GUÍA DE AUDITORÍA PARA DIAGNOSTICAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO: IEC 27001:2013

Arias Torres José Edvin
ing.edwin.arias@gmail.com
Universidad Piloto de Colombia

RESUMEN- Se determinó la creación de una guía de auditoría para evaluar el sistema de gestión de seguridad de la información con el apoyo de las directrices del anexo "A" de la norma ISO/IEC 27001:2013 y adicionalmente se crearon otros temas de evaluación con la finalidad de mitigar sus diferentes riesgos.

Para todos los temas a evaluar se sugiere ejecutar pruebas para evidenciar que se encuentren de acuerdo con los lineamientos internos.

Para la evaluación de la documentación del SGSI se precisa la solicitud del manual del sistema, políticas, procedimientos, formatos, entre otros, para los temas de riesgo, incidentes, pruebas de vulnerabilidad y clasificación de la información se requiere la metodología usada, la documentación de las capacitaciones realizadas y la herramienta utilizada.

Adicionalmente se sugiere un esquema de evaluación independiente por tema y adicionalmente una calificación global del SGSI.

ABSTRACT- The creation of an audit guide was determined to evaluate the management system of information security with the support of the guidelines in Annex "A" of ISO / IEC 27001: 2013 and additionally other assessment issues were created with in order to mitigate different risks.

For all subjects to evaluate suggested run tests to show that they are in accordance with the internal guidelines.

For the evaluation of the documentation ISMS application of the system manual, policies, procedures, formats are required, inter alia, for risk issues, incidents, vulnerability testing and information classification methodology used is required, documentation of training conducted and the tool used.

In addition, an independent evaluation scheme by subject and further an overall rating of ISMS is suggested.

PALABRAS CLAVE- auditoría, controles, políticas, vulnerabilidades.

1 INTRODUCCIÓN

El presente artículo tiene como objetivo sugerir un programa de auditoría para evaluar el estado del sistema de gestión de seguridad de la información con los lineamientos de la norma ISO/IEC 27001:2013 (anexo "A"), adicionalmente se agregaron otros temas sensibles para abarcar adecuadamente los cumplimientos regulatorios y acoger las buenas prácticas para fortalecer el control interno de la organización.

Posterior a la evaluación de la documentación (directrices, políticas, procesos, procedimientos, formatos, guías, entre otros) del sistema, el artículo sugiere ejecutar pruebas para verificar el cumplimiento de los lineamientos internos.

Se establece que se debe verificar las herramientas y metodologías utilizadas para cada tema diagnosticado, para la gestión de riesgos se sugiere diagnosticar las matrices y las evaluaciones ejecutadas, para el tratamiento de datos personales, se solicitará evidenciar los avisos de tratamiento de datos y las autorizaciones de los titulares, en función de los derechos de autor (licenciamiento de software), se debe realizar una trazabilidad entre el inventario de licencias y el software instalado en los equipos.

Sobre las pruebas de vulnerabilidad, se debe requerir la documentación de las actividades realizadas, los informes técnicos y ejecutivos. Al final se diagnosticará que las vulnerabilidades evidenciadas estén cubiertas en el plan de solución.

Para la gestión de activos se recomienda que se solicite el inventario de los mismos y verificar las actividades para dar de baja, para renovación, para devolución, entre otros, sobre el control de acceso físico y/o lógico se requiere evidenciar los temas de creación, actualización, baja de usuarios y adicionalmente solicitar las matrices de perfiles y privilegios.

La gestión de la criptografía es una parte sensible en el proceso de evaluación, por lo tanto, se sugiere solicitar y evidenciar los algoritmos utilizados para el cifrado de la información, los certificados digitales (internos y/o externos), para el tema de desarrollo de software se debe verificar el control de cambios, los requerimientos de usuario y las pruebas realizadas a los mismos.

En las redes y comunicaciones se abarcarán temas de análisis de tráfico, gestión de firewall y/o router y adicionalmente verificar la documentación sobre la continuidad del negocio en función de la seguridad de la información.

Para cada tema evaluado, se dividirá en varios subtemas (solicitudes de información y evaluaciones) a los cuales, se les dará un peso de calificación para puntualizar el estado actual del mismo. Finalmente, se condensarán los resultados de todos los temas revisados y se evidenciará el estado final del sistema de gestión de seguridad de la información.

Para el centro de cómputo se debe verificar los controles ambientales manuales y mecánicos, revisando las pruebas y/o intervenciones que se les hayan practicado para evidenciar y certificar su funcionalidad adecuada.

Revisar la resistencia al fuego que tiene los dispositivos que se encuentren inmersos en el centro de cómputo, adicionalmente, verificar que tipo de materiales se están utilizando para la limpieza.

2 GUÍA DE AUDITORÍA PARA DIAGNOSTICAR EL SGSI, SEGÚN LA ISO: IEC 27001:2013

En el desarrollo del presente artículo se establecerán los temas para evaluar el SGSI, adicionalmente se explicará el proceso a seguir para realizar la valoración de cada uno.

Los siguientes temas son extraídos del anexo “A” de la norma ISO: IEC 27001:2013 y otros fueron creados teniendo en cuenta la importancia y el riesgo de los mismos:

- Manual, PSI, documentación y generalidades del sistema de gestión de seguridad de la información.
- Sistema de gestión de riesgos.
- Gestión de incidentes.
- Pruebas de intrusión y análisis de vulnerabilidad.
- Clasificación de la información.
- Tratamiento de información personal y hábeas data.
- Criptografía.
- Seguridad en los recursos humanos.
- Gestión de activos.
- Control de acceso (físico y lógico).
- Seguridad física y ambiental.
- Seguridad en la operatividad.
- Seguridad en las telecomunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relación con los suministradores (proveedores).
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.
- Cumplimiento normativo.

2.1 MANUAL, PSI, DOCUMENTACIÓN Y GENERALIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad debería tener un manual para el sistema de gestión de seguridad de la información.
- El objetivo del manual se debe encontrar acorde con la NTC ISO 27001:2013.
- El manual indica claramente los procedimientos, responsabilidades y funciones dentro del SGSI.
- La entidad cuenta con un manual de políticas y procedimientos de sistema de información.
- Las políticas se encuentran específicas por temas, por procesos o anexo.
- Las políticas de seguridad de la información son socializadas y se dicta capacitación de las mismas por tipo de usuario.
- La entidad cuenta con procedimientos formalmente documentados y publicados para el SGSI.
- Los procedimientos del SGSI son claros e indican los responsables de cada uno de ellos, la periodicidad y la actividad a realizar.
- Los procesos del SGSI se realizan de acuerdo con los procedimientos.
- La entidad cuenta con un área de seguridad de la información.
- Hay un organigrama formalmente establecido que indique los encargados del SGSI.
- El área de seguridad de la información se encuentra de forma transversal en la operación del negocio y está alineada con las direcciones y gerencias de la compañía.
- La entidad cuenta con un oficial de seguridad de la información.
- El oficial de seguridad de la información cuenta con el perfil idóneo.

2.2 SISTEMA DE GESTIÓN DE RIESGOS

Para el presente tema en evaluación, se deberían revisar los siguientes aspectos:

- La entidad cuenta con políticas y procedimientos para la gestión de riesgos de seguridad de la información.
- La entidad gestiona los riesgos de seguridad de la información.
- La gestión de riesgos se encuentra dentro del manual de SGSI.
- La entidad cuenta con una metodología.

- La gestión de riesgos se realiza por procesos.
- El SGR (sistema de gestión de riesgos) tiene definidos los responsables de su gestión.
- La medición de riesgos tiene una metodología.
- La entidad cuenta con la matriz que permite evidenciar:
  Riesgos inherentes.
  Definición de controles.
  Riesgos residuales.
- El sistema de gestión de riesgos contempla riesgos de seguridad de la información.
- Evidenciar las actas de comité de riesgos.
- Verificar la herramienta para la gestión de los riesgos.
- Los riesgos de seguridad de la información se encuentran inscritos juntos con la evaluación de sus respectivos controles, dentro de la matriz de riesgos.

2.3 GESTIÓN DE INCIDENTES

Para el presente tema en evaluación, se deberían revisar los siguientes aspectos:

- La entidad cuenta con políticas y procedimientos para la gestión de incidentes de seguridad de la información.
- Se realiza capacitación a los diferentes usuarios sobre qué es un incidente de seguridad de la información.
- Es claro el procedimiento frente a las responsabilidades en la gestión de incidentes.
- La entidad cuenta con una herramienta para el reporte de los incidentes.
- La herramienta cumple con el objetivo establecido para la gestión de incidentes.
- Verificar la existencia de un banco de conocimiento sobre los incidentes de seguridad de la información evidenciados (aprendizaje de los incidentes de seguridad).
- La entidad cuenta con una metodología para la recolección de las evidencias. (cadena de custodia).
- La metodología para la cadena de custodia cuenta como mínimo con procedimientos para:
  Extracción o recolección de la prueba.
  Preservación y embalaje de la prueba.
  Transporte o traslado de la prueba.
  Traspaso de la misma.
  Custodia y preservación final hasta que se realice el debate.
- La entidad cuenta con un equipo de respuesta frente a incidencias de seguridad informática (CSIRT).
- Se tienen discriminadas, documentadas y formalizadas las obligaciones de los integrantes del grupo (CSIRT).
- La gestión de incidentes cumple con el ciclo establecido de reporte, clasificación, verificación del incidente, controles, actualización de la matriz seguridad de la información, documentación y monitoreo continuo.
- Se ha presentado la repetición de un incidente de seguridad de la información por más de una vez, luego de aplicar los controles establecidos para el mismo.

2.4 PRUEBAS DE INTRUSIÓN Y ANÁLISIS DE VULNERABILIDAD

Para el presente tema en evaluación, se deberían revisar los siguientes aspectos:

- La entidad cuenta con políticas y procedimientos para la gestión de vulnerabilidades.
- La entidad cuenta con leyes (políticas) que dictaminan la obligatoriedad para realizar las pruebas de vulnerabilidad.
- La entidad cuenta con una metodología para la ejecución de las pruebas de vulnerabilidad.
- La entidad ha realizado como mínimo dos veces al año el análisis de vulnerabilidades.
- Solicitar los informes realizados por los terceros, sobre el análisis de vulnerabilidades.
- Las vulnerabilidades establecidas en los informes del tercero, se encuentran clasificadas por su criticidad (alta, media, baja).
- En los informes evidenciados, las vulnerabilidades están tipificadas teniendo en cuenta los CVE publicados por la corporación Mitre.
- Entre las pruebas de vulnerabilidades realizadas, se tuvieron en cuenta:
  Pruebas de estrés a las aplicaciones.
  Pruebas de caja negra.
  Pruebas de caja gris.
  Pruebas de caja blanca.
  Pruebas de acceso físico.
  Ingeniería social.
  Pruebas de ataques del tipo D.O.S.
- Solicitar el plan de remediación sobre las vulnerabilidades encontradas.
- Se ha brindado solución a las vulnerabilidades encontradas en los tiempos adecuados, como los siguientes:
  Criticidad alta (dos meses).
  Criticidad media (cuatro meses).
  Criticidad baja (seis meses).
- Las herramientas utilizadas para el análisis de vulnerabilidades, están homologadas por el CVE (common vulnerabilitis and exposures).
- La entidad cuenta con políticas y procedimientos para la evaluación, selección y contratación del proveedor.

2.5 CLASIFICACIÓN DE LA INFORMACIÓN

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos para la clasificación de la información.
- La entidad cuenta con una metodología para la clasificación de la información.
- Sobre la metodología utilizada para la clasificación de la información, evidenciar como mínimo lo siguiente:
  Niveles de clasificación.
  Criterios de clasificación.
  Periodos de clasificación.
  Roles frente a los activos de información (responsable, custodio, usuario).
- La entidad ha realizado capacitaciones sobre la gestión para la clasificación de la información.
- Verificar el procedimiento para el etiquetado y tratamiento de la información.
- Realizar una prueba de clasificación de la información, para verificar la gestión que realiza la compañía.

2.6 TRATAMIENTO DE INFORMACIÓN PERSONAL Y HÁBEAS DATA

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos para el tratamiento de la información (datos personales y hábeas data).
- Evidenciar la cláusula de autorización frente al decreto 1377 de 2013 reglamentando la ley de protección de datos personales (1581 de 2012) con los asociados de la compañía.
- Evidenciar la cláusula de autorización frente a la ley de hábeas data (1266 de 2008) con los asociados de la compañía.
- Verificar si la compañía cuenta con un procedimiento (identificación, tratamiento, acceso, entre otros) para la gestión de la información sensible.
- Revisar si la entidad realizó adecuadamente el Registro Nacional de Bases de Datos (RNBD).

2.7 CRIPTOGRAFÍA

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos para la gestión de la criptografía.
- La entidad cuenta con políticas y procedimientos para la gestión de claves (llaves) para cifrar la información.
- La entidad cifrada su información.
- Quien tiene la custodia de las llaves privadas (recomendación - oficial de seguridad de la información, área de seguridad, control interno).
- Evidenciar la gestión frente a la utilización de las llaves privadas.
- La entidad cuenta con certificados digitales.
- La compañía cuenta con un ente certificador para legalizar los certificados digitales.
- El ente certificador para legalizar los certificados digitales es el adecuado (recomendados: Certicamara, Symantec, Comodo RSA, entre otros).
- Evidenciar que el certificado digital se encuentre vigente.
- La conexión está cifrada con mecanismos obsoletos.
- La conexión, qué algoritmo utiliza para el cifrado (recomendado AES 256).
- Qué algoritmo están utilizando para la autenticación del mensaje (revisar los mecanismos que tiene la entidad).
- Qué algoritmo están utilizando para el intercambio de claves mensaje (recomendado Diffie-Hellman).

2.8 SEGURIDAD EN LOS RECURSOS HUMANOS

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos para la gestión de los recursos humanos.
- La entidad realiza la gestión frente a la investigación de antecedentes judiciales, fiscales y disciplinarios.
- La entidad cuenta con un procedimiento para la contratación.
- En el procedimiento de contratación se tiene en cuenta el tratamiento de la información personal, evidenciar si se cuenta con cláusulas y/o autorizaciones sobre:
  Información reservada "sentencia C334 de 2010".
  Ley de protección de datos personales (1581 de 2012).
  Ley 1273 de 2009 delitos informáticos artículo 269f.
- En el procedimiento de contratación se tiene en cuenta la cláusula sobre la confidencialidad de la información, evidenciar que se precise sobre el numeral 2 del artículo 58 del código sustantivo de trabajo.
- Evidenciar si en el proceso de contratación se establece una cláusula al contrato laboral para poder revisar de forma legal las herramientas electrónicas proporcionadas por la entidad y de uso diario del colaborador (artículo 60 del código sustantivo de trabajo, numeral 8).
- La entidad cuenta con procesos disciplinarios.
- Evidenciar la educación y/o capacitación en seguridad de la información.
- Revisar si en el proceso de contratación se realiza la verificación de los representantes de

las entidades en las listas vinculantes y se deja el soporte del proceso realizado.
- Verificar la periodicidad para la verificación de antecedentes y consultas vinculantes.

2.9 GESTIÓN DE ACTIVOS

Para el presente tema en evaluación, se deberían revisar los siguientes puntos:

- La entidad cuenta con políticas y procedimientos para la gestión de activos.
- Evidenciar si la entidad tiene el inventario de los activos.
- Evidenciar en el inventario de activos, los activos dados de baja. (realizar prueba y documentar lo evidenciado).
- La entidad cuenta con procedimiento para dar de baja los activos.
- La entidad cuenta con un procedimiento para la renovación de los activos.
- La entidad cuenta con un procedimiento para devolución de los activos.
- Realizar prueba sobre el etiquetado de los activos.
- La entidad realiza análisis de riesgos a los activos de información.
- Solicitar la matriz de riesgos de los activos de información.
- La entidad tiene estipulados los requerimientos legales sobre los diferentes activos de la compañía.
- Solicitar los incidentes y/o no conformidades con la gestión de activos.
- Evidenciar las soluciones realizadas sobre los incidentes y/o no conformidades con la gestión de activos.
- La entidad cuenta con políticas y procedimientos para la gestión de compras (activos).
- Verificar los planes de contingencia, frente a los activos principales (CORE) de la organización.
- Evidenciar si periódicamente se realiza una verificación de los activos contra los inventarios para evidenciar el estado actual de los mismos.

2.10 CONTROL DE ACCESO (FÍSICO Y LÓGICO).

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos sobre el control de acceso.
- Entre los procedimientos recibidos, evidenciar los procesos para realizar las altas y bajas en el registro de usuarios (asignación, retiros, actualización, etc.).
- Revisar la gestión de usuarios con privilegios especiales y su autenticación frente a la información confidencial, sensible, entre otros.
- Realizar prueba de creación de tipo de usuario contra los privilegios de acceso, tener presente las altas, bajas y actualizaciones en el registro de usuarios.
- Informar sobre los privilegios especiales y autenticación de los usuarios frente a la información confidencialidad.
- La entidad cuenta con políticas sobre la segregación de funciones.
- Evidenciar la segregación de funciones, tener presente privilegios de procesamiento y autorización.
- Se cuenta con una bitácora para la gestión de ingreso y salida del personal ajeno a la entidad.
- La entidad cuenta con políticas y procedimientos sobre la gestión de contraseñas seguras.
- Verificar una contraseña creada, mediante la cual se corrobore lo estipulado en el procedimiento de contraseñas seguras.
- La entidad cuenta con políticas y procedimientos sobre el control de acceso a los códigos fuentes de las aplicaciones.
- Verificar los controles preventivos, disuasivos y correctivos en gestión al acceso.
- Evidenciar si se tiene un circuito cerrado de televisión (CCTV) y si se cuenta con un procedimiento formal para su gestión.

2.11 SEGURIDAD FÍSICA Y AMBIENTAL

Para el presente tema en evaluación, se debería revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos sobre la gestión de la seguridad física.
- Evidenciar los controles físicos para el ingreso a la entidad, verificar la funcionalidad de los mismos (realizar prueba).
- Verificar los controles de acceso para la seguridad del centro de cómputo (realizar prueba).
- Verificar los controles de acceso para el cuarto de seguridad (realizar prueba).
- La entidad cuenta con áreas independientes a las del procesamiento de información, para la atención y acceso del público (proveedores).
- Verificar y diagnosticar el estado del cableado estructurado de la organización.
- La entidad cuenta con políticas y procedimientos sobre el mantenimiento de equipos externamente.
- La entidad cuenta con políticas y procedimientos sobre la extracción de dispositivos fuera de las instalaciones de la compañía.
- La entidad cuenta con políticas y procedimientos para el borrado seguro.
- Cotejar la seguridad en la reutilización o retiro de dispositivos de almacenamiento (tener presente la política de borrado seguro).

- La entidad cuenta con políticas de equipo desatendido.
- Realizar prueba de equipo desatendido (bloqueo automático de equipo por no utilización en un tiempo determinado).
- La entidad cuenta con políticas de puesto de trabajo despejado.
- Realizar prueba de puesto de trabajo despejado (no se deben tener información encima de los escritorios de trabajo para el acceso de terceros).
- Revisar la seguridad e idoneidad de circuito cerrado de televisión, evidenciando si el mismo se encuentra instalado adecuadamente y si se gestionan las copias de seguridad.

2.12 SEGURIDAD EN LA OPERATIVIDAD

Para el presente tema en evaluación, se debería revisar lo siguiente:

- La entidad cuenta con procedimientos para las operaciones de la compañía.
- Verificar que los procedimientos de operación se encuentren documentados y que se encuentren a disposición de todos los usuarios que lo necesiten.
- La entidad cuenta con políticas y procedimientos para la gestión de cambios.
- La entidad tiene separados los entornos de desarrollo, prueba y producción.
- La entidad cuenta con políticas y procedimientos para la gestión del código malicioso.
- Realizar pruebas a los controles para la instalación de código malicioso.
- La entidad cuenta con políticas y procedimientos sobre las copias de seguridad.
- Realizar una prueba, para verificar el procedimiento de copias de seguridad.
- Evidenciar que todos los relojes de los servidores y/o dispositivos se encuentren sincronizados de acuerdo con la hora y fecha legal colombiana (realizar prueba).

2.13 SEGURIDAD EN LAS TELECOMUNICACIONES

Para el presente tema en evaluación, se debería revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos sobre el acceso a redes y recursos de red.
- Verificar los controles que tiene la organización para la seguridad de las redes, tener presente:
  Análisis de tráfico.
  Políticas de firewall.
  Gestión de los router.
  Políticas de acceso a Internet.
- Corroborar la segregación de las redes.
- Evidenciar que las redes inalámbricas cuenten con medios de autenticación.
- La entidad cuenta con políticas y procedimientos sobre el intercambio de información.
- Verificar la gestión que realiza la entidad frente a la política y procedimiento sobre el intercambio de información.
- Solicitar y diagnosticar el plano de redes y verificar el tipo de arquitectura de la red (evidenciar que la misma sea idónea).
- Revisar si la entidad cuenta con una DMZ, y de ser así, evidenciar si la misma está resguardando los equipos adecuados.
- Verificar si se tiene contingencia frente a los canales dedicados en caso de un incidente de seguridad.

2.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Para el presente tema en evaluación, se deberían revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos sobre la adquisición, desarrollo y mantenimiento de software.
- De los procedimientos y políticas recibidas, evidenciar los controles para el desarrollo de software seguro (requerimientos de seguridad, casos de abuso, pruebas de seguridad, análisis de estrés).
- La entidad cuanta con política para el desarrollo seguro.
- Corroborar el análisis y especificaciones de los requerimientos de seguridad de las aplicaciones (revisar los que se encuentran en desarrollo y en producción).
- Solicitar el inventario de las aplicaciones que posee la compañía.
- La entidad cuenta con políticas y procedimientos para el control de cambios en los sistemas.
- Realizar pruebas de despliegues de aplicaciones en referencia a los tiempos de autorización para la salida a producción.
- Solicitar las revisiones técnicas realizadas a las aplicaciones posteriormente a un cambio de sistema operativo.
- Corroborar la utilización de metodologías de desarrollo de software (requerimientos de seguridad, diagramas de uso, de abuso y pruebas de seguridad).
- Diagnosticar las políticas y/o procedimientos para desarrollos de software por proveedores.
- Evidenciar si se realizan pruebas de funcionalidad durante la etapa de desarrollo.
- Verificar la existencia de pruebas de aceptación de los desarrollos realizados.

- Corroborar la información entregada al final de cada desarrollo de software, tal como:
  Diccionario de bases de datos.
  Documento técnico de la aplicación.
  Diagramas de uso, de abuso, de clases.
  Flujo de datos.
  Modelo entidad relación.

2.15 RELACIÓN CON LOS SUMINISTRADORES (PROVEEDORES)

Para el presente tema en evaluación, se debería revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos para la seguridad de la información con los proveedores.
- Verificar los procedimientos de seguridad, frente al suministro de tecnologías de la información y comunicaciones a los proveedores (terceros).
- Verificar en los contratos y/ acuerdos con los proveedores, el tratamiento del riesgo.
- Corroborar las cláusulas de los niveles de acuerdos de servicio, tratamiento de información personal, confidencialidad de la información y cumplimiento del reglamento de seguridad interno.
- Observar las supervisiones y/o revisiones que se han adelantado posteriormente a los servicios prestados por terceros.
- Realizar prueba de cumplimiento del servicio adquirido, en la cual se evidencien actas de inicio de obra, seguimientos realizados, concepto del supervisor del contrato.

2.16 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.

Para el presente tema en evaluación, se debería revisar lo siguiente:

- La entidad cuenta con políticas y procedimientos sobre la continuidad de la seguridad de la información.
- La entidad cuenta con la planificación de la continuidad de la seguridad de la información.
- De la planificación de la continuidad de la seguridad de la información, evidenciar la existencia de escalas de tiempo requeridos tras la interrupción o fallo de los procesos críticos de negocio.
- Revisar los tiempos de respuesta y analizar si se encuentran dentro del umbral adecuado según el objeto social de la entidad.
- Verificar la implantación de la continuidad de la seguridad de la información (solicitar documentación).
- Corroborar las revisiones y evaluación de la continuidad de la seguridad de la información.
- Verificar la identificación de los eventos, probabilidad e impacto y consecuencias para la seguridad de la información.
- Verificar si la entidad cuenta con instalaciones alternas para brindar la continuidad en el procesamiento de la información.
- Indagar si han realizado simulacros (pruebas) sobre la continuidad del negocio, si es así, solicitar la documentación del proceso realizado.

2.17 CUMPLIMIENTO NORMATIVO

Para el presente tema en evaluación, se debería revisar lo siguiente:

- La entidad cuenta la política de seguridad sobre la legislación aplicable.
- Realizar prueba sobre “DPI” Derechos de Propiedad Intelectual (software).
- La entidad cuenta con la política de seguridad para la regulación de los controles criptográficos.
- Verificar la existencia de revisiones y/o auditorías al SGSI.
- Realizar prueba sobre el tratamiento de la información personal.

3 ESQUEMA DE EVALUACIÓN

En el presente capitulo sugiere el siguiente esquema de evaluación para determinar el estado de cumplimiento por tema y el estado final del SGSI.

3.1 EVALUACIÓN POR TEMA

A manera de ejemplo se precisa el tema de evaluación “manual y la documentación del SGSI”, en el cual se determinan 17 aspectos de cumplimiento y pruebas a ejecutar, a los cuales se les establecieron porcentajes de peso esperado, los resultados obtenidos y un porcentaje a mejorar, adicionalmente se evidencia un valor final por tema, el cual será enviado al resultado total del SGSI.

En el esquema de evaluación también se pueden indexar los papeles de trabajo y/o soportes de lo evidenciado, los cuales se encuentran programados por hipervínculos para acceder al soporte que fortalece el resultado evidenciado.

La estructura también cuenta con una programación interna de evaluación, en la cual si se desea agregar otro tema automáticamente se recalcularán los porcentajes para que se encuentren en concordancia con un 100 % en evaluación total.

En la siguiente figura se verifica la estructura de evaluación de los aspectos y las columnas de calificación, porcentajes, hipervínculos de los papeles de

trabajo y el contenido necesario que debe tener las evaluaciones a los temas.

No.	PROCEDIMIENTO DE AUDITORIA	LO OBSERVADO	COMENTARIO DEL AUDITOR	CALIFICACIÓN	RESULTADO ESPERADO (%)	RESULTADO OBTENIDO (%)	POR MEJORAR (%)	Referencia P/T
Evaluar el Manual, PSI y la Documentación soporte del Sistema de Gestión de Seguridad de la								
1	¿La Entidad tiene un Manual para el Sistema de Gestión de Seguridad de la Información?			Malo	7,14	0,00	7,14	Respuesta de la entidad
2	¿El objetivo del Manual se encuentra acorde con la NTC ISO 27001:2013?			Malo	7,14	0,00	7,14	
3	¿El Manual indica claramente los procedimientos, responsabilidades y funciones dentro del SGSI?			Malo	7,14	0,00	7,14	

Fig. 1. Evaluación por tema [4].

3.2 EVALUACIÓN GENERAL DEL SGSI

En la siguiente estructura se recopila el resultado de todos los temas evaluados y por cada tema se ejecutó el promedio de la valoración según la cantidad de aspectos verificados.

Según los posibles resultados obtenidos se estipula la siguiente estructura:

Si el campo se encuentra de color amarillo está en el marco adecuado.

Si el campo se encuentra de color verde es que tiene opciones de mejora, las cuales se deben remediar de una forma prioritaria.

Si los campos que resultan de color rojo son temas que se encuentran en riesgo de incumplimiento se deben remediar de manera inmediata.

En la siguiente figura se observa la estructura precisada anteriormente, adicionalmente en la fila “total” se evidencia lo siguiente:

El porcentaje esperado, el obtenido y el a mejorar.

Los puntos anteriores son los resultados finales del ***SGSI.***

No.	TEMA EVALUADO	RESULTADO ESPERADO (%)	RESULTADO OBTENIDO (%)	POR MEJORAR (%)
Diagnostico general del Sistema de Gestión de Seguridad de la Información				
1	Manual, PSI y la documentación soporte del Sistema de Gestión de Seguridad de la Información.	5,88	0,63	5,25
2	Sistema de Gestión de Riesgos.	5,88	0,00	5,88
3	Gestión de Incidentes.	5,88	0,86	5,02
4	Pruebas de Intrusión y Análisis de Vulnerabilidad.	5,88	0,00	5,88
5	Clasificación de la Información.	5,88	0,00	5,88
6	Tratamiento de Información Personal y Habeas data.	5,88	1,47	4,41
7	Criptografía.	5,88	3,39	2,49
8	Seguridad en los Recursos Humanos.	5,88	4,04	1,84
9	Gestión de activos.	5,88	1,58	4,31
10	Control de acceso (fisico y logico).	5,88	3,31	2,57
11	Seguridad Física y Ambiental.	5,88	2,94	2,94
12	Seguridad en la Operatividad.	5,88	5,56	0,33
13	Seguridad en las telecomunicaciones.	5,88	4,20	1,68
14	Adquisición, desarrollo y mantenimiento de los sistemas de	5,88	1,87	4,01
15	Relación con los suministradores (proveedores).	5,88	2,94	2,94
16	Aspectos de Seguridad de la Información en la Gestión de	5,88	0,00	5,88
17	Cumplimiento normativo.	5,88	1,10	4,78
	Total	100,00	33,90	66,10

Fig. 2. Evaluación final del SGSI [5].

3.3 ELABORACIÓN DE INFORME

En el presente capítulo se recomendarán los apartados que debe contener el informe final de auditoría y para cada uno de ellos se realizará una breve descripción:

Lo más adecuado es que el documento se encuentre con los logos institucionales y/o información de la empresa evaluada, adicionalmente que tenga su control de versiones.

En la primera hoja, se debe precisar la fecha y/o ciudad de la auditoría, a quién se remite (alta dirección), una breve descripción de lo realizado, la metodología utilizada y las limitaciones inherentes.

Se debe estipular el objetivo de la evaluación y tener en cuenta que el alcance es sumamente importante, pues en el mismo se puntualiza lo que se va a realizar (la muestra seleccionada) y lo que no se pudo abordar por posibles limitaciones, lo anterior en caso de alguna solicitud por no revisar un tema.

En otro capítulo se debe describir los procesos que se adelantaron en las evaluaciones, se recomienda que se aborden todos los temas diagnosticados, para tener una leve perspectiva de lo realizado.

Sobre los procedimientos adelantados, se debe establecer un capítulo con los resultados obtenidos en el que se describen de una forma sencilla, las debilidades evidenciadas en las revisiones.

Finalmente, se debe estipular un **capitulo** para describir los hallazgos evidenciados en las revisiones, la estructura de los mismos debería cumplir con los siguientes aspectos:

Cómo: bajo qué medio se realizó el proceso (verificación, indagación, prueba automática, etc.).

Dónde: la ubicación y/o proceso afectado (nomina, contabilidad, tecnología, etc.).

Qué: lo afectado (sistema, programa, metodología, proceso, etc.).

Cuánto: cada cuánto se realiza el proceso (cada mes, año, periodo, etc.).

Porqué: que ley y/o proceso se está incumpliendo.

Adicionalmente se recomienda que los hallazgos se presenten desde la perspectiva de riesgos (alto, medio, bajo) de este modo la gerencia general puede evidenciar las debilidades más sensibles que se deben remediar de forma inmediata.

En el capítulo final del informe, se deben redactar las conclusiones y recomendaciones de la revisión efectuada, para que la alta gerencia se entere de la

existencia de metodologías o mejores formas para fortalecer el control interno de tecnología.

CONCLUSIONES

En referencia a que el gobierno colombiano está exigiendo a las entidades financieras la implementación del sistema de gestión de seguridad de la información bajo los lineamientos de la norma ISO/IEC 27001:2013 el presente artículo es un adecuado compendio para realizar un análisis del mismo y evidenciar el estado del sistema.

Adicionalmente para los requerimientos legales y contractuales se realizó un análisis más minucioso de los temas (pruebas de vulnerabilidad, tratamiento de datos personales, derechos de autor) a cumplir. En el presente documento se brindan directrices para abordar los mismos y evidenciar su estado de cumplimiento.

Sobre el resultado de evaluación por tema, se tiene plantillas determinadas para evidenciar el estado de las mismas y al final centralizar el resultado de los diferentes temas abordados y establecer un estado actual del sistema, un estado ideal y el porcentaje a mejorar.

Las evaluaciones fueron analizadas desde la perspectiva profesional y con el apoyo del anexo “A” de la norma ISO/IEC 27001:2013, adicionalmente se extrajeron temas que apoyarán riesgos sensibles para dar un cumplimiento adecuado.

REFERENCIAS

[1] *TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS,* NTC-ISO-IEC 27001:2013, 2013.

[2] L. Agustín, *Punto de información y libre difusión en español de la serie de normas ISO 27000 [online].* México: Balandro, 2016 Disponible en: http://www.iso27000.es/#acerca.

[3] J.A. Gonzáles, “Formato IEEE - español”, “Universidad Pedagógica y Tecnológica de Colombia 2002”, 2002.

[4] Arias, E. (2016). Evaluación por tema. [Figura 1]. Fuente: El autor.

[5] Arias, E. (2016). Evaluación final del SGSI. [Figura 2]. Fuente: El autor.