INFORME	PERIODO EVALUADO	FECHA
INFORME DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN	AÑO 2020	10/12/2020

NORMATIVIDAD APLICABLE

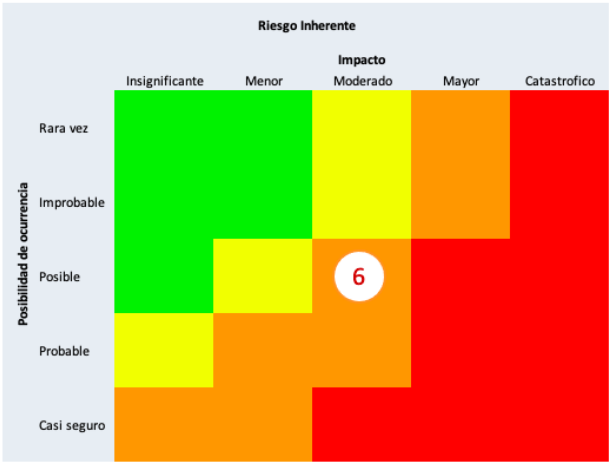
Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
Ley 1341 de 2009. " Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC y se dictan otras disposiciones"
Ley 1437 de 2011. “Procedimiento Administrativo y aplicación de criterios de seguridad”
Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”
Ley 1712 de 2014. “Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".
Decreto 2364 de 2012. “Firma electrónica”.
Decreto 2609 de 2012. “Expediente electrónico”.
Decreto 2693 de 2012. “Gobierno electrónico”.
Decreto 1510 de 2013. “Contratación pública electrónica”.
Decreto 338 de 2018.” Por el cual se expide el Decreto Único del “Sistema Integral de Gestión y Control (SIGC) del Nivel Central de la Administración Departamental”, y se dictan otras disposiciones”.
Decreto 1008 del 2018 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital".
Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad digital.
ISO 27001:2013

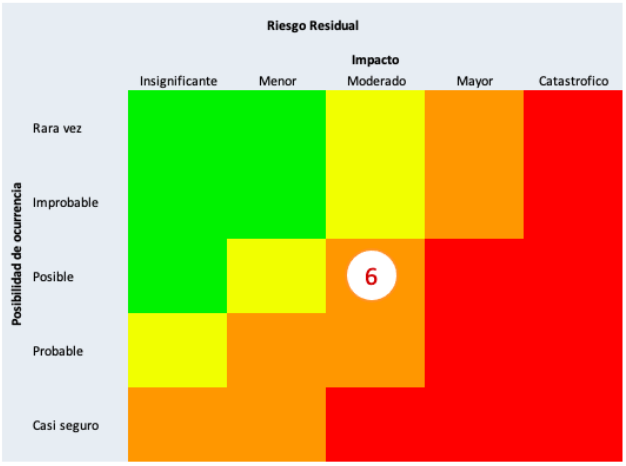
ANÁLISIS Y RESULTADOS DE LA EVALUACIÓN Y SEGUIMIENTO

La Oficina de Control Interno en cumplimiento a la ley 87 de 1993 y el Plan Anual de Auditorías vigencia 2020 aprobado el día 06 de octubre de 2020, realizo la verificación de las evidencias presentadas a la OCI por parte de la Secretaría de las Tecnologías de la Información y las Comunicaciones líder del Proceso de Gestión Tecnológica, quien lidera la Seguridad de la Información de la entidad.

Teniendo en cuenta los lineamientos impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital, Decreto 338 del 25 de octubre 2018 y la Declaración de Aplicabilidad donde se enmarcan los Controles de Seguridad de la Norma ISO 27001:2013

Se identifica el proceso de gestión tecnológica en cuanto a la valoración de los riesgos y se encontró que para la norma ISO 27001 tienen identificado un riesgo el cual se encuentra codificado en el mapa de riesgos con el numero seis (6). ver **Matriz calificación riesgos de Gestión**





OBJETIVO

Verificar el cumplimiento la Declaración de Aplicabilidad de la Norma ISO 27001:2013 aprobada por le comité de Seguridad de la Información el día 9 de octubre de 2019 como consta en el acta de comité.

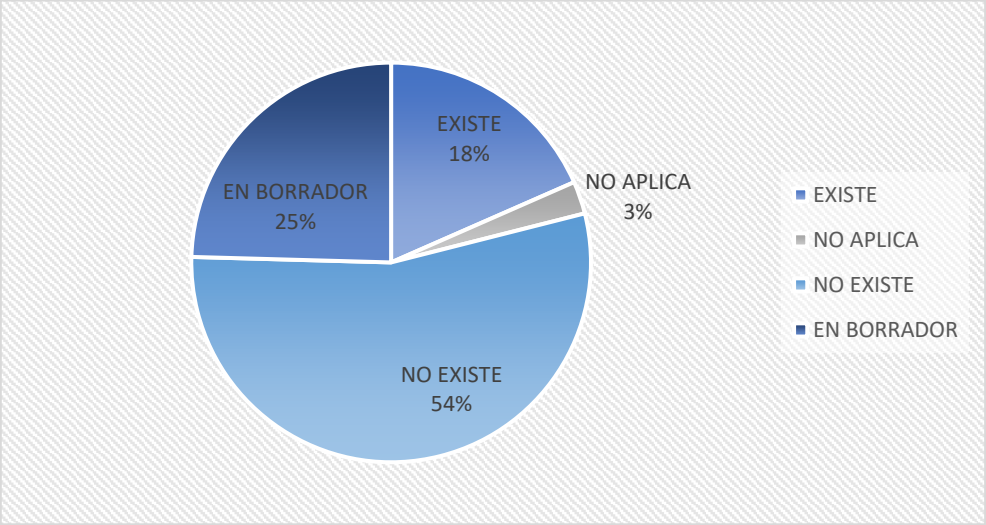
METODOLOGÍA

Teniendo en cuenta que la Secretaría de las Tecnologías de la Información y las Comunicaciones, lidera a través de la Dirección de infraestructura la implementación del Sistema de Gestión de seguridad de la Información, se realizo la solicitud por parte de la OCI con mercurio número 2020348361 y mediante el mercurio numero 2020349595 por el cual la Secretaría de las Tecnologías de la Información y las Comunicaciones da respuesta el día 20 de noviembre de 2020 a la solicitud. Es de resaltar que durante el proceso de verificación de evidencias, los datos del informe se socializaron el día 27 de Noviembre con el Ingeniero Yury Alexander Riveros Director de Infraestructura y la Oficina de Control Interno, donde se le indico que la mayoría de la información estaba en documentos Word, sin firmas ni aprobaciones por parte del comité de seguridad de la información y que el nivel de cumplimiento de la ISO 27001:2013 era muy bajo, a lo que el respondió que si era posible de allegar mas evidencias para subir el nivel de cumplimiento, de esto quedo constancia en acta y en correo solicitando las evidencias por parte de la Oficina de Control Interno, las cuales hasta el día 4 de diciembre de 2020 no allego. Lo que indica que el nivel de cumplimiento no cambio y se elabora el presente informe, así:

De las 14 secciones de norma ISO 27001:2013, se concluye que existe información la cual esta aprobada y debidamente cargada en ISOLUCIÓN que se denominara como “existe”, en borrador que aun no se ha aprobado por parte del comité de seguridad, ni ha pasado por calidad

para ser cargada en el sistema de gestión y la que no existe es porque no se evidenciaron documentación o soporte.

Cabe a notar que de estos controles el 3% no aplica a la entidad según la declaración de aplicabilidad, como se muestra en la siguiente gráfica:



En cuanto a los demás porcentajes, se puede decir que de los 114 controles que conforman las 14 secciones de Norma ISO 27001:2013 y de las evidencias presentadas solo 21 que representa el 18% son procesos, formatos y guias que están debidamente documentadas y cargadas en ISOLUCION, por otro lado el 25% lo conforman 28 controles los cuales se encuentran en borrador, ya que aun no sido aprobados por el comité de seguridad, ni pasados a calidad para ser aprobados y cargados a la herramienta de gestión, es importante tener en cuenta que son 13 políticas las que están en borrador. Por ultimo el 56% restante pertenece a 64 controles de los cuales no se evidencio soporte, lo que lleva a concluir que aun no hay información sobre estos controles.

A nivel general de las 14 secciones que conforman los 114 controles se observa que el nivel de cumplimiento es bajo como se observa en la siguiente tabla.

SECCIÓN		% cumplimiento
A.5	Políticas de Seguridad de la Información	12,5
A.6	Organización de la Seguridad de la Información	27,5
A.7	Seguridad ligada a los recursos humanos	66,7
A.8	Gestión de activos	41,7
A.9	Control de acceso	32,5
A.10	Criptografía	25,0
A.11	Seguridad física y ambiental	4,2
A.12	Seguridad de las operaciones	20,5
A.13	Seguridad en las comunicaciones	18,8

A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información	0,0
A.15	Relaciones con proveedores	4,2
A.16	Gestión de incidentes de seguridad de la información	12,5
A.17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio	0,0
A.18	Cumplimiento	7,5

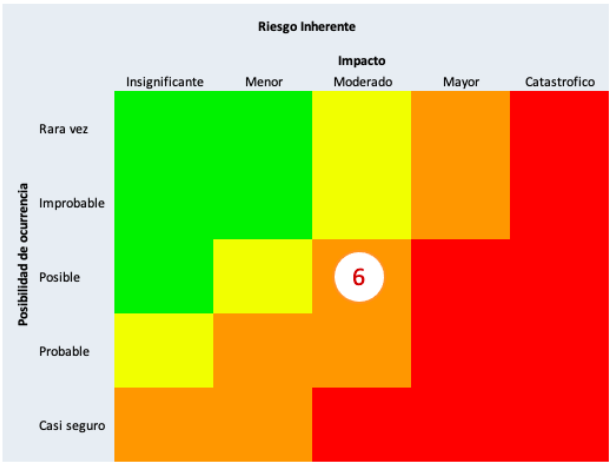
Es de anotar que la tabla anterior se realizo con base en la información que la Secretaría de las TIC allegó a la Oficina de Control Interno. En cuanto a los criterios diferenciales del Sistema de Control Interno, se evidencia la baja respuesta desde la primera y segunda línea de defensa para el desarrollo y mantenimiento de controles de TI de tal forma que se mitiguen los riesgos, suceso que también se soporta en el resultado de la evaluación de la ejecución de los controles y su ejecución.

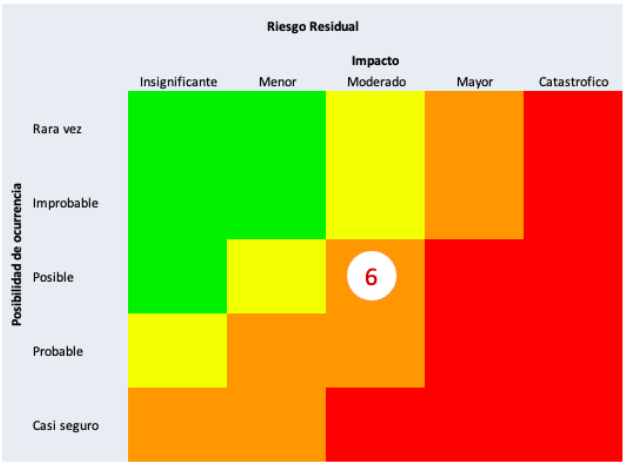
Línea de defensa	Componente asociado	Criterio diferencial o atributo de calidad	Resultado
02. Primera	04. Información y Comunicación	Cumplir con las políticas y lineamientos para generar y comunicar la información relevante, de manera accesible, oportuna, confiable, íntegra y segura, que facilite las acciones de control en la entidad.	Cumple Parcialmente
03. Segunda	03. Actividades de Control	Acorde con la estructura de la entidad, El Oficial de Seguridad de la Información verifica el desarrollo y mantenimiento de controles de TI.	Cumple Parcialmente

Durante el seguimiento se evaluó la gestión del riesgo de Seguridad de la Información identificado en el Mapa de Riesgos del Proceso de Gestión Tecnológica, donde se evaluó el diseño, ejecución y solidez del riesgo identificado, pero como se observa solo existe un Control establecido, lo que indica la baja la intención de tratar el riesgo para poderlo minimizar.

Control	Riesgo	Control	Diseño del Control	Ejecución del Control	Solidez
Gestión Tecnológica	No se tienen lineamientos estandarizados para la implementación y socialización de la norma ISO27001.	No hay control	Débil	Débil	Débil
		No hay control	Débil	Débil	Débil
		Revisión de documentación del proceso Gestión Tecnológica por parte del Equipo de Mejoramiento.	Débil	Débil	Débil
		No hay control	Débil	Débil	Débil

El resultado de los controles se ven en la valoración residual de los riesgos así:





Se observa que la valoración del riesgo residual es igual al riesgo inherente, lo que indica que a pesar de ejecutar las actividades de ese control al final no minimiza el riesgo, ni agrega valor al proceso.

RECOMENDACIONES

Se recomienda que la meta 377 sea liderada por esta Secretaría para dar cumplimiento a las funciones establecidas en el Decreto 347 del 25 septiembre de 2020 en su articulo 102 "*Funciones esenciales de la Secretaria de Tecnologias de la Informacion y las Comunicaciones*", numeral 15 donde indica "*Liderar la implementación de la Politica Digital…*" y el articulo 106 *"Funciones de la dirección de la infraestructura Tecnológica",* numeral 15 donde indica "*Estudiar, Diseñar e implementar el Sistema de Gestión de seguridad de la Información…".* Asi mismo para dar cumplimiento a los criterios establecidos por el Ministerio TIC en el Modelo de seguridad de la información.

Se recomienda que la documentación asociada al Sistema de Gestión de Seguridad de la Información sea alineada con el Modelo de seguridad de la información establecido por el Ministerio de la TIC y los controles de la norma ISO 27001:2013.

Para dar adelantar a la implementación ISO 27001:2013 se recomienda realizar los comités de seguridad en los tiempos establecidos, revisar, aprobar la documentación que actualmente este en borrador y socializarla.

Se recomienda realizar la identificación de riesgos a nivel de seguridad de la información y establecer controles efectivos.

Se sugiere que por parte de la segunda línea de defensa se tenga mas participación en el proceso.

CONCLUSIONES

De la evaluación realizada al Proceso gestión tecnológica, que la entidad no cumple con la implementación de la ISO 27001 datos que fueron arrojados de la información entregada por parte de la secretaria con un porcentaje del 18% del total.

Se evidencio que de la declaración de aplicabilidad aprobada por el comité de seguridad de la información a la entidad no le aplica el 3% lo cual lleva a que el 99% es aplicable a la entidad y que de este ultimo porcentaje no se han realizado un gran porcentaje.

Se evidencio que el 25% de las evidencias presentadas a la OCI es información borrador la cual no esta aprobada por el comité de seguridad de la información y por ende por el grupo de calidad de la entidad. Es importante que se adelante la oficialización, aprobación y publicación de esta información.
Aunque para el 54% de los controles que no existe información representan mas de la mitad. Es de gran importancia que la Secretaría de las TIC adelante documentación sobre estos controles.

Es vital que la Secretaría adelante la implementación del SGSI en la Gobernación. Ya que del informe GAP presentado y aprobado por el comité de seguridad el día 9 de octubre de 2019 no se evidencia avance a la fecha.

Es importante que las capacitaciones o socializaciones con los funcionarios y contratistas sea también del SGSI (Procedimientos, Políticas, Formatos, etc.) ya que no todos han sido socializados y es importante que todos conozcámonos sobre el sistema.

En cuanto a la revisión del riesgo plasmado en el mapa de riesgos existe carencia en la identificación de riesgos y controles establecidos para este riesgo.

Elaboró

Nombre: Yuly Andrea Huertas Alonso
Cargo: Contratista

Nombre: Yody García Gómez
Cargo: Profesional Universitario

Aprobó

Nombre: Yoana Marcela Aguirre Torres
Cargo: Jefe de Oficina de Control Interno