INFORME EJECUTIVO

AUDITORIA DE GESTION AL PROCESO DE ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

PERIODO DE EJECUCION

Entre el 04 de mayo y el 18 de junio de 2021, se llevó a cabo evaluación del proceso de Estrategia de Tecnologías de la Información y las Comunicaciones de la Secretaría General, de acuerdo con lo programado en el Plan Anual de Auditoría aprobado para el año 2021.

OBJETIVO GENERAL

Evaluar los controles claves aplicables a los procedimientos que conforman el proceso de Estrategia de Tecnologías de la Información y las Comunicaciones, que fueron objeto de modificaciones durante el julio de 2020 a abril 2021. Así como, establecer el cumplimiento de directrices y lineamientos relacionados con el Sistema de Seguridad de la Información y la Metodología para el Desarrollo y Mantenimiento de Soluciones, documentos contentivos del proceso estratégico a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

ALCANCE

Verificar la adecuada aplicación de los controles establecidos por la OTIC de los procedimientos que conforman el proceso Estrategia de Tecnologías de la Información y las Comunicaciones, correspondiente al periodo comprendido entre julio 2020 y abril 2021, con base en muestreo aleatorio y las directrices emitidas en el Manual del Sistema de Seguridad de la Información y en la Metodología para el Desarrollo y Mantenimiento de Soluciones, aplicables en la materia de acuerdo con las pruebas practicadas.

EQUIPO AUDITOR:

Jorge Eliecer Gómez Quintero - Jefe Oficina de Control Interno.
Constanza Cárdenas Aguirre – Auditora de Sistemas.

METODOLOGIA APLICADA

Para el desarrollo de las pruebas de auditoría al proceso Estrategia de Tecnologías de la Información y las Comunicaciones, se aplicaron las técnicas de auditoria internacionalmente aceptadas tales como indagación, observación, inspección y comprobación selectiva a través de muestreo, entre otros.

MARCO NORMATIVO:

- Caracterización del proceso Estrategia de Tecnologías de la Información y las Comunicaciones (4204000-PO-051 V01 de septiembre 2018).
- Elaboración del Plan Estratégico de TI basado en la Arquitectura Empresarial de TI (2213200-PR-116 V12 de agosto 2020).
- Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200-PR-106 V13 de febrero 2020)
- Activos de Información (2213200-PR-187 V09 de diciembre 2020).
- Plan Estratégico de Tecnologías de Información PETI (2211700-OT-043 V06 de octubre 2019).
- Guía para el Inventario, Clasificación, Etiquetado de Información, protección de datos personales y análisis de riesgos de los Activos de Información (2213200-GS-004 V08 de julio 2020)

- Protocolo para la elaboración de Fichas Técnicas para Adquisición de Infraestructura Tecnológica (2211700-GS-048 V02 de junio 2018).
- Manual del Sistema de Seguridad de la Información (4204000-MA-031 V02 de julio 2020)
- Manual de Políticas y procedimientos para el tratamiento de datos personales (4204000-MA-033 V01 de diciembre 2019).
- Metodología para el Desarrollo y Mantenimiento de Soluciones (2213200-OT-006 V04 de febrero 2020).
- Lineamientos para la implementación y sostenibilidad del sistema se gestión de seguridad de la información (2211700-OT-048 V02 de septiembre 2018).
- Mapa de Riesgos del proceso publicada en el Sistema Integrado de Gestión del 30 abril 2021.

LIMITACIÓN DEL ALCANCE

Con relación a los proyectos tecnológicos, no fue factible evidenciar el cumplimiento de los numerales 5.3.2, 5.4.2 y 5.5.6, de la Metodología para el Desarrollo y Mantenimiento de Soluciones (OT-006) que, de acuerdo con lo indicado en respuesta recibida de la OTIC, aplican para sistemas de información terminados y en producción, y en la población de proyectos para el periodo evaluado no se tuvieron proyectos que cumplieran con esta característica.

CONCLUSION

Como resultado de las pruebas de auditoría practicadas al proceso de Estrategia de Tecnologías de la Información y las Comunicaciones para el período comprendido entre julio de 2020 y abril de 2021, proceso a cargo de la OTIC, el cual apoya la implementación del Plan Estratégico de TI (PETI) y permite el acceso oportuno a la información requerida por la entidad, se concluyó que se encuentran implementados y operando algunos de los controles asociados a la definición del Plan Estratégico de TI como a la implementación de soluciones e identificación de los Activos de Información de la Entidad, en cuanto a:

- Se evaluó la efectividad de los controles establecidos en el documento 2211700-OT-048 – lineamientos para la implementación y sostenibilidad del Sistema de Gestión de Seguridad de la Información asociados al anexo A de la norma ISO27001:2013, obteniendo una calificación en la autoevaluación promedio del 83% de efectividad en los controles de seguridad de la información evaluados, con porcentajes bajos en los aspectos de: criptografía (40%), adquisición, desarrollo y mantenimiento de sistemas (57%), gestión de incidentes de seguridad de la información (60%), aspectos de seguridad de la información de la gestión de la continuidad del negocio (67%) y seguridad de las operaciones (76%).

- El procedimiento Activos de Información (2213200-PR-187 V09 de diciembre 2020) se encuentra debidamente actualizado, publicado y se observó efectividad en la ejecución de los controles definidos en el mismo. Asimismo, se corrigió la deficiencia encontrada en la auditoría de la vigencia anterior, relacionada con la definición de un plan de tratamiento para la mitigación de los riesgos asociados a los Activos de Información clasificados como Extremos o Altos.

- Para el procedimiento Plan Estratégico de Tecnologías de Información, se evidenció la ejecución de algunas actividades iniciales del procedimiento referentes a la formulación del PETI y un documento borrador con los avances para la construcción del PETI vigencia 2020-2024.

  No obstante, se observaron situaciones para las que se requieren acciones correctivas inmediatas y otras susceptibles de mejora, relacionadas con:

- La necesidad inmediata de implementar un cambio sustancial al procedimiento de Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200-PR-106), observación efectuada el año anterior y que se encuentra en proceso de ejecución con las acciones de mejora 417 y 418.

- Definición pronta y aprobación del Plan Estratégico de tecnologías de información - PETI (2211700-OT-043) para la vigencia 2020-2024.

- Actualización de los documentos: caracterización del proceso (4204000-PO-051), Plan Estratégico de Tecnologías de Información PETI (2213200-PR-116), formatos de Recepción documentación software (2213200-FT-744) y Ubicación Física en cuartos de Medios (2213200-FT-743).

OBSERVACIONES Y RECOMENDACIONES PRODUCTO DE LA EVALUACIÓN

Para evaluar el Proceso de Estrategia de Tecnologías de la Información y las Comunicaciones, se realizaron pruebas a los controles implementados por la Entidad para definir el Plan Estratégico de TI, la implementación de proyectos con alto contenido tecnológico y soluciones tecnológicas, la identificación de los Activos de Información sensibles y de las bases de datos personales que se manejan en la entidad.

En tal sentido a continuación, se describen los principales aspectos observados y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Documentación del Proceso en el Sistema Integrado de Gestión (caracterización, procedimientos, guías, manuales y otros procedimientos)

Oportunidad de Mejora No. 1:

Analizados los documentos en el Sistema Integrado Gestión que componen el proceso evaluado, se observó que algunos fueron actualizados durante el segundo semestre de 2020, en atención a las observaciones transmitidas por esta Oficina en la evaluación anterior; sin embargo, aún existen documentos sin actualizar y/o sin evidencia de revisión que confirme que aún se encuentran vigentes.

Los documentos son:

- Caracterización del proceso Estrategia de Tecnologías de la Información y las Comunicaciones (4204000-PO-051 V01 de septiembre 2018).
- Elaboración del Plan Estratégico de TI basado en la Arquitectura Empresarial de TI (2213200-PR-116 V12 de agosto 2020).

- Plan estratégico de tecnologías de la información – PETI 2016-2020 (2211700-OT-043 V06 de noviembre 2019), correspondiente a la vigencia 2016-2020.
- Protocolo para la elaboración de Fichas Técnicas para Adquisición de Infraestructura Tecnológica (2211700-GS-048 V02 de junio 2018).
- Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200-PR-106 V13 de febrero de 2020).
- Lineamientos para la implementación y Sostenibilidad del Sistema de Gestión de Seguridad de la Información (2211700-OT-048 V02 de julio de 2018)
- Recepción Documentación Software (2213200-FT-744 V02 de octubre de 2013)
- Ubicación Física en Cuarto de Medios (2213200-FT-743 V01 enero de 2011)

Teniendo en cuenta lo observado, se sugiere que, desde la OTIC, como oficina líder del proceso, y con el apoyo de la Oficina Asesora Planeación, se revise y actualice la Caracterización del Proceso, con base en la operatividad de los procedimientos encaminados a asegurar que todos los documentos (manuales, guías y otros documentos) estén claramente referenciados y documentados en la caracterización respectiva, y sean entendibles para todas las partes interesadas.

Asimismo, revisar detalladamente todos los documentos contentivos del proceso Estrategia de Tecnologías de la Información y las Comunicaciones para confirmar que se encuentran actualizados y establecer si los que a hoy tiene fechas antiguas del año 2011, 2015 y 2018 requieren ser actualizados o siguen vigentes en su aplicación integral.

Producto de la recomendación realizada en la auditoría de la vigencia anterior, actualmente se cuenta con los Planes de Acción No. 410, 412, 417, 418, 421 encaminados a la actualización de la caracterización del proceso y de los procedimientos PR106 Análisis, Diseño, Desarrollo e Implementación de Soluciones y PR116 Elaboración del Plan Estratégico de TI basado en la Arquitectura Empresarial de TI.

Oportunidad de Mejora No. 2:

Para algunos de los documentos actualizados durante el segundo semestre del año 2020 y el primer semestre de 2021, no se encontró evidencia de socialización de los mismos en el Subcomité de Autocontrol del área, y aunque para algunos se evidencia soporte de socialización en el informe anexo presentado por la Ingeniera a cargo del tema, no es factible concluir que si se realizó o no la presentación en el Subcomité debido a que: no hay acta del subcomité (octubre 2020) o en las actas evidenciadas (julio 2020, septiembre 2020, enero 2021) no se hace referencia a la labor realizada ni al informe presentado.

Se sugiere que luego de revisar detalladamente todos los documentos contentivos del proceso Estrategia de Tecnologías de la Información y las Comunicaciones y se confirme que se encuentran actualizados, se realice la socialización correspondiente con el equipo de trabajo y funcionarios que tengan relación con los mismos.

2. Indicador de medición del proceso GE-04 Porcentaje de Disponibilidad y Operación de los Sistemas de Información de la Secretaría General

Oportunidad de Mejora No. 3:

Analizados los resultados entre julio 2020 y abril 2021 del indicador GE-04 denominado “Porcentaje de disponibilidad y operación en los sistemas de información, páginas y sitios web de la SG”, el cual mide “la disponibilidad de Sistemas de Información y Sitios Web para que los usuarios los puedan operar y/o consultar, mediante el monitoreo de Bases de Datos, Sistemas de Información y de la Infraestructura Tecnológica”, se observó que el indicador cumple la meta definida del 96% alcanzando cumplimientos de entre el 99,8% y el 100%, entre julio 2020 y abril 2021, resultados que son reportados por la OTIC mensualmente a la OAP.

Se observaron algunas situaciones de diferencias mínimas en la ficha del indicador que se emite mensualmente a la OAP, que deben ser revisadas con el fin de asegurar la validez, utilidad y efectividad del indicador actual:

- En septiembre de 2020, en dos secciones diferentes del documento soporte, se refleja un 100% de cumplimiento y en otra parte el 99,8%, con un 59,97% de cumplimiento en los sistemas misionales.
- En noviembre de 2020, se observa un cumplimiento del 99,80%, aun cuando los porcentajes individuales están cumplidos al 60% misionales, 25% administrativos y 15% portales.
- En febrero de 2021, se presenta un 100% de cumplimiento con porcentajes de 59,96% y 59.87% en disponibilidad de los sistemas misionales, estos valores diferentes en dos sesiones del documento, aunque hacen referencia al mismo dato de disponibilidad de los sistemas misionales.

Resaltamos que este indicador se encuentra en proceso de revisión concordante con el Plan de Acción No. 413, que para el último seguimiento con corte mayo 2021, esta Oficina de Control solicitó incluir la fuente de información del indicador y los Sistemas de Información objeto de medición, pues se considera que con la revisión del indicador generado por la herramienta ADPLATEC construida hace más de 4 años y revisada en el último año pero sin generar cambios representativos en el indicador, aún no se soluciona la causa-raíz de la observación para asegurar la efectividad del indicador y garantizar la integridad de las fuentes de información y la inclusión de todos los sistemas críticos de la Entidad.

Teniendo en cuenta la respuesta recibida al informe preliminar por la OTIC, se realizará ajuste de la acción 413 incluyendo esta situación, para que la acción sea culminada cuando se realice la revisión de los reportes de indicadores en los meses de agosto, septiembre y octubre de 2021.

Oportunidad de Mejora No. 4:

Analizado el indicador del proceso denominado GE-04 “Porcentaje de disponibilidad y operación en los sistemas de información, páginas y sitios web de la SG” a la luz del objetivo del proceso, no se observa una relación directa del indicador con el objetivo del mismo.

Se observa que no se cuenta con un indicador que permita medir la efectividad del proceso Estratégico de Tecnologías de la Información, para los procedimientos contentivos del mismo, tales como: cantidad de proyectos o soluciones tecnológicas implementadas en el periodo, porcentaje de avance en el desarrollo de las soluciones tecnológicas, controles sobre activos de información validados, etc.

En consecuencia, es importante que la OTIC adelante gestiones encaminadas a revaluar las variables y fuentes de información con que se realiza el cálculo de disponibilidad y operación de los Sistemas de Información de la Entidad, garantizando así la validez del mismo y realizar los ajustes necesarios que permitan asegurar que todos los sistemas de información y variables posibles para el cálculo del mismo están siendo incluidas permitiendo a la entidad identificar oportunamente indisponibilidad de los sistemas de información y tomar medidas conducentes a solucionar la causa raíz de las fallas presentadas.

De igual forma es necesario, que se realicen revisiones periódicas del indicador, con miras a identificar mejoras constantes en el mismo o la necesidad de implementar nuevos indicadores para la medición del proceso, aspectos que, según mejores prácticas de mediciones, se gestionan cuando los indicadores existentes se encuentran estabilizados, permitiendo contar con retos y metas diferentes.

3. Plan Estratégico de Tecnología basado en la Arquitectura Empresarial de TI (2213200-PR-116)

Observación No. 1

A la fecha del cierre de la auditoría, se contaba con un documento borrador del Plan Estratégico de Tecnología – PETI 2020-2024 y aunque se evidenciaron soportes de las reuniones realizadas con algunas de las dependencias (Víctimas, Archivo y Servicio a la Ciudadanía) donde se revisaron los proyectos de cada área con alto componente tecnológico. La tarea de construcción del PETI fue suspendida por causa mayor desde finales del mes de marzo de 2021 y al momento de cierre, y al cierre de la auditoría, la OTIC se encontraba en proceso de contratar el recurso humano que pudiese dar continuidad a la labor.

Recomendación

Es importante Priorizar, construir y aprobar, en el menor tiempo posible, el Plan Estratégico de Tecnologías de la Información y Comunicaciones para la vigencia de esta administración (2020-2024), incluyendo los proyectos con alto componente tecnológico de cada una de las dependencias de la Entidad.

4. Metodología para el Desarrollo y Mantenimiento de Soluciones (OT-006) del Procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones (2213200 – PR-106)

Observación No. 2

Analizados los soportes para gestión de cambios, según lineamientos establecidos en la Metodología para el Desarrollo y Mantenimiento de Soluciones (OT-006), para una muestra de ocho (8) despliegues registrados en GLPI, cinco (5) cambios BTE y dos (2) despliegues SIAB, se obtuvieron los siguientes resultados para la muestra tomada de los 15 registros de los 112 cambios existentes:

- Todos los cambios de la muestra cuentan con una solicitud o FRC diligenciado, cumpliendo lo indicado en el punto 1-Documento de solicitud de cambio o FRC del numeral 5.7.1. Documentación requerida para el Manejo del Cambio.

- No se observó clasificación de los tipos de cambios (Menor, Normal o Emergencia), según se establece en las Condiciones Generales del Proceso de Gestión de Cambio de la Metodología. En los soportes revisados y anexos en cada caso de soporte en la herramienta GLPI, se identifica que la clasificación del cambio está dada en Mediana, Alto, Bajo para la atención del soporte en GLPI o según el impacto definido en el FRC – Formato Requerimiento del Cambio, pero no identifica si el cambio es Menor, Normal o de Emergencia.

- Cuatro (4) de los quince (15) cambios de la muestra, no cuentan con una clasificación del impacto en el FRC. Los cambios son lo que se identifican como caso de soporte con los Nos.: 180652, 174844, 204860 y 215005.

- Once (11) de los de los quince (15) cambios de la muestra, no cuentan con información sobre actualización de documentos y versionamiento, punto 3. Actualización de documentos y versionamiento de numeral 5.7.1. Documentación requerida para el Manejo del Cambio.

- Uno (1) de los doce (12) despliegues realizados en el ambiente productivo no cuentan con el Plan de Paso a Producción, incumpliendo lo indicado en el punto 4. Plan de Paso a Producción del numeral 5.7.1. Documentación requerida para el Manejo del Cambio.

- Para once (11) de los quince (15) cambios de la muestra, no se evidenció soporte de pruebas realizadas ni evidencia de aprobación de la mismas.

Observación No. 3

Revisados los Roles de la Gestión de Cambio, definidos en el numeral 5.7 Manejo del Cambio de la Metodología para el Desarrollo y Mantenimiento de Soluciones, y de acuerdo con las evidencias soporte de los cambios y soluciones tecnológicas evaluados, no se cuenta con la instancia de Comité de Cambios que en el documento mencionado se define como: “Grupo de personas con autoridad y competencia para evaluar los cambios a ejecutar, y quienes tienen potestad de aprobar, denegar o solicitar ajustes del cambio teniendo en cuenta el impacto generado a nivel técnico y funcional. El comité de cambios deberá ser convocado por el gestor del proceso de cambios, quien es el encargado de agendar las reuniones periódicas donde incluya a todos los involucrados y realizar la pre-agenda del comité”.

En el documento evaluado “OT-006 Metodología para el Desarrollo y Mantenimiento de Soluciones” se establecen lineamientos relacionados con el Comité de Cambios respecto a sus participantes, funciones, tipos de cambio que requieren aprobación del Comité; sin embargo, en la Secretaría General no se tiene implementado este Comité de Cambios (CAB).

Las anteriores situaciones mencionadas, generan riesgos de implementación de soluciones y/o cambios sin cumplir con los lineamientos establecidos por la entidad, dificultad para establecer y asignar responsabilidades ante eventuales errores o inconsistencias en los sistemas en producción.

Recomendación observaciones 2 y 3

Evaluar y actualizar la Metodología para el Desarrollo y Mantenimiento de Soluciones (2213200-OT-006), a la luz de la dinámica y operatividad que actualmente se desarrolla en la OTIC para la gestión de cambios e implementación de soluciones, definiendo la documentación soporte y de control que se requiere para cada tipo de requerimiento o necesidad tecnológica (cambio o proyecto).

Asimismo, como mejor práctica en el ciclo de desarrollo y mantenimiento de aplicaciones, implementar la instancia de aprobación del Comité de Cambios para la puesta en producción de los cambios y los proyectos, con las funciones y tareas mínimas acorde con la dinámica de la operación de la OTIC.

5. Manual del Sistema de Seguridad de la Información (4204000-MA-031)

Observación No. 4

Analizados los soportes recibidos de la OTIC respecto a las socializaciones o concientización a los funcionarios sobre las políticas para el manejo de la información realizadas durante el periodo evaluado, se observó lo siguiente:

- En el mes de Julio 2020, se realizaron capacitaciones relacionadas con el proceso de actualización de Activos de Información de las dependencias y sensibilizaciones de datos abiertos.
- En agosto, septiembre y octubre de 2020, se continuaron las capacitaciones relacionadas con el proceso de actualización de Activos de Información de las dependencias.
- En noviembre y diciembre 2020, se realizaron sensibilizaciones sobre el Manual de Seguridad de la Información a: Subdirección de Servicios Administrativos y la OTIC.
- Se evidenciaron boletines publicados en febrero, marzo y abril de 2021, relacionados con alertas sobre malware.

Asimismo, seleccionada una muestra de nueve (9) funcionarios y nueve (9) contratistas, que ingresaron o suscribieron contrato durante el periodo evaluado, para ninguno de ellos se evidenció su participación en las capacitaciones mencionadas.

Los soportes observados denotan algunas sensibilizaciones sobre temas de seguridad tanto para funcionarios como para contratistas, sin embargo, no se cuenta con un plan de capacitación preestablecido y ejecutado para el periodo evaluado. De igual forma, no se evidencian capacitaciones establecidas para los funcionarios y/o contratistas para cuando inician su relación laboral o contractual con la Entidad.

Lo anterior conlleva a riesgos de incumplimiento de políticas de seguridad establecidas en materia de Seguridad Informática, falta de compromiso y apropiación de las mismas por parte de los funcionarios y contratistas.

Recomendación

Desde la OTIC, coordinar en conjunto con el área de Talento Humano la generación de un plan anual de capacitación y/o sensibilizaciones en los temas de Seguridad de la Información, teniendo en cuenta un programa específico para cuando los funcionarios ingresan a la entidad (planta, temporales, contratistas), como sesiones de actualización y finalmente sesiones de sensibilización generales durante el año para grupos específicos según se determine.

Observación No. 5

De acuerdo con lo establecido en el Manual del Sistema de Seguridad de la Información (4204000-MA-031, en su numeral 7.1.4 Administración de las políticas, se establece que: "Todo lineamiento de seguridad de la información nuevo, modificado y/o eliminado, serán propuestos por la Oficina de Tecnologías de la Información y las Comunicaciones y serán aprobadas por el Comité Institucional de Gestión y Desempeño de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

Dichos lineamientos serán revisados como mínimo una vez al año y/o cada vez que sea requerido", se analizaron las actas del Comité Institucional de Gestión y Desempeño de la SG, sin observar la aprobación por parte de esta instancia sobre los cambios realizados en el manual V02 publicado en julio 2020 con los cambios en temas relacionados con Política de intercambio de información, Política de uso aceptable de activos, Política desarrollo seguro, Política relación con proveedores, Política copia y respaldos y control de software.

Recomendación

Dar cumplimiento al lineamiento definido en el Manual del Sistema de Seguridad de la Información (4204000-MA-031) y someter a consideración del Comité Institucional de Gestión y Desempeño la aprobación de las políticas de Seguridad de la Información establecidas en el Manual y según modificación realizada en julio 2020.

De igual forma, tener en cuenta este lineamiento y da cumplimiento al mismo cuando se realice actualización en nueva versión del Manual indicado.

Oportunidad de Mejora No. 5

Verificadas los documentos soporte (informes presentados al Subcomité de Autocontrol por la Oficial de Seguridad de la Información) se evidencian la revisión y actualización del Manual del Sistema de Seguridad de la Información, dando cumplimiento al numeral 7.3 del manual mencionado; sin embargo, no es factible identificar si para esta actualización se realizó el análisis respecto a: Incidentes de seguridad de la información, requerimientos de ley, mapa de riesgos de la entidad y nuevas vulnerabilidades detectadas, según se determina en el numeral indicado puesto que en los documentos no se mencionan estos aspectos.

Al respecto, es conveniente mencionar que el manual se encuentra actualizado, pero no se cuentan con soportes previos que permitan concluir sobre las fuentes de información utilizadas o respecto a reuniones realizadas para la actualización del mencionado manual.

Por lo anteriormente expuesto, se recomienda que en la próxima actualización del Manual se deje soporte de las fuentes de información utilizadas y las conclusiones sobre el análisis realizado a cada uno de los aspectos mencionados en el numeral 7.3 del Manual del Sistema de Seguridad de la Información, al igual que se dejen actas de las reuniones realizadas para dicha actualización.

Observación No. 6

Para una muestra de nueve (9) incidentes de una población de 452, generados del aplicativo GLPI por la OTIC, registrados durante el período de evaluación y categorizados en infraestructura/seguridad informática, se observó que corresponden a solicitudes de asignación o soporte de conexión VPN, solicitud de usuario o contraseña, solicitud de instalación de software, que no corresponden con las categorías de tipificación definidas en la Guía de Gestión de Incidentes de Seguridad en su numeral 5.Clasificación.

Analizadas las tipificaciones definidas en la Guía de Incidentes de Seguridad vs las parametrizadas en la herramienta de mesa de servicio GLPI, se observó que:

- En GLPI hay 18 categorías dentro de Seguridad Informática, de las cuales siete (7) concuerdan con las categorías de tipificación establecidas en la guía de incidentes de Seguridad.
- De diecisiete (17) categorías establecidas en la guía, no existe una tipificación en GLPI para diez (10) de ellas.
- De las dieciocho (18) categorías de GLPI, diez (10) no se encuentran definidas en la guía de incidentes de seguridad.

Recomendación

Revisar las categorías parametrizadas en la herramienta GLPI de la Mesa de Servicio vs la clasificación definida en la Guía de Gestión de Incidentes de Seguridad, y evaluar si se requiere actualizar la Guía mencionada o ajustar la parametrización en la herramienta de Mesa de Servicio de forma que sea coherente con los lineamientos establecidos en la Guía mencionada.

Observación No. 7

Revisada una muestra de nueve (9) incidentes de una población de 452, generados del aplicativo GLPI por la OTIC, respecto a la gestión y documentación requerida en su atención y análisis, según lo definido en la Guía de Gestión de Incidentes de Seguridad, se observaron las siguientes situaciones:

- Ninguno de los nueve (9) incidentes de la muestra cuenta con clasificación según el numeral 3 y 5 de la Guía Incidentes de Seguridad, no se les realizó evaluación del impacto ni se evidencia que el Oficial de Seguridad haya definido su criticidad como se establece en los mismos numerales de la Guía de Incidentes de Seguridad.

- No se cuenta con evidencia que permita identificar si se siguieron los niveles de escalamiento establecidos de acuerdo con la clasificación del incidente.

- Los incidentes de la muestra no corresponden a una tipificación de incidente de seguridad que amerite la documentación y recolección de evidencia como se indica en la guía de incidentes de seguridad.

Observación No. 8

Verificadas las actas de los Subcomités de Autocontrol de la OTIC realizadas durante el período evaluado, y según reunión realizada el 20 de mayo de 2021 con los funcionarios de la OTIC (La Oficial de Seguridad y la Gestora de Calidad), no se identificaron soportes que den cuenta de la ejecución de la labor respecto a la generación de un informe de eventos e incidentes que se haya presentado al Subcomité de Autocontrol, según lo establecido en la Guía de Gestión de Incidentes de Seguridad en la sección "Actividades Pos-incidente" del numeral 6.

Recomendación observaciones 7 y 8

Es necesario evaluar y actualizar lo más pronto posible la Guía de Gestión de Incidentes de Seguridad (2211700-GS-042), a la luz de la dinámica y operatividad que actualmente se desarrolla en la entidad para la gestión de incidentes de seguridad, definiendo la documentación soporte y de control que se requiere para cada tipo de incidente.

6. Otros temas evaluados, relacionados con Seguridad de la Información (VPN y Equipos de Cómputo en Modalidad Teletrabajo)

Oportunidad de Mejora No. 6

Recibida de la SSA, la relación de equipos de cómputo entregados a funcionarios para la modalidad de teletrabajo, se seleccionó una muestra de computadores y de otros equipos como teclados, impresoras, escáneres, observando que para una población de sesenta y ocho (68) equipos de cómputo asignados para teletrabajo:

1. Cuatro (4) de ellos, correspondiente al 5,9%, no cuentan con formato FT- 311 V06 – Autorización de Salida de Elementos. Los equipos corresponden a las placas: 37533 – Impresora Láser, 37516 – Tablet Digitalizadora, 72065 – Tablet Apple Ipad, 54653 -Teclado.

2. Dos (2) formatos, correspondiente al 3%, no cuenta con la firma del responsable del inventario en SAI, en señal de autorización o recepción del equipo por parte del funcionario a cargo del inventario respectivo según se registra en el aplicativo SAI. Placas: 42316 – Computador Portátil y 32470 – Computador Portátil.

3. Cuatro (4) formatos, correspondientes al 5.9%, no cuentan con la firma del jefe de la Dependencia. Las placas son: 24713 – Teclado, 38494 – CPU, 38535 – Monitor, 38629 – Mouse.

4. Ninguno de los ocho (8) computadores o tabletas de la muestra, cuentan con acuerdo de confidencialidad para el manejo de la información guardada en los mencionados equipos.

Sin bien es entendido que a causa de la emergencia sanitaria por la pandemia Covid19, se implementaron procedimientos contingentes alternos, y específicamente para la entrega de equipos a funcionarios en modalidad teletrabajo / trabajo remoto, se utilizó el formato FT-311 V06 y el procedimiento PR233-Movimientos de Bienes V06, ambos documentos con fecha de publicación 25/08/2018, se considera necesario actualizar los mencionados documentos de acuerdo con la dinámica actual de la operatividad y bajo el entendido de contar con una nueva modalidad que perdurará en el tiempo como es el trabajo remoto / teletrabajo.

Observación No. 9

Verificado el cumplimiento de la Política para Teletrabajo (numerales 10.2 - Política para Teletrabajo y 10.2.1 - Condiciones Obligatorias) establecida en el Manual del Sistema de Seguridad de la Información, se seleccionó una muestra de nueve (9) registros de conexiones VPN de un total de 327 registradas en GLPI durante el periodo evaluado, evidenciando que:

- Tres (3) de ellas no cuentan con firma de aprobación en el formato FT-1000 o un mail soporte de dicha aprobación (teniendo en cuenta los procedimientos alternos debido a la modalidad de teletrabajo implementada a raíz de la emergencia sanitaria por Covid19). Los registros en GLPI son: 211349, 190505, 181433.
- Dos (2) no cuentan con formato FT-1000. Los casos GLPI son: 181017 y 174968.
- Dos (2) acuerdos de confidencialidad no se encuentran diligenciados ni firmados. Los casos GLPI son: 190505, 175462
- Una VPN sin soporte de acuerdo de confidencialidad. El caso GLPI es: 181017

Recomendación

Si bien esta situación puede estar dada por la contingencia debido a la emergencia sanitaria por la pandemia Covid19, es necesario dar cumplimiento a la Política y en caso de no poderse ejecutar los controles establecidos, se implementen los controles alternos o compensatorios que mitiguen el riesgo de uso del recurso tecnológicos de conexión por VPN sin autorización o sin una manifestación (por otro medio electrónico que no requiera la firma física) del cumplimiento del Acuerdo de Confidencialidad respectivo.

7. Mapa de Riesgos y Controles en el Proceso

Verificada la matriz de riesgos del proceso, se observó que los controles definidos en la misma se encuentran actualizados y son consistentes con los puntos de control de los procedimientos del mismo, observando algunas situaciones que se consideran oportunidades de mejora, como son:

Oportunidad de Mejora No. 7

Se evidenció que el Mapa de Riesgos del proceso publicado en el SIG con fecha abril 2021, se encuentra desactualizado, por las siguientes razones:

- Solicitados los soportes de los monitoreos realizados a los controles definidos en los mapas de riesgo, se encuentran evidencias de la ejecución de los mismos, más no un monitoreo periódico que se realice desde la OTIC para concluir sobre la efectividad de los mismos y la materialización o no de los riesgos. Por ejemplo, se evidenció la descripción de las actividades realizadas con memorandos, archivos, reuniones, formatos, sin embargo, no se realiza monitoreo periódico que permita asegurar la efectividad de cada control.
- Con respecto al procedimiento PR-106 Análisis, Diseño, Desarrollo e Implementación de Soluciones, se observó que los registros documentales de los controles No. 3, 5 y 8 difieren de los establecidos en el mapa de riesgos. Asimismo, en las evidencias analizadas en cumplimiento a la ejecución del control No.3 respecto al análisis de viabilidad del requerimiento, no se observó relación entre cada solicitud realizada por las dependencias vs un caso de servicio en GLPI, no permitiendo contar con una trazabilidad adecuada sobre la ejecución del control.

Por lo anterior, es conveniente adelantar las gestiones de acompañamiento de la Oficina Asesora de Planeación para actualizar lo antes posible el procedimiento PR-106 Análisis, Diseño, Desarrollo e Implementación de Soluciones y en caso de requerirse el mapa de riesgos del proceso para asegurar la consistencia del mismo frente a los controles aplicados y los establecidos en los procedimientos.

Asimismo, es importante que en instancia del subcomité de autocontrol o las actividades cotidianas de seguimiento al proceso, es fundamental evaluar periódicamente la efectividad de los controles implementados para detectar oportunamente los fallos en su aplicación que pueden permitir la materialización de los riesgos identificados, entre otros como: desarrollo inapropiado de soluciones tecnológicas, proyectos con alto componente tecnológico sin el seguimiento adecuado.

Plan de Mejoramiento

Producto de la evaluación practicada y resultado del análisis del informe preliminar, la Oficina de Tecnologías de la Información y las Comunicaciones, definió acciones de mejora dirigidas a subsanar y prevenir las observaciones identificadas como gestionar las oportunidades de mejora, las cuales conforman el plan de mejoramiento establecido que hace parte integral del informe final, a efecto de adelantar los respectivos seguimientos por los responsables como por la Oficina de Control Interno para su cumplimiento.

Criterios de clasificación de conceptos derivados de la auditoría.

Tipo de observación	Descripción
Observación	Incumplimiento de normas o procedimientos internos que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

Elaborado por: Constanza Cárdenas Aguirre – Contratista, Auditora de Sistemas
Revisado y Aprobado por: Jorge Eliecer Gómez Quintero – Jefe Oficina de Control Interno