INFORME DE AUDITORÍA A LA IMPLEMENTACION DEL PROYECTO SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN - SGSI

Contenido

Objetivo

- Verificar el estado de avance e implementación del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta la primera fase establecida internamente para el desarrollo del mismo y las disposiciones normativas establecidas para su implementación.
- Evaluar el alcance, la política y la identificación y tratamiento de los riesgos del SGSI para los procesos definidos.
- Revisar la declarativa de aplicabilidad de los controles necesarios implementar.

Alcance

La evaluación del avance del sistema de gestión de seguridad de la información comprende la primera fase desarrollada (fase establecida para los procesos de construcción y mantenimiento de ítems-C1, aseguramiento de recursos-C2 y registro-C3). La revisión incluirá el análisis de riesgos establecido y la declarativa de aplicabilidad propuesta para este sistema. Para lo anterior, se tendrá en cuenta las disposiciones normativas y administrativas (procedimiento: H3. Gestión de Seguridad de la Información) y las mejores prácticas para la gestión de seguridad de la información. La revisión se realiza del 15 de junio de 2016 al 29 de julio de 2016.

Metodología

Durante la auditoría se desarrollaron:

- Acceso a los controles de Información
  Acceso a los controles de seguridad de la información implementados
- Entrevistas
  Entrevista con: Subdirección de Información
  Grupo de Gestión de seguridad de la información
- Documentación
  Documentación recolectada del proceso.

Información Solicitada

Con el fin de realizar la labor inicial se solicitó:

INFORMACIÓN SOLICITADA	ÁREA GENERADORA DE INFORMACIÓN
Documentación del proyecto de gestión de seguridad de la información. Documentación sobre la gestión de riesgos de seguridad de información definido para los procesos y los activos de información del Instituto. Documentación sobre la implementación de controles propuestos en la declarativa del sistema de gestión de seguridad de la información. Documentación sobre la implementación de controles que mitigan y corrigen los riesgos encontrados en las pruebas de vulnerabilidad.	Subdirección de Información

Desarrollo de Auditoría

Con base en la información recolectada y las entrevistas efectuadas se realizaron las siguientes actividades:

- Análisis y evaluación de la información suministrada, arriba enunciada, y entrevista realizada con el grupo encardo de liderar el sistema de gestión de seguridad -SGSI y con el subdirector de información.

- Análisis de información del sistema de gestión disponible en el sistema.
- Evaluación de la primera fase y de los avances realizados para todos los procesos Instituto.

Resultados

De la revisión realizada al sistema de gestión de seguridad de la información-SGSI, se observó la siguiente situación:

<u>Revisión del estado del SGSI:</u>

Comprende verificación del estado y avance de implementación del sistema de gestión de seguridad de información.	
Observación	1. Se observa que se han desarrollo y se tienen publicadas, por parte de la Dirección de Tecnología, 18 políticas de seguridad de la información. El documento "Política de clasificación de la información – Seguridad de la información, Julio de 2012" publicada en la intranet, no incluye algunas especificaciones normativas, posteriores a la fecha de revisión de la política, entre otras, directrices reglamentarias de ley de transparencia 1712 de 2014. <u>*Recomendación*</u> *Realizar actualización de la política de clasificación de la información, de tal manera que incluya la reglamentación señalada en el decreto 103 de 2015 y ley 1712 de 2014.* 2. El estándar ISO 27002 en su numeral "5.1.1 - política de seguridad de la información" hace

	precisión sobre declaraciones propuestas al contenido y alcance de la política. El Instituto ha desarrollado un conjunto de políticas en materia de seguridad de información (18 documentos), de los cuales no se encontró directrices (políticas) para: - Uso aceptable de los activos (8.1.3). - Restricción de instalación y uso de software (12.6.2). - Protección contra códigos maliciosos (12.2). - Gestión de vulnerabilidades técnicas (12.6.1). <u>*Recomendación*</u> *Evaluar la conveniencia de definir, documentar y publicar las políticas arriba enunciadas, para que sean parte integral de los lineamientos de seguridad de la información. Las políticas de seguridad definen las directrices de compromiso con el SGSI. Los objetivos de control y los controles definen las especificaciones y características del mecanismo de seguridad para cumplir con las políticas de seguridad.* *El estándar ISO 27002 en el numeral 5.1.1. propone una lista de directrices que ayuda a estructurar la política de seguridad de información.* 3. Como resultado de las pruebas de vulnerabilidad y penetración -ethical hacking- y medidas mínimas de seguridad en el módulo construcción de ítems realizadas en la primera fase del SGSI, el informe hace una descripción

	de las desviaciones de seguridad tecnológica encontradas, las cuales requieren de la definición y ejecución de un plan de corrección y tratamiento, pendiente de definir y documentar. <u>*Recomendación*</u> *Elaborar y desarrollar un plan de trabajo que determine, en el corto y mediano plazo, las actividades para implementar los controles necesarios, con el fin de mitigar las vulnerabilidades a las cuales se encuentran expuestos y comprometidos los componentes informáticos que se relacionan en los informes de las pruebas realizadas (equipos de red interna, aplicaciones web y módulo construcción de items). Las pruebas de perpetración y el análisis de vulnerabilidades permiten detectar el nivel de seguridad interno y externo que tienen los sistemas de información.*
Estándares y regulaciones - Política de clasificación de la información -Seguridad de la Información- Icfes, Julio de 2012; Manual de políticas y procedimientos de protección de datos personales – Icfes, 2016. - Decreto 103 de 2015 Reglamenta gestión de la información pública; Ley 1712 de 2014 de transparencia y del derecho de acceso a la información pública Decreto 1377 de 2012 Reglamenta protección de datos personales; Ley 1581 de 2012 Protección de datos personales; Decreto 2573 de 2014 Lineamientos generales de la estrategia de gobierno en línea. - ISO 27001 Sistema de Gestión de seguridad de la información; ISO 27002 Código de practica para los controles de seguridad de la información.	

Verificación análisis de riesgos - SGSI:

Comprende revisión al compendio de actividades que se realizan en el marco de referencia para la gestión del riesgo.	
Observación - Recomendación	4. En el mapa de riesgos se identifican 22 riesgos para los activos de seguridad de información de los procesos de la primer fase, lo cual es una lista de riesgos amplia que al ser analizada en el conjunto de riesgos de los procesos resulta ser extensa, pues algunos riesgos se describen en función de la fuente o amenaza de riesgo (causa de error y mal intención). Por ejemplo: - 1.a Destrucción de la información por error 1.b Eliminación de la información mal intencionada. - 2.a Fuga de información por error 2.b Fuga de información mal intencionada. - 3.a Modificación de la información por error 3.b Modificación mal intencionada de información. - 4.a Denegación del servicio por error 4.b Denegación del servicio mal intencionada. - 5.a Malware y 5.b malware por error. El grupo de seguridad de la información de la Subdirección de Información realiza un plan de actividades tendientes a evaluar la lista de riesgos. Igualmente, ha solicitado a la oficina de Planeación su intervención para homologar metodológicamente los criterios y el mapa de

	riesgos de seguridad de la información con los riesgos de operación definidos en los procesos. *<u>Recomendación</u>* *Si bien la lista de vulnerabilidades y amenazas de los elementos de software puede resultar extensa, la lista se perfecciona con la revisión periódica de los funcionarios expertos en cada proceso.* *Además, es importante que la lista de riesgos de seguridad de la información, propenda y se integre con los lineamientos generales establecidos en el procedimiento interno de riesgos de procesos.* *El estándar NTC ISO 27005 en su numeral 8.2 (ocho - dos) análisis del riesgo en la seguridad de la información establece los siguientes pasos en la identificación del riesgo: 1. Introducción a la identificación del riesgo, 2. Identificación de los activos, 3. Identificación de las amenazas, 4. Identificación de los controles existentes, 5. Identificación de las vulnerabilidades y 6. Identificación de las consecuencias, los cuales son guía para identificar el riesgo con mejor precisión, pero indicando que debe ser una lista extensa e inmanejable que siempre conduce a una misma opción del tratamiento del riesgo, luego es necesario revisar periódicamente los riesgos para avanzar en la estandarización y mitigación de los mismos.* 5. El "Mapa análisis de riesgos" de los activos de información, en la primera fase, identifica la amenaza y riesgo que tiene cada activo en su

	proceso. Este mapa (archivo) contiene los siguientes datos: tipo de riesgo; subproceso; activo; tipo de activo (información, hardware, software, red, estructura organizacional y ubicación); confidencialidad del activo; integridad del activo, disponibilidad del activo; importancia, amenazas, probabilidad, impacto y clasificación. De la revisión a los datos del archivo (mapa), se observa que la "importancia" del activo (a partir de los valores de "confidencialidad", "disponibilidad" e "integridad") no es tenida en cuenta en la valoración (que corresponde al producto de la probabilidad e impacto) del riesgo del activo. Además, el criterio de "importancia" del activo, en cuanto a la "confidencialidad", no incluye en su cómputo o valoración, los niveles de clasificación de la información (pública, clasificada o reservada) definidos en la normatividad de transparencia y derecho de acceso a la información pública. <u>*Recomendación*</u> *Considerar incluir en la calificación del riesgo (probabilidad e impacto), la ponderación de importancia que tiene el activo en los componentes de confidencialidad, disponibilidad e integridad. Igualmente, para el cálculo de la confidencialidad es importante incluir en el cálculo los niveles de clasificación de la información (pública, clasificada o reservada) definidos en la ley 1712 de 2014.*

	El estándar ISO 27005 Gestión del riesgo de seguridad de la información, corresponde a uno de los componentes fundamentales del SGSI, el cual es concordante con la aplicabilidad del estándar ISO 9001 e ISO 31000. En consecuencia, los procedimientos internos referentes a las actividades para la administración y manejo de Riesgos deben estar en armonía con la normatividad (Guía para la gestión del riesgo del DAFP) y con las mejores prácticas. 6. Con relación al mapa de riesgo del sistema de gestión de seguridad de la información -SGSI, se observó que no se han establecido los criterios (financiera, legal, costo-beneficio, técnico, institucional) para dar tratamiento del riesgo y aceptación de riesgos residuales, los cuales son esenciales para determinar el alcance de las acciones que debe adoptar el Instituto para mitigar los riesgos evaluados en el sistema de gestión. <u>*Recomendación*</u> *Es importante que el comité de dirección determine el nivel de tolerancia al riesgo (apetito al riesgo) que acepta el Instituto para establecer los criterios (financiera, legal, costo-beneficio, técnico, institucional) que se deben seguir para dar el alcance que debe tener el tratamiento de riesgos evaluados en el sistema de gestión de seguridad de la información.* *Lo anterior atendería a lo señalado en el elemento de valoración de controles de la Guía*

	para la Administración del Riesgo del DAFP y al numeral 8 (ocho) de valoración del riesgo de la norma Gestión del Riesgo en la Seguridad de la Información ISO 27005, las cuales determinan la selección de las opciones de tratamiento del riesgo (a. Evitar el riesgo, b. reducir el riesgo, c. compartir o transferir el riesgo y d. asumir el riesgo). Dicha selección implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales que se deben considerar (viabilidad jurídica, técnica, institucional, financiera o económica y análisis de costo-beneficio) en la valoración del control. Una vez implementadas las acciones para el manejo de los riesgos, se determina la valoración del riesgo resultante o residual. 7. El documento "Metodología de Análisis de riesgos de seguridad de la información", el cual se fundamenta en normas y estándares, define las etapas que involucra el análisis de riesgo en el Instituto (Identificación, estimación, evaluación y tratamiento de los riesgos de seguridad de la información, comunicación y consulta y monitoreo y revisión), no obstante, en el documento no se hace un detalle de evaluación de controles de la gestión de seguridad de la información, como lo señala la guía "Seguridad y privacidad de la información" Gobierno en Línea y la guía de Riesgos DAFP, en cuanto a: tipo de control (probabilidad o impacto) y valoración de controles (puntaje).

	<u>Recomendación</u> *Evaluar las directrices y lineamientos señalados en la guía "Seguridad y privacidad de la información" Gobierno en Línea y la guía de Riesgos del DAFP, para complementar y fortalecer el documento de la metodología de análisis de riesgos de seguridad de la información.* *La guía para la administración del riesgo del DAFP, en su capítulo de valoración de controles, propone unos parámetros (herramientas para ejercer control y elementos de seguimiento al control), criterios, tipo de control (probabilidad e impacto) y rangos para la calificación de los controles.* 8. El "Mapa de riesgo" de seguridad de información contiene no menos de 235 actividades propuestas realizar para cumplir con la lista de controles, relacionada en el anexo A de la ISO 27001, sin embargo, en la lista del mapa no se identifica claramente los controles que están operando o los pendientes de implementar a la fecha, con el fin de conocer con mejor criterio la valoración del riesgo residual. El grupo de seguridad de la información de la subdirección de información, viene realizando tareas en la identificación de los controles implementados y en la definición de la programación de los controles pendientes de instalar.

<u>Recomendación</u>

El resultado de las tareas que realiza el grupo de trabajo de seguridad, en cuanto al inventario de controles, tiene un efecto importante en la valoración del riesgo residual. Una vez lo anterior, se realiza una evaluación al cálculo del riesgo residual, el cual se obtiene de aplicar los controles existentes al riesgo expuesto del activo, luego si el riesgo no se encuentra dentro de la zona tolerable, es necesario determinar el tratamiento a cumplir para mitigar el riesgo.

9. Al comparar el archivo "Mapa análisis de riesgos de los activos de seguridad" con los activos registrados en el archivo "Inventario de activos de información" publicados en la página web Icfes, se observó que no todos los activos en la categoría de "información" son reportados simultáneamente en ambos archivos. Por ejemplo: para el proceso "C1. Construcción y mantenimiento de Ítems", se encontró:

Activo de información	**Observación**
Carpetas de gestión de los procesos de codificación	No se incluye el activo en el Mapa análisis de riesgo
Bases de datos de los participantes de gestión de pruebas	No se incluye el activo en el Mapa análisis de riesgo
Documentos de los participantes en procesos de diagramación, edición, armado, construcción	No se incluye el activo en el Mapa análisis de riesgo
Acta de entrega material para impresión	No se incluye el activo en el Mapa análisis de riesgo
Control de préstamos de las pruebas	No se incluye el activo en el Mapa análisis de riesgo
Cuadernillos. Conjunto de ítems que se aplican	No se incluye el activo en el Mapa análisis de riesgo
Base de datos de codificaciones a las	No se incluye el activo en el Mapa análisis de riesgo.

respuestas de preguntas abiertas	
Acta de Compromiso de Confidencialidad	No se incluye el activo en el inventario activo de información – web
Asignación de Items	No se incluye el activo en el inventario activo de información – web
Acta de destrucción de información confidencial	No se incluye el activo en el inventario activo de información – web

<u>Recomendación</u>

Revisar los activos de información que se tiene relacionados tanto en el "Mapa análisis *de riesgos de los activos de seguridad" como los reportados en el archivo "Inventario de activos de información" publicados en la página web Icfes, con el fin de que exista uniformidad en la cantidad y clase o calificación del activo información.*

En la normatividad (Decreto 103 de 2015) se indican las directrices para la calificación de los activos de información, los cuales son tenidos en cuenta en la identificación de la información del Instituto.

Estándares y regulaciones

- Guía para la administración del riesgo – DAFP.
- Decreto 103 de 2015 reglamenta la ley 1712 de 2014.
- ISO 27001 Sistema de Gestión de seguridad de la información; ISO 27002 Código de practica para los controles de seguridad de la información; ISO 27005 Gestión del riesgos en la seguridad de la información e ISO 31000 Gestión del riesgo.

<u>Evaluación declarativa de aplicabilidad - SGSI</u>

La declarativa determina los objetivos de control y controles de referencia que el Instituto adopta para el sistema de gestión de seguridad de la información.

<table>
<tr>
<td>Observación - Recomendación</td>
<td>
10. La declaración de aplicabilidad (lista de controles de seguridad que se acepta implementar) reconoce y propone la pertinencia de todos controles del anexo A del estándar. sin embargo, en el mapa análisis de riesgos de seguridad de la información, no se relacionan los siguientes controles para los procesos definidos en la primera fase, por ejemplo:
<table>
<tr><th>Proceso</th><th>Control no incluido</th></tr>
<tr><td>C.4.P.4 Inscripción</td><td rowspan="2">A.12.1.3 Gestión de capacidad</td></tr>
<tr><td>C.4.P.5 Citación</td></tr>
<tr><td>C.1.P.1 Construcción de Items</td><td rowspan="4">A.13.2.4 Acuerdos de confidencialidad o de no divulgación</td></tr>
<tr><td>C.3.P.1 Aseguramiento de Infraestructura</td></tr>
<tr><td>C.3.P.3 Aseguramiento de Material</td></tr>
<tr><td>C.3.P.4 Aseguramiento distribución de material</td></tr>
</table>
Igualmente, a fecha de revisión, no se tiene análisis de riesgo del resto de procesos establecidos en el Instituto.

<u>Recomendación</u>
Es importante evaluar los controles, arriba enunciados, para determinar su importancia en la aplicabilidad del proceso o en caso contrario, justificar la no aplicabilidad del control de seguridad de información en la declarativa.
Así mismo, evaluar la pertinencia de la transversalidad de los controles de seguridad de información, la cual involucra todos los procesos del Instituto.
El anexo A de ISO 27001 relaciona los objetivos de control y los controles que sugieren aplicar. El literal “d” del requisito “6.1.3 - Tratamiento de riesgos de la seguridad de la información”,
</td>
</tr>
</table>

	ISO 27001, señala la importancia del documento: "Producir una declaración de aplicabilidad, que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del anexo A."
Estándares y regulaciones - ISO 27001 Sistema de Gestión de seguridad de la información, Anexo A; ISO 27002 Código de practica para los controles de seguridad de la información; ISO 27005 Gestión del riesgos en la seguridad de la información e ISO 31000 Gestión del riesgo.	

Conclusiones

Como resultado de la evaluación realizada al sistema de gestión de seguridad de la información, presentamos la siguiente conclusión:

- Se evidencia un avance en la implementación de controles definidos para el sistema de gestión de seguridad de la información en el porcentaje del 40% establecido para 2015 y en lo determinado para 2016 (60%) por Gobierno en Línea, sin embargo, se observan algunas oportunidades de mejora, como las arriba citadas, en cuanto: documentación, procedimiento, mapa de riesgos y controles del sistema, las cuales requieren ser gestionadas.

- Fortalecer los mecanismos metodológicos internos de valoración y tratamiento de riesgos de seguridad de la información, con el fin de ser concordantes e integrados al sistema general de riesgos, pues es base fundamental en los sistemas de gestión que el Instituto adopte.

- La declaración de aplicabilidad determina los controles de seguridad de la información que el Instituto aplica para el sistema de gestión de seguridad de la información, la cual es importante evaluar en tiempo y costo, para los mecanismos de control por implementar.