] Antivirus	[E.1] ERRORES DE LOS USUARIOS	P		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		10%	10%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	P		20%	20%		
	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	P		1%			
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	10%		
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		100 %	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.22] MANIPULACIÓN DE PROGRAMAS	P		100 %	100 %		
[SO] Sistema Operativo	[E.1] ERRORES DE LOS USUARIOS	P		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		10%	10%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	P		20%	20%		
	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	MA		1%			
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	10%		
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		100 %	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.22] MANIPULACIÓN DE PROGRAMAS	P		100 %	100 %		
[PLAT_SG] Plataforma Sistema de Gestión	[E.1] ERRORES DE LOS USUARIOS	P		10%	10%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		10%	10%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	P		20%	20%		
	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	MA		1%			
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	10%		
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		100 %	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.22] MANIPULACIÓN DE PROGRAMAS	P		100 %	100 %		
[MICROLAB]	[E.1] ERRORES DE LOS USUARIOS	P		10%	10%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
Plataforma MICROLAB 1.0	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		10%	10%		
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	P		20%	20%		
	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	MA		1%			
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		50%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	10%		
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	P		100 %	100 %		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.22] MANIPULACIÓN DE PROGRAMAS	P		100 %	100 %		
[PC] Computadoras	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[E.25] PÉRDIDA DE EQUIPOS	MA			10%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.7] USO NO PREVISTO	P		1%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	MA			10%		
[IMP] Impresoras	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.25] PÉRDIDA DE EQUIPOS	P			10%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.7] USO NO PREVISTO	P		1%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	P			50%		
[FIREWALL] Firewall	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.25] PÉRDIDA DE EQUIPOS	P			10%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.7] USO NO PREVISTO	P		1%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	P			50%		
[SWT] Switch	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.25] PÉRDIDA DE EQUIPOS	P			10%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.7] USO NO PREVISTO	P		1%	10%		
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	P			50%		
[WIFI] Router Wifi	[I.11] EMANACIONES ELECTROMAGNÉTICAS	P			1%		
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	P			10%		
	[E.10] ERRORES DE SECUENCIA	P		10%			
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.25] PÉRDIDA DE EQUIPOS	P			50%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		10%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%	100 %	
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.9] [RE-]ENCAMIENTO DE MENSAJES	P			10%		
	[A.10] ALTERACIÓN DE SECUENCIA	P		10%			
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%	100 %	
	[A.12] ANÁLISIS DE TRÁFICO	P			2%		
	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		10%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P			50%		
	[A.25] ROBO DE EQUIPOS	P			50%		
[LAN_SFC] Red LAN	[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	P	50%				
	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P	20%	20%	20%		
	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	P			10%		
	[E.10] ERRORES DE SECUENCIA	P		10%			
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[E.24] CAÍDA DEL SISTEMA POR	P	50%				

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	AGOTAMIENTO DE RECURSOS						
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		10%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%	100 %	
	[A.7] USO NO PREVISTO	P	10%	10%	10%		
	[A.9] [RE-]ENCAMIENTO DE MENSAJES	P			10%		
	[A.10] ALTERACIÓN DE SECUENCIA	P		10%			
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%	100 %	
	[A.12] ANÁLISIS DE TRÁFICO	P			2%		
	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	P			1%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		10%			
	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	P	50%				
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
	[A.24] DENEGACIÓN DE SERVICIO	MA	50%				
[TEL] Telefonía	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	P			10%		
	[E.10] ERRORES DE SECUENCIA	P		10%			
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		10%	50%	100 %	

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%	100 %	
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.9] [RE-]ENCAMIENTO DE MENSAJES	P			10%		
	[A.10] ALTERACIÓN DE SECUENCIA	P		10%			
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%	100 %	
	[A.12] ANÁLISIS DE TRÁFICO	P			2%		
	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		10%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
[IE] Internet	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	P		20%	20%		
	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	P			10%		
	[E.10] ERRORES DE SECUENCIA	P		10%			
	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		1%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		10%	50%	100 %	
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%	100 %	
	[A.7] USO NO PREVISTO	P		10%	10%		
	[A.9] [RE-]ENCAMIENTO DE MENSAJES	P			10%		
	[A.10] ALTERACIÓN DE SECUENCIA	P		10%			

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[A.11] ACCESO NO AUTORIZADO	P		10%	50%	100 %	
	[A.12] ANÁLISIS DE TRÁFICO	P			2%		
	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	P			5%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		10%			
	[A.19] REVELACIÓN DE INFORMACIÓN	P			50%		
[UPS] UPS	[N.1] FUEGO	PP	1%				
	[N.2] DAÑOS POR AGUA	PP	1%				
	[N.*] DESASTRES NATURALES	PP	1%				
	[I.1] FUEGO	P	1%				
	[I.2] DAÑOS POR AGUA	P	1%				
	[I.*] DESASTRES INDUSTRIALES	P	1%				
	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	PP	1%				
	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	P	1%				
	[A.7] USO NO PREVISTO	P	1%				
	[A.23] MANIPULACIÓN DEL HARDWARE	P	1%				
	[A.25] ROBO DE EQUIPOS	P	1%				
	[A.26] ATAQUE DESTRUCTIVO	P	1%				
[SIS_VIG] Sistema de Vigilancia	[N.1] FUEGO	PP	100 %				
	[N.2] DAÑOS POR AGUA	PP	50%				
	[N.*] DESASTRES NATURALES	PP	100 %				
	[I.1] FUEGO	P	100 %				
	[I.2] DAÑOS POR AGUA	P	50%				

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	[I.*] DESASTRES INDUSTRIALES	P	100 %				
	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	PP	50%				
	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	P	10%				
	[A.7] USO NO PREVISTO	P	50%	1%	1%		
	[A.23] MANIPULACIÓN DEL HARDWARE	P	50%		50%		
	[A.25] ROBO DE EQUIPOS	P	10%				
	[A.26] ATAQUE DESTRUCTIVO	P	10%				
[CPD] CPD	[I.11] EMANACIONES ELECTROMAGNÉTICAS	PP			1%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		10%	50%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.7] USO NO PREVISTO	P		10%	50%		
	[A.11] ACCESO NO AUTORIZADO	MA		10%	50%		
	[A.27] OCUPACIÓN ENEMIGA	P			50%		
[SFC] Empresa	[I.11] EMANACIONES ELECTROMAGNÉTICAS	PP			1%		
	[A.5] SUPLANTACIÓN DE IDENTIDAD	P		10%	50%		
	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	P		10%	50%		
	[A.11] ACCESO NO AUTORIZADO	MA		10%	50%		
	[A.27] OCUPACIÓN ENEMIGA	P			50%		
[DIR_CALIDAD]	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
Directora Aseguramiento de Calidad	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[RRHH] Director de Talento Humano/ HSE	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[DT] Directora técnica	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[ASIST_DIR_CALID] Asistente Dirección de Aseguramiento de Calidad	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA	P		20%	20%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	SOCIAL						
[AN_FQ] Analista de Fisicoquímico	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[JF_CC] Jefe de Control de Calidad	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[AUX_MICRO] Auxiliar de Microbiología	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[JF_MICRO] Jefe de Microbiología	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE	MA			20%		

Activos	Amenazas	Probabilidad	Degradación				
			[D]	[I]	[C]	[A]	[T]
	INFORMACIÓN						
	[A.29] EXTORSIÓN	P		20%	20%		
	[A.30] INGENIERÍA SOCIAL	P		20%	20%		
[AN_STM] Analista de sistemas	[E.15] ALTERACIÓN DE LA INFORMACIÓN	P		10%			
	[E.19] FUGAS DE INFORMACIÓN	P			10%		
	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	P		50%			
	[A.19] REVELACIÓN DE INFORMACIÓN	MA			20%		
	[A.29] EXTORSIÓN	P		100 %	100 %		
	[A.30] INGENIERÍA SOCIAL	P		100 %	100 %		

Fuente: El Autor.

Tabla 11. Probabilidad de ocurrencia.

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	MUY BAJO
MR	MUY RARA
0	-

Fuente: EAR/PILAR 5.4.5.

Tabla 12. Degradación de las amenazas.

Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% – 89%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Fuente: EAR/PILAR 5.4.5.

8.5. IDENTIFICACIÓN DE RIESGOS

8.5.1. Identificación de riesgos críticos. Todos los activos de las organizaciones se encuentran expuestos a riesgos, por lo cual se hace importante conocer cuales poseen un mayor nivel de riesgo para implementar salvaguardas (tratamiento de riesgos) con el fin de que las amenazas puedan materializarse.

Una vez se han evaluado y clasificado los activos y se conocen las amenazas a las que están expuestos, se toman los activos con mayor riesgo para implementar las salvaguardas…Véase el Anexo E...

8.6. SALVAGUARDAS

Las salvaguardas o contramedidas son aquellos procedimientos, elementos técnicos o mecanismo que reducen los riegos. Durante esta fase se identifican las salvaguardas que se consideran efectivas para la organización y que permitan mitigar los riesgos encontrados[38]. Esta fase está compuesta de:

- Identificación de las salvaguardas más adecuadas.
- Valoración de las salvaguardas.

8.6.1. Identificación y valoración de las salvaguardas. Para identificar las salvaguardas de cada activo utilizaremos la herramienta PILAR, la cual nos permite seleccionar la salvaguarda que mejor se ajuste a las amenazas ya identificadas…Véase la Figura 8…

Una vez se han identificado las salvaguardas se deben valorar para determinar su eficacia…Véase la Tabla 13…

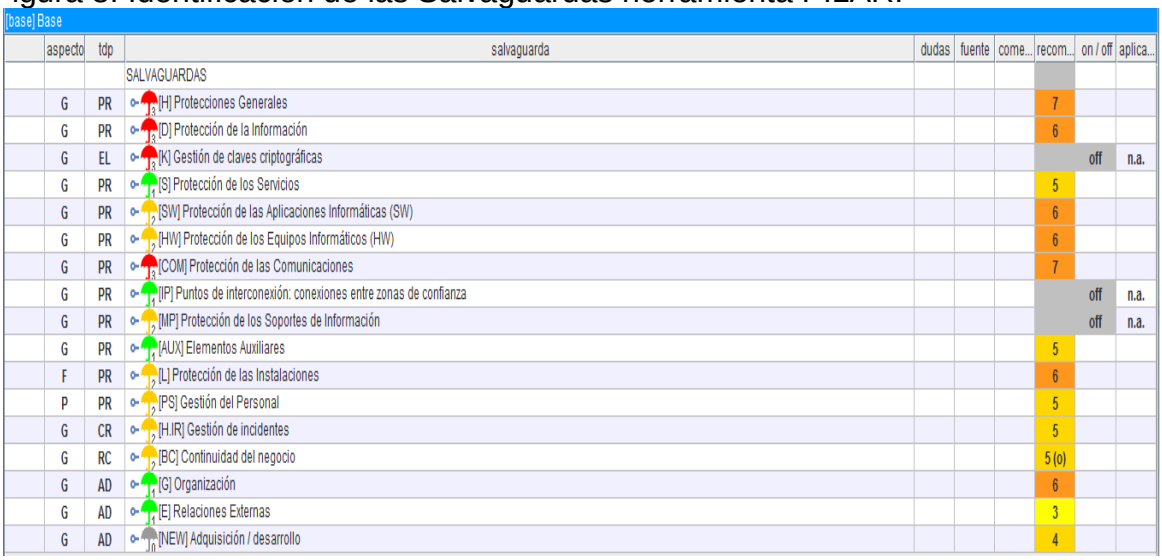
[38] BARRERA GARCIA, L. F. (2013). AUDITORIA AL NIVEL DE SALVAGUARDAS DE LA APLICACIÓN CONTABLE CG/IFS DE LA EMPRESA PUBLICA MUNICIPAL DE TELECOMUNICACIONES, AGUA POTABLE, ALCANTARILLADO Y SANEAMIENTO DE CUENCA - ETAPA EP. Universidad de Cuenca. Consultado el 25 de octubre de 2015 en: http://dspace.ucuenca.edu.ec/bitstream/123456789/5071/1/TESIS.pdf

Tabla 13. Niveles de Madurez herramienta PILAR.

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicia/ad hoc	Iniciado
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Fuente: EAR/PILAR 5.4.5.

Figura 8. Identificación de las Salvaguardas herramienta PILAR.



Fuente: EAR/PILAR 5.4.5.

Tabla 14. Identificación y valoración de Salvaguardas.

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN			
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	L0	0%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 6.1.2 SEPARACIÓN DE DEBERES	L0	0%
	A 6.1.3 CONTACTO CON LAS AUTORIDADES	L3	90%
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	L3	90%
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	L0	0%
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	L0	0%
	A 6.2.2 TELETRABAJO	L0	0%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS			
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	L3	90%
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO	L3	90%
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	L2	50%
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A.7.2.3 PROCESO DISCIPLINARIO	L3	90%
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	L2	50%
A.8 GESTION DE ACTIVOS			
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	L2	50%
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	L2	50%
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	L0	0%
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	L2	50%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	L0	0%
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN	L0	0%
	A 8.2.3 MANEJO DE ACTIVOS	L0	0%
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	L0	0%
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS	L0	0%
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.	L0	0%
A.9 CONTROL DE ACCESO			
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	L0	0%
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	L1	10%
A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	L0	0%
	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS	L0	0%
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	L1	10%
	A 9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	L0	0%
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	L0	0%
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	L0	0%
A 9.3 RESPONSABILIDADES DE LOS USUARIOS	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	L0	0%
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	L0	0%
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.	L0	0%
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.	L0	0%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	L3	90%
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.	L0	0%
A. 10 CRIPTOGRAFIA			
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	L0	0%
	A 10.1.2 GESTIÓN DE LLAVES	L0	0%
A. 11 SEGURIDAD FISICA Y DEL ENTORNO			
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	L0	0%
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS	L0	0%
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	L0	0%
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	L1	10%
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS	L0	0%
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA	L1	10%
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	L1	10%
	A 11.2.2 SERVICIOS DE SUMINSITRO	L2	50%
	A 11.2.3 SEGURIDAD DEL CABLEADO	L2	50%
	A 11.2.4 MANTENIMIENTO DE EQUIPOS	L0	0%
	A 11.2.5 RETIRO DE ACTIVOS	L0	0%
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	L0	0%
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	L0	0%
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO	L0	0%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	L0	0%
A.12 SEGURIDAD DE LAS OPERACIONES			
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	L4	95%
	A 12.1.2 GESTIÓN DE CAMBIOS	L4	95%
	A 12.1.3 GESTIÓN DE CAPACIDAD	L2	50%
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	L2	50%
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	L0	0%
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	L3	90%
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	L0	0%
	A12.4.1 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	L0	0%
	A12.4.1 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	L0	0%
	A12.4.1 SINCRONIZACIÓN DE RELOJES	L0	0%
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	L0	0%
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	L1	10%
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFTWARE	L0	0%
A 12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	L2	50%
A. 13 SEGURIDAD DE LAS COMUNICACIONES			
A 13.1 GESTIÓN	A 13.1.1 CONTROLES DE REDES	L1	10%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
DE LA SEGURIDAD DE LAS REDES	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	L0	0%
	A 13.1.3 SEPARACIÓN EN LAS REDES	L0	0%
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	L0	0%
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	L0	0%
	A 13.2.3 MENSAJERIA ELECTRÓNICA	L0	0%
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	L3	90%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	L2	50%
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	L0	0%
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	L0	0%
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	L0	0%
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	L0	0%
	A 14.2.3 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	L1	10%
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	L0	0%
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	L0	0%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO	L0	0%
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	L0	0%
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	L1	10%
	A 14.2.9 PRUEBA DE ACEPTACIÓN DE SISTEMAS	L1	10%
A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	L1	10%
A.15 RELACIONES CON LOS PROVEEDORES			
A. 15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	A 15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	L0	0%
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	L0	0%
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	L0	0%
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	L4	95%
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	L2	50%
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	L0	0%
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	L3	90%
	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	L3	90%
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	L0	0%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	L0	0%
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	L3	90%
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA	L0	0%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	L2	50%
A. 18 CUMPLIMIENTO			
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	L1	10%
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	L0	0%
	A 18.1.3 PROTECCIÓN DE REGISTROS	L1	10%
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	L0	0%
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	L0	0%
A 18.2 REVISIONES DE SEGURIDAD DE	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	L0	0%

CONTROLES NTC-ISO-IEC 27001:2013			
OBJETIVOS DE CONTROL	**CONTROLES**	**NIVEL**	**EFICACIA**
LA INFORMACIÓN	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	L0	0%
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	L0	0%

Fuente: LABORATORIOS SFC LTDA.

8.6.2. Evaluación de Madurez respecto a los controles. La efectividad de los controles se encuentra distribuida así:

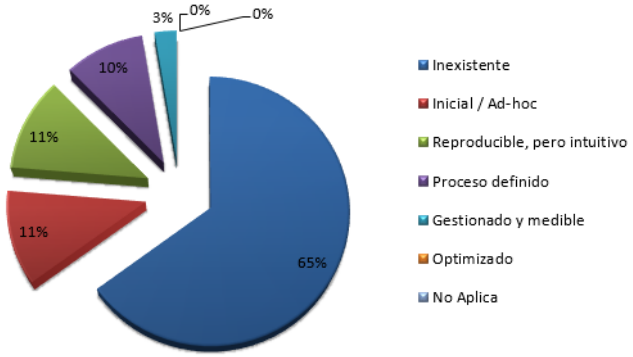
Tabla 15. Distribución de Controles.

NIVEL	CONTROLES
Inexistente	74
Inicial / Ad-hoc	13
Reproducible, pero intuitivo	13
Proceso definido	11
Gestionado y medible	3
Optimizado	0
No Aplica	0
TOTAL	**114**

Fuente: El Autor.

Los resultados anteriores se interpretarían gráficamente de la siguiente forma:

Figura 9. Nivel de Madurez de los Controles.



Fuente: El Autor.

8.7. PLAN DE TRATAMIENTO DE RIESGOS

Todos los puntos tratados anteriormente son necesarios para conocer, clasificar, evaluar y valorar las amenazas a las que están expuestos los activos, la probabilidad que ocurra la amenaza y el impacto que tendría si dicha amenaza se materializa. Todas estas fases deben estar soportadas por un plan de tratamiento de riesgos, el cual es un plan de seguridad que permite establecer las medidas, actividades, responsables y recursos para dar tratamiento a los riesgos…Véase el Anexo E...

8.8. INFORME DE EVALUACIÓN DE RIESGOS

8.8.1. Proceso de evaluación y tratamiento de riesgos de la información. Todo el proceso de evaluación y tratamiento de riesgos ha sido realizado en conformidad con la Metodología de evaluación y tratamiento de riesgos (MAGERIT).

8.8.2. Metodología aplicada. Para la evaluación y tratamiento de riesgos se utilizó la metodología MAGERIT la cual permite cuantificar la materialización de una amenaza sobre un activo expresándolo en valores económicos, además de concientizar a los responsables de los sistemas de información sobre la existencia de riesgos y la necesidad de tratarlos a tiempo.

8.8.3. Opciones para el tratamiento del riesgo. Las acciones o estrategias para el tratamiento de los riesgos después de su evaluación son[39]:

- ACEPTAR: Aplica cuando valor del riesgo no es relevante para la empresa y por tanto no se tomará ninguna acción. La organización puede optar por aceptar este tipo de riesgos cuando la valoración del riesgo es un “Bajo Riesgo” y no recurre en un riesgo Alto o que por el momento pueda causar un gran impacto en la calidad del producto, del servicio, de la compañía o en la confidencialidad de la información.

[39] RIVAS, Alejandra; ESPINOZA P., Miguel y SUDARIO, Paúl. Implementación de un sistema de gestión de seguridad de la información aplicada al dominio gestión de activos para la empresa plásticos internacionales PLASCINCA C.A. Escuela Superior Politécnica del Litoral. Trabajo de grado Analista de Sistemas. Escuela de Diseño y Comunicación Visual, 2011. Consultado el 31 de octubre de 2015 en: http://www.dspace.espol.edu.ec/bitstream/123456789/21624/1/Manual%20SGSI%20Aplicada%20a%20la%20Gestion%20de%20Activos.pdf

- MITIGAR: Es definir que el valor del riesgo amerita que sean evaluadas alternativas para aplicar salvaguardas acordes con las necesidades y recursos de la organización, se tiene en cuenta que el resultado del riesgo sea un “Medio Riesgo” o “Alto riesgo”. Lo que se busca es generar acciones para disminuir la probabilidad de aparición de una amenaza o su impacto si llegara a materializarse.
- TRANSFERIR: Es definir que el valor del riesgo hace que la entidad primero implemente medidas de mitigación y que aun habiéndolas aplicado el valor resultante del riesgo es “Alto Riesgo”, aunque su probabilidad sea baja su impacto puede ser catastrófico para la compañía en caso de materializarse el riesgo. Por ejemplo: adquirir una póliza de seguros para la empresa, la cual tenga cubierta en caso de un siniestro (incendio, inundación, etc.).
- EVITAR: Es definir las condiciones bajo las cuales la empresa dejará de realizar ciertas actividades en razón al elevado valor del riesgo y los costos asociados al tratamiento. Esto puede redundar en posibilidades de SUBCONTRATAR o entregar ciertas actividades a un tercero que pueda aceptar dicho riesgo. Se puede evitar el riesgos siempre y cuando permita eliminar la etapa donde se presenta el riesgo siempre y cuando no afecte la calidad del producto, servicio y la confidencialidad del a información.

Los riesgos que serán tratados con controles deben garantizar su reducción hasta un nivel aceptable, dichos riesgos se encuentran establecidos en el Plan de tratamiento de riesgos del SGSI de la organización.

8.8.4. Monitoreo. Con el fin de verificar la eficacia de los controles implementados el monitoreo debe ser continuo y periódico el cual permita calificar los riesgos identificados en la matriz para obtener un riesgo residual.

8.8.5. Revisiones periódicas de la evaluación y el tratamiento de riesgos. La valoración de los riesgos será revisada a intervalos planificados una vez al año o cuando se presenten cambios significativos en:

- La organización
- La tecnología
- Procesos de negocio

De este proceso de evaluación y valoración de riesgos se debe conservar información documentada.

Todo control que se aplique para reducir un riesgo debe ser medible a través de su eficacia. La aplicación de un control no significa que el riesgo se reducirá totalmente, por el contrario se busca con la implementación de controles reducir los riesgos a un nivel aceptable por la organización. Los controles deben evaluarse constantemente ya que si se producen resultados no esperados deberán aplicarse acciones de mejora aplicando nuevamente el ciclo PHVA.

8.9. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad…Véase Anexo F… tiene como objetivo definir qué controles son adecuados para implementar en la organización, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

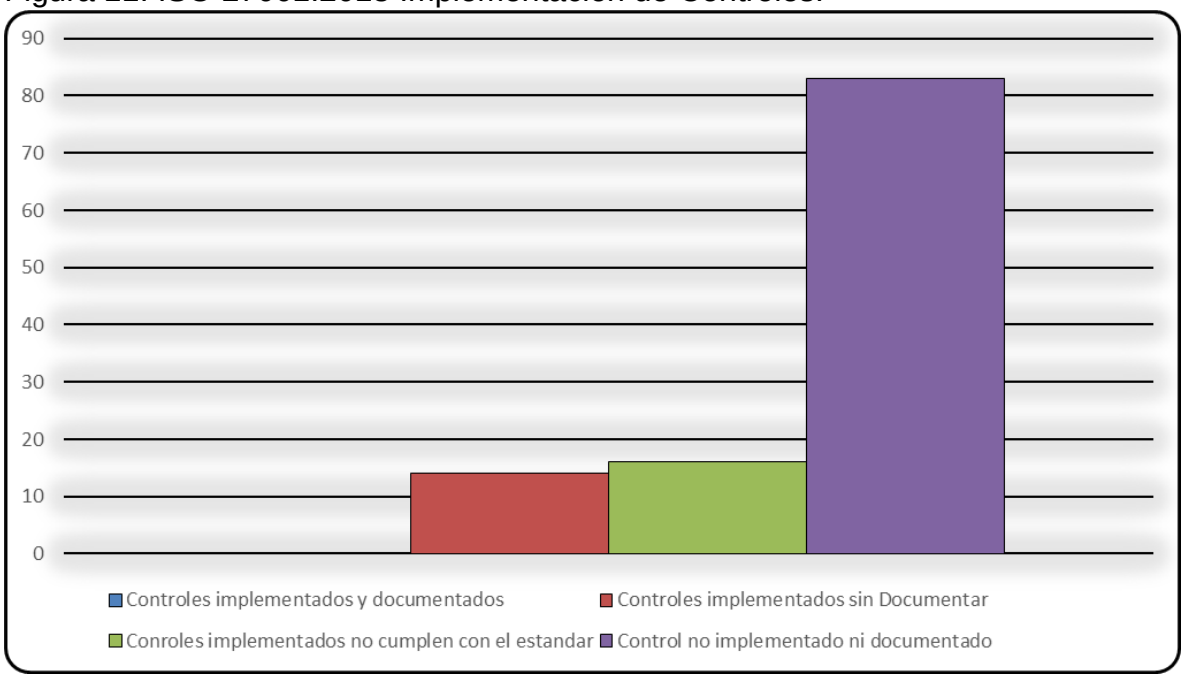
Figura 10. Cumplimiento inicial ISO 27001 X Dominio.

Fuente: El Autor.

Los controles seleccionados del Anexo A de la Norma ISO 27001:2013 para el diseño del SGSI (Sistema de Gestión de Seguridad de la Información) en LABORATORIOS SFC LTDA presentan las siguientes convenciones:

- L: Requerimiento regulatorio.
- C: Obligación Contractual.
- N: Requerimiento del negocio.
- R: Análisis de Riesgo.

Figura 11. ISO 27001:2013 Implementación de Controles.



Fuente: El Autor.

8.10. DEFINICIÓN DE FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD

Tabla 16. Funciones y Responsabilidades.

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
CONTEXTO DE LA ORGANIZACIÓN.							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	**Jefe de microbiología**	**Jefe de control de calidad**	**Directora técnica**	**Directora aseguramiento de calidad**	**Director de Talento Humano/HSE**	**Analista de sistemas**
Determinar el Contexto de la Organización.							
Determinar el alcance del SGSI.							
Apoyar la decisión estratégica y autónoma de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información - SGSI en la entidad, usando como parámetro de aplicación la norma técnica colombiana NTC-ISO-IEC 27001 en su versión 2013.							
LIDERAZGO.							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
Demostrar el liderazgo y compromiso con el SGSI, mediante el establecimiento de la POLÍTICA que rige este subsistema al interior del Sistema Integrado de Gestión.							
Establecer una política y objetivos de Seguridad de la Información.							
Asignar y Comunicar roles, responsabilidades y autoridades en la organización							
Asegurar que se logre la integración de los requisitos del SGSI en los procesos de la							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
organización, que se disponga de los recursos necesarios para el SGSI, que el SGSI logre los resultados previstos.							
Asegurar que se comunica la importancia del SGSI y el cumplimiento conforme de los requisitos del SGSI de forma eficaz.							
Asegurar que las autoridades y responsabilidades para los roles aplicables a la seguridad de la información se asignen y comuniquen.							
Asegurar que el SGSI sea conforme con la Norma							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	**Jefe de microbiología**	**Jefe de control de calidad**	**Directora técnica**	**Directora aseguramiento de calidad**	**Director de Talento Humano/HSE**	**Analista de sistemas**
usada como guía de implementación (NTC/ISO 27001).							
PLANIFICACIÓN.							
Definir y aplicar un proceso de evaluación de riesgos del SGSI (Metodología).							
Definir y aplicar un proceso de tratamiento de riesgos.							
Objetivos de seguridad de la Información y planes para lograrlos							
SOPORTE.							
Determinar y proporcionar los recursos para establecer, implementar, mantener y mejorar el SGSI.							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	**Jefe de microbiología**	**Jefe de control de calidad**	**Directora técnica**	**Directora aseguramiento de calidad**	**Director de Talento Humano/HSE**	**Analista de sistemas**
Determinar la competencia de las personas que realizan un trabajo							
Asegurar que las personas sean competentes.							
Establecer mecanismos para la comunicación interna							
Establecer mecanismos para la comunicación externa							
INFORMACIÓN DOCUMENTADA.							
Control de Información Documentada							
OPERACIÓN.							
llevar a cabo evaluaciones de riesgos							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
Implementar el plan de tratamiento de riesgos.							
Implementar el Plan de continuidad del Negocio.							
EVALUACIÓN DEL DESEMPEÑO.							
Evaluar el desempeño del SGSI y la eficacia del SGSI.							
Hacer seguimiento, revisar y cuando sea pertinente auditar con regularidad la prestación de servicios de los proveedores.							
Revisar con regularidad el cumplimiento del procesamiento adecuado y los							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
procedimientos establecidos para el manejo de la información dentro de su área de responsabilidad, acordes con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.							
MEJORA.							
Manejo de No Conformidades y acciones Correctivas							
Promover la mejora continua del SGSI.							
AUTORIDAD							
Nombrar formalmente a un responsable del SGSI.							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
Establecer políticas.							
Avalar y documentar el SGSI.							
Establecer directrices para la implementación, mantenimiento, revisión y perfeccionamiento del SGSI.							
Tomar decisiones acerca del SGSI.							
Informar a la Alta Dirección sobre el desempeño del SGSI.							
Informar cuando se identifiquen condiciones o actos inseguros en materia de seguridad de la información.							
Tomar							

ACTIVIDAD	FUNCIONES Y RESPONSABILIDADES						
	Alta Dirección	Jefe de microbiología	Jefe de control de calidad	Directora técnica	Directora aseguramiento de calidad	Director de Talento Humano/HSE	Analista de sistemas
acciones Disciplinarias.							
Implementar los controles de Seguridad de la información.							
Aprobar los recursos para el funcionamiento del SGSI.							
Vigilar la implementación, mantenimiento y mejora del SGSI.							
Exigir a todos los empleados y contratistas la aplicación de la Seguridad de la Información de acuerdo con las políticas y procedimientos establecidos.							

Fuente: El Autor.

9. CONTROLES

9.1. INVENTARIO DE ACTIVOS

LABORATORIOS SFC LTDA posee un inventario de activos el cual permite identificar todos los activos que están asociados a cada sistema informático y sus respectivos propietarios…Véase el Anexo K…

9.2. USO ACEPTABLE DE LOS ACTIVOS

Todos los trabajadores, consultores, contratistas y terceras partes, que usen activos de información que sean propiedad de LABORATORIOS SFC LTDA, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable de activos para dar un uso adecuado a los recursos asignados.

9.2.1. Condiciones generales para la Navegación en internet. La empresa realiza campañas de concientización dirigidas a todos los usuarios que navegan por internet para garantizar que las personas estén informadas sobre los peligros que conlleva descargar archivos de Internet (malware, troyanos, spyware y atacantes externos), acceder a sitios desconocidos, de baja confianza y aceptar cualquier mensaje que busque instalar software que brinde el navegador.

La empresa busca garantizar de manera técnica que se controle y limite el acceso a todos los sitios web que puedan afectar la productividad de la organización, la seguridad de su información o su personal, de igual manera se prohibirá el uso de servicios interactivos, redes sociales o mensajería instantánea como Facebook, twitter, ares, Whatsapp Messenger, Skype o similares durante la jornada laboral, de no acatarse será valorado como una conducta anti-ética.

Los usuarios se comprometen a no visitar sitios web restringidos por la empresa de manera explícita o implícita, o sitios que afecten la productividad y el rendimiento de la misma. Así mismo, está prohibida la descarga y uso de cualquier software malicioso o documentación que brinden información sobre como perjudicar o atentar contra la seguridad de la información.

Los empleados se comprometen a no brindar cualquier tipo de información de la empresa en sitios no autorizados o acceder a sitios que puedan comprometer la seguridad del equipo.

Los usuarios de la organización se comprometen a no descargar y/o utilizar archivos de sonido, imagen o similares que puedan estar protegidos por derechos de autor sin una previa autorización de los mismos. Igualmente no deben descargar ningún tipo de software de Internet bajo ninguna circunstancia.

El personal de la organización se compromete a no instalar ningún tipo software en sus equipos o en otras máquinas, incluso si el software es de código abierto; la única persona autorizada para instalar software es el analista de sistemas.

El software proveniente de sitios de almacenamiento en la nube no debe ser descargado a ningún equipo de la empresa a menos que sea recibido directamente de una fuente confiable y que se hayan empleado herramientas de detección de código malicio como un antivirus.

Los usuarios que utilizan sistemas de navegación son conscientes que estos son utilizados para propósitos meramente lícitos y en cumplimiento de las funciones específicas de su cargo.

La empresa facilita el acceso a plataformas para comercio electrónico, transacciones bancarias, pago de facturas y el acceso a correos personales, pero no asume ninguna responsabilidad por el uso de estas, ni recomienda su uso dentro de la organización, además prohíbe la participación en cualquier foro de discusión o chats.

9.2.2. Condiciones generales para el uso del Correo electrónico. El personal de la organización no puede emplear direcciones de correo electrónico diferentes a las cuentas corporativas que han sido suministradas por la organización.

Todos los mensajes de correo electrónico que utiliza el personal de la empresa, contiene el logo de la empresa, nombre y apellidos del remitente, cargo, dirección de la empresa, número telefónico, extensión, dirección web, aviso de confidencialidad y de tratamiento de datos personales.

Los usuarios no pueden contribuir a la creación de un ambiente de trabajo hostil ni crear, enviar o reenviar correos electrónicos que fomenten el acoso laboral.

Los empleados no pueden enviar o crear cualquier tipo de mensaje que pueda ser considerado difamatorio, acosador (laboral o sexual) o que pueda ofender a las demás personas con base en su raza, nacionalidad, género, orientación sexual, discapacidad, religión o política.

El personal es consciente de no utilizar en ningún caso los servicios y sistemas de la empresa para la transmisión de correos masivos no autorizados.

El personal de la empresa es consciente de no utilizar versiones digitalizadas de sus firmas adjunto a los mensajes de correo electrónico.

El personal es consciente de no abrir archivos, documentos o imágenes que se encuentren adjuntos a los correos electrónicos, a menos que hayan sido analizados posteriormente por el software antivirus aprobado por la empresa.

El personal del laboratorio es consciente de no abrir correos electrónicos cuyos remitentes son extraños, ofrecen premios o poseen enlaces para re-direccionar a otros servicios. Se consideran los siguientes correos como sospechosos y deben reportarse al personal del departamento de Sistemas para su validación:

- Se solicita proporcionar el nombre de usuario o contraseña u otro dato personal, datos de cuenta bancaria, número de tarjeta de crédito.
- Se solicita ingresar a un sitio web para actualizar datos personales de correo electrónico, redes sociales, datos del banco, etc.
- Se solicita descargar e instalar un archivo que dice contener una notificación o multa de la empresa.
- Se ofrecen premios actualizando datos o descargando y ejecutando archivos.
- Ofertas de empleo donde el usuario nunca ha iniciado sesión.

9.2.3. Condiciones generales para el uso de herramientas que comprometen la seguridad. Se prohíbe intentar realizar sin permiso del administrador del sistema o autorización expresa por LABORATORIOS SFC LTDA, cualquiera de los siguientes actos:

- Acceder al sistema o red (acceso indebido o forzado, engañando sistemas de autenticación, etc.).
- Monitorear datos o tráfico de red.
- Utilizar herramientas de hacking o accesos al Firewall.
- Atentar contra la vulnerabilidad del sistema o de las redes.
- Violar las medidas y políticas de seguridad.

La única persona autorizada para utilizar herramientas que permitan recuperar, restaurar o monitorear eventos específicos de los sistemas es el analista de sistemas.

9.2.4. Condiciones generales para recursos compartidos. El administrador de sistemas es el encargado de establecer e implementar la configuración de acceso a las carpetas de red.

- El usuario que dispone de un recurso compartido (carpeta de red) es responsable por las acciones y accesos en dicha carpeta.
- Se deben definir los tipo de acceso y los roles de usuarios sobre las carpetas de red (lectura, escritura, modificación y borrado).
- El acceso a carpetas compartidas se limita a los usuarios que las necesitan y se encuentra protegida contra apertura.
- Los usuarios que no cuenten con antivirus corporativo no pueden ingresar a los recursos de la red.

9.3. CONTROL DE ACCESO A LA INFORMACIÓN

El laboratorio implementa medidas y acciones de seguridad necesarias con el fin de evitar la pérdida, adulteración, consulta, fuga acceso o uso no autorizado, basándose en el principio del menor privilegio.

9.3.1. Condiciones generales de control de acceso a la información - gestión de acceso a usuarios. El responsable de la seguridad de los sistemas de información, establece procedimientos formales para controlar la asignación de perfiles, roles y derechos de acceso de los usuarios. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida de los usuarios (registro inicial, roles, eliminación, desactivación, etc.).

9.3.2. Condiciones generales de control de acceso a la información - registro de usuarios. Todos los usuarios deben tener una identificación personal única (usuario y contraseña) que se utilizara para el seguimiento de las actividades desempeñadas con sus privilegios asignados. Se debe verificar que el nivel de acceso otorgado al usuario sea adecuado de acuerdo a su cargo y funciones.

9.3.3. Condiciones generales de Control de Acceso a la Información - Responsabilidades del usuario. Todos los usuarios son conscientes de sus responsabilidades con relación al uso y manejo de contraseñas. El encargado de la seguridad de los sistemas de información implementa los procedimientos necesarios que permitan controlar los procesos de creación, modificación, eliminación de usuarios, gestión de contraseñas y permisos de acceso a los recursos de la red.

El personal tanto interno como externo que ingrese a las instalaciones de la empresa es consciente de las condiciones de acceso para mantener total confidencialidad en el uso de sus contraseñas personales.

9.3.4. Condiciones generales de Control de acceso a la red. El laboratorio proporciona a sus colaboradores el acceso a los servicios de red únicamente al personal autorizado y de acuerdo a sus privilegios. El laboratorio utiliza métodos apropiados de autenticación para el control de acceso remoto y redes inalámbricas de los usuarios que lo soliciten.

9.3.5. Condiciones generales de control de acceso a las aplicaciones. Todos aquellos programas utilizados por los usuarios que puedan comprometer los controles implementados son restringidos y estrictamente intervenidos.

Las sesiones inactivas son bloqueadas automáticamente después de un tiempo de inactividad determinado con el fin de evitar accesos no autorizados.

El personal del laboratorio es consciente de cambiar las contraseñas predeterminadas después de la instalación de una aplicación.

9.4. PROCEDIMIENTOS OPERATIVOS PARA GESTIÓN DE TI

El laboratorio define los lineamientos para el almacenamiento y recuperación de la información mantenida en medios de almacenamiento (unidades extraíbles, discos duros, etc.). Antes de abandonar la oficina los usuarios son conscientes de organizar, guardar y asegurar el material confidencial, información sensible o equipo costosos. Igualmente cerrar bajo llave archivadores, cajones y oficinas antes de abandonar la empresa.

9.4.1. Condiciones generales para el respaldo y protección de la información. El personal del laboratorio vela en todo momento por el cumplimiento a los principios de confidencialidad, integridad y disponibilidad de la información de la empresa y sus clientes.

La información de la empresa se mantiene disponible a las personas autorizadas en el momento en que se necesite.

La empresa se encarga de identificar y proponer mecanismos que permitan que las actividades de respaldo y recuperación de la información sean apropiadas con relación a costo / beneficio.

Los respaldos o Backup se realizan de acuerdo al procedimiento CD-01I3 “Protección de la información”.

El responsable de seguridad de la información realiza seguimiento a los Backups a partir del formato CD-01I3F1 “Bitácora de backup SFC”.

9.4.2. Condiciones generales para el escritorio organizado y limpio durante la jornada laboral. Cada usuario es responsable de proteger la información, por lo que es consciente de no dejar a la vista documentos o datos confidenciales, por ejemplo:

- Nombre de Usuario y Contraseñas
- Resultados de control de calidad
- Listas de Clientes o proveedores
- Formulas maestras

- Números de Cuenta
- Contratos
- Cualquier información que no desea publicar

Antes de abandonar la oficina los usuarios se toman el tiempo necesario para organizar, guardar y asegurar el material confidencial, información sensible o equipo costos.

Todos los usuarios son conscientes de dejar bajo llave archivadores, cajones y oficinas antes de abandonar la empresa.

9.4.3. Condiciones generales para el bloqueo de la estación de Trabajo. Si un usuario no se encuentra frente a su estación de trabajo esta debe encontrarse con la sesión bloqueada.

Para las ocasiones eventuales donde la estación de trabajo se encuentre desatendida y sin bloquear, como plan de apoyo la empresa programa el bloqueo automático de la estación de trabajo

La organización sensibiliza al personal con capacitaciones en el uso del bloqueo de sesión.

Los usuarios son conscientes de bloquear la sesión de su equipo al apartarse de él, procurando minimizar el tiempo en que la estación de trabajo queda desatendida.

9.4.4. Condiciones generales de protección contra software malicioso. Los usuarios son conscientes de no descargar software de cualquier sitio o sistema por fuera de la empresa.

El personal es consciente de no utilizar software descargado u obtenido de internet o fuera de la empresa, cuya fuente no sea confiable o no haya sido analizado por el departamento de sistemas en busca de virus y debidamente aprobado para su uso.

Todos los equipos sin excepción cuentan con un antivirus actualizado y licenciado, además los usuarios analizan con el antivirus cualquier archivo que vaya ser descomprimido y haya sido descargado de internet.

El personal se asegura que todos los archivos estén libres de virus antes de ser enviados por correo electrónico u otro medio a una entidad externa a LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA.

Los usuarios son conscientes de no desarrollar, escribir, copiar, generar, depurar, almacenar, propagar, ejecutar o intentar introducir cualquier código malicioso que este diseñado para auto replicarse, dañar o que dificulte el desempeño de cualquier sistema de LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA.

9.4.5. Condiciones generales de Seguridad en los equipos. Los servidores que almacenen información confidencial son mantenidos en un ambiente seguro y contienen al menos las siguientes medidas:

- Controles de acceso a instalaciones y seguridad física.
- Detectores de incendio y sistemas de extinción.
- Controles de humedad y temperatura.
- Sistemas eléctricos regulados (UPS).

Los usuarios son conscientes de no alojar información de la organización en servidores externos o gratuitos sin una debida aprobación (escrita o correo electrónico) por parte del departamento de sistemas.

Los equipos más importantes de comunicaciones deben ser alimentados por UPS y conectados a una corriente regulada para evitar interrupciones eléctricas.

9.5. POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Todas las actividades desarrolladas por personal que pertenece a empresas proveedoras y presta sus servicios a LABORATORIOS SFC LTDA.

9.5.1. Condiciones generales para la prestación de servicios a LABORATORIOS SFC LTDA. La información que se suministre en el registro debe ser completamente cierta y verificable.

La entidad que suministre bienes y/o servicios a LABORATORIOS SFC LTDA., debe estar legalmente constituida y vigente.
Todo proveedor debe estar dispuesto a que se le audite en cualquier momento.

Las actividades desarrolladas por las empresas proveedoras se realizarán de acuerdo a lo establecido en el contrato de proveedores vigente.

Todo proveedor deberá asegurar que todo su personal tiene la formación adecuada para el desarrollo del servicio y se encuentra debidamente capacitado en materia de seguridad y manejo de la información, por lo que deberá asegurarse y comprometerse a cumplir con la presente política dándola a conocer a todo su personal.

Cualquier intercambio de información entre LABORATORIOS SFC LTDA y el proveedor se entenderá que ha sido realizado dentro del marco establecido por el contrato vigente, de tal manera que la información no podrá ser utilizada en ningún caso ni para diferentes fines fuera de los dispuesto en dicho contrato.

LABORATORIOS SFC LTDA podrá verificar los antecedentes del personal profesional en caso de requerirlo.

9.5.2. Consideraciones generales de confidencialidad de la Información con proveedores. Los proveedores o personal externo que tengan acceso a información de LABORATORIOS SFC LTDA deberán considerar que dicha información es de carácter confidencial y exclusiva, a excepción que hayan tenido acceso a través de medios de difusión pública dispuestos por LABORATORIOS SFC LTDA.

Deberá evitarse la divulgación, modificación, destrucción o uso inadecuado de información en cualquier soporte informático. Igualmente la información confidencial de terceros se almacenara por tiempo indefinido y con la máxima reserva.

Ningún colaborador deberá poseer para usos diferentes a sus responsabilidades contratadas material o información propia de LABORATORIOS SFC LTDA.

Todas las obligaciones presentes en la política continuaran vigentes tras la finalización de las actividades que los proveedores desarrollen para LABORATORIOS SFC LTDA.

La información de carácter personal de LABORATORIOS SFC LTDA contenida en archivos ofimáticos u otro tipo de aplicación no deberá ser transferida en medios de almacenamiento externos o encontrarse almacenada en equipos de acceso público. Dichos archivos deberán ser eliminados al finalizar las actividades contractuales.

Los proveedores deben ponerse en contacto con LABORATORIOS SFC LTDA en caso de sufrir un incidente relacionado con la seguridad de la información.

Los proveedores deberán poseer una política de seguridad física o garantizar que se cumplan con los requisitos o medidas mínimas de seguridad física.

9.5.3. Consideraciones generales de intercambio de información con proveedores. Ningún proveedor debe manipular su identidad u ocultarla bajo ninguna circunstancia.

Ningún proveedor transferirá información de la organización cualquiera que sea el medio (físico o magnético) a terceras partes no autorizadas.

Todas las actividades que puedan dañar la imagen o reputación de LABORATORIOS SFC LTDA están totalmente prohibidas ya sea por internet u otro medio.

9.5.4. Condiciones generales para el uso apropiado de los recursos. Los proveedores se comprometen a dar un uso adecuado a los recursos y activos con los que proporcionan el servicio.

Todos los que equipos de proveedores que se conecten a la red de LABORATORIOS SFC LTDA no podrán tener acceso a los recursos de red

(Documentos compartidos) y se someterá a cumplir con la política de seguridad de la información y uso adecuado de los activos.

Se prohíbe expresamente:

- Conectarse a la red y recursos de LABORATORIOS SFC LTDA sin autorización expresa.
- Introducir en los sistemas de información contenido amenazante, obsceno, inmoral, etc.
- Introducir en la red de LABORATORIOS SFC LTDA cualquier tipo de virus, malware, etc., que pueda causar alteración o daño a los recursos informáticos.
- Intentar obtener acceso u otros privilegios a los recursos de red o sistemas de información del laboratorio.
- Intentar copiar, modificar, alterar, eliminar o sustraer información contenida en los sistemas de información o recursos de red de LABORATORIOS SFC LTDA.

9.5.5. Condiciones generales para auditoría de seguridad a proveedores. Todos los proveedores que contengan información confidencial de LABORATORIOS SFC LTDA deberán cumplir las siguientes obligaciones de la política de auditoría de seguridad:

- Permitir auditorias de seguridad de por lo menos una vez al año..
- LABORATORIOS SFC LTDA se reserva el derecho de realizar auditorías extraordinarias adicionales.
- Las auditorias se llevan a cabo siguiendo la planificación acordada con el proveedor.

9.6. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El laboratorio establece los lineamientos generales para la gestión de incidentes de seguridad de la información, con el objetico de tratar adecuadamente los incidentes de seguridad de la información y no sufrir un daño en la confidencialidad, integridad y disponibilidad de la información.

9.6.1. Consideraciones generales en la gestión de incidentes de seguridad de la información. La gerencia general reconoce la importancia de la gestión de

incidentes, por tal motivo designa un equipo responsable para la gestión de incidentes de seguridad de la información.
El laboratorio con el fin de concientizar a todos sus empleados divulga la política de gestión de incidentes de seguridad de la información a todo el personal sin excepción.

El personal del laboratorio consciente de la importancia de la gestión de incidentes reporta cualquier tipo de evento de seguridad por medio de correo electrónico, helpdesk, etc., al equipo responsable de gestión de incidentes de seguridad de la información.

9.6.2. Condiciones generales del equipo de gestión de incidentes de seguridad de la información. Adoptar medidas de seguridad eficientes para proteger los activos de información críticos del laboratorio.

Analizar los eventos de seguridad informática reportados por los usuarios para determinar si se trata de un incidente de seguridad de la información.

Informar inmediatamente al gerente general en caso de presentarse un incidente de seguridad que afecte activos de información críticos del laboratorio.

Ejecutar procedimientos de repuesta inmediata a incidentes para contener y mitigar el incidente.

Aprender de los incidentes de seguridad de la información y capacitar al personal, para prevenir nuevas ocurrencias.

Crear cadenas de custodia de las evidencias.

9.7. POLITICA DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS

Esta política aplica para cualquier software desarrollado por el área de sistemas para el cumplimiento de las operaciones de negocio. Esta política incluye el software:

- El desarrollo interno.
- Desarrollo para cumplimiento de las necesidades de un proyecto o solicitud.

9.7.1. Consideraciones generales para el desarrollo de software interno. Todo desarrollo realizado deberá tener definido su alcance, además de utilizar código fuente de tipo open source o código abierto, si es tomado de una fuente referenciarlo en los comentarios del código.

Todo desarrollo realizado al interior de LABORATORIOS SFC LTDA, deberá tener definido los requisitos de seguridad de la información y dar cumplimiento al objetivo de control de desarrollo de software seguro de la norma NTC ISO 27001, cumpliendo como mínimo alguno de los siguientes requisitos:

- Tener un sistema de administración de perfiles de usuarios que garanticen los privilegios y acceso.
- Guardar de forma encriptada en la base de datos las claves de los usuarios.
- El personal encargado del desarrollo deberá firmar un acuerdo de confidencialidad donde se declara la no divulgación ni uso de cualquier modulo o parte del código desarrollado para LABORATORIOS SFC LTDA.
- El personal debe cumplir con el procedimiento de control de cambios.
- Si el personal requiere subcontratar para el cumplimiento de la labor un tercero, este se someterá al cumplimiento de la política y todos los requisitos de seguridad de la información.

La alta gerencia y áreas involucradas se comprometen a brindar todo el apoyo, documentación técnica e información requerida para el desarrollo del sistema de información.

Se deberá definir un ciclo de vida y tiempo estimado para el desarrollo del sistema de información.

Para la fase de puesta en producción, se instalara el sistema en un único equipo para observar su funcionamiento durante un día con el usuario además de suministrar los respectivos manuales para su revisión.

El software o sistema de información desarrollado debe estar documentado con suficiente detalle y apropiadamente validado o verificado (ISO 17025).

El sistema de información deberá ser entregado a la alta gerencia con sus respectivos manuales: manuales de instalación, tanto como el de sistema como el de usuario, modelo entidad relación de base de datos, modelo de datos, código fuente si aplica, documentación del código fuente, medios de instalación, Diagrama de clases, diagrama de casos de uso, diagramas de secuencia, diagramas de implementación, documentación de pruebas realizadas, capacitación al personal que utilizara el sistema de información, y toda la documentación requerida a la alta gerencia. Antes de entrar en producción el sistema de información deberá estar aprobado mediante acta en la que conste dicha aprobación.

Si se requieren realizar cambios en la funcionalidad o características del sistema de información una vez este en producción, el usuario que lo solicite deberá realizar una solicitud por escrito especificando con el mayor detalle posible los cambios requeridos, esta solicitud será evaluada por los desarrolladores quienes definirán y comunicaran las alternativas al solicitante.

Antes de adquirir un software por contratación de servicios de desarrollo personalizado o compra de software comercialmente distribuido, la empresa define los requisitos específicos de seguridad de la información para implementar en la aplicación. Estos requisitos deben quedar por escrito y pueden estar conformados por:

- Manejo de Audit Trails.
- Cumplir con la 21CFR parte 11 en el caso de firmas electrónicas.
- Usuarios y privilegios independientes (controles de acceso).
- El sistema debe estar debidamente validado con el suficiente detalle de acuerdo a las Gamp5.
- Se le deben aplicar y documentar todas las pruebas necesarias (IQ, OQ, PQ).
- Se deben validar: los datos de entrada, el procesamiento interno, la autenticación de mensajes y los datos de salida.
- El desarrollador debe utilizar herramientas licenciadas (si aplica).
- Incluir recomendaciones de la OWASP (Top 10).
- Contar con una metodología de desarrollo seguro.
- Firmar un acuerdo de confidencialidad.

9.8. POLITICA DE CONTINUIDAD DEL NEGOCIO

LABROATORIOS SFC LTDA., define los lineamientos necesarios a seguir antes, durante y después de una interrupción en sus operaciones, con el fin de responder asertivamente frente a eventos que afecten los servicios del laboratorios; de igual forma gestionar la continuidad y restauración de sus operaciones con un mínimo impacto.

9.8.1. Consideraciones generales de continuidad del negocio. El laboratorio establece como elementos primordiales para la aplicación del plan de continuidad del negocio la protección de los activos de la organización, salvaguardar la vida humana y la continuidad de sus operaciones.

El laboratorio consciente de la importancia de la continuidad del negocio establece un comité de continuidad del negocio conformado por los jefes de áreas, analista de sistemas y brigadistas.

La alta gerencia consciente de los riesgos presentes en el entorno y la importancia de adoptar un plan de continuidad del negocio brinda los recursos necesarios para capacitar al personal clave encargado de la gestión de continuidad del negocio. Igualmente se concientiza al personal del laboratorio para adoptar conductas responsables ante la prevención de incidentes.

Para el desarrollo del plan de continuidad del negocio la organización tiene como referencia la norma ISO 22301:2012 “Continuidad del negocio”.

Correspondientes al comité de continuidad del negocio:

- Velar por la aplicación de la política de continuidad del negocio.
- Validar los procesos críticos que se incluyen en el plan de continuidad del negocio, igualmente estimar el tiempo máximo de interrupción de los servicios del laboratorio.
- Mantener actualizado el análisis de vulnerabilidades y amenazas, igualmente evaluar periódicamente los riesgos y su probabilidad de materialización.
- Mantener actualizado el plan de continuidad del negocio y garantizar la disponibilidad de los procedimientos asociados a la gestión de incidentes.

- Asegurar que se encuentre actualizado la evaluación de proveedores para procesos críticos y evaluar periódicamente el stock de repuestos para procesos críticos.

Unificar el plan de continuidad del negocio enfocado en seguridad de la información con los demás sistemas de gestión del laboratorio.

9.9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA SFC dedica sus esfuerzos a fabricar productos veterinarios de marca propia y maquilar a terceros; además realiza análisis fisicoquímicos y microbiológicos para externos.

Con la implementación de la NTC/ISO 27001:2013 se busca garantizar la confidencialidad, disponibilidad e integridad de la información, salvaguardándola contra amenazas internas y externas, mediante la identificación, valoración, selección e implementación de controles, monitoreo y seguimiento de los niveles de riesgo.

La organización se compromete a cumplir con las disposiciones constitucionales, contractuales, legales y reglamentarias relacionadas con la seguridad de la información, además de preservar en todo momento la seguridad de la información como parte de la mejora continua, apoyando el logro de sus objetivos y el cumplimiento de los compromisos organizacionales con la confidencialidad de la información, el manejo y divulgación adecuada de la información.

La alta dirección se compromete a brindar las herramientas necesarias para que sus empleados y contratistas cumplan con los lineamientos de la seguridad de la información.

La Organización se compromete a cumplir con los requisitos especificados en la ISO 27001:2013, y a gestionar cada oportunidad que se presente como marco de referencia para mejorar continuamente.

La Organización se compromete a cumplir con los requisitos especificados en la ISO 27001:2013, y a gestionar cada oportunidad que se presente como marco de referencia para mejorar continuamente.

9.10. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACION

- Concientizar al personal de la organización en seguridad de la información y buenas prácticas de seguridad para la prevención de incidentes que afecten la continuidad de las operaciones.
- Mantener en niveles óptimos la confidencialidad de la información contenida en los resultados e informes de tipo papel y electrónico.
- Gestionar la atención oportuna cuando se generen reportes que afecten la seguridad de la información.
- Cerciorarse que todos los registros puedan ser rápidamente recuperables, almacenados y retenidos adecuadamente contra modificaciones, accesos no autorizados y estén disponibles para el personal autorizado cuando se requiera.

10. FORMACIÓN Y CONCIENCIACIÓN

Las políticas de seguridad de la información buscan proteger la organización y garantizar la continuidad de los sistemas de información de todas aquellas amenazas presentes en sus actividades diarias. Es importante incluir las políticas de seguridad como parte de la cultura organizacional, para asegurar esto se debe tener un compromiso de la alta dirección para una correcta difusión, consolidación y cumplimiento de las políticas.

10.1. CAPACITACION

Para que las políticas de seguridad sean eficaces, todos los empleados de la organización, y cuando sea necesario, clientes o terceros deberán recibir una adecuada capacitación y actualización relacionado con la política de seguridad de la información y procedimientos. Este proceso comprende los requerimientos de seguridad, responsabilidades y uso correcto de las instalaciones de TI y recursos en general.

El jefe de Talento Humano será la persona encargada de coordinar las acciones necesarias para las capacitaciones.

El material correspondiente a las capacitaciones será revisado cada 6 meses o cuando se presenten cambios significativos. El personal nuevo recibirá la capacitación y un material informativo para mejorar sus conocimientos con relación a las amenazas que puedan presentarse, este proceso se realizara antes de definir sus privilegios de acceso a los sistemas, además será evaluado con el fin de medir la efectividad de la capacitación. Todo lo anterior con el fin crear conciencia y cultura de seguridad de la información al interior de la organización…Véase Anexo N…

11. CONCLUSIONES

Diseñar un Sistema de Gestión de Seguridad de la información en LABORATORIOS SFC LTDA., será un gran avance para el desarrollo de sus labores y la reputación de la compañía frente a sus cliente, ya que dicha organización maneja información de carácter confidencial dentro de sus labores diarias (Información de clientes y proveedores, información de productos, información de análisis de productos y materias primas, etc.).

Clasificar y valorar los activos informáticos permitió a la organización comprenderlos y analizarlos de acuerdo al uso que se les da. Valorarlos y determinar su nivel de criticidad permitió a la organización ubicar dentro de una escala cualitativa el valor y rango de criticidad a la que están expuestos los activos.

El análisis y determinación de riesgos, amenazas y vulnerabilidades es una labor necesaria dentro de toda organización ya que permite conocer todos los riesgos y amenazas a las que se encuentra expuesta una empresa, esto con el fin de mitigarlas o eliminarlas para que no afecten en consideración el proceso de negocio. Una vez se determinaron los riesgos, amenazas, su probabilidad de ocurrencia e impacto, se seleccionaron las salvaguardas o contramedidas más adecuadas para dar tratamiento a dichas amenazas.

La norma NTC-ISO 27001:2013 establece una serie de controles y contramedidas que le permiten a la empresa determinar las políticas y procedimientos más adecuados con el fin de preservar la confidencialidad, integridad y disponibilidad de la información. Todos los controles presentados en esta norma deben ajustarse a los objetivos del negocio, ser comunicados, cumplidos y aprobados por la alta gerencia.

LABORATORIOS SFC LTDA es una empresa con alto nivel de competitividad en el mercado farmacéutico veterinario, el establecimiento de la política de seguridad de la información permitió generar en su personal una visión más global y asertiva en términos de seguridad de la información, además el apoyo y aprobación por parte de la alta gerencia demuestra el compromiso que tiene la organización con el manejo y tratamiento de información de clientes y todas las terceras partes que buscan que su información sea tratada dentro de estándares seguros.

12. RESULTADOS Y DISCUSIÓN

Los resultados obtenidos del presente proyecto dan cumplimiento a los objetivos específicos establecidos anteriormente con el propósito de cumplir el objetivo general del proyecto.

Se llevaron a cabo las siguientes actividades:

- Diagnóstico inicial para determinar el nivel de madurez de la organización, respecto a la seguridad de la información.
- Identificación y valoración de riesgos.
- Desarrollo de políticas y procedimientos.
- Para el desarrollo de cada una de las actividades del proyecto se utilizaron diferentes métodos como entrevistas, documentación física y electrónica, asesorías, etc.

Una vez se inició la aplicación de los controles, se concluye que aún falta mucho por hacer, sin embargo la organización se ha integrado en un proceso de cambio y mejoramiento continuo de la seguridad de la información. Actualmente los controles se encuentran distribuidos de la siguiente forma:

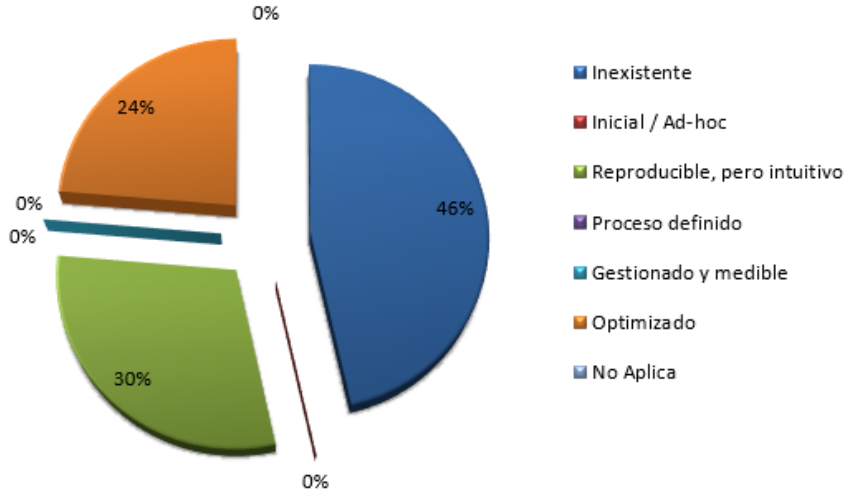
Tabla 17. Controles por nivel de cumplimiento.

NIVEL	CONTROLES
Inexistente	53
Inicial / Ad-hoc	0
Reproducible, pero intuitivo	34
Proceso definido	0
Gestionado y medible	0
Optimizado	27
No Aplica	0
TOTAL	**114**

Fuente: El Autor.

Gráficamente la distribución de los controles puede representarse de la siguiente manera:

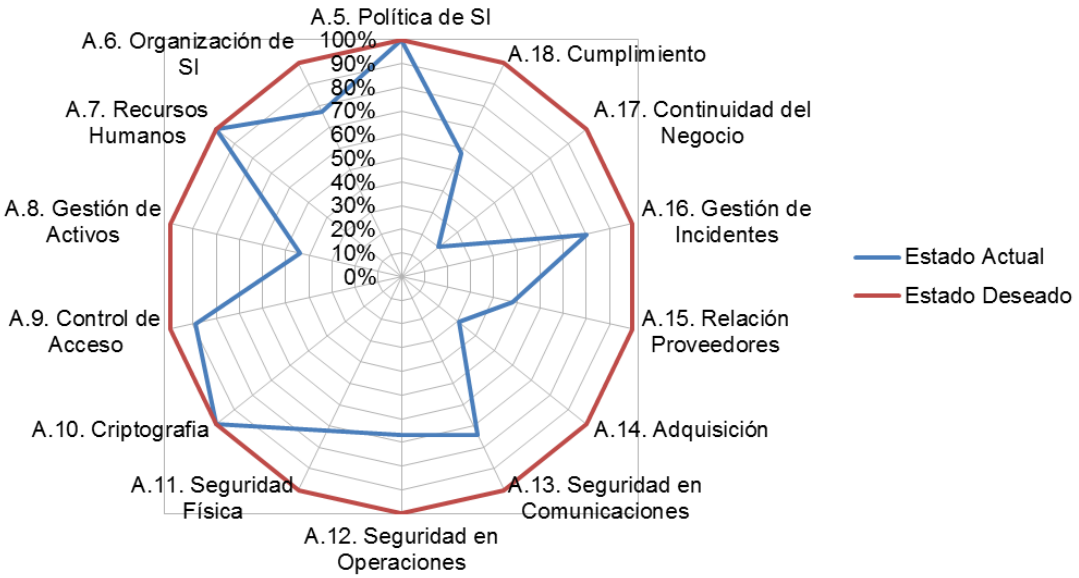
Figura 12. Estado de madurez de los controles.



Fuente: El Autor.

Por último se representa el cumplimiento de la ISO 27001:2013 por dominio contra el estado esperado de acuerdo al estado actual de la declaración de aplicabilidad…Véase Anexo S…, para esta representación se utiliza un gráfico de tipo radar.

Figura 13. Cumplimiento actual ISO 27001 X Dominio.



Fuente: El Autor.

13. DIVULGACIÓN

Es importante divulgar dentro de la entidad y de forma adecuada el Sistema de Gestión de Seguridad de la Información y las políticas de seguridad de la información, lo anterior con el objetivo de que los colaboradores y terceras partes comprendan las políticas para ayudar a proteger la confidencialidad, integridad y disponibilidad de la información…Véase Anexo M…

El Manual de Seguridad de la Información desarrollado en LABORATORISO SFC LTDA (SC – 02M "MANUAL DE SEGURIDAD DE LA INFORMACIÓN") se encuentra basado en la Norma ISO/IEC 27001:2013 y dentro del cual se presentan las siguientes políticas:

- Uso aceptable de los activos.
- Control de acceso a la información.
- Procedimientos operativos para gestión de TI (Tecnologías de la Información).
- Política de seguridad para proveedores.
- Política para gestión de incidentes.
- Política de construcción de los sistemas seguros.
- Política de continuidad del negocio.

Las Políticas de Seguridad de la Información se han definido en el documento SC-02MA4 "Políticas de seguridad de la información", dichas políticas son de cumplimiento obligatorio para todos los colaboradores que laboran e igualmente los terceros que prestan sus servicios en LABORATORIOS SFC LTDA.

14. CRONOGRAMA DE ACTIVIDADES

Tabla 18. Convenciones.

CONVENCIONES	
En proceso	
Fecha Cumplimiento	
Retrasado	
Cumplido	

Fuente: El Autor.

Tabla 19. Cronograma de actividades.

Actividad		JUN				JUL				AGO				SEP				OCT				NOV			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Revisión del Alcance																								
2	Revisión de ciclo PHVA																								
3	Documentación Metodología de riesgos																								
4	Metodología de clasificación y etiquetado																								
5	Declaración de aplicabilidad																								
6	Desarrollo manual de seguridad																								
7	Políticas																								

Fuente: El Autor.

BIBLIOGRAFIA

AREIZA, B, RINCÓN, L. Hacia un Modelo de Madurez para la Seguridad de la Información, Universidad EAFIT - Colombia, Congreso Iberoamericano de Seguridad Informática CIBSI'05, 21-25 de Noviembre de 2005, Valparaíso, Chile. [en línea]. <http://cibsi05.inf.utfsm.cl/presentaciones/sesion10/Modelo_de_madurez_SI.pdf> [citado en 10 de Octubre de 2015]

BATISTA, E. Escalas de actitudes para la investigación sociológica, psicológica y pedagógica. Medellín: Copiyepes, 1982. pp. 40-6.

BSCONSULTORES. Continuidad del negocio y recuperación de desastres. [en línea]. <http://www.bscconsultores.cl/descargas/D.5%20%20Continuidad%20del%20NegoNeg%20y%20%20recuperacin%20de%20desastres%20ISACA.pdf> [citado en 10 de Octubre de 2015]

CRESSON WOOD, Charles. Políticas de Seguridad Informática – Mejores Prácticas Internacionales, Version 9.0. Texas: NetIQ, Inc., 2002. 758 p. ISBN 1-881585-09-3

DÍAZ BECERRA, J. C. Los sistemas de gestión en la sostenibilidad de las organizaciones. Normas & Calidad, 2006. 26-32 p.

GERENCIE.com. Auditoria de sistemas de información. [en línea]. <http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html> [citado 17 de Mayo de 2015]

HERNANDEZ R., FERNANDEZ C., BAPTISTA P. Metodología de la investigación. Cuarta Edición. McGraw Hill, México, 2006.

HERNÁNDEZ, T., & GODÍNEZ, C. L. (2007). Procedimiento para el diseño e implantación de un sistema de gestión integrado en el BIOCEN. Ingeniería Industrial, 28, 27-33.

ICONTEC. Norma técnica NTC-ISO/IEC colombiana 27001. [en línea]. <http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf> [citado en 10 de Octubre de 2015]

ICONTEC. Compendio tesis y otros trabajos de grado. Quinta Actualización. Instituto Colombiano de Normas Técnicas y Certificación – ICONTEC, Bogotá D.C., Colombia, 2006.

INCIBE. Herramienta de autodiagnóstico. [en línea]. <https://www.incibe.es/empresas/Herramienta_de_autodiagnostico/> [citado en 13 de Octubre de 2015]

INEI. Guía práctica para el desarrollo de planes de contingencia de sistemas de información. [en línea]. <http://www.ongei.gob.pe/seguridad/seguridad2_archivos/lib5131/libro.pdf> [citado en 30 de Octubre de 2015]

INTECO. Guía práctica para PYMES: cómo implantar un plan de continuidad de negocio. [en línea]. <https://www.incibe.es/CERT/guias_estudios/guias/guia_continuidad> [citado en 20 de Octubre de 2015]

INTECO-CERT. Curso De Sistemas De Gestión De La Seguridad De La Información Según La Norma UNE-ISO/IEC 27000. España: INTECO-CERT, 2010. 91 p.

ISO2700.es. ¿Qué es un SGSI?. [en línea]. <http://www.iso27000.es/sgsi.html> [citado en 15 de Octubre de 2015]

ISO27000.es. Sistema de Gestión de la Seguridad de la Información. [en línea]. <http://www.iso27000.es/doc_sgsi_all.htm> [citado en 15 de Octubre de 2015]

ISO 27001: La Seguridad de la Información en la Gestión de la Continuidad de Negocio. [en línea]. <http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/> [citado en 15 de Octubre de 2015]

JIMÉNEZ, L. Guía de desarrollo de un plan de continuidad de negocio. [en línea]. <http://www.criptored.upm.es/guiateoria/gt_m001r.htm> [citado en 30 de Octubre de 2015]

LERMA, Héctor Daniel. Metodología de la investigación. Bogotá: Ecoe Ediciones, 2004.

MENDEZ, C. Metodología, Diseño y Desarrollo del proceso de Investigación. Tercera Edición, McGraw Hill, Colombia, 2001.

NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos

NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información.

POVEDA, J. Gestión y tratamiento de los riesgos, 2007. [en línea]. <http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf> [Consulta: 01 Julio 2015]

SISTESEG. Política de continuidad del negocio (BCP, DRP). [en línea]. <http://www.sisteseg.com/files/Microsoft_Word_POL_TICA_DE_CONTINUIDAD_DEL_NEGOCIO.pdf> [citado en 25 de Octubre de 2015]

SANDSTROM, O. Proceso de implantación de un SGSI, adoptando la ISO 27001. Arsys Internet. [en línea]. <http://www.borrmart.es/articulo_redseguridad.php?id=1724&numero=33 (noviembre de 2009) > [citado en 4 de Octubre de 2015]

TORO, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

ANEXO A. AVAL PROYECTO DE GRADO

LABORATORIOS
NIT. 830.001.242-1

LABORATORIOS S.F.C. LTDA.
SERVICIOS FARMACÉUTICOS DE CALIDAD
Integramos la Calidad al Servicio

BOGOTA D.C., Mayo 20 de 2015

SEÑORES
COMITÉ DE TRABAJOS DE GRADO
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
Ciudad

REF.AVAL PROYECTO DE GRADO

Apreciados Señores:

Por medio de la presente *LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA – SFC* en su calidad de laboratorio farmacéutico veterinario, se permite comunicarles que ha concedido autorización y apoya el proyecto de grado denominado "**DESARROLLO E IMPLEMENTACION DE UN SGSI (SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION) BASADO EN ISO27000 E ISO27001 PARA LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA**". El cual será desarrollado e implementado por el estudiante de Especialización en Seguridad Informática:

JORGE LEONARDO RODRIGUEZ
C.C. 1.097.035.128

Dicho proyecto tiene como objetivo desarrollar e implementar el SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN BAJO NTC-ISO-IEC 27001 con sus respectivos controles y procedimientos reglamentarios.

Para constancia se firma en Bogotá a los 20 días del mes de Mayo de 2015

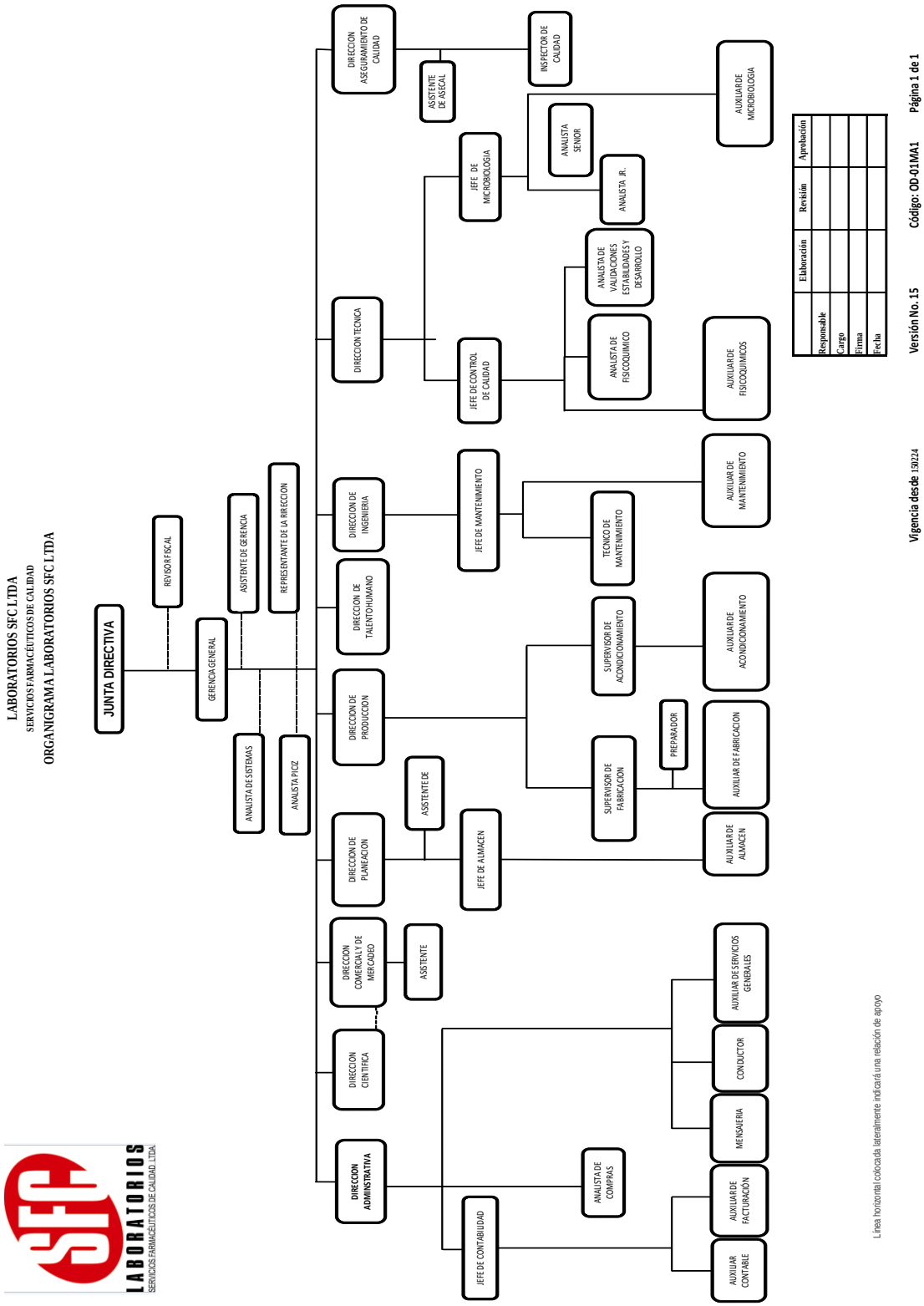
Valerio Castaño Marín
Gerente General

Cra. 106 No. 15-25
Casillero 084
Tel: 4395155
Zona Franca Bogotá
COLOMBIA

Carrera 106 Nº 15 - 25 Casillero 0084
PBX: 439 5155 Cel.: 314 2373923
Fax: 621 1393 - 439 5155 Ext. 26
E-mail: racyma@cable.net.co
Zona Franca de Bogotá - Colombia

Fuente: El Autor.

ANEXO B. ORGANIGRAMA LABORATORIOS SFC LTDA



Fuente: LABORATORIOS SFC.

ANEXO C. LISTADO DE ACTIVOS SFC

CÓDIGO	NOMBRE
10 ALMACEN	
1001	Ascensor de Servicio No. 1
1001-01	Moto reductor
1002	Báscula No. 1
1004	Termo higrómetros ALM
1004-01	Termo higrómetro ALM-01TH
1004-02	Termo higrómetro ALM-02TH
1006	Computador ALM-01PC
1006-01	Monitor ALM
1006-02	C.P.U ALM
1009	Unidad Cortina de Almacén No. 1
1009-01	Moto ventilador
1011	Teléfono ALM-01Te
1012	Balanza No. 2
1015	Termómetros ALM
1015-01	Termómetro ALM-01T
1015-02	Termómetro digital ALM 02-T
3024	Nevera No. 1
20 MICROBIOLOGIA	
2001	Agitador Vortex No. 1
2003	Autoclave No. 2
2003-1	Manómetro AC2-08
2005	Baño Termostatado No. 1
2008	Cabina de Flujo Laminar No. 3
2009	Cabina de Flujo Laminar tipo II No. 4
2010	Cuenta Colonias No. 1
2011	Bomba de Vacío No. 4
2011-01	Manómetro BV4-01
2013	Incubadora No. 7
2014	Incubadora Precisión Scientific No. 2
2015	Incubadora Sanyo No. 3
2016	Micro pipeta 0.5 a 5 mL No. 2
2017	Micro pipeta 0.5 a 5 mL No. 1
2018	Microscopio No. 1
2019	Nevera No. 3
2020	Incubadora B-28 No. 1
2021	Termómetro MB 01-T

CÓDIGO	NOMBRE
2021-04	Termómetro digital MB 04-T
2021-05	Termómetro digital MB 05-T
2021-06	Termómetro digital MB 06-T
2021-07	Termómetro infrarrojo MB 07-T
2022	Computadores MB
2022	Computador MB-01PC
2022-1	Monitor MB-01PC
2022-2	C.P.U MB-01PC
2024	Teléfono MB-01Te
2025	Computador MB-02PC
2025-1	Monitor MB-02PC
2025-2	C.P.U MB-02PC
2026	Autoclave No. 3
2026-01	Manómetro AC3-01
2027	Micro pipeta de 20 a 200 µL No. 3
2028	Horno Despirogenizador No. 2
2029	PH Metro No. 5
2030	Muestreador de Aire No. 1
2031	Micro pipeta de 0.5 a 5 mL No. 4
-	Termo higrómetros MB
2032	Termo higrómetro MB-01TH
2032-02	Termo higrómetro MB-02TH
2032-03	Termo higrómetro MB-03TH
2032-04	Termo higrómetro MB-04TH
2032-05	Termo higrómetro MB-05TH
2032-06	Termo higrómetro MB-06TH
2033	Termómetro infrarrojo MB 03-T
2034	Computador portátil MB-03PC
2035	Congelador No. 1
2037	Nevera No. 5
2038	Fotocopiadora
2039	Muestreador de Aire No. 2
2041	Muestreador de aire No. 3
2042	Micro pipeta de 100 a 1000 µL No. 5
2044	Micro pipeta de 100 a 1000 µL No. 6
2045	Micro pipeta de 100 a 1000 µL No. 7
2046	Teléfono MB-02Te
2047	Baño Termostatado No. 2
2048	Agitador Vortex No. 2

CÓDIGO	NOMBRE
2049	Secador de Manos No. 5
2050	Autoclave No. 4
2050-01	Manómetro AC4-01M
2050-02	Manómetro AC4-02M
2052	Equipo de Filtración No. 1
2053	Equipo de Filtración No. 2
2054	Impresora MB-01Im
2506	Espectrofotómetro No. 1
2510	Incubadora No. 4
2531	Incubadora No. 6
3011	Cabina de Flujo Laminar No. 1
3011-1	Manómetro Magnehelic CFL1-01
2057	Nevera No. 4
2058	Nevera No. 7
2059	Plancha de agitación No. 5
2060	Plancha de agitación No. 6
2061	Balanza No. 9
2061-01	Impresora para balanza 9
2062	Balanza No. 10
2062-01	Impresora para balanza 10
2063	Balanza No. 11
2063-01	Impresora para balanza 11
2064	Computador MB-04PC
2065	Compuatdor MB-05PC
2066	Data Logger MB
2066-01	Data Logger MB-01TW
2066-02	Data Logger MB-02TW
2066-03	Data Logger MB-03TW
2066-04	Data Logger MB-04TW
2066-05	Data Logger MB-05TW
2066-06	Data Logger MB-06TW
2066-07	Data Logger MB-07TW
2066-08	Data Logger MB-08TW
2066-09	Data Logger MB-09TW
2066-10	Data Logger MB-010TW
2066-11	Data Logger MB-11TW
2067	Computador Servidor de MB
2068	Nevera No. 8
2069	Aire acondicionado Portátil

CÓDIGO	NOMBRE
2070	Cuenta Colonias No. 2
2071	Muestreador de Aire No. 4
25 FISICOQUÍMICO	
2501	Balanza Analítica No. 6
2502	Balanza Analítica No. 4
2503	Cabina de Extracción No. 1
2504	Conductivimetro No. 1
2507	Estufa de Secado No. 1
2508	Estufa No. 2
2509	HPLC No. 1
2509-01	Interface
2509-02	Detector
2509-03	Bomba
2509-04	Desgasificador
2511	Lava Ojos No. 2
2512	PH Metro No. 2
2513	PH Metro No. 1
2514	Termo higrómetros FQ
2514-01	Termo higrómetro FQ-01TH
2514-02	Termo higrómetro FQ-02TH
2514-04	Termo higrómetro FQ-04TH
2516	Viscosímetro No. 1
2517	Computadores FQ
2517-10	Computador HPLC No. 1
2517-10-01	Monitor FQ-01PC
2517-10-01	CPU F1-01PC
2517-30	Computador FQ-03PC
2517-30-01	Monitor FQ-03PC
2517-30-02	CPU FQ-03PC
2518	Impresora FQ-01Im
2522	Bomba de vacío No. 3
2522-01	Manómetro BV3-1
2523	Titulador No. 1
2523-01	Bomba
2523-02	Agitador
2524	Ultrasonido No. 1
2525	Incubadora No. 5
2526	Nevera No. 2
2527	Termómetros FQ

CÓDIGO	NOMBRE
2527-01	Termómetro FQ 01-T
2527-04	Termómetro digital FQ 04-T
2514-03	Termo higrómetro FQ-03TH
2529	Teléfono FQ No. 1
2530	Cámara de Estabilidad Natural No. 1
2532	Cámara de Estabilidad Acelerada No. 2
2527-03	Termómetro FQ 03-T
2535	HPLC No. 2
2535-01	Organizador
2535-02	Detector L-2455
2535-03	Automuestreador L-2200
2535-04	BombaL-2130
2517-20	Computador HPLC No. 2
2517-20-01	Monitor FQ-02PC
2517-20-02	CPU FQ-02PC
2519	Impresora FQ-02Im
2537	Plancha de agitación No. 2
2538	Dispensador Análogo No. 1
2539	Dispensador Digital
2540	Dispensador Análogo No. 2
2542	Refractómetro
2543	Fusiómetro
2544	Centrifuga
2547	Plancha de Agitación No. 4
2548	Calibrador Control de Calidad
2545	Plancha de Agitación No. 3
2549	HPLC No. 3
2549-01	Bomba
2549-02	Automuestreador
2549-03	Columna termostato
2549-04	Detector DAD
2550	Computador HPLC 3
2550-01	CPU computador HPLC 3
2550-02	Monitor Computador HPLC 3
4507	Data Logger Testo
30 FABRICACION	
3001	Agitador No. 1
3003	Anillo de Distribución de Agua
3003-1	Tablero de control

CÓDIGO	NOMBRE
3003-2	Tanque pulmón de 500 L
3003-3	Bomba No. 3 CHI
3003-4	Sensor de nivel bajo
3003-5	Sensor de nivel alto
3003-6	Carcaza de Venteo
3003-7	Lámpara U.V. No. 2
3003-8	Filtro de 0.22 µm 5"
3003-9	Bomba No. 4 CHI
3003-10	Manómetro AD-1
3004	Autoclave No. 1
3004-1	Bomba vacío No. 1
3004-2	Bomba vacío No. 2
3004-3	Impresora HP LASERJET 1020
3004-04	Manómetros Autoclave No. 1
3004-04-01	Manómetro AC1-1
3004-04-02	Manómetro AC1-2
3004-04-03	Manómetro AC1-3
3004-04-04	Manómetro AC1-4
3004-04-05	Manómetro AC1-5
3004-04-06	Manómetro AC1-6
3004-04-07	Manómetro AC1-7
3005	Balanza ACUWEIGH No. 3
3006	Balanza ACUWEIGH No. 5
3007	Báscula ACUWEIGH No. 2
3008	Bomba de vacío No. 2
3008-01	Manómetro BV2-1
3009	Bomba Esfero No. 1
3010	Bomba No. 4
3013	Carcazas para filtros
3013-01	Carcaza para Filtro No. 1
3013-02	Carcaza para Filtro No. 2
3013-03	Carcaza para Filtro No. 3
3013-04	Carcaza para Filtro No. 4
3013-05	Carcaza para Filtro No. 5
3013-06	Carcaza para Filtro No. 6
3013-07	Carcaza para Filtro No. 7
3013-08	Carcaza para Filtro No. 8
3013-09	Carcaza para Filtro No. 9
3014	Envasadora No. 1

CÓDIGO	NOMBRE
3015	Envasadora No. 2
3017	Grafadora No. 1
3018	Grafadora No. 2
3019	Grafadora No. 3
3020	Horno Despirogenizador No. 1
3020	Manómetro H1
3020	Manómetro H2
3021	Lavaojos No. 1
3022	Marmita No. 1
3023	Molino Coloidal
3025	Pistones para envasar
3025-01	Pistón para envase No. 1
3025-02	Pistón para envase No. 2
3025-03	Pistón para envase No. 3
3025-04	Pistón para envase No. 4
3026	Planta de Tratamiento de Agua
3026-1	Tanque de agua potable
3026-2	Bomba No. 1 MQ
3026-3	Filtro de arena
3026-4	Filtro de carbón
3026-5	Filtro 5 µm
3026-6	Lámpara U.V. No. 1
3026-7	Filtro de 1µm
3026-8	Membranas de osmosis
3026-9	Filtro de 0.22µm 10"
3026-10	Bomba No. 2 MQ
3026-11-01	Manómetro PTA-1
3026-11-02	Manómetro PTA-2
3026-11-03	Manómetro PTA-3
3026-11-04	Manómetro PTA-4
3026-11-05	Manómetro PTA-5
3026-11-06	Manómetro PTA-6
3026-11-07	Manómetro PTA-7
3026-11-08	Manómetro PTA-8
3026-11-09	Manómetro PTA-9
3027	Regletas para envasar
3027-01	Regleta para envasar No. 1
3027-02	Regleta para envasar No. 2
3027-03	Regleta para envasar No. 3

CÓDIGO	NOMBRE
3027-04	Regleta para envasar No. 4
3032	Reloj Tarjetero No. 1
3033	Revisadora No. 1
3034	Revisadora No. 2
3035	Revisadora No. 3
3036	Selladora de Colapsibles No. 1
3037	Tanque Preparación No. 2 de 500 L.
3037-1	Agitador No.2
3038	Tanque Preparación No. 3 300 L
3039	Tanque Preparación No. 4 300 L
3040	Tanque Preparación No. 5 58 L
3041	Tanque Preparación No. 6 55 L
3042	Tanque Preparación No. 7 200 L
3043	Tanque Pulmón No. 1
3043-01	Manómetro TP-1
3044	Balanza Trumax No. 8
3045	Tanque Pulmón No. 3
3045-01	Manómetro TP-3
3046	Tanque Pulmón No. 2
3046-01	Manómetro TP-2
3047-10	Termómetro FAB 01-T
3047-20	Termómetro digital FAB 02-T
3047	Termómetro de inmersión FAB 03-T
3047-34	Termómetro de inmersión FAB 04-T
3047-35	Termómetro de inmersión FAB 05-T
3047-36	Termómetro de inmersión FAB 06-T
3050	Secador de Manos No. 3
3051	Unidad Cortina de Aire paso Materiales No. 2
3052	Unidad Cortina de Aire paso Personal No. 3
3053	Unidad Cortina de Aire corredor Fabricación No. 4
3054	Teléfono FAB
3056	PH Metro No. 3
3056-06	PH Metro No. 6
3056-07	PH Metro No. 7
3056-08	PH Metro No. 8
3057	Agitador No. 4
3058	Cabezotes de Grafado
3058-01	Cabezote de Grafado No. 1
3058-02	Cabezote de Grafado No. 2

CÓDIGO	NOMBRE
3058-03	Cabezote de Grafado No. 3
3058-04	Cabezote de Grafado No. 4
3058-05	Cabezote de Grafado No. 5
3060	Tablero Variador No. 1 Preparación 1
3061	Tablero Variador No. 2 Preparación 2
3064	Llenadora de jeringas
3066	Bomba Esfero No. 2
3067	Selladora de colapsibles No. 2
3068	Bomba No. 3
3069	Tanque Preparación No. 9 110 L
3070	Revisadora No. 4
3071	Tanque auxiliar No. 1
3072	Módulo de Flujo Laminar No. 1
3072-01	Manómetro MFL1-01
3073	Módulo de Flujo Laminar No. 2
3073-01	Manómetro MFL2-01
3074	Módulo de Flujo Laminar No. 3
3074-01	Manómetro MFL3-01
3075	Módulo de Flujo Laminar No. 4
3075-01	Manómetro MFL4-01
3076	Banda Transportadora No. 3
3077	Banda Transportadora No. 4
3078	Tanque de Preparación No. 10 500 L
3078-01	Agitador No. 5 Tanque No. 10
3079	Agitador Móvil No. 6
3080	Tanque Pulmón No. 4
3080-01	Agitador No. 7 Tanque pulmón no. 4
3080-02	Manómetro TP4-01M
3080-03	Manómetro TP4-02M
3081	Nevera No. 9
2004	Balanza No. 1
2036	Balanza No. 7
ACONDICIONAMIENTO	
3501	Banda Transportadora No. 1
3502	Banda Transportadora No. 2
3504	Computador ACN-01PC
3504-1	Monitor ACN-01
3504-2	CPU ACN-01
3505	Pistola Termoencogible No 1

CÓDIGO	NOMBRE
3506	Teléfono ACN
3507	Reloj tarjetero No. 3
3508	Printjet INKJET
3509	Pistola Termoencogible No. 2
3510	Termo higrómetro ACOND 01-TH
3511	Pistola Termoencogible No. 3
40 MANTENIMIENTO	
4001	Sistema de vapor
4001-1	Caldera
4001-2	Tablero de control
4001-3	Tanque de condensados No. 1
4001-4	Bomba de condensados No. 1
4001-5	Bomba de condensados No. 2
4001-06	Suavizador
4001-08	Manómetros Caldera
4001-08-01	Manómetro C-1
4001-08-02	Manómetro C-2
4001-08-03	Manómetro C-3
4001-08-04	Manómetro C-4
4001-08-05	Manómetro C-5
4003	Moto compresor
4003-02	Red de Distribución de Aire Comprimido
4003-02-01	Unidad Reguladora de Aire Comprimido 1
4003-02-02	Manómetro Regulador de Aire Comprimido RAC-1
4003-02-03	Unidad Reguladora de Aire Comprimido 2
4003-02-04	Manómetro Regulador de Aire Comprimido RAC-2
4003-02-05	Unidad Reguladora de Aire Comprimido 3
4003-02-06	Manómetro Regulador de Aire Comprimido RAC-3
4003-02-07	Unidad Reguladora de Aire Comprimido 4
4003-02-08	Manómetro Regulador de Aire Comprimido RAC-4
4003-03	Manómetros Motocompresor
4003-03-01	Manómetro MC-1
4003-03-02	Manómetro MC-2
4003-03-03	Manómetro MC-3
4003-03-04	Manómetro MC-4
4003-03-05	Manómetro MC-5
4004	Sistema de suministro de Nitrógeno
4004-01	Estación reguladora de Nitrógeno
4004-01-10	Unidad reguladora de Nitrógeno ERN-1

CÓDIGO	NOMBRE
4004-01-11	Manómetro ERN 1-1
4004-01-12	Manómetro ERN 1-2
4004-01-20	Unidad reguladora de Nitrógeno ERN-2
4004-01-21	Manómetro ERN 2-1
4004-01-22	Manómetro ERN 2-2
4004-01-30	Unidad reguladora de Nitrógeno ERN-3
4004-01-31	Manómetro ERN 3
4004-01-40	Válvula de Seguridad
4004-02	Red de distribución de Nitrógeno
3028	Reguladora de Nitrógeno RN-1
4004-02-11	Manómetro RN 1-1
4004-02-12	Manómetro RN 1-2
3029	Reguladora de Nitrógeno RN-2
4004-02-21	Manómetro RN 2-1
4004-02-22	Manómetro RN 2-2
3030	Reguladora de Nitrógeno RN-3
4004-02-31	Manómetro RN 3-1
4004-02-32	Manómetro RN 3-2
3031	Reguladora de Nitrógeno RN-4
4004-02-41	Manómetro RN 4-1
4004-02-42	Manómetro RN 4-2
4004-02-50	Reguladora de Nitrógeno RN-5
4004-02-51	Manómetro RN 5-1
4004-02-52	Manómetro RN 5-2
4005	Subestación 150 KVA
4010	Unidad de Suministro Acondicionamiento y Oficinas
4007	Unidad de Extracción Acondicionamiento y Oficinas
4027	Unidad de Extracción Baños
4010-03	Manómetros Ductos AC
4010-03-01	Manómetro SAC 01
4010-03-02	Manómetro SAC 02
4010-03-03	Manómetro EAC 01
4011	Unidad de Suministro Fabricación
4008	Unidad de Extracción Fabricación
4006	Unidad de Extracción Puntual
4035	Unidad de Extracción Preparación 1
4036	Unidad de Extracción Puntual Preparación 1
4011-06	Manómetros FAB
4011-06-01	Manómetro FAB 1

CÓDIGO	NOMBRE
4011-06-02	Manómetro FAB 2
4011-06-03	Manómetro FAB 3
4011-06-04	Manómetro FAB 4
4011-06-05	Manómetro FAB 5
4011-06-07	Manómetro FAB 7
4011-06-08	Manómetro FAB 8
4011-06-09	Manómetro FAB 9
4011-06-10	Manómetro FAB 10
4011-06-11	Manómetro FAB 11
4011-06-12	Manómetro FAB 12
4011-06-13	Manómetro FAB 13
4011-06-14	Manómetro FAB 14
4011-06-15	Manómetro FAB 15
4011-06-16	Manómetro FAB 16
4011-06-17	Manómetro FAB 17
4011-06-18	Manómetro FAB 18
4011-06-19	Manómetro FAB 19
4011-06-20	Manómetro FAB 20
4011-07	Manómetros Ductos FAB
4011-07-01	Manómetro SFB 01
4011-07-02	Manómetro SFB 02
4011-07-03	Manómetro EFB 01
4011-07-04	Manómetro EPE 01
4011-08-01	Variador de frecuencia No. 1
4012	Unidad de Suministro Microbiología
4009	Unidad de Extracción Microbiología
4012-03	Manómetros CC
4012-03-01	Manómetro Mark II CC-01
4012-03-02	Manómetro Mark II CC-02
4012-03-03	Manómetro Mark II CC-03
4012-03-04	Manómetro Mark II CC-04
4012-03-05	Manómetro Mark II CC-05
4012-03-06	Manómetro Mark II CC-06
4012-03-07	Manómetro Mark II CC-07
4012-03-08	Manómetro Mark II CC-08
4012-03-09	Manómetro Mark II CC-09
4012-03-10	Manómetro Mark II CC-10
4012-04	Manómetros Ductos MB
4012-04-01	Manómetro SMB 01

CÓDIGO	NOMBRE
4012-04-02	Manómetro SMB 02
4012-04-03	Manómetro EMB 01
4012-05	Variador de frecuencia No. 2
4013	UPS Minuteman 6 kVA
4013-1	Banco de Baterías
4014	Equipo de Presión
4014-1	Tablero de control
4014-2	Bomba No. 1
4014-3	Bomba No. 2
4014-4	Tanque Hidroneumático
4015	Tablero Control Unidades Manejadoras de Aire
4016	Tablero Control Fabricación
4017	Tablero Control Microbiología
4018	Tablero Control Unidades Almacén
4026	Computador Mantenimiento MT-01PC
4026-01	CPU MT-01PC
4026-02	Monitor MT-01PC
4028	Computador Dir. Ingeniería MT-02PC
4028-1	Portátil MT-1
4034	Unidad de Suministro Almacén
4033	Unidad de Extracción Almacén
4034-03	Manómetros ALM
4034-03-01	Manómetro ALM-01
4034-03-02	Manómetro ALM-02
4034-04	Manómetros Ductos AL
4034-04-01	Manómetro SAL 01
4034-04-02	Manómetro SAL 02
4034-04-03	Manómetro EAL 01
4035	Tablero de Control Piso 3
45 METROLOGIA	
4501	Termómetro ING 01-T
4502	Termo higrómetro digital ING 01-TH
4502-02	Termo higrómetro digital ING 02-TH
4503	Juego de Pesas 1g – 1 kg Clase F1
5001	Computador Gerencia General 2
50 SERVICIOS GENERALES	
5001-1	Portátil
5002	Computador DIRECCION TECNICA
5002-1	Monitor

CÓDIGO	NOMBRE
5002-2	C.P.U
5025	Computador Asistente ASECAL y
5025-01	Monitor
5025-02	C.P.U
5003	Computador Asistente de planeación
5003-1	Monitor
5003-2	CPU
5004	Computador Compras
5004-1	Monitor
5004-2	C.P.U
5004-3	Impresora Samsung ML -2010
5004-5	Teléfono
5005-1	Monitor
5005-2	C.P.U
5005-3	Impresora HP LASERJET 1000 SERIES
N/E	Computador Contabilidad No. 2
5005-4	Monitor
5005-5	C.P.U
5005-6	Máquina de escribir eléctrica
5005-7	Teléfono
5006	Computador dirección científica
5006-1	Monitor
5006-2	C.P.U
5006-3	Teléfono
5007	Computador Dirección Técnica
5007-1	Monitor
5007-2	C.P.U
5007-3	Teléfono
5007-4	Impresora samsung ML -2010
5008	Computador Gerencia General 1
5008-1	Monitor
5008-2	C.P.U
5008-3	Impresora HP 4000
5008-4	Teléfono
5009	Computador HSMA
5009-1	Monitor
5009-2	C.P.U
5009-3	Scanner
5009-4	Teléfono

CÓDIGO	NOMBRE
5010	Computador Director de Ventas
5010-1	Portátil
5011	Secador de Manos No. 4
5012	Horno Microondas
5013	Nevera No. 6
5015	Secador de Manos No. 1
5016	Secador de Manos No. 2
5017	Equipos de Comunicaciones
5017-1	Planta telefónica
5017-2	Convertidor
5018	Sistemas de Información
5018-1	Suichi Internet DES 1005D
5019	Computador Servidor
5019-1	Monitor
5019-2	CPU
5021	Computador de Gerencia de producción
5021-1	Monitor
5021-2	CPU
5021-3	Teléfono
5022	Computador de Ingeniería
5022-1	Portátil
5023	Computador Fisicoquímico
5023-1	Monitor
5023-2	CPU
5024	Fotocopiadora

Fecha de emisión: 161011

Responsable: _____

JEFE DE MANTENIMIENTO

Fuente: LABORATORIOS SFC.

ANEXO D. MATRIZ DE ANÁLISIS DE RIESGO

Matriz de Análisis de Riesgo SFC — Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

CAPAS	ACTIVO	Clasificación: Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	[N] DESASTRES NATURALES: [N.1] FUEGO	[N.2] DAÑOS POR AGUA	[N.*] DESASTRES NATURALES	[I] DE ORIGEN INDUSTRIAL: [I.1] FUEGO	[I.2] DAÑOS POR AGUA	[I.*] DESASTRES INDUSTRIALES	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[I.11] EMANACIONES ELECTROMAGNÉTICAS
								3	3	2	3	2	2	3	2	2
[B] ACTIVOS ESENCIALES	1. [SRV_PPAL] Servidor Principal		X	X	X	X	4									8
	2. [SRV_MICRO] Servidor Microbiología		X	X	X	X	4									8
	3. [HPLC] Equipos HPLC		X	X	X	X	4									8
	4. [FORM_MTRAS] Formulas Maestras		X	X	X	X	4									
	5. [BD_SG] BD Sistema de Gestión		X	X	X	X	4									
	6. [BD_MICRO] BD MICROLAB		X	X	X	X	4									
	7. [HD_BKP] Disco Duro Backups		X	X	X	X	4									8
[IS] SERVICIOS INTERNOS	1. [ANAL_MTRAS] Análisis de Muestras	X		X	X	X	4									

CAPAS	ACTIVO	[E] ERRORES Y FALLOS NO INTENCIONADOS: [E.1] ERRORES DELOS USUARIOS	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	[E.10] ERRORES DE SECUENCIA	[E.15] ALTERACIÓN DE LA INFORMACIÓN	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	[E.19] FUGAS DE INFORMACIÓN	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[E.25] PÉRDIDA DE EQUIPOS
		3	3	3	2	2	3	2	3	3	3	3	3	2
[B] ACTIVOS ESENCIALES	1. [SRV_PPAL] Servidor Principal		12											8
	2. [SRV_MICRO] Servidor Microbiología		12											8
	3. [HPLC] Equipos HPLC		12											8
	4. [FORM_MTRAS] Formulas Maestras	12	12				12		12					
	5. [BD_SG] BD Sistema de Gestión	12	12				12		12					
	6. [BD_MICRO] BD MICROLAB	12	12				12		12					
	7. [HD_BKP] Disco Duro Backups	12	12				12		12					8
[IS] SERVICIOS INTERNOS	1. [ANAL_MTRAS] Análisis de Muestras	12	12				12	8	12				12	

CAPAS	ACTIVO	[A] ATAQUES DELIBERADOS: [A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD LOG)	[A.5] SUPLANTACIÓN DE IDENTIDAD	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	[A.7] USO NO PREVISTO	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[A.9] [RE-]ENCAMIENTO DE MENSAJES	[A.10] ALTERACIÓN DE SECUENCIA	[A.11] ACCESO NO AUTORIZADO	[A.12] ANÁLISIS DE TRÁFICO	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[A.19] REVELACIÓN DE INFORMACIÓN	[A.22] MANIPULACIÓN DE PROGRAMAS	[A.23] MANIPULACIÓN DEL HARDWARE	[A.24] DENEGACIÓN DE SERVICIO	[A.25] ROBO DE EQUIPOS	[A.26] ATAQUE DESTRUCTIVO	[A.27] OCUPACIÓN ENEMIGA	[A.29] EXTORSIÓN	[A.30] INGENIERÍA SOCIAL
		2	2	3	2	3	2	2	2	2	2	2	3	2	3	3	3	2	3	2	2	2	3
[B] ACTIVOS ESENCIALES	1. [SRV_PPAL] Servidor Principal			12	8				8								12		12				
	2. [SRV_MICRO] Servidor Microbiología			12	8				8								12		12				
	3. [HPLC] Equipos HPLC			12	8				8								12		12				
	4. [FORM_MTRAS] Formulas Maestras		8	12					8				12		12								
	5. [BD_SG] BD Sistema de Gestión		8	12					8				12		12								
	6. [BD_MICRO] BD MICROLAB		8	12					8				12		12								
	7. [HD_BKP] Disco Duro Backups		8	12	8				8				12		12		12		12				
[IS] SERVICIOS INTERNOS	1. [ANAL_MTRAS] Análisis de Muestras		8	12	8				8		8		12	8	12			8					

CAPAS	ACTIVO	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	[N.1] FUEGO	[N.2] DAÑOS POR AGUA	[N.*] DESASTRES NATURALES	[I.1] FUEGO	[I.2] DAÑOS POR AGUA	[I.*] DESASTRES INDUSTRIALES	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[I.11] EMANACIONES ELECTROMAGNÉTICAS
Matriz de Análisis de Riesgo SFC								Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta] — [N] DESASTRES NATURALES			[I] DE ORIGEN INDUSTRIAL					
		Clasificación						3	3	2	3	2	2	3	2	2
	2. [RTDO_ANAL] Resultado de Análisis	X		X	X	X	4									
[E] EQUIPAMENTO	1. [PGN_WEB] Página web			X	X	X	1									
	2. [HER_OFI] Herramientas de ofimática					X	1									
	3. [ANT_VIR] Antivirus					X	2									
	4. [SO] Sistema Operativo					X	3									
	5. [PLAT_SG] Plataforma Sistema de Gestión		X	X	X	X	3									
	6. [MICROLAB] Plataforma MICROLAB 1.0		X	X	X	X	4									
	1. [PC] Computadoras			X		X	4									8
	2. [IMP] Impresoras					X	3									6

ACTIVO	[E.1] ERRORES DELOS USUARIOS	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	[E.10] ERRORES DE SECUENCIA	[E.15] ALTERACIÓN DE LA INFORMACIÓN	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	[E.19] FUGAS DE INFORMACIÓN	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[E.25] PÉRDIDA DE EQUIPOS
[E] ERRORES Y FALLOS NO INTENCIONADOS													
	3	3	3	2	2	3	2	3	3	3	3	3	2
2. [RTDO_ANAL] Resultado de Análisis	12	12				12	8	12				12	
1. [PGN_WEB] Página web	3	3	3			3		3	3	3			
2. [HER_OFI] Herramientas de ofimática	3	3	3			3		3	3	3			
3. [ANT_VIR] Antivirus	6	6	6			6		6	6	6			
4. [SO] Sistema Operativo	9	9	9			9		9	9	9			
5. [PLAT_SG] Plataforma Sistema de Gestión	9	9	9			9		9	9	9			
6. [MICROLAB] Plataforma MICROLAB 1.0	12	12	12			12		12	12	12			
1. [PC] Computadoras		12											8
2. [IMP] Impresoras		9											6

ACTIVO	[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)	[A.5] SUPLANTACIÓN DE IDENTIDAD	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	[A.7] USO NO PREVISTO	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[A.9] [RE-]ENCAMIENTO DE MENSAJES	[A.10] ALTERACIÓN DE SECUENCIA	[A.11] ACCESO NO AUTORIZADO	[A.12] ANÁLISIS DE TRÁFICO	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[A.19] REVELACIÓN DE INFORMACIÓN	[A.22] MANIPULACIÓN DE PROGRAMAS	[A.23] MANIPULACIÓN DEL HARDWARE	[A.24] DENEGACIÓN DE SERVICIO	[A.25] ROBO DE EQUIPOS	[A.26] ATAQUE DESTRUCTIVO	[A.27] OCUPACIÓN ENEMIGA	[A.29] EXTORSIÓN	[A.30] INGENIERÍA SOCIAL
[A] ATAQUES DELIBERADOS																						
	2	2	3	2	3	2	2	2	2	2	2	3	2	3	3	3	2	3	2	2	2	3
2. [RTDO_ANAL] Resultado de Análisis		8	12	8				8				12	8	12			8					
1. [PGN_WEB] Página web		2	3	2	3			2				3		3	3							
2. [HER_OFI] Herramientas de ofimática		2	3	2	3			2				3		3	3							
3. [ANT_VIR] Antivirus		4	6	4	6			4				6		6	6							
4. [SO] Sistema Operativo		6	9	6	9			6				9		9	9							
5. [PLAT_SG] Plataforma Sistema de Gestión		6	9	6	9			6				9		9	9							
6. [MICROLAB] Plataforma MICROLAB 1.0		8	12	8	12			8				12		12	12							
1. [PC] Computadoras			12	8				8								12		12				
2. [IMP] Impresoras			9	6				6								9		9				

Matriz de Análisis de Riesgo SFC								Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																																											
CAPAS	ACTIVO	Clasificación					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	[N] DESASTRES NATURALES			[I] DE ORIGEN INDUSTRIAL						[E] ERRORES Y FALLOS NO INTENCIONADOS													[A] ATAQUES DELIBERADOS																					
		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		[N.1] FUEGO	[N.2] DAÑOS POR AGUA	[N.*] DESASTRES NATURALES	[I.1] FUEGO	[I.2] DAÑOS POR AGUA	[I.*] DESASTRES INDUSTRIALES	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[I.11] EMANACIONES ELECTROMAGNÉTICAS	[E.1] ERRORES DELOS USUARIOS	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	[E.10] ERRORES DE SECUENCIA	[E.15] ALTERACIÓN DE LA INFORMACIÓN	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	[E.19] FUGAS DE INFORMACIÓN	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[E.25] PÉRDIDA DE EQUIPOS	[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD LOG)	[A.5] SUPLANTACIÓN DE IDENTIDAD	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	[A.7] USO NO PREVISTO	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[A.9] [RE-]ENCAMIENTO DE MENSAJES	[A.10] ALTERACIÓN DE SECUENCIA	[A.11] ACCESO NO AUTORIZADO	[A.12] ANÁLISIS DE TRÁFICO	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[A.19] REVELACIÓN DE INFORMACIÓN	[A.22] MANIPULACIÓN DE PROGRAMAS	[A.23] MANIPULACIÓN DEL HARDWARE	[A.24] DENEGACIÓN DE SERVICIO	[A.25] ROBO DE EQUIPOS	[A.26] ATAQUE DESTRUCTIVO	[A.27] OCUPACIÓN ENEMIGA	[A.29] EXTORSIÓN	[A.30] INGENIERÍA SOCIAL
								3	3	2	3	2	2	3	2	2	3	3	3	2	2	3	2	3	3	3	3	3	2	2	2	3	2	3	2	2	2	2	2	2	3	2	3	3	3	2	3	2	2	2	3
	3. [FIREWALL] Firewall			X		X	3									6		9											6			9	6				6				9				9		9				
	4. [SWT] Switch					X	4									8		12											8			12	8				8				12				12		12				
	1. [WIFI] Router Wifi		X				2									4		6		4	4	6		6					4		4	6	4		4	4	4	4		4	6		6		6		6				
	2. [LAN_SFC] Red LAN	X				X	4								8			12		8	8	12		12				12			8	12	8		8	8	8	8		8	12	8	12			8					
	3. [TEL] Telefonía		X				3											9		6	6	9		9							6	9	6		6	6	6	6		6	9		9								
	4. [IE] Internet		X	X			4											12		8	8	12		12							8	12	8		8	8	8	8		8	12		12								
	1. [UPS] UPS	X					3	9	9	6	9	6	6	9													9						6												9		9	6			
	2. [SIS_VIG] Sistema de Vigilancia	X					3	9	9	6	9	6	6	9													9						6												9		9	6			
[L] INSTALACI	1. [CPD] CPD			X		X	4									8															8	12	8				8												8		

Matriz de Análisis de Riesgo SFC								Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																																											
CAPAS	ACTIVO	Clasificación					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	[N] DESASTRES NATURALES			[I] DE ORIGEN INDUSTRIAL						[E] ERRORES Y FALLOS NO INTENCIONADOS													[A] ATAQUES DELIBERADOS																					
		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		[N.1] FUEGO	[N.2] DAÑOS POR AGUA	[N.*] DESASTRES NATURALES	[I.1] FUEGO	[I.2] DAÑOS POR AGUA	[I.*] DESASTRES INDUSTRIALES	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[I.11] EMANACIONES ELECTROMAGNÉTICAS	[E.1] ERRORES DELOS USUARIOS	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	[E.10] ERRORES DE SECUENCIA	[E.15] ALTERACIÓN DE LA INFORMACIÓN	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	[E.19] FUGAS DE INFORMACIÓN	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[E.25] PÉRDIDA DE EQUIPOS	[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD LOG)	[A.5] SUPLANTACIÓN DE IDENTIDAD	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	[A.7] USO NO PREVISTO	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[A.9] [RE-]ENCAMIENTO DE MENSAJES	[A.10] ALTERACIÓN DE SECUENCIA	[A.11] ACCESO NO AUTORIZADO	[A.12] ANÁLISIS DE TRÁFICO	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[A.19] REVELACIÓN DE INFORMACIÓN	[A.22] MANIPULACIÓN DE PROGRAMAS	[A.23] MANIPULACIÓN DEL HARDWARE	[A.24] DENEGACIÓN DE SERVICIO	[A.25] ROBO DE EQUIPOS	[A.26] ATAQUE DESTRUCTIVO	[A.27] OCUPACIÓN ENEMIGA	[A.29] EXTORSIÓN	[A.30] INGENIERÍA SOCIAL
								3	3	2	3	2	2	3	2	2	3	3	3	2	2	3	2	3	3	3	3	3	2	2	2	3	2	3	2	2	2	2	2	2	3	2	3	3	3	2	3	2	2	2	3
ONES	2. [SFC] Empresa			X		X	4									8														8	12	8				8											8		
[P] PERSONAL	1. [DIR_CALIDAD] Directora Aseguramiento de Calidad			X			4															12		12																	12		12							8	12
	2. [RRHH] Director de Talento Humano/HSE			X			4															12		12																	12		12							8	12
	3. [DT] Directora técnica			X			4															12		12																	12		12							8	12
	4. [ASIST_DIR_CALID] Asistente Dirección de Aseguramiento de Calidad			X			3															9		9																	9		9							6	9
	5. [AN_FQ] Analista de Fisicoquímico			X			3															9		9																	9		9							6	9
	6. [JF_CC] Jefe de Control de Calidad			X			4															12		12																	12		12							8	12
	7. [AUX_MICRO] Auxiliar de Microbiología			X			4															12		12																	12		12							8	12

Matriz de Análisis de Riesgo SFC								Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																																												
CAPAS	ACTIVO	Clasificación					Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	[N] DESASTRES NATURALES			[I] DE ORIGEN INDUSTRIAL						[E] ERRORES Y FALLOS NO INTENCIONADOS													[A] ATAQUES DELIBERADOS																					
		Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad		[N.1] FUEGO	[N.2] DAÑOS POR AGUA	[N.*] DESASTRES NATURALES	[I.1] FUEGO	[I.2] DAÑOS POR AGUA	[I.*] DESASTRES INDUSTRIALES	[I.3] CONTAMINACIÓN MEDIOAMBIENTAL	[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[I.11] EMANACIONES ELECTROMAGNÉTICAS	[E.1] ERRORES DELOS USUARIOS	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[E.9] ERRORES DE [RE-]ENCAMINAMIENTO	[E.10] ERRORES DE SECUENCIA	[E.15] ALTERACIÓN DE LA INFORMACIÓN	[E.18] DESTRUCCIÓN DE LA INFORMACIÓN	[E.19] FUGAS DE INFORMACIÓN	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[E.25] PÉRDIDA DE EQUIPOS	[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD LOG)	[A.5] SUPLANTACIÓN DE IDENTIDAD	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	[A.7] USO NO PREVISTO	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[A.9] [RE-]ENCAMIENTO DE MENSAJES	[A.10] ALTERACIÓN DE SECUENCIA	[A.11] ACCESO NO AUTORIZADO	[A.12] ANÁLISIS DE TRÁFICO	[A.13] REPUDIO (NEGACIÓN DE ACTUACIONES)	[A.14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[A.19] REVELACIÓN DE INFORMACIÓN	[A.22] MANIPULACIÓN DE PROGRAMAS	[A.23] MANIPULACIÓN DEL HARDWARE	[A.24] DENEGACIÓN DE SERVICIO	[A.25] ROBO DE EQUIPOS	[A.26] ATAQUE DESTRUCTIVO	[A.27] OCUPACIÓN ENEMIGA	[A.29] EXTORSIÓN	[A.30] INGENIERÍA SOCIAL
								3	3	2	3	2	2	3	2	2	3	3	3	2	2	3	2	3	3	3	3	3	2	2	2	3	2	3	2	2	2	2	2	2	3	2	3	3	3	2	3	2	2	2	3
	8. [JF_MICRO] Jefe de Microbiología			X			4															12		12																	12		12							8	12
	9. [AN_STM] Analista de sistemas			X			4															12		12																	12		12							8	12

Bajo Riesgo	1 - 6	
Medio Riesgo	8 - 9	
Alto Riesgo	12 - 16	

Fuente: El Autor.

ANEXO E. PLAN DE TRATAMIENTO DE RIESGOS

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
1	[E.1] ERRORES DE LOS USUARIOS	4. [FORM_MTRAS] Formulas Maestras 5. [BD_SG] BD Sistema de Gestión 6. [BD_MICRO] BD MICROLAB 7. [HD_BKP] Disco Duro Backups 1. [ANAL_MTRAS] Análisis de Muestras 2. [RTDO_ANAL] Resultado de Análisis 6. [MICROLAB] Plataforma MICROLAB 1.0	Capacitaciones internas y externas del personal, con incentivos. concientización, píldoras y material de seguridad, llamados de atención, seguimiento al personal, promover el sentido de pertenencia y compromiso institucional	Analista de Sistemas. RRHH	Tiempo, Sistemas de telecomunicación, área de conferencias	Formato de registro y Cronograma de Capacitaciones y actividades o incentivos
2	[E.2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD	1. [SRV_PPAL] Servidor Principal 2. [SRV_MICRO] Servidor Microbiología 3. [HPLC] Equipos HPLC 4. [FORM_MTRAS] Formulas Maestras 5. [BD_SG] BD Sistema de Gestión 6. [BD_MICRO] BD MICROLAB 7. [HD_BKP] Disco Duro	Procedimientos de Seguridad. Guías de trabajo, backups actualizados y en bases de datos, control, seguimiento y soporte	Analista de Sistemas	Disco Duro Externo o servidor para Backups,	Manual de funciones, plan de Mantenimientos

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
		Backups				
		1. [ANAL_MTRAS] Análisis de Muestras				
		2. [RTDO_ANAL] Resultado de Análisis				
		6. [MICROLAB] Plataforma MICROLAB 1.0				
		1. [PC] Computadoras				
		4. [SWT] Switch				
		2. [LAN_SFC] Red LAN				
		4. [IE] Internet				
3	[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	5. [PLAT_SG] Plataforma Sistema de Gestión	Mantener el Antivirus Actualizado, No instalar software sin autorización del administrador. Políticas de seguridad vigente y actualizada. Servidor de usuarios y control de acceso por usuario. Correcta configuración de firewall de seguridad.	Analista de Sistemas. RRHH	Adquirir Licenciamiento de antivirus	Plan de instalación y difusión de Software

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
4	[E.15] ALTERACIÓN DE LA INFORMACIÓN	4. [FORM_MTRAS] Formulas Maestras 5. [BD_SG] BD Sistema de Gestión 6. [BD_MICRO] BD MICROLAB 7. [HD_BKP] Disco Duro Backups 1. [ANAL_MTRAS] Análisis de Muestras 2. [RTDO_ANAL] Resultado de Análisis 6. [MICROLAB] Plataforma MICROLAB 1.0 2. [LAN_SFC] Red LAN 4. [IE] Internet	Controlar los cambios en los sistemas, control de accesos de usuarios, firewall actualizado, incentivar el compromiso institucional al personal	Dirección de Aseguramiento de Calidad	N.A.	Procedimiento para determinar roles y privilegios de usuarios
5	[E.19] FUGAS DE INFORMACIÓN	4. [FORM_MTRAS] Formulas Maestras 5. [BD_SG] BD Sistema de Gestión 6. [BD_MICRO] BD MICROLAB 7. [HD_BKP] Disco Duro Backups 1. [ANAL_MTRAS] Análisis de Muestras	Procedimientos, avisos de confidencialidad en la documentación y contratos de trabajo. Capacitación interna y externa al personal, control de tráfico en la red, bloqueo de puertos de comunicación	Analista de sistemas	N.A.	Procedimiento confidencialidad y política de datos personales

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
		2. [RTDO_ANAL] Resultado de Análisis 6. [MICROLAB] Plataforma MICROLAB 1.0 2. [LAN_SFC] Red LAN 4. [IE] Internet	innecesarios, implementación de claves complejas.			
6	[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	6. [MICROLAB] Plataforma MICROLAB 1.0	Realizar ataques dirigidos, utilizar herramientas para detectar vulnerabilidades, Pruebas de penetración en los servidores principales. Auditorías internas, hacking ético para reforzar la seguridad.	Analista de Sistemas	N.A.	N.A.
7	[E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	6. [MICROLAB] Plataforma MICROLAB 1.0	Realizar mantenimientos correctivo, preventivo y Backups a BD y código fuente. Suministrar una fuente continua de energía para que no queden procesos incompletos.	Analista de Sistemas	N.A.	Plan de mantenimiento, cronograma de mantenimiento, Bitácoras de Backup

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
8	[E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1. [ANAL_MTRAS] Análisis de Muestras 2. [RTDO_ANAL] Resultado de Análisis	Revisión de capacidades del sistema	Analista de Sistemas	Compra de equipo cuando sea necesario	N.A.
9	[A.6] ABUSIVO DE PRIVILEGIOS DE ACCESO	1. [SRV_PPAL] Servidor Principal 2. [SRV_MICRO] Servidor Microbiología 3. [HPLC] Equipos HPLC 4. [FORM_MTRAS] Formulas Maestras 5. [BD_SG] BD Sistema de Gestión 6. [BD_MICRO] BD MICROLAB 7. [HD_BKP] Disco Duro Backups 1. [ANAL_MTRAS] Análisis de Muestras 2. [RTDO_ANAL] Resultado de Análisis 6. [MICROLAB] Plataforma MICROLAB 1.0 1. [PC] Computadoras	Manual de funciones, control en los roles y privilegios, Capacitación al personal sobre políticas de seguridad en la compañía	Analista de Sistemas	N.A.	manual de funciones, Políticas de seguridad informática

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
		4. [SWT] Switch 2. [LAN_SFC] Red LAN 4. [IE] Internet 1. [CPD] CPD 2. [SFC] Empresa				
10	[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	6. [MICROLAB] Plataforma MICROLAB 1.0	No instalar software sin autorización del administrador. Control de Acceso de los usuarios y privilegios	Analista de Sistemas	N.A.	Política de seguridad
11	[A.15] MODIFICACIÓN DE LA INFORMACIÓN	4. [FORM_MTRAS] Formulas Maestras 5. [BD_SG] BD Sistema de Gestión 6. [BD_MICRO] BD MICROLAB 7. [HD_BKP] Disco Duro Backups 1. [ANAL_MTRAS] Análisis de Muestras 2. [RTDO_ANAL] Resultado de Análisis 6. [MICROLAB] Plataforma MICROLAB 1.0 4. [SWT] Switch	Controlar los cambios en los sistemas y la documentación, control de accesos de usuarios, acceso restringido a las bases de datos	Analista de Sistemas. Dirección de Aseguramiento de Calidad	N.A.	Procedimiento para control de cambios y modificación de información, listado de usuarios y privilegios

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
		2. [LAN_SFC] Red LAN				
		4. [IE] Internet				
		1. [DIR_CALIDAD] Directora Aseguramiento de Calidad				
		2. [RRHH] Director de Talento Humano/HSE				
		3. [DT] Directora técnica				
		6. [JF_CC] Jefe de Control de Calidad				
		7. [AUX_MICRO] Auxiliar de Microbiología				
		8. [JF_MICRO] Jefe de Microbiología				
		9. [AN_STM] Analista de sistemas				
12	[A.19] REVELACIÓN DE INFORMACIÓN	4. [FORM_MTRAS] Formulas Maestras	Crear cláusula de confidencialidad de la información. Capacitación al personal sobre políticas de seguridad informática	RRHH	N.A.	Políticas de seguridad informática
		5. [BD_SG] BD Sistema de Gestión				
		6. [BD_MICRO] BD MICROLAB				
		7. [HD_BKP] Disco Duro Backups				
		1. [ANAL_MTRAS] Análisis de Muestras				

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
		2. [RTDO_ANAL] Resultado de Análisis				
		6. [MICROLAB] Plataforma MICROLAB 1.0				
		2. [LAN_SFC] Red LAN				
		4. [IE] Internet				
		1. [DIR_CALIDAD] Directora Aseguramiento de Calidad				
		2. [RRHH] Director de Talento Humano/HSE				
		3. [DT] Directora técnica				
		6. [JF_CC] Jefe de Control de Calidad				
		7. [AUX_MICRO] Auxiliar de Microbiología				
		8. [JF_MICRO] Jefe de Microbiología				
		9. [AN_STM] Analista de sistemas				
13	[A.22] MANIPULACIÓN DE PROGRAMAS	6. [MICROLAB] Plataforma MICROLAB 1.0	Incluir Manual de seguridad de la información. Capacitación al personal de políticas de seguridad informática	Analista de Sistemas	N.A.	Manual de seguridad de la información.

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
14	[A.23] MANIPULACIÓN DEL HARDWARE	1. [SRV_PPAL] Servidor Principal 2. [SRV_MICRO] Servidor Microbiología 3. [HPLC] Equipos HPLC 7. [HD_BKP] Disco Duro Backups 1. [PC] Computadoras 4. [SWT] Switch	Identificar personal clave y asignar autorizaciones. Capacitación al personal de políticas de seguridad informática, asignación de perfiles idóneos para la ejecución de tareas y control de acceso.	Analista de Sistemas	N.A.	Matriz de funciones y responsabilidades. Políticas de seguridad informática
15	[A.25] ROBO DE EQUIPOS	1. [SRV_PPAL] Servidor Principal 2. [SRV_MICRO] Servidor Microbiología 3. [HPLC] Equipos HPLC 7. [HD_BKP] Disco Duro Backups 1. [PC] Computadoras 4. [SWT] Switch	Crear un acta de entrega a la persona responsable del equipo, asignar custodias, implementación de un sistema IDS y de un sistema de CCTV (casos locativos)	Analista de Sistemas. RRHH	Instalación de equipos de monitoreo CCTV	Acta de recibo y entrega Equipo, inventario de activos, acta de custodia de equipo
16	[A.30] INGENIERÍA SOCIAL	1. [DIR_CALIDAD] Directora Aseguramiento de Calidad 2. [RRHH] Director de Talento Humano/HSE 3. [DT] Directora técnica	Capacitar al personal de lo vulnerables que son ante las tácticas de los atacantes. Incentivar al personal para que denuncie cualquier caso	Analista de Sistemas. RRHH	N.A.	Acta de reunión y Acta de capacitación.

Riesgo N°	Descripción del Riesgo	Activo(s) Afectado(s)	Tratamiento del Riesgo	Persona Responsable	Personal y/o Recursos	Registros Asociados
		6. [JF_CC] Jefe de Control de Calidad	oportunamente			
		7. [AUX_MICRO] Auxiliar de Microbiología				
		8. [JF_MICRO] Jefe de Microbiología				
		9. [AN_STM] Analista de sistemas				

Fuente: El Autor.

ANEXO F. DECLARACIÓN DE APLICABILIDAD INICIAL

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN									
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	SI	Se establecerá, aprobara y comunicara una política de seguridad de la información la cual buscará concientizar a los empleados y partes externas pertinentes. Igualmente dicha política deberá ser revisada a intervalos planificados de tiempo para asegurar su idoneidad			X		El control no está implementado
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN		SI				X		El control no está implementado
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN									
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	SI	La empresa mediante su política de seguridad de la información asignara responsabilidades para el cumplimiento de la política. Para mantener protegida su información se realizara revisión del SGSI, acuerdos de confidencialidad, mantener contacto con las autoridades y grupos especializados en seguridad, y tratar seguridad de la información en la gestión de proyectos existentes.			X		El control no está implementado
	A 6.1.2 SEPARACIÓN DE DEBERES		SI				X		El control no está implementado
	A 6.1.3 CONTACTO		SI		X		X		El control esta

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	CON LAS AUTORIDADES								implementado pero no Documentado
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL		SI	Se deben incluir aspectos de seguridad de la información en la gestión de proyectos.	X		X		El control esta implementado pero no Documentado
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.		SI				X		El control no está implementado
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	SI	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.			X		El control no está implementado
	A 6.2.2 TELETRABAJO		SI	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.	X		X		El control no está implementado
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS									
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	Asegurar que los empleados y contratistas	SI	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			X		El control esta implementado pero no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
		comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		clasificación de la información a la cual se va a tener acceso y los riesgos percibidos					Documentado
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO		SI	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.			X		El control esta implementado pero no Documentado
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	SI	Teniendo en cuenta que el personal contratado interactúa permanentemente con la información, se deben establecer controles para asegurar las responsabilidades y deberes en la seguridad de la información, además de concientizar y capacitar al personal en materia de seguridad de la información de acuerdo a sus funciones laborales. La organización establecerá medidas disciplinarias para saber cómo actuar en caso de que se cometa alguna violación de seguridad, aunque la alta dirección exigirá a su personal cumplir con las políticas y procedimientos establecidos con el fin de evitar incidentes de seguridad.			X		El control no cumple con el estándar y debe ser rediseñado
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN		SI				X		El control no está implementado
	A.7.2.3 PROCESO DISCIPLINARIO		SI				X		El control esta implementado pero no Documentado
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE	Proteger los intereses de la organización	SI	La empresa debe establecer controles que permitan asegurar que los empleados una vez finalicen su contrato, renuncien o hayan cambios de personal harán devolución de los activos de la organización y se les retiraran los derechos de y roles de accesos.			X		El control no cumple con el estándar y debe

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	RESPONSABILIDADES DE EMPLEO	como parte del proceso de cambio o terminación del empleo.							ser rediseñado
A.8 GESTION DE ACTIVOS									
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	SI	La empresa debe realizar y mantener un inventario de todos los activos de información que posee, identificar los propietarios de estos activos y garantizar el uso adecuado través de reglas documentadas e implementadas para el uso aceptable de información. La empresa debe asegurar que todos los activos sean regresados por sus colaboradores cuando se presenten renuncias, terminación del contrato o cambio de personal.			X	X	El control no cumple con el estándar y debe ser rediseñado
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS		SI				X	X	El control no está implementado
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS		SI				X	X	El control no está implementado
	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS		SI				X	X	El control no está implementado
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	Asegurar que la organización recibe un nivel apropiado de	SI	La empresa se encargara de implementar controles y procedimientos que permitan dar a la información el nivel de protección, manejo y etiquetado adecuado, teniendo en cuenta los requisitos legales, la importancia, sensibilidad y valor para la empresa.			X	X	El control no está implementado
	A 8.2.2 ETIQUETADO		SI				X	X	El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	DE LA INFORMACIÓN	protección de acuerdo con su importancia para la organización.							está implementado
	A 8.2.3 MANEJO DE ACTIVOS		SI	Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización			X	X	El control no está implementado
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	SI	La empresa debe implementar procedimientos para asegurar que se eviten divulgaciones, modificaciones, uso indebido, retiro, destrucción o accesos no autorizados.			X	X	El control no está implementado
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS		SI				X	X	El control no está implementado
	A 8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS.		SI				X	X	El control no está implementado
A.9 CONTROL DE ACCESO									
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	Limitar el acceso a información y a instalaciones de procesamiento de información.	SI	La empresa cuenta con una red LAN y sistemas de procesamiento de información, de acuerdo a esto se deben establecer y documentar controles de acceso para asegurar que la información solo esté disponible a los usuarios que están autorizados.			X		El control no está implementado
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED		SI				X		El control no está implementado
A 9.2 GESTIÓN DE ACCESO DE	A 9.2.1 REGISTRO Y CANCELACIÓN DEL	Asegurar el acceso de los	SI	Se debe crear un procedimiento para el registro y cancelación de usuarios en el cual se detalle los casos en los cuales se removera los derechos de acceso de los usuarios.			X		El control no está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
USUARIOS	REGISTRO DE USUARIOS	usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.							implementado
	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS		SI	Debido a que los empleados manejan diferentes tipos de información por los diferentes proyectos en los que participan, se hace necesario establecer un proceso formal y controles para gestionar de manera adecuada os usuarios, los cuales aseguren el acceso a usuarios autorizados y eviten los no autorizados. Estos accesos deben revisarse a intervalos de tiempo y retirarse al terminar el empleo o contrato.			X		El control no está implementado
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO		SI				X		El control no está implementado
	A 9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS		SI				X		El control no está implementado
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS		SI				X		El control no está implementado
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.		SI				X		El control no está implementado
A 9.3	A 9.3.1 USO DE	Hacer que los	SI	Se debe crear un procedimiento para definir las buenas prácticas de seguridad de la			X		El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
RESPONSABILIDADES DE LOS USUARIOS	INFORMACIÓN DE AUTENTICACIÓN SECRETA	usuarios rindan cuentas por la custodia de su información de autenticación.		organización en el uso de información confidencial para la autenticación.					está implementado
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	Prevenir el uso no autorizado de sistemas y aplicaciones.	SI	La empresa provee a su personal un usuario y contraseña únicos e intransferibles los cuales son actualizados 1 vez al mes. Se debe definir una política de control de acceso a los sistemas y aplicaciones.			X		El control no está implementado
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.		SI				X		El control no está implementado
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.		SI				X		El control no está implementado
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.		SI				X		El control esta implementado pero no Documentado
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.		SI				X		El control no está implementado
A. 10 CRIPTOGRAFIA									

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	SI	Para el uso de llaves criptográficas la empresa debe implementar una política sobre el uso de controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información. Igualmente esta política debe incluir aspectos relevantes para el cifrado de información.			X		El control no está implementado
	A 10.1.2 GESTIÓN DE LLAVES		SI				X		El control no está implementado
A. 11 SEGURIDAD FISICA Y DEL ENTORNO									
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	SI	Aunque la empresa ya posee medios de seguridad en la infraestructura, es necesario adoptar controles de seguridad para evitar el acceso físico no autorizado, el daño a la infraestructura y los activos de la empresa.			X		El control no está implementado
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS		SI				X		El control no cumple con el estándar y debe ser rediseñado
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES		SI				X		El control no cumple con el estándar y debe ser rediseñado
	A 11.1.4 PROTECCIÓN		SI				X		El control no está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	CONTRA AMENAZAS EXTERNAS Y AMBIENTALES								implementado
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS		SI	Se deben diseñar y aplicar mecanismos para la protección física y las directrices para trabajar en áreas seguras.			X		El control no está implementado
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA		SI	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.			X		El control no está implementado
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	SI	Como la empresa cuenta con diferentes equipos de procesamiento de información es necesario establecer controles para evitar y reducir riesgos, amenazas, accesos no autorizados, daño, robo, fallas de energía, etc., conservándolos en lugares adecuados y que aseguren la disponibilidad e integridad continua. Se definen responsabilidades para que el personal en el manual de funciones, además de una política de escritorio y pantalla limpios.			X		El control no está implementado
	A 11.2.2 SERVICIOS DE SUMINSITRO		SI				X		El control no cumple con el estándar y debe ser rediseñado
	A 11.2.3 SEGURIDAD DEL CABLEADO		SI				X		El control no cumple con el estándar y debe ser rediseñado
	A 11.2.4 MANTENIMIENTO		SI				X		El control no cumple con el

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	DE EQUIPOS								estándar y debe ser rediseñado
	A 11.2.5 RETIRO DE ACTIVOS		SI	Como la empresa cuenta con diferentes equipos de procesamiento de información es necesario establecer controles para evitar y reducir riesgos, amenazas, accesos no autorizados, daño, robo, fallas de energía, etc., conservándolos en lugares adecuados y que aseguren la disponibilidad e integridad continua. Se definen responsabilidades para que el personal en el manual de funciones, además de una política de escritorio y pantalla limpios.			X		El control no está implementado
	A 11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES		SI				X		El control no está implementado
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS		SI				X		El control no está implementado
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO		SI				X		El control no está implementado
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.		SI				X		El control no está implementado
A.12 SEGURIDAD DE LAS OPERACIONES									
A 12.1	A 12.1.1	Asegurar las	SI	Los procedimientos se deben documentar, mantener y estar disponibles para todos los			X		El control esta

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	operaciones correctas y seguras de las instalaciones de procesamiento de información.		usuarios que los necesiten.					implementado pero no Documentado
	A 12.1.2 GESTIÓN DE CAMBIOS		SI	Se deben establecer controles que garanticen que los cambios son controlados, sometidos a revisión y prueba para evitar la fuga de información que pueda comprometer la seguridad del sistema. Antes de instalar un software se deben hacer pruebas en ambientes diferentes para reducir los riesgos.			X		El control esta implementado pero no Documentado
	A 12.1.3 GESTIÓN DE CAPACIDAD		SI				X		El control no cumple con el estándar y debe ser rediseñado
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.		SI				X		El control no está implementado
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	Asegurarse de que la información y las instalaciones de procesamiento de información	SI	Debido a que en la empresa se utilizan servicios como internet, ejecución de software, los cuales pueden afectar el correcto funcionamiento de activos de información se hace necesario implementar controles que permitan la deteccion, prevención y toma de conciencia para prevenir códigos maliciosos.			X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
		estén protegidas contra códigos maliciosos.							
A 12.3 COPIAS DE RESPALDO	A 12.3.1 RESPALDO DE LA INFORMACIÓN	Proteger contra la pérdida de datos.	SI	Para dar continuidad con el proceso de negocio se deben implementar controles de seguridad que aseguren la ejecución de procedimientos de backup de los equipos informáticos de la empresa.			X		El control no está implementado
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	Registrar eventos y generar evidencia.	SI	La empresa debe establecer controles que permitan la detección oportuna de actividades no autorizadas, guardar y proteger los registros de actividades.			X		El control no está implementado
	A12.4.1 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO		SI				X		El control no está implementado
	A12.4.1 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR		SI				X		El control no está implementado
	A12.4.1 SINCRONIZACIÓN DE RELOJES		SI	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 confiable.			X		El control no está implementado
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN	Asegurarse de la integridad de los sistemas	SI	Teniendo en cuenta que la empresa cuenta con diferentes sistemas operativos se deben establecer controles para garantizar la protección y correcta operación de los equipos y restringiendo la instalación de programas o aplicaciones.			X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	SISTEMAS OPERATIVOS	operacionales.							
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	Prevenir el aprovechamiento de las vulnerabilidades técnicas.	SI	Teniendo en cuenta que la empresa cuenta con diferentes sistemas operativos se deben establecer controles para garantizar la protección y correcta operación de los equipos para evitar riesgos producidos por las vulnerabilidades técnicas.			X		El control no está implementado
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFTWARE		SI				X		El control no está implementado
A 12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.	SI	La empresa cuenta con variedad de sistemas operativos, por esta razón es necesario establecer controles que garanticen el uso de herramientas de auditorías sin interrumpir los sistemas mientras se encuentren operativos.			X		El control no está implementado
A. 13 SEGURIDAD DE LAS COMUNICACIONES									
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A 13.1.1 CONTROLES DE REDES	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento	SI	Debido a que la empresa posee un red LAN se deben establecer controles para asegurar que la información que se encuentra en red este protegida de amenazas.			X		El control no está implementado
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED		SI				X		El control no cumple con el estándar y debe

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
		de información de soporte.							ser rediseñado
	A 13.1.3 SEPARACIÓN EN LAS REDES		SI	Se deben crear segmentos de redes o separar las redes (Redes Virtuales - VLANS) de los distintos procesos de la empresa con el fin de minimizar el impacto de un incidente de seguridad de la información.			X		El control no está implementado
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	SI	Dentro de las actividades propias de la organización se encuentra el intercambio de información con clientes y empleados, debido a esto se hace necesario implementar controles y políticas de intercambio de información buscando asegurar que no se presente un uso inadecuado de la información. Dentro de esta política se establecen acuerdos de confidencialidad o no divulgación de la información.		X	X		El control no está implementado
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN		SI			X	X		El control no está implementado
	A 13.2.3 MENSAJERIA ELECTRÓNICA		SI			X	X		El control no está implementado
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN		SI			X	X		El control no cumple con el estándar y debe ser rediseñado
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS									
A 14.1 REQUISITOS	A 14.1.1 ÁNALISIS Y	Asegurar que la	SI	Se deben implementar controles de seguridad que permitan garantizar que los cambios			X		El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.		en la tecnología no afectan los requisitos del negocio. Deben aplicarse también controles de seguridad como PIN, Tokens, etc.					está implementado
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS		SI				X		El control no está implementado
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES		SI				X		El control no está implementado
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de	SI	Algunas veces se desarrolla software dentro de la organización, por esta razón es necesario establecer reglas, buenas prácticas y controles que permitan un desarrollo seguro. Estos controles deben garantizar un control en los cambios para no comprometer la seguridad, un ambiente seguro de desarrollo, protección de acceso al código fuente, pruebas de funcionalidad y actualización contando con servidores de prueba antes de la puesta en producción.			X		El control no está implementado
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS		SI				X		El control no está implementado
	A 14.2.3 REVISIÓN		SI				X		El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	TÉCNICA DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	información.							está implementado
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE		SI	Se debe limitar a los cambios en los paquetes de software y se deben controlar estrictamente.			X		El control no está implementado
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS		SI	Algunas veces se desarrolla software dentro de la organización, por esta razón es necesario establecer reglas, buenas prácticas y controles que permitan un desarrollo seguro. Estos controles deben garantizar un control en los cambios para no comprometer la seguridad, un ambiente seguro de desarrollo, protección de acceso al código fuente, pruebas de funcionalidad y actualización contando con servidores de prueba antes de la puesta en producción.			X		El control no está implementado
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO		SI				X		El control no está implementado
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE		SI				X		El control no está implementado
	A 14.2.8 PRUEBAS		SI				X		El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	DE SEGURIDAD DE SISTEMAS								está implementado
	A 14.2.9 PRUEBA DE ACEPTACIÓN DE SISTEMAS		SI	Se deben establecer planes de pruebas y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.			X		El control no está implementado
A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	Asegurar la protección de los datos usados para pruebas.	SI	Los datos de pruebas se deben seleccionar cuidadosamente y se deberían proteger y controlar.			X		El control no está implementado
A.15 RELACIONES CON LOS PROVEEDORES									
A. 15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	A 15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	SI	La empresa documentara todos los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos		X	X		El control no está implementado
	A 15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES		SI			X	X		El control no está implementado
	A 15.1.3 CADENA DE		SI			X	X		El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN								está implementado
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	SI	La empresa deberá realizar seguimiento y auditar la prestación de servicios de los proveedores en aspectos relacionados a la seguridad de la información.		X	X		El control no cumple con el estándar y debe ser rediseñado
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES		SI	Se deben administrar los cambios de los servicios provistos que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos.		X	X		El control no está implementado
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION									
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la	SI	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.			X		El control no está implementado
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN		SI	Los eventos de seguridad de la información se deben informar lo antes posible utilizando los canales de administración definidos por la organización.			X		El control no está implementado
	A 16.1.3 REPORTE DE DEBILIDADES DE		SI				X		El control no está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	SEGURIDAD DE LA INFORMACIÓN	comunicación sobre eventos de seguridad y debilidad.							implementado
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS		SI	Se deben evaluar los eventos de seguridad de la información y decidir si deben ser clasificados como incidentes			X		El control no está implementado
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN		SI	Se debe responder ante los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.			X		El control no está implementado
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		SI	Se debe utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro. Se debe crear una base de datos de conocimientos.			X		El control no está implementado
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA		SI	Se debe definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.			X		El control no está implementado
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO									

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	SI	Para evitar las interrupciones en las actividades del negocio la empresa debe implementar y documentar un procedimiento que asegure la continuidad del negocio para minimizar el impacto.			X		El control no está implementado
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN		SI				X		El control no está implementado
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN		SI				X		El control no está implementado
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	SI	Se debe contar con equipos de respaldo para servicios críticos buscando garantizar la disponibilidad de la información.			X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A. 18 CUMPLIMIENTO									
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	SI	Es necesario implementar controles de seguridad que permitan el cumplimiento de todos los requisitos legales y contractuales.	X		X		El control no está implementado
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL		SI		X		X		El control no está implementado
	A 18.1.3 PROTECCIÓN DE REGISTROS		SI		X	X	X		El control no está implementado
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES		SI		X	X	X		El control no está implementado
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS		SI		X		X		El control no está implementado
A 18.2 REVISIONES	A 18.2.1 REVISIÓN	Asegurar que la	SI	La empresa debe establecer un compromiso con su política de seguridad de la			X		El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
DE SEGURIDAD DE LA INFORMACIÓN	INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.		información, velando por mantener protegidos sus activos mediante la revisión de su SGSI. En este orden de ideas es necesario garantizar que el personal conoce y aplica las políticas de seguridad de la información y sus controles adoptados.					está implementado
	A 18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD		SI	La Alta Dirección debe revisar regularmente el cumplimiento de los procedimientos de acuerdo a su responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.			X		El control no está implementado
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO		SI	Se debe revisar regularmente los sistemas para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.			X		El control no está implementado

Fuente: El Autor.

Fecha de Elaboración: 161104 Fecha de Actualización: 171104

ANEXO G. REPORTE DE INCIDENTES DE CONTINGENCIA

Información de Identificación			
Fecha del Incidente		Hora de Ocurrencia	
Duración del Incidente		Proceso Afectado	
Área		Lugar del Incidente	

Descripción del Riesgo

Descripción del Incidente (Problema Ocasionado)

Causas del Incidente

Medidas contingentes adoptadas		
Acción	**Participantes**	
	Nombre	**Cargo**

Efectos en el funcionamiento de la organización

Retorno a la Operación normal
Lecciones aprendidas

Fuente: ICETEX. Manual de administración del plan de continuidad de negocios. [en línea]. <https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/ manuales/Manual_continuidad_negocio.pdf> [citado en 31 de Octubre de 2015]

ANEXO H. FORMATO ENCUESTA INSTRUMENTO 01

Objetivo: El propósito del presente instrumento es obtener información relevante por parte de los jefes de las áreas más críticas de LABORATORIOS SFC LTDA, con el fin de determinar la importancia de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) bajo la NTC – ISO 27001. (Encuesta estrictamente académica.)

Fecha: _____

Nombre: _____ Cargo: _____

Preguntas

1. **¿Guarda una copia de seguridad de sus documentos más importantes?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

2. **¿Cambia con regularidad las claves de su equipo o de su correo corporativo?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

3. **¿Usted cree que es responsable de su equipo informático?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

4. **¿Existe un documento donde se especifique las políticas de seguridad de la información?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

5. **¿Se le brinda capacitación por parte de LABORATORIOS SFC LTDA acerca de seguridad de la información?**

Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

6. **¿Se le comunica y concientiza cuando se establece algún procedimiento o política relativa a la seguridad de la información?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

7. **¿La empresa le ha informado sobre el sistema de Gestión de Seguridad de la Información (SGSI)?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre ( )

8. **¿Cree Usted, que es de suma importancia la elaboración de políticas de seguridad de la información para LABORATORIOS SFC LTDA?**
   Si ( ) No ( )

   ¿Por qué?
   _____
   _____
   _____
   _____

ANEXO I. ENCUESTA INSTRUMENTO 01

Universidad Nacional Abierta y a Distancia

Objetivo: El propósito del presente instrumento es obtener información relevante por parte de los jefes de las áreas más críticas de LABORATORIOS SFC LTDA, con el fin de determinar la importancia de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) bajo la NTC – ISO 27001. (Encuesta estrictamente académica.)

Fecha: 151029
Nombre: [illegible] Cargo: Dirección Técnica

Preguntas

1. **¿Guarda una copia de seguridad de sus documentos más importantes?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

2. **¿Cambia con regularidad las claves de su equipo o de su correo corporativo?**
   Nunca ( ) A veces ( ) Casi siempre (X) Siempre ( )

3. **¿Usted cree que es responsable de su equipo informático?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre (X)

4. **¿Existe un documento donde se especifique las políticas de seguridad de la información?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

5. **¿Se le brinda capacitación por parte de LABORATORIOS SFC LTDA acerca de seguridad de la información?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

6. **¿Se le comunica y concientiza cuando se establece algún procedimiento o política relativa a la seguridad de la información?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

7. **¿La empresa le ha informado sobre el sistema de Gestión de Seguridad de la Información (SGSI)?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

8. **¿Cree Usted, que es de suma importancia la elaboración de políticas de seguridad de la información para LABORATORIOS SFC LTDA?**
   Si (X) No ( )

   ¿Por qué?
   La seguridad en la información es muy importante porque son la base del conocimiento de la empresa

Fuente: El Autor.

ANEXO I. (Continuación).

Universidad Nacional Abierta y a Distancia

Objetivo: El propósito del presente instrumento es obtener información relevante por parte de los jefes de las áreas más críticas de LABORATORIOS SFC LTDA, con el fin de determinar la importancia de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) bajo la NTC – ISO 27001. (Encuesta estrictamente académica.)

Fecha: 151028
Nombre: Juan Sebastián Sánchez Cargo: Jefe Control Calidad.

Preguntas

1. **¿Guarda una copia de seguridad de sus documentos más importantes?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre (X)

2. **¿Cambia con regularidad las claves de su equipo o de su correo corporativo?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

3. **¿Usted cree que es responsable de su equipo informático?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre (X)

4. **¿Existe un documento donde se especifique las políticas de seguridad de la información?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

5. **¿Se le brinda capacitación por parte de LABORATORIOS SFC LTDA acerca de seguridad de la información?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

6. **¿Se le comunica y concientiza cuando se establece algún procedimiento o política relativa a la seguridad de la información?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre (X)

7. **¿La empresa le ha informado sobre el sistema de Gestión de Seguridad de la Información (SGSI)?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

8. **¿Cree Usted, que es de suma importancia la elaboración de políticas de seguridad de la información para LABORATORIOS SFC LTDA?**
   Si (X) No ( )

   ¿Por qué? Permite gestionar la seguridad de la información que es vital para la continuidad del negocio.

Fuente: El Autor.

ANEXO I. (Continuación).

Universidad Nacional Abierta y a Distancia

Objetivo: El propósito del presente instrumento es obtener información relevante por parte de los jefes de las áreas más críticas de LABORATORIOS SFC LTDA, con el fin de determinar la importancia de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) bajo la NTC – ISO 27001. (Encuesta estrictamente académica.)

Fecha: 15/10/28
Nombre: Leonardo Ramirez Cargo: Director Talento Humano / HSE

Preguntas

1. **¿Guarda una copia de seguridad de sus documentos más importantes?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre (x)

2. **¿Cambia con regularidad las claves de su equipo o de su correo corporativo?**
   Nunca ( ) A veces (x) Casi siempre ( ) Siempre ( )

3. **¿Usted cree que es responsable de su equipo informático?**
   Nunca ( ) A veces ( ) Casi siempre ( ) Siempre (x)

4. **¿Existe un documento donde se especifique las políticas de seguridad de la información?**
   Nunca (x) A veces ( ) Casi siempre ( ) Siempre ( )

5. **¿Se le brinda capacitación por parte de LABORATORIOS SFC LTDA acerca de seguridad de la información?**
   Nunca ( ) A veces (x) Casi siempre ( ) Siempre ( )

6. **¿Se le comunica y concientiza cuando se establece algún procedimiento o política relativa a la seguridad de la información?**
   Nunca (x) A veces ( ) Casi siempre ( ) Siempre ( )

7. **¿La empresa le ha informado sobre el sistema de Gestión de Seguridad de la Información (SGSI)?**
   Nunca ( ) A veces (x) Casi siempre ( ) Siempre ( )

8. **¿Cree Usted, que es de suma importancia la elaboración de políticas de seguridad de la información para LABORATORIOS SFC LTDA?**
   Si (x) No ( )

   ¿Por qué?
   Porque la información, es uno de los activos más valiosos y en caso de perderlos o ser plagiados se afectaría de manera significativa la organización.

Fuente: El Autor.

ANEXO I. (Continuación).

Universidad Nacional Abierta y a Distancia

Objetivo: El propósito del presente instrumento es obtener información relevante por parte de los jefes de las áreas más críticas de LABORATORIOS SFC LTDA, con el fin de determinar la importancia de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) bajo la NTC – ISO 27001. (Encuesta estrictamente académica.)

Fecha: 15/10/18
Nombre: Yenny Salgado Cargo: Director Aseguramiento

Preguntas

1. **¿Guarda una copia de seguridad de sus documentos más importantes?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

2. **¿Cambia con regularidad las claves de su equipo o de su correo corporativo?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

3. **¿Usted cree que es responsable de su equipo informático?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

4. **¿Existe un documento donde se especifique las políticas de seguridad de la información?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

5. **¿Se le brinda capacitación por parte de LABORATORIOS SFC LTDA acerca de seguridad de la información?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

6. **¿Se le comunica y concientiza cuando se establece algún procedimiento o política relativa a la seguridad de la información?**
   Nunca ( ) A veces (X) Casi siempre ( ) Siempre ( )

7. **¿La empresa le ha informado sobre el sistema de Gestión de Seguridad de la Información (SGSI)?**
   Nunca (X) A veces ( ) Casi siempre ( ) Siempre ( )

8. **¿Cree Usted, que es de suma importancia la elaboración de políticas de seguridad de la información para LABORATORIOS SFC LTDA?**
   Si (X) No ( )

   ¿Por qué?
   Es muy importante elaborar politicas de seguridad porque con esto se garantiza la seguridad de los equipos, documentos de la empresa y se mantiene un sistema de gestion que soporte la parte de aseguramiento de calidad en cuanto a la seguridad informatica.

Fuente: El Autor.

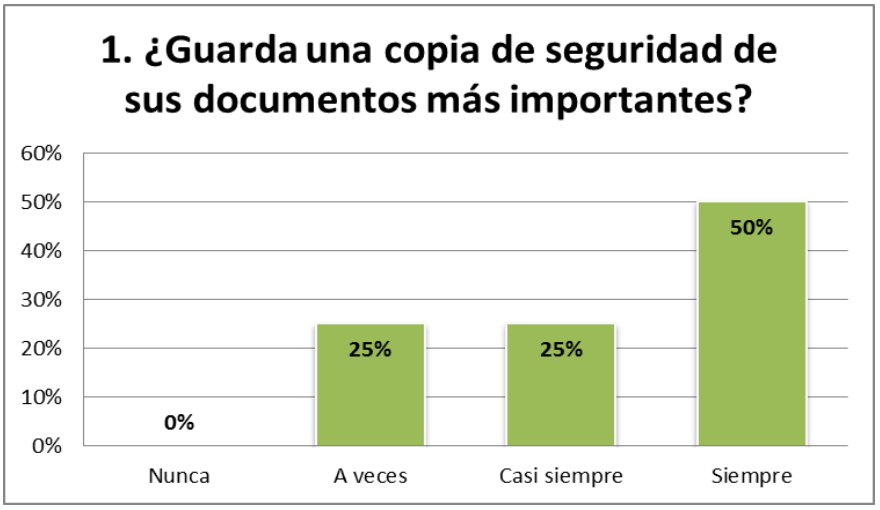
ANEXO J. TABULACIÓN DE RESULTADOS

ANÁLISIS DE LA INFORMACIÓN POR CADA PREGUNTA PARA LA TOTALIDAD DE LAS ENCUESTAS

Una vez obtenido los resultados del instrumento se procede a realizar el análisis estadístico de la siguiente manera:

1. ¿Guarda una copia de seguridad de sus documentos más importantes?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	0	0%
A veces	1	25%
Casi siempre	1	25%
Siempre	2	50%
TOTAL	4	100%

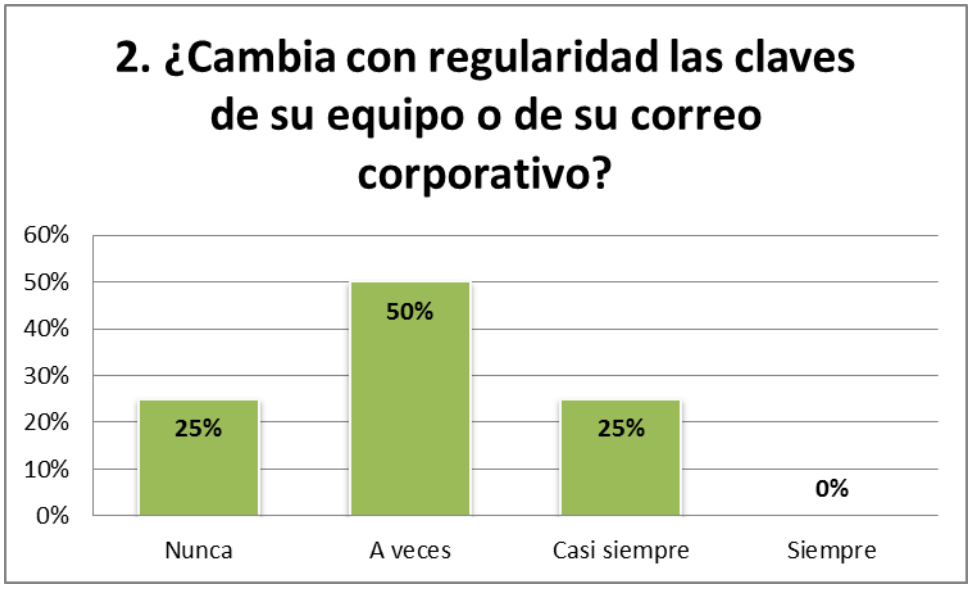


Un 25% de la poblacion encuestada afirma que a veces guarda una copia de seguridad de los documentos mas importantes, mientras que un 25% casi siempre guarda una copia, asi como 50% respondio que siempre guarda una copia de seguridad de sus documentos mas importantes.

ANALISIS PREGUNTA 1: De acuerdo a los resultados obtenidos se puede clarificar que “Siempre” las personas encuestadas guardan una copia de seguridad de sus documentos mas importantes.

2. ¿Cambia con regularidad las claves de su equipo o de su correo corporativo?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	1	25%
A veces	2	50%
Casi siempre	1	25%
Siempre	0	0%
TOTAL	4	100%

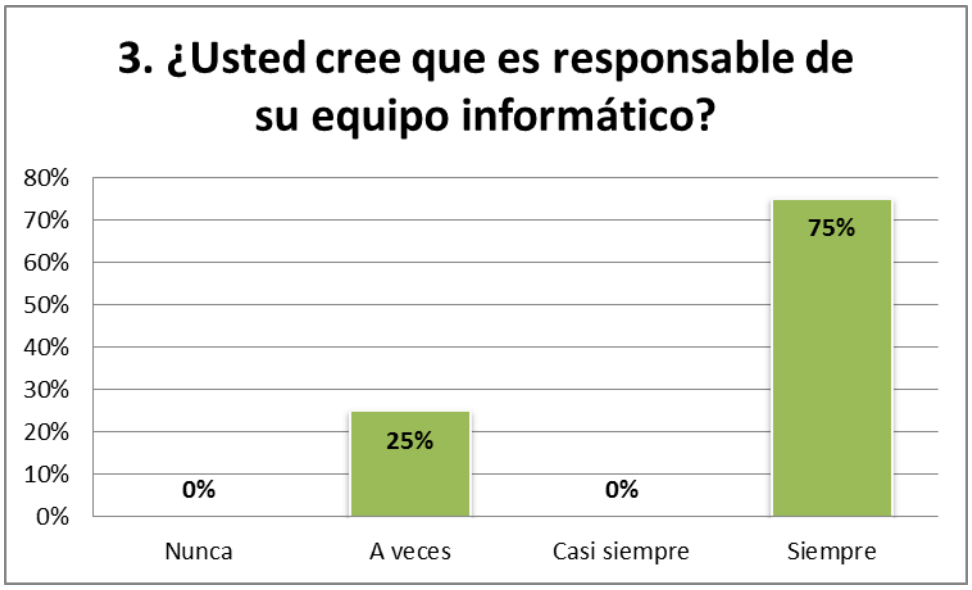


De las encuestas realizadas a los jefes de las areas mas criticas de LABORATORIOS SFC LTDA, el 25% respondio que nunca cambia sus claves, frente a un 50% que afirma cambiar con regularidad las claves de su equipo de computo y correo corporativo, un 25% dice que casi siempre cambia con regularidad sus claves.

ANALISIS PREGUNTA 2: En los resultados obtenidos se pude observar que “A veces” el personal cambia regularmente sus claves de acceso tanto para su equipo de computo como su correo corporativo.

3. ¿Usted cree que es responsable de su equipo informático?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	0	0%
A veces	1	25%
Casi siempre	0	0%
Siempre	3	75%
TOTAL	4	100%

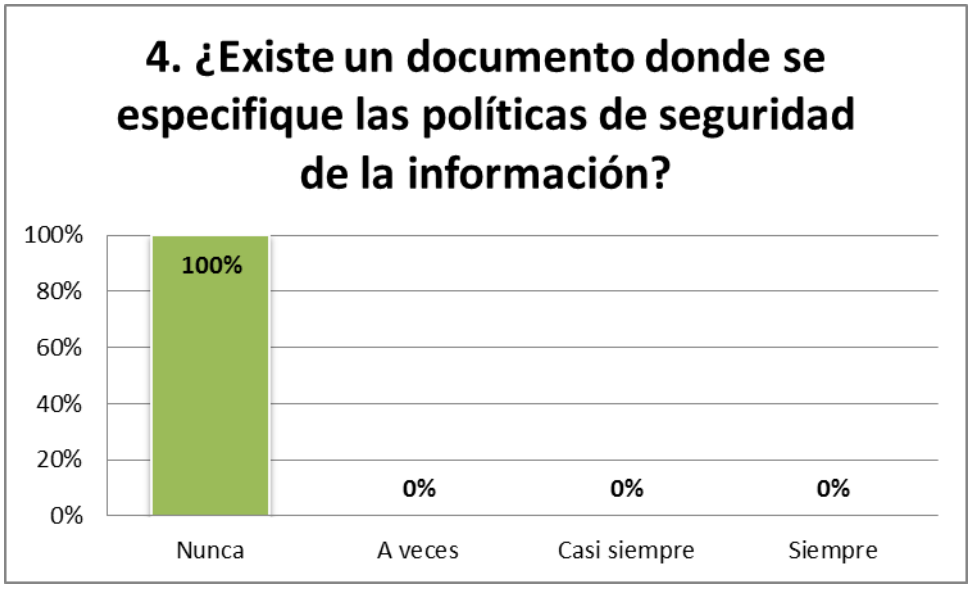


Un 25% de la poblacion encuestada afirma que a veces cree ser responsable de su equipo informatico, mientras que un 75% considera que siempre es responsable por el equipo informatico que le asigna la organización.

ANALISIS PREGUNTA 3: De acuerdo a los resultados obtenido se puede clarificar que “Siempre” los usuarios creen que son responsables por el equipo informatico que la empresa pone a su disposición.

4. ¿Existe un documento donde se especifique las políticas de seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	4	100%
A veces	0	0%
Casi siempre	0	0%
Siempre	0	0%
TOTAL	4	100%

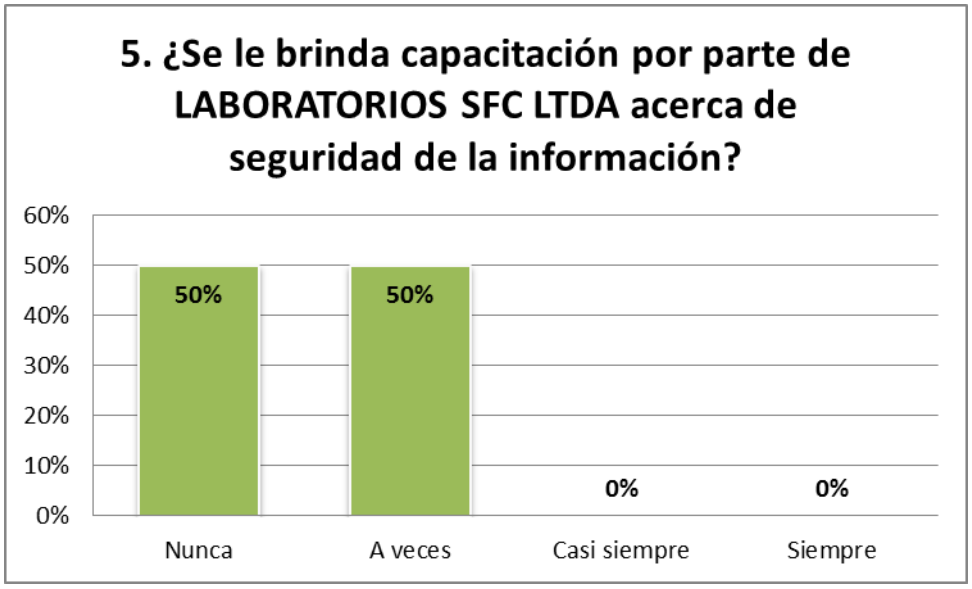


El 100% de la poblacion encuestada considera que nunca ha existido un documento que especifique las politicas de seguridad adoptadas por la organización.

ANALISIS PREGUNTA 4: Se puede mostrar de acuerdo a los resultados obtenido de los jefes de areas, “nunca” ha existido en la empresa un documento referente a politicas de seguridad de la informacion al interior de la organización.

5. ¿Se le brinda capacitación por parte de LABORATORIOS SFC LTDA acerca de seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	2	50%
A veces	2	50%
Casi siempre	0	0%
Siempre	0	0%
TOTAL	4	100%

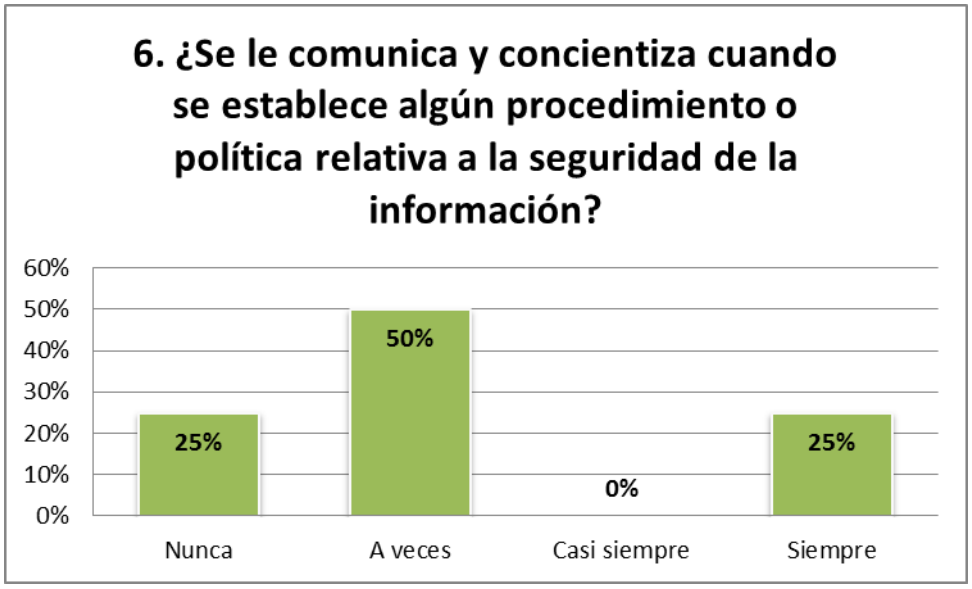


La poblacion encuestada dividio sus opiniones respondiendo que: el 50% piensa que nunca se le ha brindado capacitacion en temas referentes a seguridad de la información, asi mismo el 50% respondió que a veces se le brinda capacitación en el tema de seguridad de la información.

ANALISIS PREGUNTA 5: Se puede demostrar que de acuerdo a los resultados obtenidos la población encuestada considera que “nunca” y “a veces” se le ha brindado capacitación en temas referentes a seguridad de la información.

6. ¿Se le comunica y concientiza cuando se establece algún procedimiento o política relativa a la seguridad de la información?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	1	25%
A veces	2	50%
Casi siempre	0	0%
Siempre	1	25%
TOTAL	4	100%

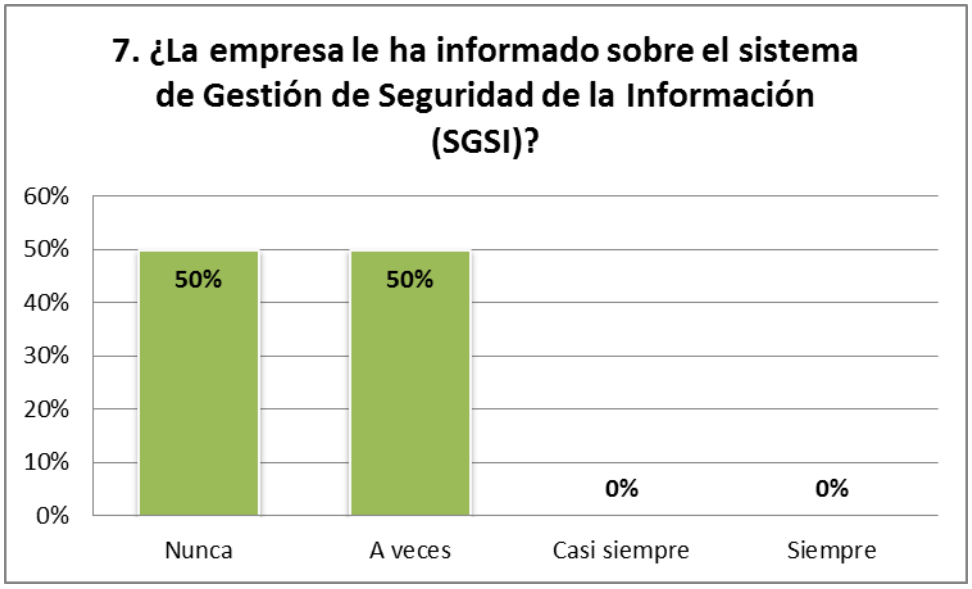


El 25% de los jefes de area encuestados opina que nunca se le comunica y concientiza cuando se establece algun procedimiento referente a la seguridad de la información, un 50% considera que a veces se le comunica y concientiza, por otro lado un 25% señalo que siempre se le comunica y concientiza cuando se establece algun procedimiento o politica referente a la seguridad de la información dentro de la organización.

ANALISIS PREGUNTA 6: Con los resultados obtenidos la poblacion experimental afirma que “a veces” se le comunica y concientiza cuando se establece algun procedimiento o politica relativa a la seguridad de la información.

7. ¿La empresa le ha informado sobre el sistema de Gestión de Seguridad de la Información (SGSI)?

RESPUESTA	FRECUENCIA	PORCENTAJE
Nunca	2	50%
A veces	2	50%
Casi siempre	0	0%
Siempre	0	0%
TOTAL	4	100%

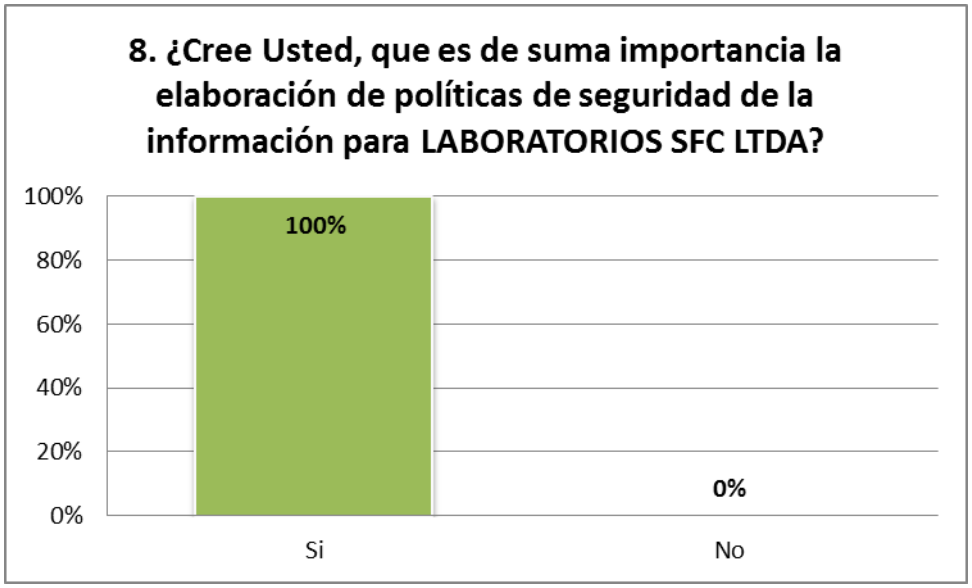


Un 50% de la poblacion encuestada respondio que “nunca” y “a veces” la empresa le ha informado sobre el SGSI (Sistema de Gestión de Seguridad de la Información).

ANALISIS RESPUESTA 7: La poblacion encuestada afirma que “nunca” y “a veces” la empresa le ha informado sobre el SGSI (Sistema de Gestión de Seguridad de la Información) que va a implementar.

8. ¿Cree Usted, que es de suma importancia la elaboración de políticas de seguridad de la información para LABORATORIOS SFC LTDA?

RESPUESTA	FRECUENCIA	PORCENTAJE
Si	4	100%
No	0	0%
TOTAL	4	100%



Un 100% de la población encuestada afirma que si es de suma importancia la elaboración de políticas de seguridad de la información.

ANALISIS PREGUNTA 8: la población experimental respondió que “si” consideran de suma importancia la elaboración de políticas de seguridad de la información para la organización.

ANEXO K. FORMATO ACTIVOS SFC

Código Activo: _____

CPU				
Procesador		**Memoria RAM**		
Disco Duro 1		**Disco Duro 2**		
CD-ROM		**Floppy:**	**SI**	**NO**

Monitor		**Código Activo**	
Teclado		**Mouse**	

IMPRESORA			
Marca		**Modelo**	
Código Activo			

SOFTWARE INSTALADO:

OS:		**OFFICE:**	
NOVASOFT:		**OTRO:**	

OBSERVACIONES:

_____

_____

ANEXO L. LISTA DE VERIFICACIÓN AUDITORÍA INTERNA NTC – ISO/IEC 27001:2013

FECHA: _____ **PROCESO:** _____

AUDITOR: _____ **AUDITADO:** _____

Objetivo: verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumplen con los requisitos de la norma ISO/IEC 27001.

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	¿Se encuentra establecida y documentada la(s) política(s) de seguridad de la información?						
	¿Existe una normativa relativa a la seguridad de la información?						
	¿Existe una persona responsable de las políticas, normas y procedimientos de seguridad de la información?						
	¿Existen mecanismos definidos para la comunicación de las políticas a empleados y partes interesadas?						
	¿Existen mecanismos planificados para la revisión de las políticas?						
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	¿Se encuentran definidos y asignados los roles y responsabilidades para las personas involucradas en la seguridad de la información?						
	¿Se mantiene el contacto apropiado con las autoridades pertinentes?						
	¿Se mantiene el contacto apropiado con grupos o profesionales especializados en seguridad?						
	¿Se encuentra establecida y documentada una política de uso de dispositivos móviles?						
	¿Se encuentra establecida y documentada una política de teletrabajo?						

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	¿Se verifican los antecedentes de los candidatos a un empleo de acuerdo a los requisitos del negocio y clasificación de la información?						
	¿Se Presenta en los contratos los términos, condiciones de confidencialidad y responsabilidades en cuanto a seguridad de la información?						
	¿Se Capacita adecuada a los empleados y partes interesadas en seguridad de la información y actualización de políticas?						
	¿Se encuentra definido un proceso disciplinario para la violación de la seguridad de la información?						
A.8. GESTIÓN DE ACTIVOS.	¿Se encuentra definido un inventario de activos documentado y actualizado?						
	¿Existen procedimientos para el uso aceptable de activos de información e instalaciones de procesamiento de información?						
	¿Existe evidencia de la devolución de activos?						
	¿Los activos se encuentran clasificados de tipo: Datos, Software, Equipos y Servicios?						
	¿Los activos se encuentran clasificados de acuerdo a su nivel de criticidad?						
	¿Se encuentran definidos procedimientos de etiquetado de la información?						
	¿Se encuentran definidos procedimientos para clasificar la información de la organización?						
	¿Existen procedimientos para la gestión de medios removibles?						
	¿Existen procedimientos formales para disponer de los medios que ya no se utilizan?						

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
|A.9. CONTROL DE ACCESO.	¿Se encuentra establecida y documentada una política de control de accesos?						
	¿Se encuentra establecida y documentada una Política sobre el uso de los servicios de red?						
	¿Se encuentra establecido un procedimiento formal para el registro y baja de usuarios?						
	¿Se permite y restringe el acceso a los recursos de la red y privilegios de usuario?						
	¿Se encuentra establecido un procedimiento para la asignación de información secreta?						
	¿Se hace una revisión de los derechos de acceso de los usuarios?						
	¿Existe un mecanismo de gestión de contraseñas?						
A.10. CRIPTOGRAFÍA	¿Se encuentra establecida una Política sobre el uso de controles criptográficos?						
	¿Existe una política sobre el uso, protección y tiempo de vida de las llaves criptográficas?						
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	¿Se encuentra definido un perímetro de seguridad?						
	¿Se encuentran definidos controles de entrada para proteger las instalaciones frente al acceso de personal no autorizado?						
	¿Se han diseñado y establecido mecanismos de seguridad para oficinas e instalaciones?						
	¿Se han diseñado y establecido mecanismos para la protección contra riesgos físicos?						
	¿Existen procedimientos para aéreas seguras?						
	¿Existen controles para el acceso de áreas de despacho y carga?						

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
	¿Los equipos están ubicados para minimizar los accesos innecesarios?						
	¿Existen mecanismos contra fallas de energía?						
	¿E cableado se encuentra protegido contra daños e interrupciones?						
	¿Se mantienen correctamente los equipos para asegura la disponibilidad e integridad?						
	¿Existen mecanismos o lineamientos para proteger equipos desatendidos?						
	¿Se encuentran establecidas políticas de limpieza en puestos de trabajo?						
A.12. SEGURIDAD DE LAS OPERACIONES.	¿Existen procedimientos operativos para gestión de TI?						
	¿Todos los procedimientos operativos que se han identificado en la política de seguridad de la información se encuentran documentados?						
	¿Se dispone de mecanismos o lineamientos para el control de cambios?						
	¿Existe una separación de los ambientes de desarrollo, prueba y operación?						
	¿Existen controles o mecanismos contra códigos maliciosos?						
	¿Existe una política de copias de respaldo? ¿Se encuentra aprobada?						
	¿Existen mecanismos para realizar copias de respaldo de la información?						
	¿Existen registros de logs de actividades y eventos generados en los sistemas?						
	¿Se registran las actividades del administrador y operador del sistema?						

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
A.13. SEGURIDAD DE LAS COMUNICACIONES.	¿Se encuentra establecido algún mecanismo para el control de las redes?						
	¿Existen acuerdos de servicio de red?						
	¿Se encuentra establecida e implementada políticas y procedimientos para la transferencia de información?						
	¿Existe algún acuerdo para la transferencia de información?						
	¿Se tienen medidas de seguridad para la mensajería electrónica?						
	¿Se han establecido e implementado medidas para la confidencialidad y no divulgación de la información?						
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	¿Se encuentra establecida e implementada una política de desarrollo seguro?						
	¿Existe un procedimiento para controlar los cambios en los sistemas?						
	¿Se encuentra establecido y documentado principios para la construcción de sistemas seguros?						
	¿Existen ambientes de desarrollo seguro?						
	¿Se encuentra establecida una política de desarrollo por terceros?						
	¿Existen pruebas de seguridad para los sistemas desarrollados?						
	¿Existen programas de prueba para los nuevos sistemas e información?						
	¿Existen controles para la protección de los dato de prueba?						

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
A.15. RELACIONES CON LOS PROVEEDORES.	¿Se encuentra establecida y documentada una Política de seguridad de la información para las relaciones con proveedores?						
	¿La política e relaciones con los proveedores cubren todo los requisitos de seguridad asociados con riesgos de seguridad y tratamiento de la información?						
	¿Existe un registro de auditoria a proveedores?						
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	¿Se han definido los responsables y los procedimientos para los incidentes de seguridad de la información?						
	¿Se encuentra establecido y documentado un Procedimiento para la gestión de incidentes?						
	¿Existe un reporte de los eventos de seguridad?						
	¿Se reportan las debilidades de seguridad de la información?						
	¿Se han establecido procedimientos para la identificación, recolección, adquisición y preservación de información que pueda considerarse como evidencia?						
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	¿Se han establecido Procedimientos de la continuidad del negocio?						
	¿Se han establecido y documentado un plan de continuidad del negocio y análisis de impacto?						
	¿Existe una revisión de los controles de continuidad de la seguridad de la información?						
A.18. CUMPLIMIENTO.	¿Se han identificado los Requisitos legales, normativos y contractuales aplicables a la organización?						
	¿Existen procedimientos para resguardar el derecho a la propiedad intelectual?						

CONTROL A VERIFICAR	REQUERIMIENTO DE LA NORMA	CUMPLIMIENTO		EVIDENCIA OBJETIVA Y/O OBSERVACIONES	HALLAZGOS		
		SI	NO		C	NC	OM
	¿Lo registros son protegidos de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio?						
	¿Existen controles criptográficos que cumplan con los requisitos legislativos y reglamentarios?						
	¿Se realiza una revisión de las políticas y procedimientos de seguridad?						
	¿Se realizan auditorías a las políticas y procedimientos de seguridad de la información?						

CONVENCIONES
C: Conforme
NC: No Conforme
OM.: Oportunidades de Mejora

ANEXO M. DIVULGACIÓN DEL SGSI

LABORATORIOS S.F.C. LTDA SERVICIOS FARMACEUTICOS DE CALIDAD			
REGISTRO DE CAPACITACIÓN			
Código: PE-01F1	Versión: No. 5	Fecha de Emisión: 150601	Página: 1 de 1

TEMA: Divulgación Sistema de Gestion de Seguridad de la Informacion (SGSI) Para laboratorios SFC Ltda	FECHA: 160421
CAPACITADOR: Jorge Leonardo Rodriguez	FIRMA: [illegible]
HORA INICIAL: 7:00 A.M.	HORA FINAL: 9:00 A.M

APLICA EVALUACION: SI [X] NO [NA]

METODO DE EVALUACIÓN:

Prueba Escrita [NA] Examen Verbal [NA] Actividad durante la reunión [X]

NOMBRE	CARGO	FIRMA
Juan Sebastián Sánchez	Jefe Control Calidad	S. Sánchez
Ernesto Galvis	Jefe de Almacen	Ernesto
Jose Emilio Perez C	Jefe de Contabilidad	[illegible]
Judith Ordoñez	DT	[illegible]
Marcela Rodriguez	Jefe de Microbiologia	[illegible]
Nelly Perez	Directora Planeación	[illegible]
John H. Vergel	Jefe de Mantenimiento	J. Vergel
Santiago Mejia Velez	Director de Ingenieria	[illegible]
Ana Catalina Sánchez	Directora Científica	[illegible]
Yenny Salgado	Directora Aseguramiento	Yenny Salgado
Leonardo Ramirez	Director de Talento Humano/HSE	[illegible]
Ruth Alvarez.	Supervisora de Acondicionamiento	[illegible]
Valerio Castaño	Gerencia	[illegible]
Mario Alley U. Sanchez	Supervisor de fabricación	M Sanchez
NA	NA	NA

Resultados de la Evaluación: Se realizaron ejemplos practicos de Seguridad de la informacion

Fuente: El Autor.

ANEXO M. (Continuación).

	LABORATORIOS S.F.C. LTDA SERVICIOS FARMACEUTICOS DE CALIDAD		
	REGISTRO DE CAPACITACIÓN		
Código: PE-01F1	Versión: No. 5	Fecha de Emisión: 150601	Página: 1 de 1

TEMA: Divulgación Sistema de Gestión de Seguridad de la información (SGSI) Para laboratorios SFC Ltda	FECHA: 160422
CAPACITADOR: Jorge Leonardo Rodriguez Correa	FIRMA:
HORA INICIAL: 7:00 a.m	HORA FINAL: 9:00 a.m

APLICA EVALUACION: SI [X] NO [NA]

METODO DE EVALUACIÓN:

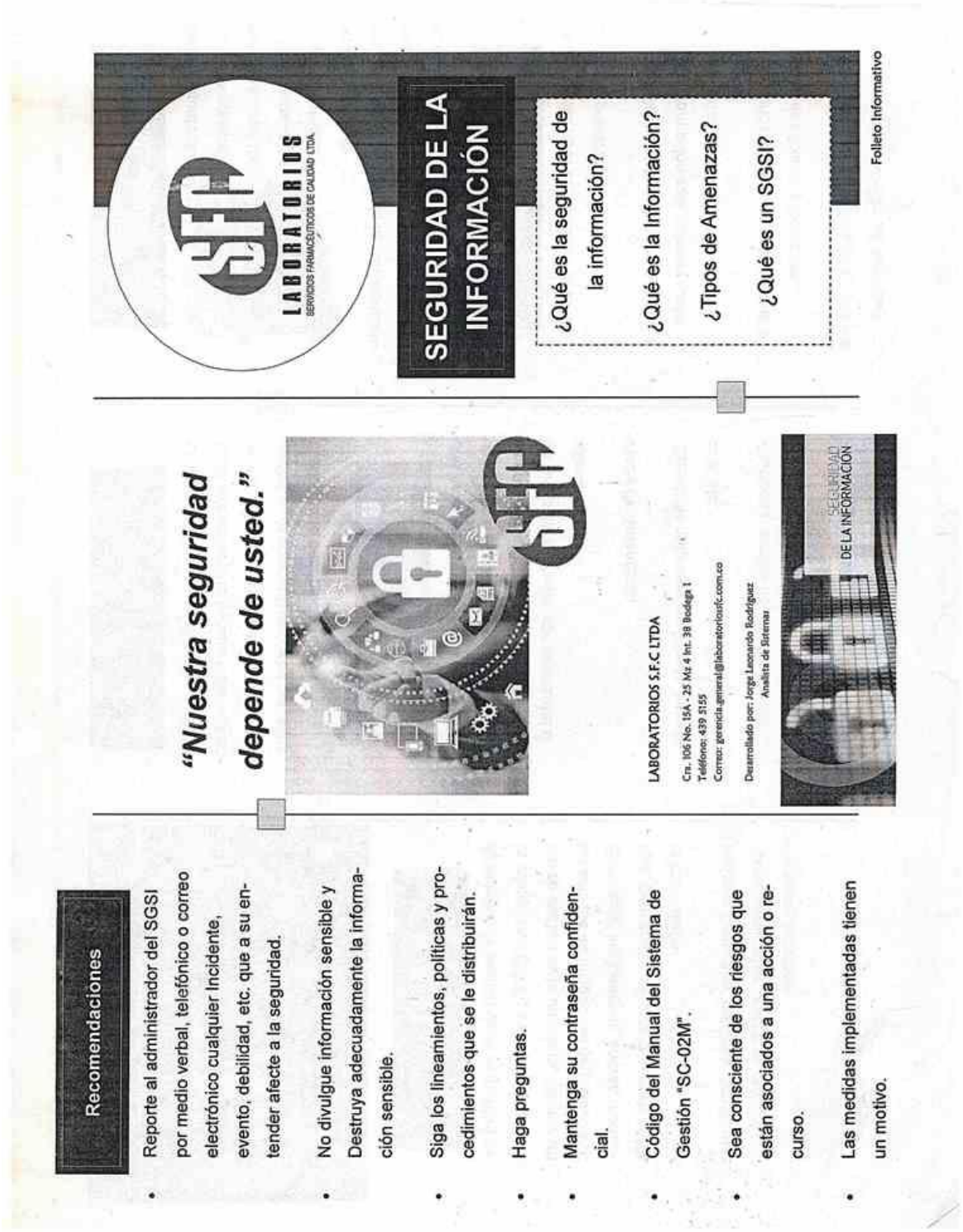
Prueba Escrita [NA] Examen Verbal [NA] Actividad durante la reunión [X]

NOMBRE	CARGO	FIRMA
Natalia Sarmiento	Facturación	Natalia Sa.
Jose Perez C	Jefe contabilidad	
Francy Aguilar G	Aux. contable	
Claudia E. Cruz B	Analista de campos	Claudia Cruz

Resultados de la Evaluación: Se realizaron ejemplos practicos de Seguridad de la Información

Fuente: El Autor.

ANEXO N. MATERIAL INFORMATIVO



Fuente: El Autor.

ANEXO N. (Continuación).

Fuente: El Autor.

ANEXO O. PRESUPUESTO SGSI 2017

Presupuesto SGSI 2017														
Tema	**ENE**	**FEB**	**MAR**	**ABR**	**MAY**	**JUN**	**JUL**	**AGO**	**SEP**	**OCT**	**NOV**	**DIC**	**Presupuesto**	**Observaciones**
Norma NTC ISO/IEC 27001:2013													$ 58.000	
Servidor de Backups													$ 2.780.000	Para Backups fuera de la empresa.
Servidor Interno													$ 2.780.000	Para el sistema de control de calidad
Impresora Multifuncional													$ 820.000	Para FQ
Software control de calidad													$ 11.000.000	Sistema para microbiología y FQ
cables utp cat 6													$ 7.000.000	Instalación de 32 puntos nuevos de datos y 14 de voz, instalación de tubería EMT, canaleta para cambiar red existente de Cat. 5e a 6.
Licencia antivirus													$ 2.868.320	Renovación anual
Gabinetes con llave													$ 400.000	Para almacenar documentación del director técnico y jefe de control de calidad.
Computadoras													$ 5.549.770	Cambiar PCs obsoletos
Termo higrómetro														Medir temperatura del cuarto de servidores
Consultor externo													$ 600.000	Asesorías
Curso de auditor													$ 3.600.000	Curso de auditor

Presupuesto SGSI 2017														
Tema	**ENE**	**FEB**	**MAR**	**ABR**	**MAY**	**JUN**	**JUL**	**AGO**	**SEP**	**OCT**	**NOV**	**DIC**	**Presupuesto**	**Observaciones**
interno														interno ISO27001 / 3 personas
Auditor externo													$ 1.300.000	Acompañamiento en primera auditoria al SG
Plan Eléctrica													$ 134.000	
Disco duro para Servidor de archivos													$ 400.000	
Disco duro extraíble													$ 379.000	Almacenar hojas de vida.
Subtotal													**$ 39.669.090**	**Presupuesto total para el año 2017 para las actividades sin imprevistos**
Otros													$ 3.966.909	El 10 % del subtotal se tomará como imprevistos, cosas que pueden ocurrir.
Total													**$ 43.635.999**	**Total con imprevistos**

Fuente: El autor.

ANEXO P. CRONOGRAMA DE ACTIVIDADES SGSI 2017

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**Implementar medidas de seguridad en los equipos computarizados**																																															
1.2	Programa de Capacitaciones																																															
2	***Capacitación y sensibilización:***																																															
2.1	Capacitación "Amenazas y virus más comunes"																																															
2.2	Capacitación "Un buen empleado"																																															
2.3	Capacitación "Importancia de la seguridad																																															

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	de la información"																																															
2.4	Capacitación "contraseñas seguras"																																															
2.5	Capacitación "seguridad en los puestos de trabajo"																																														
2.6	Capacitación "Infección a través de redes sociales"																																														
2.7	Capacitación ¿Cómo cuido mi información personal?																																														
2.8	Capacitación ¿Qué es el Phishing?																																														
2.9	Capacitación ¿Qué es																																														

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	Malware?																																															
2.10	Capacitación ¿Qué es el ransomware y cómo afecta a los entornos corporativos?																																														
2.11	Capacitación ¿Qué es ingeniería Social y cómo afecta a la organización?																																														
2.12	Distribución material de sensibilización																																														
3	**Políticas Faltantes (desarrollo, formalización y divulgación)**																																														

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
4	**Divulgar SGSI a personas faltantes**																																															
4.1	Procedimiento entrega y devolución del equipo de computo																																															
4.2	Revisar Inventario de equipos de computo																																															
4.3	Revisar controles de seguridad																																															
5	***Implementar controles:***																																															
5.1	Uso aceptable de los activos																																															
5.2	Política de control de acceso																																															
5.3	Procedimientos																																															

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	operativos para gestión de TI																																															
5.4	Seguridad para proveedores																																															
5.5	Gestión de incidentes																																															
5.6	Continuidad del negocio																																															
5.7	Inspecciones puestos de trabajo																																															
6	**Revisiones periódicas de la eficacia del SGSI**																																															
7	**Medir la efectividad de los controles para verificar que se han cumplido los requisitos de**																																															

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	seguridad.																																															
8	**Identificar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI**																																														
9	**Programa de auditoría**																																														
9.1	Seleccionar Equipo auditor																																														
9.2	Resultados de las auditorías internas																																														
9.3	Identificación de las no conformidades																																														
9.4	levantamiento de No																																														

Actividad		ENE				FEB				MAR				ABR				MAY				JUN				JUL				AGO				SEP				OCT				NOV				DIC			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	Conformidades																																															
10	**Revisión por la dirección**																																															
12	**Capacitación de Ingreso SGSI**																																															

Fuente: El autor.

ANEXO Q. ACUERDO DE CONFIDENCIALIDAD ASESORIA PROFESIONAL

LABORATORIOS S.F.C. LTDA.
SERVICIOS FARMACÉUTICOS DE CALIDAD
Integramos la Calidad al Servicio.

Acuerdo de Confidencialidad

Entre **Laboratorios S.F.C. Ltda. Con Nit. 830.001.242-1 (INFORMANTE),** y el asesor profesional en Sistemas de Gestión de Seguridad de la información Hugo Fernando Ramirez Ospina con C.C.79.576.007 (RECEPTOR).

En atención a lo anterior, este documento que suscriben las partes, es el Acuerdo de Confidencialidad, el cual consta de las siguientes cláusulas:

PRIMERA. Definición de Información Confidencial. "Información Confidencial" significa información en cualquier forma incluyendo, pero no limitado a, la información verbal, escrita y digital con respecto a su actividad comercial, financiera o a las operaciones, proyectos, procesos, productos (e incluyendo, con relación a procesos específicos o productos, información relativa a la fórmula, composición, método de fabricación, uso potencial u otra característica técnica o científica), negocios, planes, programas, plantas industriales, secretos comerciales, fabricación, pedido de materias primas y su utilización, marketing, investigación y desarrollo, tecnología, equipos y otros bienes, muestras, prototipos, planos, cómputos, compilaciones, datos, base de datos, know-how, conceptos, propiedad intelectual, costos, ganancias, ventas, nómina de clientes, requerimientos de los clientes, métodos desarrollados internamente a pedido del cliente, la identidad u otros datos sobre los potenciales clientes y los ya existentes, convenios con clientes o proveedores, cotización de precios, facturas, informes cuantitativos, informes sobre el aseguramiento de la calidad y adquisiciones o desinversiones posibles recibidas por la parte informante, de sus representantes o de terceros a pedido de la parte informante.

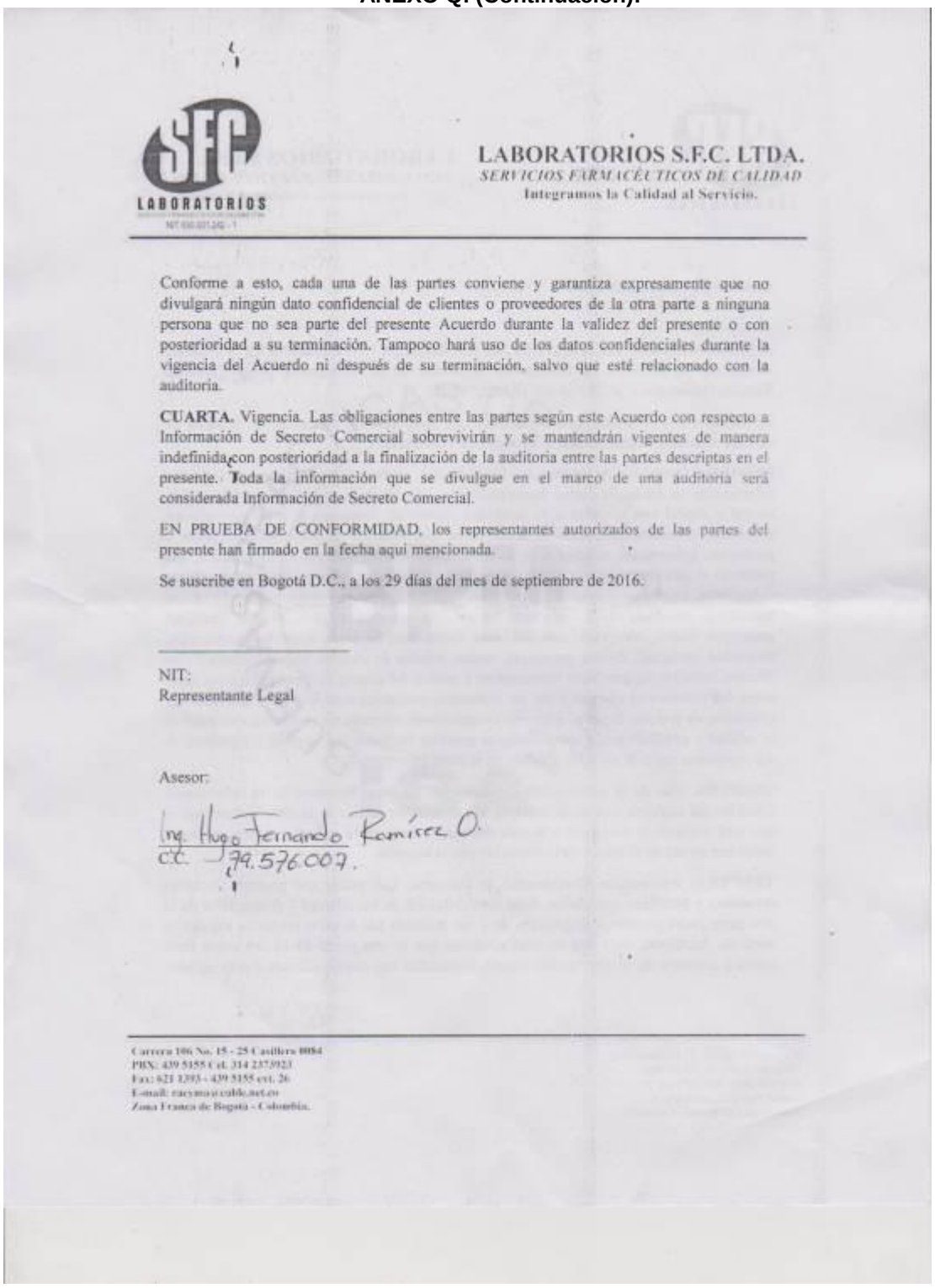
SEGUNDA. Uso de la Información Confidencial. La parte receptora de la Información Confidencial conviene que no la utilizará, sin el permiso escrito de la parte informante, el que será otorgado o denegado a la sola discreción de la parte informante, por cualquier razón que no sea en el marco de lo requerido por la asesoría.

TERCERA. Información Confidencial de Terceros. Las partes del presente Acuerdo reconocen y certifican que ciertos datos confidenciales de los clientes y proveedores de la otra parte podrá ponerse a disposición de o ser utilizada por la parte receptora durante la asesoría. Asimismo, cada una de ellas reconoce que la otra podrá en ciertos casos estar sujeta a acuerdos de no divulgación o confidencialidad con ciertos clientes o proveedores.

Carrera 106 No. 15 - 25 Casillero 0084
PBX: 439 5155 Cel. 314 237 3923
Fax: 621 1393 - 439 5155 ext. 26
E-mail: [illegible]
Zona Franca de Bogotá - Colombia.

Fuente: El autor.

ANEXO Q. (Continuación).



LABORATORIOS

LABORATORIOS S.F.C. LTDA.
SERVICIOS FARMACÉUTICOS DE CALIDAD
Integramos la Calidad al Servicio.

Conforme a esto, cada una de las partes conviene y garantiza expresamente que no divulgará ningún dato confidencial de clientes o proveedores de la otra parte a ninguna persona que no sea parte del presente Acuerdo durante la validez del presente o con posterioridad a su terminación. Tampoco hará uso de los datos confidenciales durante la vigencia del Acuerdo ni después de su terminación, salvo que esté relacionado con la auditoria.

CUARTA. Vigencia. Las obligaciones entre las partes según este Acuerdo con respecto a Información de Secreto Comercial sobrevivirán y se mantendrán vigentes de manera indefinida con posterioridad a la finalización de la auditoria entre las partes descriptas en el presente. Toda la información que se divulgue en el marco de una auditoria será considerada Información de Secreto Comercial.

EN PRUEBA DE CONFORMIDAD, los representantes autorizados de las partes del presente han firmado en la fecha aquí mencionada.

Se suscribe en Bogotá D.C., a los 29 días del mes de septiembre de 2016.

NIT:
Representante Legal

Asesor:

Ing. Hugo Fernando Ramírez O.
c.c. 79.576.007.

Carrera 106 No. 15 - 25 Casillero 8084
PBX: 439 5155 (ct. 314 237.9323
Fax: 621 1393 - 439 5155 ext. 26
E-mail: sacyma@colde.net.co
Zona Franca de Bogotá - Colombia.

Fuente: El autor.

ANEXO R. DIVULGACIÓN MANUAL DE SEGURIDAD Y POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

	LABORATORIOS S.F.C. LTDA. SERVICIOS FARMACEUTICOS DE CALIDAD		
CONOCIMIENTO DEL DOCUMENTO			
Código: CD-01F3	Versión No. 4	Vigencia Desde 100209 Hasta N/A	Página: N/A

Nombre del Documento: MANUAL DE SEGURIDAD DE LA INFORMACION

Código: SC-02M Versión: 1

NOMBRE	CARGO	FECHA
Henry Salgado	Dir. Aseguramiento	160307
Jorge Leonardo Rodriguez	Analista de Sistemas	160307
V. Cortazo.	Gerencia	16 03 07
Leonardo Ramez S.	Director Talento Humano/HSE	160307
Sebastián Sánchez	DT	160307
Marcela Rodriguez	Jefe de Microbiologia	160307
Jidy Perez	Directora Planeacion	160307
Ing Emilio Perez	Jefe de Contabilidad	160307
Claudia Cruz.	Analista Compras	160307

Fuente: El autor.

ANEXO S. DECLARACIÓN DE APLICABILIDAD ACTUAL

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN									
A 5.1 ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	SI	Mediante el procedimiento SC-02M "Manual de Seguridad de la Información", en el capítulo 5.2., se describe la política de Seguridad de la Información adoptada por la organización. Para su divulgación y apropiación se solicita al área de talento humano, la inclusión de un capítulo sobre el SGSI en el PE-01F2 "Cronograma de capacitación al personal". Su divulgación se realiza también el página web del laboratorio http://laboratoriossfc.com.co/?p=566			X		El control cumple con el estándar y está Documentado
	A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN		SI	La organización ha definido las políticas de obligatorio cumplimiento según la guía de implementación NTC/ISO 27001:2013, que son publicadas en el procedimiento SC-02M "Manual de Seguridad de la Información" Al igual que la política del SGSI, estas políticas son divulgadas a través del PE-01F2 "Cronograma de capacitación al personal" y a través de las carteleras físicas de la organización.			X		El control cumple con el estándar y está Documentado
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN									
A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	SI	En el procedimiento SC-02M "Manual de Seguridad de la Información" se identificaron los roles y responsabilidades frente al SGSI. Estos serán incluidos en los procedimientos: • OD-01M "Manual de Funciones: Departamento Administrativo". • OD-02M "Manual de Funciones: Departamento Técnica y departamento de calidad (ASECAL)". • OD-04M "Manual de Funciones: Departamento de Ingeniería"			X		El control cumple con el estándar y está Documentado
	A 6.1.2 SEPARACIÓN DE DEBERES		SI	De acuerdo al documento SC-03MA2 "Matriz de funciones y responsabilidades" Se realizá un diagnóstico de los cargos VS Actividades críticas con el fin de realizar un			X		El control esta implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				análisis de riesgos asociados a las cargas de trabajo para identificar las actividades que puedan afectar alguno de los pilares de la seguridad de la información. Se pretende evitar la materialización de riesgos como corrupción o riesgos asociados con fatigas por sobrecarga de trabajo.					pero no Documentado
	A 6.1.3 CONTACTO CON LAS AUTORIDADES		SI	El laboratorio ha determinado que las autoridades pertinentes con relación al cumplimiento de la ley, los organismos de regulación y las autoridades son: • ICA. • INVIMA. FNE (FONDO NACIONAL DE ESTUPEFACIENTES). • UIAF (UNIDAD DE INFORMACIÓN Y ANALISIS FINANCIERO). • IDEAM. • MINISTERIO DE TRABAJO. Los encargados de entablar las comunicaciones con las autoridades se definen en el documento SC-03M4 "Matriz de comunicación".	X		X		El control cumple con el estándar y está Documentado
	A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL		SI	Con el fin de asegurar el contacto con grupos de interés se formalizará un documento en el cual se listen los grupos de interés del laboratorio para facilitar su mantenimiento. Los grupos de interés están conformados por: A nivel de negocio: - ICONTEC. - ONAC.	X		X		El control esta implementado pero no Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				- USP (FARMACOPEA). - INVIMA. - ICA. - IDEAM. - UIAF. - FNE. - Policía (Antecedentes Judiciales) - E-Journal. - Sigma-Aldrich - SUPERINTENDENCIA DE INDUSTRIA Y SOCIEDADES. - SEGUROS BOLIVAR. - OMECOL (Organización Metrológica Colombiana). - STV (Servicios Técnicos de Validación). A nivel de TI: - Dell. - HP - Khymos. - Kyocera. - GAE. - DLink					

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				- Microsoft. El laboratorio garantiza que los mecanismos de protección permitan el acceso seguro a los sitios identificados y se mantengan números de teléfonos actualizados de los contactos.					
	A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.		SI	El desarrollo de nuevos productos es pensado en conjunto por varios departamos en la compañía que aportan sus conocimientos técnicos, académicos y comerciales para establecer el diseño de un producto nuevo desde las bases literarias, desarrollo, elaboración hasta su finalización con la elaboración de dossier ante el ICA. A nivel de seguridad de la información los integrantes del grupo de desarrollo aceptan y aplican la política de confidencialidad, no deben divulgar ni compartir información sobre los desarrollos, no discuten información fuera de las reuniones del grupo de desarrollo, etc. Se formalizará el documento "Instructivo para desarrollo de nuevos productos", en el cual se describe la metodología usada por el grupo de desarrollo de nuevos productos y la aplicación de la seguridad de la información.			X		El control esta implementado pero no Documentado
A 6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO	A 6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	SI	En el procedimiento SC-02M "Manual de Seguridad de la Información" se incluye la Política para dispositivos móviles con el fin de adoptar medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.			X		El control cumple con el estándar y está Documentado
	A 6.2.2 TELETRABAJO		SI	En el procedimiento PE-05 "Reglamento interno de trabajo" se incluirá un capítulo sobre el teletrabajo. Con el fin de presentar una alternativa a los colaboradores que quieran optar por Teletrabajo. LEY 1221 DE 2008.	X		X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS									
A 7.1 ANTES DE ASUMIR EL EMPLEO	A 7.1.1 SELECCIÓN	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	SI	En el procedimiento PE-06 "Selección de Personal" se describen las pautas a seguir para la selección del personal aspirante a ocupar vacantes en Laboratorios SFC Ltda.			X		El control cumple con el estándar y está Documentado
	A 7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO		SI	La organización ha establecido Cláusulas de confidencialidad anexas en los contratos de los colaboradores con el fin de preservar la confidencialidad sobre la información y la propiedad intelectual. Los empleados se comprometen a cumplir la Política de confidencialidad incluida en el procedimiento CD-01I3 "Protección de la Información".			X		El control cumple con el estándar y está Documentado
A 7.2 DURANTE LA EJECUCIÓN DEL EMPLEO	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	SI	En la política de seguridad de la información incluida en el procedimiento SC-02M "Manual de seguridad de la información" se indica que la Alta Dirección es responsable de brindar las herramientas necesarias para que sus empleados y contratistas cumplan con los lineamientos de la seguridad de la información.			X		El control cumple con el estándar y está Documentado
	A 7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN		SI	En el procedimiento PE-01 "Capacitaciones" se definen los lineamientos para todo el personal en cuanto a capacitaciones y entrenamiento.			X		El control cumple con el estándar y está Documentado
	A.7.2.3 PROCESO DISCIPLINARIO		SI	En el procedimiento PE-05 "Reglamento interno de trabajo" en el capítulo XIII se detalla la escala de faltas y sanciones disciplinarias previstas por incumplimiento de la Política de Seguridad de la Información.			X		El control cumple con el estándar y está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
									Documentado
A 7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	A7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	SI	La terminación del empleo se desarrolla como se ha definido en el procedimiento PE-05 "Reglamento interno de trabajo", Cuando un empleado cambia de cargo o se retira de la organización se da de baja en todos sistemas de información, aplicativos y demás servicios y accesos de red una vez sea notificada el área de TI. Con relación al cambio de responsabilidades se aplica un "OTRO SI AL CONTRATO".			X		El control cumple con el estándar y está Documentado
A.8 GESTION DE ACTIVOS									
A 8.1 RESPONSABILIDAD POR LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	SI	Se formalizará el procedimiento "gestión de activos" en el cual se detallará quién, cómo y cuándo se debe actualizar el inventario de activos, además se detalla la forma en cómo se asigna la responsabilidad o propiedad de cada activo de información. Se incluye el inventario de activos.			X	X	El control no cumple con el estándar y debe ser rediseñado
	A 8.1.2 PROPIEDAD DE LOS ACTIVOS		SI	La organización mantiene todos los activos dentro del inventario, se incluirá el área responsable de los activos.			X	X	El control no cumple con el estándar y debe ser rediseñado
	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS		SI	En el procedimiento SC-02M "Manual de Seguridad de la información" se incluye la Política de Uso Aceptable de los Activos.			X	X	El control cumple con el estándar y está Documentado
	A 8.1.4 DEVOLUCIÓN		SI	Se incluirá en el procedimiento "gestión de activos" el proceso para realizar la devolución			X	X	El control no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	DE LOS ACTIVOS			de los activos y la forma cómo se da de baja o se retiran definitivamente los activos de la organización.					cumple con el estándar y debe ser rediseñado
A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	SI	En el instructivo SC-02MI2 "Clasificación y etiquetado de información" se detalla la manera como la organización realiza la clasificación y etiquetado de la información.			X	X	El control cumple con el estándar y está Documentado
	A 8.2.2 ETIQUETADO DE LA INFORMACIÓN		SI				X	X	El control cumple con el estándar y está Documentado
	A 8.2.3 MANEJO DE ACTIVOS		SI	El manejo de los activos se realiza de acuerdo a la política de uso aceptable de los activos y al esquema de clasificación de la información adoptado por el laboratorio, adicionalmente el uso de los mismos se realiza de acuerdo a las especificaciones de los fabricantes.			X	X	El control esta implementado pero no Documentado
A 8.3 MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de	SI	Se formalizará el procedimiento "Manejo de medios" en el cual se definirá la manera de cómo se usan, transportan, protegen y disponen los medios removibles (CD, DVD, USB, DDE y otros)			X	X	El control no está implementado
	A 8.3.2 DISPOSICIÓN DE LOS MEDIOS		SI				X	X	El control no está implementado
	A 8.3.3 TRANSFERENCIA DE		SI				X	X	El control no está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	MEDIOS FÍSICOS.	soporte.							implementado
A.9 CONTROL DE ACCESO									
A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESO	Limitar el acceso a información y a instalaciones de procesamiento de información.	SI	En el procedimiento SC-02M "Manual de seguridad de la información" se incluye la Política de control de acceso la cual cubre los aspectos físicos y lógicos que son usados en la organización para minimizar la posibilidad de ingresos no autorizados a la información y/o los activos relacionados.			X		El control cumple con el estándar y está Documentado
	A 9.1.2 ACCESO A REDES Y A SERVICIOS EN RED		SI	En la política de control de acceso incluida en el procedimiento SC-02M se describe el control de acceso a redes y a servicios de red.			X		El control cumple con el estándar y está Documentado
A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	SI	En el procedimiento SC-02M "Manual de seguridad de la información" se incluirá la política de Gestión de usuario, que abarca todo el proceso de creación, mantenimiento, bloqueo, desbloqueo, revisión periódica, asignación o revocación de permisos, cancelación de cuentas de usuario, asignación de claves, política de registros automáticos de acceso a servicios (activos) críticos. En el procedimiento CD-01I3 "Protección de la información" se incluye la política de asignación y uso de contraseñas.			X		El control esta implementado pero no Documentado
	A 9.2.2 SUMINSITRO DE ACCESO DE USUARIOS		SI	La organización realiza la alta (registro) y baja (cancelación) de usuarios a través de las solicitudes recibidas vía correo electrónico, son implementadas por el analista de sistemas quien es el responsable del directorio activo, para posibilitar la asignación de los derechos de acceso a través de perfiles de usuario acordes con los permisos requeridos y alineados con la política de acceso y la identificación de derechos de acceso privilegiado.			X		El control esta implementado pero no Documentado
	A 9.2.3 GESTIÓN DE DERECHOS DE ACCESO		SI				X		El control esta implementado pero no

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	PRIVILEGIADO								Documentado
	A 9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS		SI	Se cuenta con una política de asignación y uso de contraseñas incluida en el procedimiento CD-01I3 "Protección de la información" donde se advierte a los usuarios de mantener de manera confidencial la contraseña y utilizar técnicas que impidan su revelación (No escribirlas en papel); Realizar cambios a intervalos de un mes y aplicar técnicas de calidad (longitud mínima, uso de mayúsculas, minúsculas, número, caracteres alfanuméricos, que sean fáciles de recordar, no estén basadas en información familiar o personal y no sean vulnerables a ataques de diccionario); Además se asignan contraseñas temporales que se deben cambiar en el primer inicio de sesión. Este control se refuerza con el Programa de capacitación.			X		El control cumple con el estándar y está Documentado
	A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS		SI	El laboratorio revisa los derechos de acceso y privilegios en las aplicaciones a intervalos planificados (1 mes) o cuando un usuario lo solicite se hace el ajuste necesario y se retiran dichos permisos cuando se ha terminado su contrato o cuando hay un cambio de cargo.			X		El control cumple con el estándar y está Documentado
	A 9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.		SI				X		El control cumple con el estándar y está Documentado
A 9.3 RESPONSABILIDADES DE LOS USUARIOS	A 9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	Hacer que los usuarios rindan cuentas por la custodia de su información de	SI	Adicional al procedimiento "Gestión de usuarios" se incluirá en el programa de capacitación anual el tema "Uso adecuado de Contraseñas", para promover y divulgar aspectos sobre el buen uso de las contraseñas, los cambios periódicos, y la importancia de que sean privadas			X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
		autenticación.							
A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	Prevenir el uso no autorizado de sistemas y aplicaciones.	SI	El acceso a la información (carpetas de red) y a la funcionalidad de las aplicaciones utilizadas en el laboratorio está restringido por perfiles de usuario y privilegios de acceso que se evidencia en los menús que se despliegan y las operaciones permitidas de acuerdo al perfil del usuario.			X		El control cumple con el estándar y está Documentado
	A 9.4.2 PROCEDIMIENTO DE INGRESO SEGURO.		SI	En la política de asignación y uso de contraseñas incluida en el procedimiento CD-01I3 "Protección de la información" se describe la forma como se valida la autenticidad de quien ingresa a un sistema por medio de "audit trail" o rastreo de auditoria. Dichos ingresos quedan registrados en logs que se respaldan y salvaguardan con el fin de una posterior auditoría de control de acceso.			X		El control cumple con el estándar y está Documentado
	A 9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS.		SI	En la política de “asignación y uso de contraseñas”, incluida en el procedimiento CD-01I3 "Protección de la información" se describe la forma como se suministran y protegen las contraseñas en los diferentes recursos de TI.			X		El control cumple con el estándar y está Documentado
	A 9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.		SI	Se restringe el uso de programas utilitarios como el CMD o POWERSHELL únicamente para los administradores del sistema operativo, o administradores del dominio. En la política de Uso aceptable de los activos se menciona que está prohibido el uso de programas utilitarios o instalación de software no autorizado por la empresa.			X		El control cumple con el estándar y está Documentado
	A 9.4.5 CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.		SI	En el procedimiento SC-02M "Manual de seguridad de la información" se encuentra incluida la política de desarrollo tercerizado controlado donde se incluye derecho de revisión de código fuente y sesión de propiedad intelectual. Se prohíbe el uso de herramientas de ingeniería inversa para ser utilizadas en el software licenciado.			X		El control cumple con el estándar y está Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A. 10 CRIPTOGRAFIA									
A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	SI	En el procedimiento SC-02M "Manual de Seguridad de la Información" se incluye la política Sobre uso de controles criptográficos para la protección de la información.			X		El control cumple con el estándar y está Documentado
	A 10.1.2 GESTIÓN DE LLAVES		SI	En la política sobre controles criptográficos se incluye la Gestión de Llaves que describe el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.			X		El control cumple con el estándar y está Documentado
A. 11 SEGURIDAD FISICA Y DEL ENTORNO									
A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	SI	Se incluirá en el procedimiento SC-02M "Manual de seguridad de la información" la política de seguridad Física y del entorno con en la cual se integraran los servicios tercerizados de vigilancia, los servicios de monitoreo, los controles internos de acceso, la identificación de áreas críticas o de acceso restringido, las puertas de seguridad, la señalización preventiva y prohibitiva. Las políticas de adquisición y mantenimiento de pólizas de seguros.			X		El control no cumple con el estándar y debe ser rediseñado
	A 11.1.2 CONTROLES DE ACCESO FÍSICOS		SI	En el CPD (centro de procesamiento de datos) se tienen puertas con cerradura bajo llave, estas llaves son almacenadas en una caja de llaves, ubicada en la oficina del gerente (para acceder a una llave se debe pedir autorización del gerente o director de ingeniería). Se lleva un registro de las personas que ingresan a la empresa y al CPD; además están deben portar en todo momento la identificación que los acredita en un lugar visible y estar siempre acompañados por personal de la empresa.			X		El control cumple con el estándar y está Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	A 11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES		SI	En el procedimiento SC-02M "Manual de seguridad de la información" se incluye la política para "procedimiento operativos para gestión de TI" la cual contiene el apartado "Escritorio Limpio después de la jornada laboral" donde se indica que todas las oficinas deben quedar bajo llave al terminar la jornada laboral y cada vez que se encuentre vacía.			X		El control cumple con el estándar y está Documentado
	A 11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES		SI	La organización cuenta con Sistema de vigilancia prestado por un tercero. Para la protección contra amenazas externas y ambientales cuenta con el procedimiento SEG-01M "Plan de emergencias" el cual define los lineamientos que le permiten a la compañía responder de forma eficiente y eficaz a las situaciones de emergencia.			X		El control cumple con el estándar y está Documentado
	A 11.1.5 TRABAJO EN ÁREAS SEGURAS		SI	El laboratorio ha definido el acceso restringido "Solo para personal autorizado" el área de microbiología y el área de fisicoquímico, el ingreso debe realizarse de acuerdo a los procedimientos PE-04I4 "Ingreso área de microbiología" y PE-04I5 "Ingreso al área de Fisicoquímico" donde se detallan los controles para el ingreso a dichas áreas como por ejemplo: No ingresar sin autorización, diligenciar la bitácora de ingreso al área, no portar celulares o cámaras dentro del área, no comer, beber o fumar, utilizar la indumentaria adecuada suministrada por la organización, etc. Estas áreas están restringidas por la información que se maneja (confidencial) y por el uso de sustancias químicas y microbiológicas. Las oficinas de Dirección técnica y la gerencia también son de acceso restringido porque en ellas se almacena formulas maestras, contratos con los clientes y maquiladores, cheques de gerencia, sellos, etc. Ninguna persona debe entrar sin autorización expresa del Gerente general o del Director Técnico.			X		El control cumple con el estándar y está Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	A 11.1.6 ÁREAS DE DESPACHO Y CARGA		SI	En el procedimiento AL-02 "Almacenamiento de materiales" se describen las medidas de control físicas en las áreas de despacho y carga para evitar vulnerabilidades como perdidas, accesos no autorizados y fraudes. El almacén cuenta con un extintor especial y kit de derrames para el tipo de mercancía que se almacena (material primas y reactivos).			X		El control cumple con el estándar y está Documentado
A 11.2 EQUIPOS	A 11.2.1 UBICACIÓN Y PROTECCION DE LOS EQUIPOS	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	SI	Los equipos que se encuentran asignados al personal están ubicados en oficinas que cuentan con cámaras de video, los equipos están debidamente identificados con su código de activo. El personal conoce claramente las directrices acerca de no comer o beber cerca a los equipos. Los equipos están conectados a una red regulada que impide fallas por energía, puesta a tierra que los protege contra descargas eléctricas; además cuentan con una UPS para evitar que el equipo se apague bruscamente.			X		El control esta implementado pero no Documentado
	A 11.2.2 SERVICIOS DE SUMINSITRO		SI	Se desarrollará una matriz de identificación para los servicios de suministro conformada por: • Proveedor que suministra el servicio. • Probabilidad de falla. • Alternativas de Operación. Con el fin de identificar los servicios críticos y las alternativas de operación en caso de una falla de los servicio de suministro (conectividad a internet, luz, materias primas).			X		El control no está implementado
	A 11.2.3 SEGURIDAD DEL CABLEADO		SI	El cableado de la organización se encuentra de la siguiente forma: • El Director de ingeniería y el analista de sistemas son las únicas personas autorizadas para acceder al Rack. • Las llaves del Rack se encuentran en un gabinete ubicado en la oficina del Gerente General, para acceder a ellas debe existir una previa autorización por el			X		El control cumple con el estándar y está Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				gerente. • El cableado de red es categoría 6. • La topología de Red es en Estrella. • Existe una bitácora para el acceso al cuarto Rack. • la conexión a internet es de fibra óptica. • Existen canaletas por donde se encuentra el cableado a las oficinas. • Los puntos de red están debidamente rotulados con relación a los puertos del Switch. • El cableado de red y de teléfono se encuentran separados. • El modem, Firewall y los Switch se encuentran conectados a la UPS. • El Rack posee un sistema de aire acondicionado para controlar la temperatura. • Al lado de la puerta del rack se encuentra un extintor debidamente identificado y recargado. • El cuarto del Rack posee un DataLogger para medir la temperatura.					
	A 11.2.4 MANTENIMIENTO DE EQUIPOS		SI	El mantenimiento de equipos se desarrolla de acuerdo a los siguientes documentos: - CD-01I4 "Instructivo mantenimiento correctivo y preventivo de equipos de cómputo" - MAN-01P "Programa de mantenimiento y calibración anual"			X		El control cumple con el estándar y está Documentado
	A 11.2.5 RETIRO DE ACTIVOS		SI	Se incluirá dentro del procedimiento "Gestión de activos" los lineamientos para el ingreso y retiro de activos de información de la organización, así como los mecanismos de protección aplicables.			X		El control no está implementado
	A 11.2.6 SEGURIDAD DE EQUIPOS Y		SI	Se incluirá dentro del procedimiento "Gestión de activos" los lineamientos para el uso de equipos fuera de la organización. Se implementan medidas de capacitación dentro del			X		El control no está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	ACTIVOS FUERA DE LAS INSTALACIONES			programa de capacitación anual y validación periódica.					implementado
	A 11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS		SI	Antes de disponer de un equipo o reutilizarlo se debe realizar un borrado seguro del disco duro completo utilizando alguna herramienta como por ejemplo "DARIK'S BOOT AND NUKE", antes de realizar el borrado se debe verificar que no posea información sensible, en caso de que la posea se debe hacer una copia a un disco duro extraíble. La disposición de equipos se realiza de acuerdo al procedimiento IYM-03 "Manejo de residuos".			X		El control esta implementado pero no Documentado
	A 11.2.8 EQUIPOS DE USUARIO DESATENDIDO		SI	En el procedimiento SC-02M "Manual de Seguridad de la Información" en la política Procedimientos operativos para Gestión de TI se detalla el numeral de Bloqueo de la estación de Trabajo cuando un equipo se encuentre desatendido.			X		El control cumple con el estándar y está Documentado
	A 11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.		SI	En el procedimiento SC-02M "Manual de Seguridad de la Información" en la política Procedimientos operativos para Gestión de TI se detalla el numeral Escritorio limpio y Bloqueo de Sesión con el fin de almacenar la información sensible que se encuentre en su escritorio. En cuanto a la pantalla esta debe contener únicamente iconos autorizados para su uso.			X		El control cumple con el estándar y está Documentado
A.12 SEGURIDAD DE LAS OPERACIONES									
A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A 12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	Asegurar las operaciones correctas y seguras de las instalaciones de	SI	El laboratorio tiene documentada las actividades operacionales que se ejecutan en cada uno de los procesos y están disponibles al personal que lo necesite, al igual que todas aquellas actividades relacionadas con el SGSI. Todos estos documentos pueden listarse en el SC-01MA1 "Listado maestro de la Documentación".			X		El control cumple con el estándar y está Documentado
	A 12.1.2 GESTIÓN DE		SI	En el procedimiento CD-01 "Norma Fundamental de la documentación" se describe el			X		El control

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	CAMBIOS	procesamiento de información.		proceso para la gestión de cambios.					cumple con el estándar y está Documentado
	A 12.1.3 GESTIÓN DE CAPACIDAD		SI	Se propone la creación del procedimiento "Gestión de la Capacidad" con el fin de medir la capacidad Instalada (lo que se tiene) contra la capacidad Usada para determinar el momento adecuado de cuando la organización debe adquirir o reemplazar un nuevo equipo para evitar lentitud o perdida de las operaciones.			X		El control no está implementado
	A 12.1.4 SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.		SI	En el procedimiento CT-01 "Flujo de muestras para análisis en el laboratorio" se describe el ciclo de vida de la muestra y el tratamiento que se le da a esta, desde su recepción hasta la emisión del certificado, los analistas reciben muestras ciegas con el fin de preservar la confidencialidad de la información; igualmente la única persona encargada de firmar los certificados de análisis microbiológicos es la Jefe de microbiología.			X		El control cumple con el estándar y está Documentado
A 12.2 PROTECCION CONTRA CODIGOS MALICIOSOS	A.12.2.1 CONTROLES CONTRA CÓDIGOS MALICIOSOS	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	SI	El procedimiento CD-01I3 "Protección de la Información" incluye el numeral "7,4 Política de Antivirus" donde se describen los parámetros para el uso del antivirus y de las aplicaciones descargadas de internet ya sean licenciadas u open source. La organización cuenta con un antivirus licenciado en cada una de sus estaciones de trabajo, además realiza verificación semanal de las estaciones de trabajo con el fin de validar que el antivirus, Firewall y el Sistema Operativo se encuentre activado y actualizado. La organización posee un Firewall dedicado encargado de realizar un filtro y bloquear páginas no deseadas. El CPD se encuentra con una puerta bajo llave y posee una cámara de vigilancia.			X		El control cumple con el estándar y está Documentado
A 12.3 COPIAS DE	A 12.3.1 RESPALDO	Proteger contra	SI	El procedimiento CD-01I3 "Protección de la Información" incluye el numeral "7.1 Política			X		El control

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
RESPALDO	DE LA INFORMACIÓN	la pérdida de datos.		de Backup" donde se describe el procedimiento para respaldar la información de los equipos de cómputo.					cumple con el estándar y está Documentado
A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO DE EVENTOS	Registrar eventos y generar evidencia.	SI	se formalizará un documento de política de registro y protección de eventos (LOGS) donde se incluirá la manera como se registran, protegen y eliminan los registros de servidores, bases de datos y aplicaciones; además de quienes revisan o tienen acceso a dichos Logs.			X		El control no cumple con el estándar y debe ser rediseñado
	A12.4.1 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO		SI				X		El control no cumple con el estándar y debe ser rediseñado
	A12.4.1 REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR		SI	Se incluirá en la política de registro y protección de eventos (LOGS) un capítulo donde se detalle que los administradores no pueden borrar los logs del sistema, estos deben conservarse como evidencia de registro y deben ser respaldados periódicamente.			X		El control no cumple con el estándar y debe ser rediseñado
	A12.4.1 SINCRONIZACIÓN DE RELOJES		SI	El laboratorio tiene implementado y en funcionamiento el protocolo NTP (Network Time Protocol - Protocolo de Internet para sincronizar los relojes) de tal manera que se tienen sincronizados los relojes de los equipos en red con el directorio activo, este a su vez se encuentra sincronizado con el instituto nacional de metrología de Colombia (INM) el cual establece la hora legal para Colombia.			X		El control cumple con el estándar y está Documentado
A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DE SOFTWARE EN	Asegurarse de la integridad de los sistemas	SI	El laboratorio controla la instalación de software en las estaciones de trabajo por medio del directorio activo. Los cambios que se le realicen a algún sistema de información se detallan y controlan en el documento CD-01F1 "solicitud de documento"			X		El control cumple con el estándar y está

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	SISTEMAS OPERATIVOS	operacionales.							Documentado
A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	Prevenir el aprovechamiento de las vulnerabilidades técnicas.	SI	Antes de la instalación de un parche del sistema operativo se prueba en una máquina fuera del dominio y con la aplicación WSUS (Windows Server Update Services) se verifica que la actualización haya quedado instalada correctamente y después se libera en los demás equipos de la compañía. Para las actualizaciones de programas con desarrollo externo esta se desarrolla de acuerdo al contrato previamente establecido buscando preservar siempre que la actualización no afecte todo el sistema.			X		El control esta implementado pero no Documentado
	A 12.6.2 RESTRICCIÓN SOBRE LA INSTALACION DE SOFTWARE		SI	Por medio del directorio activo se gestionan los privilegios de los usuarios además de restringir la instalación de todo tipo de software no aprobado por la empresa, para el caso de software libre este debe estar aprobado por el departamento de sistemas. En la política de uso aceptable de activos incluida en el procedimiento SC-02M "Manual de seguridad de la información" se restringe la instalación de cualquier tipo de software en equipos o máquinas.			X		El control cumple con el estándar y está Documentado
A 12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	A 12.7 CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.	SI	Se incluirá en la política de registro y protección de eventos (LOGS) un capítulo donde se detalle que los usuarios no pueden borrar los rastros de auditoría (audit trails) ya que únicamente son de consulta para los usuarios autorizados.			X		El control no está implementado
A. 13 SEGURIDAD DE LAS COMUNICACIONES									

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A 13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	A 13.1.1 CONTROLES DE REDES	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	SI	En la política de control de acceso a la información incluida en el procedimiento SC-02M "Manual de seguridad de la información" se definen los controles utilizados para la red del laboratorio. Dentro de estos controles está el uso de Firewall para filtrado de red, privilegios de acceso a las carpeta de red, VLAN para separar el departamento de control de calidad del resto de la empresa. Se utilizaran herramientas para analizar y monitorear el tráfico de la red. Se evaluará la pertinencia de adoptar una herramienta de IDS (Sistema de Detección de Intrusos).			X		El control cumple con el estándar y está Documentado
	A 13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED		SI	El laboratorio tiene implementado un Firewall interno para controlar y filtrar tanto las conexiones como el tráfico de red. Por medio de su directorio activo controla los privilegios de los usuarios y el servidor posee diferentes carpetas a las cuales solo pueden acceder usuarios autorizados.			X		El control cumple con el estándar y está Documentado
	A 13.1.3 SEPARACIÓN EN LAS REDES		SI	Para los servicios de red de la compañía se cuenta con una VLAN (Redes Virtuales) separando El departamento de control de calidad del resto de la organización conectados al firewall interno para filtrar el acceso e impedir conexiones no autorizadas.			X		El control cumple con el estándar y está Documentado
A 13.2 TRANSFERENCIA DE INFORMACIÓN	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	SI	Se formalizará una política y un procedimiento para la transferencia de la información donde se describa el paso a paso para la entrega de la información a clientes y entes regulatorios. En el caso de certificados de análisis que son enviados por el mensajero de la compañía, estos deben ir en un sobre de carta sellado, con información del destinatario y del remitente y deben ser entregados únicamente al destinatario autorizado quien debe firmar un acta de entrega; el mensajero debe abstenerse de abrir los sobres en cualquier momento. En el caso de enviar un parcial del certificado de análisis por correo electrónico, este debe enviarse en formato pdf y con contraseña de		X	X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				acceso que corresponde a los últimos 3 dígitos del Nit del cliente. Se debe pedir confirmación de recibido del mensaje o comunicarse vía teléfono para asegurar la recepción del mensaje. Se incluirá la capacitación sobre la política y el procedimiento en el plan de capacitación anual.					
	A 13.2.2 ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN		SI	Se incluirá en los contratos de los clientes un acuerdo de transferencia de información detallando el paso a paso para la transferencia de información.		X	X		El control no cumple con el estándar y debe ser rediseñado
	A 13.2.3 MENSAJERIA ELECTRÓNICA		SI	En la política uso aceptable de activos incluida en el procedimiento SC-02M "Manual de seguridad de la información" se detalla el uso adecuado y las buenas prácticas para el uso del correo electrónico, además se detallan las consideraciones generales al uso del servicio de mensajería o IM dentro de la organización, por ejemplo: WhatsApp, Hangout, Line, Facebook Messenger, etc.		X	X		El control cumple con el estándar y está Documentado
	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN		SI	La organización cuenta con acuerdos de confidencialidad y no divulgación a través de los contratos firmados con clientes y prestadores de servicios, además existe un acuerdo de confidencialidad firmado por cada uno de los funcionarios de la organización el cual se encuentra anexo a su contrato de trabajo.		X	X		El control cumple con el estándar y está Documentado
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS									
A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA	Asegurar que la seguridad de la información sea una parte integral	SI	Antes de adquirir un software, la empresa define los requisitos específicos de seguridad de la información para implementar en la aplicación. Estos requisitos deben quedar por escrito y pueden estar conformados por: • Manejo de Audit Trails.			X		El control esta implementado pero no Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	INFORMACIÓN	de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.		• Cumplir con la 21CFR parte 11 en el caso de firmas electrónicas. • Usuarios y privilegios independientes (controles de acceso). • El sistema debe estar debidamente validado con el suficiente detalle de acuerdo a las Gamp5. • Se le deben aplicar y documentar todas las pruebas necesarias (IQ, OQ, PQ). • Se deben validar: los datos de entrada, el procesamiento interno, la autenticación de mensajes y los datos de salida. • El desarrollador debe utilizar herramientas licenciadas. • Incluir recomendaciones de la OWASP. Lo anterior se incluirá en la política de desarrollo seguro como las consideraciones para establecimiento de requisitos de seguridad.					
	A 14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS		SI	Se revisarán las recomendaciones de seguridad generadas por la OWASP (Proyecto Abierto de Seguridad de Aplicaciones Web) con relación a las buenas prácticas y vulnerabilidades encontradas. Dentro del proceso de revisión de OWASP se observaran los siguientes elementos: • Guía de Desarrollo. • Guía de revisión de código. • Guía de Pruebas de aplicaciones.			X		El control esta implementado pero no Documentado
	A 14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE		SI	Con el fin de proteger las transacciones electrónicas realizadas en el laboratorio, se creará un instructivo para la protección de las transacciones electrónicas, en el cual se describirá la forma adecuada para realizar este tipo de transacciones y como proteger los mecanismos de autenticación que se utilizan, por ejemplo:			X		El control no está implementado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	LAS APLICACIONES			• Utilizar solo tokens suministrador por la entidad bancaria. • Bloquear la estación de trabajo donde se realizan las transacciones. • Acceder solo a páginas HTTPS. • No dejar ningún elemento utilizado en las transacciones a la vista de personas ajenas.					
A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	SI	Se creará la política de desarrollo seguro (tanto interno como externo) de los sistemas de información para validar que las aplicaciones cumplan con los requerimientos contractuales y se encuentren desarrolladas de acuerdo a las buenas prácticas de seguridad de la información. Se asegurará también que todo software desarrollado (por un externo) cuente con un nivel de soporte adecuado para el laboratorio.			X		El control no cumple con el estándar y debe ser rediseñado
	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS		SI	Se incluirá dentro de la política de desarrollo seguro el procedimiento de control de cambios en los sistemas con el fin de minimizar los riesgos de alteración a los sistemas de información. Para ello se deben contemplar los siguientes controles a. Verificar que los cambios sean propuestos por usuarios autorizados y no comprometan la calidad de los procesos. b. Documentar los cambios realizados en el documento CD-01F1 "Solicitud de documentos". c. Solicitar la revisión por parte del responsable de Seguridad de la Información y el departamento de aseguramiento de calidad para garantizar que no se violen los			X		El control no cumple con el estándar y debe ser rediseñado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				requerimientos de seguridad que debe cumplir el software. d. Mantener un control de versiones para todas las actualizaciones de software.					
	A 14.2.3 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN		SI	Se incluirá en la política de desarrollo seguro las consideraciones para la revisión de las aplicaciones después de realizado algún cambio, además se incluirá en el contrato con el desarrollador externo las condiciones sobre las cuales se realizarán las actualizaciones o instalación de algún parche. Se revisarán y probaran las aplicaciones cuando se efectúen cambios para asegurar que no impacten adversamente en la seguridad o en el funcionamiento de la aplicación. Se debe garantizar que los cambios realizados por el desarrollador sean informados con antelación a la organización antes de implementarlos.			X		El control no cumple con el estándar y debe ser rediseñado
	A 14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE		SI	Se incluirá dentro de la política de desarrollo seguro las restricciones en los cambios de paquetes de software. Se incluirán las consideraciones para evitar que cualquier persona intente realizar un cambio no permitido a un software del laboratorio.			X		El control no cumple con el estándar y debe ser rediseñado
	A 14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS		SI	Se debe establecer requerimientos y controles de seguridad para el ciclo de vida del software de acuerdo a las recomendaciones realizadas por la OWASP en su guía de desarrollo seguro, definiendo requisitos acuerdo a las fases del ciclo de vida: • Fase de requerimientos (Control de autenticación, control de roles y privilegios, requerimientos orientados al riesgo y aprobación de privilegios). • Fase de Análisis y diseño (Acceso a componentes, Pistas de auditoría, Gestión de sesiones, datos históricos, manejo apropiado de errores, separación de			X		El control no cumple con el estándar y debe ser rediseñado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				funciones). • Fase de Implementación y codificación (Aseguramiento del ambiente de desarrollo, elaboración de documentación técnica, codificación segura). • Fase de pruebas (Inspección del código por fases, caja negra (Guía de pruebas OWASP)). • Fase de mantenimiento (Pruebas de seguridad después de los cambios). Estos requerimientos deben incluirse en el contrato con el desarrollador externo y deben quedar documentados para el laboratorio.					
	A 14.2.6 AMBIENTE DE DESARROLLO SEGURO		SI	En el procedimiento SC-02M "Manual de seguridad de la información" se encuentra incluido la política de backup que aplica para todos los equipos computacionales o sistemas computarizados de la empresa. Con el fin de proteger el ambiente de desarrollo se programa un backup en la máquina que contenga la base de datos del software.			X		El control no cumple con el estándar y debe ser rediseñado
	A 14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE		SI	Para el caso del desarrollo de software contratado externamente se establecerán siguientes normas: a. Acuerdos de licencias, propiedad de código y derechos de Propiedad Intelectual. b. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías. c. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software			X		El control esta implementado pero no Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013										
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
				establecidos.					
	A 14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS		SI	Solicitar la autorización para contratar un análisis de código fuente a las aplicaciones desarrolladas por terceros. Si el desarrollador realiza las pruebas este deberá documentarlas con el suficiente detalle y suministrarlas al laboratorio.			X		El control no cumple con el estándar y debe ser rediseñado
	A 14.2.9 PRUEBA DE ACEPTACIÓN DE SISTEMAS		SI	Antes de liberar una actualización o un módulo de desarrollo se deberán realizar pruebas de aceptación con la persona que género el requerimiento para validar que lo desarrollado era lo esperado y se comporta de acuerdo a lo solicitado. Estas pruebas las ejecutará el desarrollador externo habilitando únicamente el requerimiento en el módulo del usuario que lo necesitaba antes de habilitarlo en todo el sistema.			X		El control no está implementado
A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	Asegurar la protección de los datos usados para pruebas.	SI	Se deben generar copias de seguridad de los datos usados en prueba para reproducir resultados y validar eventos de aceptación.			X		El control no cumple con el estándar y debe ser rediseñado
A.15 RELACIONES CON LOS PROVEEDORES									
A. 15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	A 15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	SI	En el procedimiento SC-02M "Manual de seguridad de la información" se encuentra incluida la política de seguridad para proveedor la cual define los lineamientos de seguridad de la información para las relaciones con los proveedores.		X	X		El control cumple con el estándar y está Documentado
	A 15.1.2 TRATAMIENTO DE		SI	Se debe crear una cláusula de seguridad de la información para proveedores anexa a los contratos, además de divulgar y aplicar la política de seguridad para proveedores		X	X		El control no cumple con el

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES			incluida en el procedimiento SC-02M "Manual de seguridad de la información"					estándar y debe ser rediseñado
	A 15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN		SI	El departamento de ingeniería desarrollará un listado actualizado de los proveedores de tecnología, maquinaria y comunicaciones para los equipos críticos de la organización, este listado posee 2 contactos por equipo.		X	X		El control esta implementado pero no Documentado
A 15.2 GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	A 15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	SI	El laboratorio realiza seguimientos y auditoría a proveedores para revisar los servicios prestados contra lo recibido, esto se realiza de acuerdo a los procedimientos: • AU-01G1 "Guía de auditoría a proveedores de Materias Primas" • AU-01G2 "Guía de auditoría a proveedores de servicios" • AU-01G3 "Guía de auditoría a proveedores de insumos " Se incluirán criterios de seguridad de la información para la auditoria a proveedores (Tratamiento de la información).		X	X		El control no cumple con el estándar y debe ser rediseñado
	A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES		SI	Se debe incluir en los contratos de los proveedores una cláusula para la gestión de cambios, ya que todo cambio que el proveedor vaya a realizar debe dar aviso por anticipado.		X	X		El control no cumple con el estándar y debe ser rediseñado
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION									

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
A 16.1 GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	SI	El laboratorio implementará un procedimiento para la gestión de incidentes estableciendo responsabilidades para registrar, atender y analizar los eventos relacionados con seguridad de la información.			X		El control esta implementado pero no Documentado
	A 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN		SI	El laboratorio estableció como canal de comunicación para reportar eventos y debilidades (vulnerabilidades) de seguridad de la información el correo electrónico; además de sensibilizar a todo el personal para que reporten cualquier incidente de seguridad.			X		El control esta implementado pero no Documentado
	A 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN		SI				X		El control esta implementado pero no Documentado
	A 16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS		SI	Con el fin de evaluar los eventos de seguridad de la información reportados por los usuarios, se realizará la propuesta de adquirir una herramienta de apoyo a los servicios de tecnología (mesa de ayuda o helpdesk) la cual funcione como un repositorio para el registro y evaluación de eventos de seguridad de la información.			X		El control esta implementado pero no Documentado
	A 16.1.5 RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN		SI	En el procedimiento de gestión de incidentes se describirá la forma para dar respuesta a un incidente de seguridad de la información, responsables, herramientas que se pueden utilizar y cómo actuar en el momento que el riesgo se materializó.			X		El control esta implementado pero no Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	A 16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		SI	Con el fin de obtener un aprendizaje de los incidentes de seguridad de la información se realizarán sensibilizaciones por medio de capacitaciones de los casos más relevantes, esta sensibilización se incluirá en el PE-01F2 "Cronograma de capacitación al personal". El laboratorio implementará en su herramienta de mesa de ayuda un KDBM (Knowledge Data Base Management) – Base de datos de conocimiento donde se registra el aprendizaje obtenido de los incidentes de seguridad de la información y así reducir la posibilidad o el impacto de incidentes futuros.			X		El control esta implementado pero no Documentado
	A 16.1.7 RECOLECCIÓN DE EVIDENCIA		SI	Se incluirá en el procedimiento de gestión de incidentes las consideraciones sobre las cuales la empresa aplicará la informática forense para la recolección de evidencia (por ejemplo herramientas de informática forense como CAIN, autopsy, etc.).			X		El control esta implementado pero no Documentado
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO									
A 17.1 CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	SI	Se formulará un proyecto de continuidad de negocios con énfasis en aspectos de seguridad de la información, basado en la Norma ISO 22301:2012 "Continuidad de Negocio" sobre los procesos cubiertos por el alcance en caso de un evento catastrófico. Se diseñara un cronograma de implementación para el proyecto de continuidad y las personas responsables en su desarrollo.			X		El control no cumple con el estándar y debe ser rediseñado
	A 17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN		SI				X		El control no cumple con el estándar y debe ser rediseñado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN		SI	La organización verificará a intervalos regulares de tiempo los controles de continuidad de la seguridad de la información que se hayan establecido e implementado, con el fin de asegurar su validez y eficacia frente a situaciones adversas. Estos controles se definirán en el proyecto de continuidad de negocios.			X		El control no cumple con el estándar y debe ser rediseñado
A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	SI	Se incluirá en el plan de contingencia alternativas para ofrecer continuidad de los servicios de Seguridad de la Información en caso de materializarse un evento catastrófico sobre los procesos incluidos en el alcance del SGSI, por ejemplo: instalaciones alternas.			X		El control no cumple con el estándar y debe ser rediseñado
A. 18 CUMPLIMIENTO									
A 18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de	SI	Se incluirá dentro de la matriz de requisitos legales de SGSST (Sistema de Gestión de Seguridad y Salud en el Trabajo) los requisitos legales aplicables a seguridad de la información; además se evaluará con cada una de las personas responsables de los sistemas de gestión para construir una matriz integral.	X		X		El control esta implementado pero no Documentado
	A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL		SI	En el numeral "7.2.1. Procedimiento de confidencialidad" incluido en el procedimiento CD-01I3 "Protección de la Información" se define que la propiedad intelectual (marcas, licencias, material fotográfico, formulas, artes, etc.) desarrollada o concebida mientras el funcionario se encuentre en el sitio de trabajo, es propiedad exclusiva de LABORATORIOS	X		X		El control cumple con el estándar y está Documentado

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
		cualquier requisito de seguridad.		SFC LTDA.					
	A 18.1.3 PROTECCIÓN DE REGISTROS		SI	Se creará el procedimiento de protección de registros donde se definan los lineamientos para la protección de registros (físicos y electrónicos) contra pérdida, falsificación, destrucción, accesos no autorizados, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X	X	X		El control no está implementado
	A 18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES		SI	En el procedimiento CD-01I1 "Política de tratamiento de datos personales" se definen los lineamientos para la protección y tratamiento de los datos personales.	X	X	X		El control cumple con el estándar y está Documentado
	A 18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS		SI	Se detallará en la Política sobre el uso de controles criptográficos, que estos deben cumplir con los todos los acuerdos, legislación y reglamentación pertinentes.	X		X		El control no está implementado
A 18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	SI	Se solicitará formalmente a la dirección de aseguramiento de calidad que se incluya como un criterio de auditoría el SGSI y que esto se plasme en el plan de revisión y auditorías del siguiente año como una revisión de sistemas integrados. Las auditorías se realizan de acuerdo a los siguientes procedimientos: • AU-01 "Auditorías de calidad y autoinspecciones" • AU-01G6 "Guía de auditoría interna al SGSI 27001: 2013" • AU-01A1 "Cronograma y registro de auditorías internas y autoinspecciones" • AU-01F1 "Reporte de resultados de Auditorías y autoinspecciones "			X		El control no cumple con el estándar y debe ser rediseñado
	A 18.2.2		SI	El analista de sistemas en conjunto con los jefes de las áreas relacionados en el alcance			X		El control esta

DECLARACIÓN DE APLICABILIDAD SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NTC-ISO-IEC 27001:2013									
OBJETIVOS DE CONTROL	**CONTROLES**	**OBJETIVOS**	**APLICABILIDAD (SÍ/NO)**	**JUSTIFICACIÓN DE ELECCIÓN / NO ELECCIÓN**	**Razones para la selección de controles**				**ESTADO**
					L	**C**	**N**	**R**	
	CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD			del SGSI se encargarán de verificar constantemente la aplicación de las políticas de seguridad de la información, valorando los riesgos y oportunidades con el fin de reducir efectos indeseados en los procesos. En conjunto con el departamento de aseguramiento de calidad implementa planes de acción para cerrar las No Conformidades.					implementado pero no Documentado
	A 18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO		SI	La persona encargada del SGSI en conjunto con el departamento de aseguramiento de calidad revisaran periódicamente el SGSI para determinar el cumplimiento de las políticas de seguridad de la información; igualmente se conservará evidencia del acta de reunión.			X		El control esta implementado pero no Documentado

Fuente: El Autor.

Fecha de Elaboración: 161104 Fecha de Actualización: 171104

RESUMEN ANALITICO EDUCATIVO
RAE

Título del texto	DISEÑO DE UN SGSI (SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION) BASADO EN ISO27001 PARA LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.
Nombres y Apellidos del Autor	RODRIGUEZ CORREA, Jorge Leonardo
Año de la publicación	2017

Resumen del texto:

El diseño de un SGSI en LABORATORIOS SFC LTDA implica una labor de compromiso por parte de la alta dirección, ya que es esta quien se encarga de aprobarla y proveer todos los recursos necesarios para su desarrollo, mantenimiento y mejora continua.

La metodología empleada para el diseño del SGSI fue el ciclo PHVA (Planear – Hacer – Verificar - Actuar), un enfoque basado en procesos el cual permite establecer, implementar, operar, hacer seguimiento, mantener y mejorar un sistema de gestión.

Palabras Claves	Vulnerabilidades, , diseñar, amenazas, SGSI, Laboratorios SFC LTDA, políticas, seguridad de la información, sistema de gestión, PHVA, riesgos, planear, salvaguardas, activos, confidencialidad, integridad, disponibilidad, sistema de gestión de seguridad de la información.

Problema que aborda el texto:

¿De qué manera un enfoque basado en procesos permite diseñar el SGSI (Sistema de Gestión de Seguridad de la Información) para garantizar la confidencialidad, integridad y disponibilidad de la información en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA?

Objetivos del texto:

- Clasificar los activos informáticos existentes en la empresa LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.
- Realizar un análisis de las vulnerabilidades, amenazas y riesgos presentes en la organización con el fin de seleccionar las salvaguardas más adecuadas que ayuden a reducir los riesgos detectados.
- Determinar los controles existentes de acuerdo a la norma ISO/IEC 27001 e ISO/IEC 27002.
- Elaborar un manual para la implementación del SGSI en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.

Hipótesis planteada por el autor:

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO27001 mediante el Ciclo PHVA que permita preservar la integridad, confidencialidad y disponibilidad de la información en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA – SFC

Tesis principal del autor:

Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) Basado en ISO27001 para Laboratorios Servicios Farmacéuticos de Calidad SFC LTDA.

Argumentos expuestos por el autor:

LABORATORIOS SFC LTDA es un laboratorio farmacéutico veterinario que presta los servicios de maquila, análisis fisicoquímico, análisis microbiológico y validación de productos, la información que se maneja es de carácter confidencial pero aun así no posee el nivel adecuado de seguridad y procedimientos definidos que garanticen la confidencialidad de la misma. La información confidencial como certificados de análisis microbiológicos o procedimientos se encuentran en un estado crítico, ya que su protección es mínima y los riesgos a los que están expuestos no se han identificado claramente. Al no contar con un sistema o procedimientos claros y definidos que permitan articular adecuadamente los procedimientos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información, se hace necesario el diseño de un SGSI (sistema de gestión de seguridad de la información) para proteger, minimizar los riesgos y darle el tratamiento adecuado a la información que posee la organización.

Como objetivo principal se busca Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO27001 mediante el Ciclo PHVA que permita preservar la integridad, confidencialidad y disponibilidad de la información en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD LTDA – SFC. Adicional a esto se busca cumplir los siguientes objetivos específicos:

- Clasificar los activos informáticos existentes en la empresa LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.
- Realizar un análisis de las vulnerabilidades, amenazas y riesgos presentes en la organización con el fin de seleccionar las salvaguardas más adecuadas que ayuden a reducir los riesgos detectados.
- Determinar los controles existentes de acuerdo a la norma ISO/IEC 27001 e ISO/IEC 27002.
- Elaborar un manual para la implementación del SGSI en LABORATORIOS SERVICIOS FARMACEUTICOS DE CALIDAD SFC LTDA.

El diseño metodológico adoptado para el diseño del SGSI en LABORATORIOS SFC LTDA está basado en el ciclo PHVA de la Norma ISO27001:2013 en la cual se contextualiza cada uno de sus ciclos y como se desarrollan. Para realizar el análisis de riesgos se utiliza la metodología MAGERIT, la cual permite determinar las medidas apropiadas para cuantificar y dar el tratamiento adecuado a los activos que posee la empresa.

Se llevaron a cabo al interior de la organización las siguientes actividades:

- Diagnóstico inicial para determinar el nivel de madurez de la organización, respecto a la seguridad de la información.
- Encuesta a los jefes de áreas para determinar las áreas más críticas de la organización.
- Identificación y valoración de activos.
- Identificación y valoración de riesgos (Metodología MAGERIT).
- Declaración de aplicabilidad.
- Desarrollo de políticas y procedimientos de seguridad de la información.
- Desarrollo de una metodología de análisis y gestión de riesgos enfocada en seguridad de la información.
- Desarrollo del manual de seguridad de la información.
- Para el desarrollo de cada una de las actividades del proyecto se utilizaron diferentes métodos como entrevistas, documentación física y electrónica, asesorías, etc.

El Manual de Seguridad de la Información (SC – 02M "Manual de seguridad de la información") se encuentra basado en la Norma ISO/IEC 27001:2013 y dentro del cual se presentan las siguientes políticas:

- Uso aceptable de los activos.
- Control de acceso a la información.
- Procedimientos operativos para gestión de TI.
- Política de seguridad para proveedores.
- Política para gestión de incidentes.
- Política de construcción de los sistemas seguros.
- Política de continuidad del negocio.

Conclusiones del texto:

LABORATORIOS SFC LTDA es una empresa con alto nivel de competitividad en el mercado farmacéutico veterinario, el establecimiento de la política de seguridad de la información permitió generar en su personal una visión más global y asertiva en términos de seguridad de la información, además el apoyo y aprobación por parte de la alta gerencia demuestra el compromiso que tiene la organización con el manejo y tratamiento de información de clientes y todas las terceras partes que buscan que su información sea tratada dentro de estándares seguros.

El análisis y determinación de riesgos, amenazas y vulnerabilidades es una labor necesaria dentro de toda organización ya que permite conocer todos los riesgos y amenazas a las que se encuentra expuesta una empresa, esto con el fin de mitigarlas o eliminarlas para que no afecten en consideración el proceso de negocio.

Bibliografía citada por el autor:

Areiza, B, Rincón, L. (2005). Hacia un Modelo de Madurez para la Seguridad de la Información. Valparaíso, Chile. Recuperado de http://cibsi05.inf.utfsm.cl/presentaciones/sesion10/Modelo_de_madurez_SI.pdf

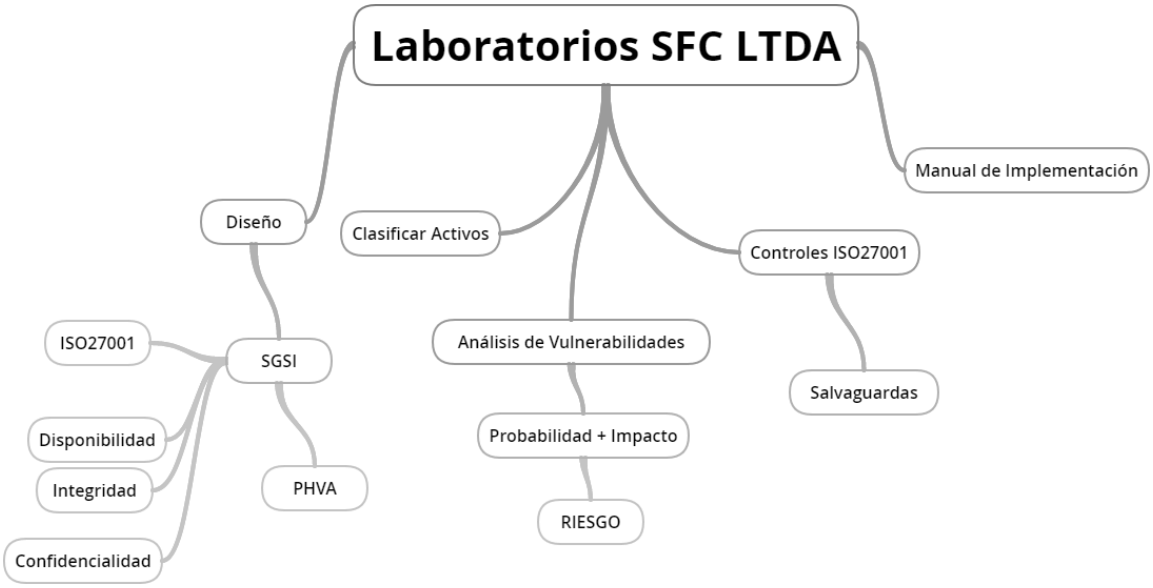
Hernández R., Fernández C., Baptista P. (2006). Metodología de la investigación. Cuarta Edición, McGraw Hill. México.

ICONTEC. (2006). Norma técnica NTC-ISO/IEC colombiana 27001. Recuperado de http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

INEI. (2001). Guía práctica para el desarrollo de planes de contingencia de sistemas de información. Recuperado de http://www.ongei.gob.pe/seguridad/seguridad2_archivos/lib5131/libro.pdf

Nombre y apellidos de quien elaboró este RAE	Jorge Leonardo Rodriguez Correa
Fecha en que se elaboró este RAE	20/07/2017

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:



Comentarios finales:

Una vez se inició la aplicación de los controles, se concluye que aún falta mucho por hacer, sin embargo la organización se ha integrado en un proceso de cambio y mejoramiento continuo de la seguridad de la información. Se recomienda revisar las políticas de seguridad y los controles a intervalos planificados de por lo menos una vez al año, con el fin de mantener actualizado el sistema de gestión y cada una de sus políticas y procedimientos.