|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Generalidades del programa** | | | | | | | | |
| Programa No. | 1 | Duración: | Septiembre 2018 – Agosto 2019 | | | No. de Auditorías | | 4 |
| Objetivos: | Vigilar y mejorar los sistemas de información de la organización.  — Contribuir con la mejora del sistema de gestión y su desempeño.  — Obtener y mantener confianza en la capacidad de los empleados.  — Determinar la efectividad del sistema informático.  — Evaluar la compatibilidad y alineación de los objetivos del sistema de información con las políticas y objetivos generales de la organización. | | | | | | | |
| Alcance: | Aplica para todos los procesos relacionados con los sistemas de información existentes en la organización. | | | | | | | |
| Tipo de auditorías: | Según su forma | | | | Según su alcance | | | |
| Únicas: | | | X | Internas o de primera parte: | | X | |
| Combinadas: | | |  | Externas o de segunda parte: | |  | |
| Conjuntas: | | |  | Externas de certificación o de tercera parte: | |  | |

|  |
| --- |
| **Especificaciones del programa de auditorías** |
| Procedimiento del programa de auditoría:  Conforme a los procedimientos documentados en la norma ISO 19011 en su edición 2011  Criterios de auditoría:  Los criterios que se van a tomar en cuenta para la auditoria se tomaron del plan de políticas informáticas.   1. Asignación y uso de recursos:    1. Personal con usuarios y contraseñas para los equipos de cómputo.    2. Uso de internet con fines laborales.    3. Reportes de fallas en los equipos. 2. Seguridad de la información.    1. Respaldos de las bases de datos cada 12 horas.    2. Sesiones de Windows y del sistema “StorePhone Doctor: Point of Sale” con contraseñas.    3. Registros de escaneos mensuales en los equipos informáticos en busca de virus.    4. Accesos a los puertos USB, CD o Diskettes deshabilitados.    5. Reportes de fallas. 3. Mantenimiento y buen uso de la infraestructura.    1. Equipos con las actualizaciones más recientes.    2. Uso de los equipos únicamente para el personal. Revisión de permisos para equipo de uso personal.    3. Evidencia de que el software instalado sea únicamente el autorizado por el área de sistemas.    4. Registros y respaldos y su correspondiente documentación. 4. Control general organizativo.    1. Personal que tenga conocimiento del código de ética y conducta y lo aplique en sus labores diarias.    2. Personal que tenga conocimiento del reglamento y de las consecuencias que implica el caso omiso a este.    3. Reportes mensuales del comportamiento del personal.   Métodos de auditoría:  En fase de planificación  En sitio sin interacción humana  Revisión de la información documentada (1.3, 2.5, 3.4, 4).  Observación del trabajo realizado. (1.2, 2.3, 2.4, 4)  Completar listas de verificación. (1.1, 2.2, 2.5, 3.1, 3.4)  Muestreo (Funcionamiento del sistema).  En fase de realización  En sitio con interacción humana  Completar listas de verificación y cuestionarios con la participación del auditado. (1, 2, 3, 4)  Revisión documental con participación del auditado. (1,2,3, 4)  El equipo auditor, auditado, observadores y expertos técnicos se sujetarán a los procesos para manejo de confidencialidad, seguridad de la información, salud y seguridad definidos por StorePhone Doctor. |

# Equipos de auditores internos

La selección, formación, evaluación y mejora de las competencias de los auditores internos de StorePhone Doctor se llevará a cabo tal y como lo específica el método documentado ISO 19011:2011 (E).

Equipos de auditores disponibles para el presente programa.

|  |  |  |
| --- | --- | --- |
| **Equipo A** | **Equipo B** | **Equipo C** |
| Auditor Líder del equipo:  Juan Pablo Duran Rendón | Auditor Líder del equipo:  Luis Norberto Paloma Rodriguez | Auditor Líder del equipo:  Juan Pablo Duran Rendón |
| Auditor(es):  1. Isaías Manuel Aranda Leal | Auditor(es):  1. Mayra Patricia Pérez Martínez | Auditor(es):  1. Isaías Manuel Aranda Leal |
| Experto Técnico (s):  1. Juan Pablo Duran Rendón | Experto Técnico (s):  1. Juan Pablo Duran Rendón | Experto Técnico (s):  1. Juan Pablo Duran Rendón |
| Observador(es):  1. María del Carmen Islas López | Observador(es):  1. María del Carmen Islas López | Observador(es):  1. María del Carmen Islas López |

# Cronograma de auditorías internas

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Requisitos/Proceso/Actividad** | **Criterios** | **Equipo auditor** |  |  |  |  |  | **Mes** | |  |  | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| 1 | Sistema de Gestión de Calidad | ISO 9011:15 | A |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Reclutamiento y Selección de Personal | ISO 9011:15 | A |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Asignación y uso de recursos | 1.1, 1.2, 1.3 | A |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Seguridad de la información | 2.1, 2.2, 2.3, 2.4, 2.5 | A |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Mantenimiento y buen uso de la infraestructura | 3.1, 3.2, 3.3, 3.4 | A |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Control general organizativo | 4.1, 4.2, 4.3 | A |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# Riesgos del programa

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | **Impacto** | | |  |
|  | **Probabilidad** | | **Alto** | | **Mediano** | | **Bajo** |
| **Alta** | | Extrema | | Alta | | Mediana |
| **Mediana** | | Alta | | Mediana | | Baja |
| **Baja** | | Mediana | | Baja | | Mínima |
| **Riesgos** | | **Probabilidad** | | **Impacto** | **Calificación del riesgo** | **Acción para mitigar riesgo** | | |
| **Riesgos de planeación** | | | | |  | | | |
| Falla para establecer objetivos de auditoría relevantes y para determinar el alcance del programa de auditoría. | | Baja | | Alto | Baja | Verificar la relevancia de los objetivos establecidos en el programa de la auditoria así como si estos se encuentran dentro del alcance establecido. | | |
| **Riesgos de recursos** | | | | |  | | | |
| No permitir tiempo suficiente para desarrollar el programa de auditoría o para llevarlas a cabo | | Mediana | | Alto | Alto | Hacer una verificación de la disponibilidad de tiempo de los equipos y la organización para acoplar el cronograma y de este modo, cumplir con el programa de auditoria en tiempo y forma. | | |
| **Riesgos de selección del equipo auditor** | | | | |  | | | |
| El equipo no tiene la competencia colectiva para llevar a cabo auditorías de manera efectiva | | Baja | | Alto | Mediano | Capacitar al personal para el desarrollo de las competencias requeridas para llevar a cabo auditorias de manera efectiva. | | |
| **Riesgos de implementación** | | | | |  | | | |
| Comunicación inefectiva del programa de auditoría | | Baja | | Mediano | Baja | Crear una comunicación efectiva del programa de auditoria. | | |
| **Riesgos de los registros y su control** | | | | |  | | | |
| Falla para proteger adecuadamente los registros de auditoría  que demuestren la efectividad del programa de auditoría | | Mediana | | Mediano | Mediana | Establecer un sistema que proteja adecuadamente el programa de auditoria ante los posibles riesgos. | | |
| **Riesgos del monitoreo, revisión y mejora del programa de auditoría** | | | | | | | | | |
| Monitoreo inefectivo de los resultados del programa de auditoría | | Mediana | | Mediano | Mediana | Establecer un sistema con el que se puedan monitorear y verificar los resultados del programa de auditoría. | | | |

# Recursos del programa

El objetivo de determinar los recursos del programa anual de auditorías internas es clarificar qué recursos se necesitan y qué costos tendrá.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Recurso** | **Tipo** | **Con quién gestionarlo** | **Presupuesto** |
| 1 | Norma ISO 19011:2011 | Formativo |  | $ 99 usd |
| 2 | Curso de capacitación auditor interno | Formativo |  | $ 166 usd |
| 3 | Curso de capacitación auditor líder | Formativo |  | $ 790 usd |

# Revisión y aprobación

|  |  |  |
| --- | --- | --- |
| **ELABORÓ** | **REVISÓ** | **APROBÓ** |
| Luis Norberto Paloma Rodríguez & Mayra Patricia Pérez Martínez  Colaboradores en  StorePhone Doctor  30/07/2018 | María del Carmen Islas López  Supervisora Externa  01/08/2018 | María del Carmen Islas López  Supervisora Externa  01/08/2018 |