#### PROCEDIMIENTO DE AUDITORIA INTERNA

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Autor** | **Descripción** |
| 0.1 | XXXXXXX | XXXXXXX | Borrador inicial |
| 1.0 | XXXXXXX | XXXXXXX | Actualizado y modificado para seguir la misma línea del certificado global y el SGSI. |
| 1.1 | XXXXXXX | XXXXXXX | Propiedad modificada del documento y aprobadores para reflejar los cambios en el Manual SGSI |
| 1.2 | XXXXXXX | XXXXXXX | Revision anual |
| 1.3 | XXXXXXX | XXXXXXX | Actualización. |
| 1.4 | XXXXXXX | XXXXXXX | Revision |

Analizar y establecer los requisitos externos especificados para cumplir con las metas y objetivos de la COMPAÑIA en relación con su postura de gestión de la seguridad de la información.

1.2 Asegurar que las deficiencias y mejoras al SGSI se identifiquen claramente y cuando sea necesario: de acuerdo con las acciones correctivas requeridas, implementadas y consideradas adecuadas para lograr los objetivos del SGSI y se realiza como parte de un proceso de auditoría interna independiente para asegurar segregación razonable de los derechos.

###### Alcance

* 1. Este procedimiento es específico para todas las ubicaciones definidas por el alcance de dicho SGSI e incluye: planificación, ejecución, notificación y requisitos de seguimiento como parte de la auditoría interna del SGSI y se aplica a todos los departamentos y servicios definidos como dentro del alcance del SGSI.

###### Responsabilidades de Auditoría Interna

* 1. Representante de Gestión de la Seguridad de la Información (ISMR)
     + Nombra al Auditor Principal y al Equipo de Auditoría (El Equipo de Auditoría). El Auditor Principal también puede ser el ISMR.
     + El Equipo de Auditoría revisa las acciones Correctivas y Preventivas para dicho lugar y las auditorías de seguimiento realizadas sobre la base del informe de auditoría interna presentado.
     + Mantiene la confidencialidad de los resultados de la auditoría.
  2. Auditor principal
     + Prepara un Plan de Auditoría / Notificación como base para la planificación de la auditoría y para la difusión de información sobre la auditoría.
     + Preside las actividades de auditoría interna.
     + Coordina el cronograma de auditoría con los jefes de departamento / sección interesados.
     + Planifica la auditoría, prepara los documentos de trabajo e informa al equipo de auditoría.
     + Consolidar todos los hallazgos y observaciones de auditoría y preparar el informe de auditoría interna.
     + Reporta inmediatamente las no conformidades críticas a la parte auditada.
     + Informar a la parte auditada, los resultados de la auditoría de forma clara y sin demora
     + Realiza la reunión de apertura y cierre. 3.3 Equipo de auditoría
     + Apoya las actividades del Auditor Líder.
     + Realiza la auditoría utilizando la lista de comprobación de auditoría consolidada.
     + Reporta las no conformidades y recomienda sugerencias para mejorar.
     + Mantiene la confidencialidad de los hallazgos de la auditoría.
     + Actuar de manera ética en todo momento. 3.4 Parte auditada
     + Recibe el informe de auditoría y determina, así como inicia el seguimiento requerido de la (s) acción (es) correctiva (s).

###### 4.0 Procedimiento de auditoría 4.1 General

* + 1. Se debe mantener un programa de auditoría que refleje todas las auditorías programadas y planeadas para el año calendario de auditoría. Esto incluirá un cronograma de auditorías internas, auditorías realizadas a proveedores, auditoría a realizar por clientes y auditorías de terceros, cuando corresponda.
    2. Cada lugar sujeto al SGSI de la COMPAÑIA estará sujeto a una auditoría interna anual. Pueden realizarse auditorías adicionales si un lugar en particular tiene un gran número de conclusiones en su contra.
    3. Los auditores deben ser independientes de la ubicación en la que están obligados a realizar la auditoría, ya que no tienen obligación de rendir cuentas al centro sujeto a la auditoría.
    4. Como se menciona en la Sección 3.1, todos los miembros del Equipo de Auditoría Interna serán nombrados por el ISMR.
    5. El Auditor Principal supervisará la actividad del Equipo de Auditoría.
    6. Se enviará un Memo de Notificación de Auditoría a la ubicación / departamento / sección para ser auditado por lo menos tres (5) días hábiles antes de la auditoría.

###### Planificación y preparación de la auditoría

* + 1. El auditor principal elaborará un documento anual del programa de auditoría y será aprobado por el responsable del programa del SGSI y estará sujeto a revisión de acuerdo con los cambios en el calendario.
    2. A partir de este programa de auditoría, el Auditor Líder preparará los respectivos planes de auditoría.
    3. El Auditor de Cuentas / Notificación deberá ser preparado por el Auditor Líder, revisado y aprobado por el ISMR. Se comunicará a los auditores ya la parte auditada. Se diseñará para ser flexible con el fin de permitir cambios basados en la información recogida durante la auditoría. El plan incluirá:
* Objetivo y alcance de la auditoría
* Departamento / Sección y responsables.
* Miembros del equipo de auditoría. El número de auditores depende del tamaño del área de auditoría.
* Tipo de sistema de gestión a auditar
* Fecha, lugar, hora de la auditoría y fecha de distribución del informe de auditoría

###### Reunión previa a la auditoría

* + 1. La reunión previa a la auditoría entre el ISMR, el auditor principal y los auditores se llevará a cabo a más tardar un día antes de la auditoría propiamente dicha. Los objetivos son los siguientes:
* Asegurar la disponibilidad de todos los recursos necesarios y otra logística que pueda requerir el auditor.
* El alcance de la auditoría se verifica en el Plan de Auditoría

###### Reunión de apertura

* + 1. La reunión de apertura, cuando lo considere apropiado el ISMR y el auditor principal, se celebrará el día de la auditoría, pero antes de la auditoría propiamente dicha. Durante la reunión de apertura se discutirá lo siguiente:
* El propósito y alcance de la auditoría.
* Confirmación del plan de auditoría
* Es necesario aclarar otros asuntos antes de que se realice la auditoría

###### Ejecución de auditoría

* + 1. Los auditores realizarán la auditoría interna utilizando varias listas de verificación que se describen a continuación:
       - Lista de Verificación de Auditoría Interna / Formulario de Observación- contiene elementos específicos que son específicos de la unidad organizacional a ser auditada. Los auditores asignados son responsables de generar preguntas usando este formulario.
       - La Lista de Verificación de Requisitos del Sistema contiene elementos relacionados con los requisitos de ISO 27001: 2013
       - Lista de verificación de los requisitos de control - contienen elementos relacionados con los controles que se encuentran en el Apéndice A de la Norma ISO 27001: 2013.
       - Los resultados de la auditoría se recogen a través de entrevistas, examen de documentos y observación de actividades y condiciones en las áreas de preocupación y se escribirán en las listas de verificación mencionadas anteriormente.
       - Evidencias que sugieren no conformidades deben ser anotadas sí parecen significativas, aunque no estén cubiertas por la lista de verificación. Otras indicaciones y/u observaciones objetivas que puedan reflejarse positivamente o negativamente en el sistema de gestión de la seguridad de la información también se enumerarán en el espacio previsto en las listas de verificación antes mencionadas.