

<b>Proceso Auditado:</b>	Sistema de Gestión de Seguridad de la Infomación-SGSI Norma ISO 27001:2013	<b>Responsable del Proceso Auditado:</b>	Edgar Martin Cubides Rojas
<b>Auditor(a):</b>	Carlos Orlando León Valenzuela- Sandra Patricia Camago Rodriguez-Martha Cecilia Gallo Medina	<b>Fecha de Seguimiento:</b>	Abril 26 de 2023

Ítem	FUENTE	HALLAZGO	RIESGO IDENTIFICADO	ACCIÓN	INDICADOR	FECHA INICIO	FECHA FIN	RESPONSABLE	ESTADO	OBSERVACIÓN
1	Auditoría Interna	<p><b>N.C:</b> La Dirección de las Tecnologías de la Información y las comunicaciones-DTIC informa que los roles y responsabilidades y autoridades del SGSI se encuentran en la Resolución 406 de 2020, revisada la mencionada Resolución se evidencia las responsabilidades de los procesos frente a las Dimensiones Operativas del MIPG, el Comité de Gestión y Desempeño, el Modelo Integrado de Planeación y Gestión-MIPG, los responsables de los sistemas de gestión y frente al SGSI solo relaciona la responsabilidad del Director de Tecnologías de Información y Comunicaciones, pero no se relacionan las responsabilidades y autoridades respecto a otros niveles de la organización que hacen parte del SGSI, tampoco se evidenció algún otro documento que presentará los roles y responsabilidades el SGSI en el listado maestro de documentos del Sistema, incumpliendo con el numeral 5.3 Roles, Responsabilidades y Autoridades en la Organización literales a) y b) de la norma ISO 27001:2013.</p>	Desconocimiento de los roles, responsabilidades y autoridad en la Entidad respecto al SGSI	Generar un documento que especifique claramente los roles, responsabilidades y autoridades que hacen parte de del Sistema de Gestión de Seguridad de la Información conforme al numeral 5.3 de la norma NTC-ISO-27001.	Un Documento aprobado y socializado	03/10/2022	31/12/2022	Director de TIC	A	<p>Mediante correos de fecha 20 y 21 de abril de 2023, el Proceso allega Proyecto de documento denominado "ROLES Y RESPONSABILIDADES SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI", el cual se encuentra pendiente de aprobación por parte del Comité Institucional de Gestión y Desempeño - CIGD.</p> <p>DTIC señala que están solicitando ampliar el plazo de terminación de esta acción para junio 30 de 2023, debido a que no fue posible dar cumplimiento oportuno porque la contratación de los profesionales que realizarían esta actividad se gestionó hasta mediados del mes de marzo de 2023.</p> <p>Por lo anterior, la Oficina de Control Interno considera mantener <b>ABIERTA</b> esta No Conformidad hasta tanto el documento "ROLES Y RESPONSABILIDADES SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI" se encuentre aprobado y socializado, como lo establece su Indicador.</p>
2	Auditoría Interna	<p><b>N.C:</b> La DTIC entrega como medición de los objetivos del SGSI el instrumento llamado "Diagnóstico Actual y Brechas ISO 27001- MSPI - Personería de Bogotá", verificado el documento Diagnóstico Actual y Brechas se evidenció que este instrumento realiza mediciones del Anexo A Objetivos de Control y Controles de Referencia Norma ISO 27001:2013, también evalúa el grado de avance del Modelo de Seguridad de la Información-MSPI, pero no hace seguimiento y medición de los objetivos del SGSI. Así mismo, verificados los planes que se encuentran en el listado maestro de documentos del SGSI y los planes presentados por DTIC, se evidenció que estos planes tienen objetivos diferentes a los del SGSI y tampoco existe evidencia de su medición y seguimiento. Por lo anterior, no se realiza el seguimiento de los objetivos del Sistema de Gestión de Seguridad de la Información, como tampoco se evidenciaron los planes para lograrlos, incumpliendo con el numeral 6.2 Objetivos de Seguridad de la Información y Planes para Lograrlos literales f), g), h), i) y j) de la norma ISO 27001:2013.</p>	Incumplimiento de los objetivos del SGSI por falta de seguimiento y medición.	Diseñar una metodología del SGSI enfocado a la medición de los objetivos y alineado a los diferentes planes según lo establecido en el numeral 6.2 de la NORMA NTC-IEC27001	Una metodología de medición y seguimiento a los objetivos del SGSI	03/10/2022	31/12/2022	Director de TIC	C	<p>Mediante correos de fecha 20 y 21 de abril de 2023, el Proceso allega los siguientes documentos: en formato EXCEL la Matriz_SGSI_2023 y en formato PDF el Acta de fecha 12/04/2023 relacionada con la revisión y aprobación de la Matriz Sistema de Gestión de Seguridad de la Información - SGSI.</p> <p>DTIC señala que ya se encuentran ajustados y aprobados dichos documentos por parte del Director de la DTIC, adicionalmente informa que se ajustaron de ocho (8) a cinco (5) los Objetivos del SGSI, los cuales fueron aprobados en el Comité Institucional de Gestión y Desempeño del 20/04/2023 y se encuentra pendiente la publicación en los canales institucionales, prevista para realizarse en el mes de abril de 2023.</p> <p>Por lo anterior, la Oficina de Control Interno considera dar <b>CIERRE</b> a esta No Conformidad.</p>

<b>Proceso Auditado:</b>	Sistema de Gestión de Seguridad de la Información-SGSI Norma ISO 27001:2013	<b>Responsable del Proceso Auditado:</b>	Edgar Martin Cubides Rojas
<b>Auditor(a):</b>	Carlos Orlando León Valenzuela- Sandra Patricia Camago Rodriguez-Martha Cecilia Gallo Medina	<b>Fecha de Seguimiento:</b>	Abril 26 de 2023

Ítem	FUENTE	HALLAZGO	RIESGO IDENTIFICADO	ACCIÓN	INDICADOR	FECHA INICIO	FECHA FIN	RESPONSABLE	ESTADO	OBSERVACIÓN
3	Auditoría Interna	<p>N.C:Verificados los documentos del SGSI en la página web de la Entidad en el link MIPG (<a href="https://www.personeriabogota.gov.co/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-lainformacion-sgsi">https://www.personeriabogota.gov.co/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-lainformacion-sgsi</a>), Sistemas de Gestión, Sistema de Gestión de Seguridad de la Información, se evidenció publicado el alcance del SGSI con un enfoque a los activos de información, plataformas tecnológicas y procesos; posteriormente verificado el documento Política General de Seguridad de la Información y del cual hace parte también la publicación del alcance del SGSI mostrando el alcance aprobado por la Alta Dirección y que difiere en su contenido de la publicación del alcance que hace la presentación del sistema de gestión.</p> <p>Así mismo, se revisa el contenido de la intranet de la Entidad por el enlace MIPG (<a href="https://intranet.personeriabogota.gov.co/mipg/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-lainformacion">https://intranet.personeriabogota.gov.co/mipg/sistemas-de-gestion/sistema-de-seguridad-y-gestion-de-lainformacion</a>), Sistemas de Gestión, Sistema de Gestión de Seguridad de la Información en el cual se presenta nuevamente el alcance del SGSI con una información que complementa las informaciones anteriores del alcance y que no fue aprobada por la Alta Dirección. Por lo anterior, la comunicación es confusa y se pierde la integridad de la información, incumpliendo con el numeral 7.4 Comunicación literal a) de la norma ISO 27001:2013.</p>	Perdida de integridad de la información comunicada del SGSI.	Realizar la actualización conforme a la guía para la actualización de portales web e intranet institucionales 03-GU-01	Contenido del SGSI actualizados en los canales institucionales.	03/10/2022	31/12/2022	Director de TIC	C	<p>Mediante correo de fecha 20 de abril de 2023, el Proceso allega los siguientes documentos: en formato PDF Correo institucional "Actualización micrositos SGSI en Portal Web e Intranet - Plan de Mejoramiento", Accesos a la Intranet y al Portal WEB, que incluyen: Introducción, Alcance, Principios, Objetivos y Políticas del SGSI.</p> <p>DTIC señala a corte de diciembre 31 de 2022, que: "Se actualizó y estandarizó la información en los portales institucionales de la entidad".</p> <p>Por lo anterior, la Oficina de Control Interno considera dar <b>CIERRE</b> a esta No Conformidad.</p>

<b>Proceso Auditado:</b>	Sistema de Gestión de Seguridad de la Infomación-SGSI Norma ISO 27001:2013	<b>Responsable del Proceso Auditado:</b>	Edgar Martin Cubides Rojas
<b>Auditor(a):</b>	Carlos Orlando León Valenzuela- Sandra Patricia Camago Rodriguez-Martha Cecilia Gallo Medina	<b>Fecha de Seguimiento:</b>	Abril 26 de 2023

Ítem	FUENTE	HALLAZGO	RIESGO IDENTIFICADO	ACCIÓN	INDICADOR	FECHA INICIO	FECHA FIN	RESPONSABLE	ESTADO	OBSERVACIÓN
4	Auditoría Interna	<p><b>N.C:</b> Se evidenció documento formato de acta de reunión código 01-FR-06 versión 4 del 18/07/2019 donde se revisaron y aprobaron los indicadores del SGSI. Por otra parte, se evidenciaron formatos de seguimiento a los eventos e incidentes de seguridad de la información del año 2021 y año 2022; el formato de seguimiento del año 2022 no cuenta con codificación del SGSI. Así mismo, se observaron hojas de vida de los indicadores Tratamiento de Eventos de la Seguridad de la Información y Plan de Comunicación, Sensibilización y Capacitación del SGSI con mediciones hasta el mes de septiembre de 2021, pero en las fichas del indicador aparece el año 2020 y para el año 2022 con mediciones hasta los meses de junio y agosto, no obstante, lo anterior los indicadores están enfocados a objetivos y metas que no están relacionados con los objetivos del SGSI. Finalmente, se evidenció documento Plan de Seguimiento y Revisión del SGSI código 03-PL012 versión 1 vigente desde el 01/10/2021; sin embargo, no se evidencia documento de revisión y seguimiento del mencionado plan que den cuenta de los responsables del seguimiento, medición, análisis y evaluación de los planes y objetivos del SGSI y demás insumos de información requeridos para determinar la eficacia del Sistema. Incumpliendo lo establecido en el numeral 9.1 Seguimiento, Medición, Análisis y Evaluación literales a), b), c), d), e) y f) de la norma ISO 27001:2013.</p>	Falta de medición para evaluar el desempeño y eficacia del Sistema de Gestión de Seguridad de la información	Diseñar una metodología del SGSI enfocado a la medición de los objetivos y alineado a los diferentes planes según lo establecido en el numeral 9.1 de la NORMA NTC-IEC27001	Una metodología de medición y seguimiento al Plan de Seguimiento y Revisión del SGSI	03/10/2022	31/12/2022	Director de TIC	C	<p>Mediante correos de fecha 20 y 21 de abril de 2023, el Proceso allega los siguientes documentos: en formato EXCEL la Matriz_SGSI_2023 y en formato PDF el Acta de fecha 12/04/2023 relacionada con la revisión y aprobación de la Matriz Sistema de Gestión de Seguridad de la Información - SGSI.</p> <p>DTIC señala que ya se encuentran ajustados y aprobados dichos documentos por parte del Director de la DTIC.</p> <p>Por lo anterior, la Oficina de Control Interno considera dar <b>CIERRE</b> a esta No Conformidad.</p>
5	Auditoría Interna	<p><b>N.C:</b> Respecto a la Revisión por la Dirección, el Proceso DTIC entrega como evidencias los siguientes documentos Plan de Seguridad y Privacidad de la Información, cumplimiento de objetivos del SGSI, Plan de Comunicación Sensibilización y Capacitación del SGSI, Formato Plan de Auditoría 2021, Formato Informe Auditoría, Informe Auditoría Externa, Plan de Mejoramiento Proceso y Plan de Seguimiento y Revisión del SGSI. Así mismo, el proceso mediante correo electrónico de fecha 26/08/2022 ratifica los documentos y entrega nuevo documento denominado estado actual de la seguridad y privacidad de la información PETI arquitectura empresarial. Los documentos presentados contienen algunos insumos para realizar la Revisión por la Dirección, pero no corresponde a la Revisión por la Dirección del año 2021. Por lo anterior, no se evidenció documento o acta de la Revisión por la Dirección con los elementos de entrada y salida establecidos en la norma ISO para el SGSI; incumpliendo el numeral 9.3 Revisión por la Dirección literales a), b), c), d), e) y f) de la Norma ISO 27001:2013.</p>	Falta de Revisión por la Dirección del Sistema de Gestión de Seguridad de Información.	Presentar a la alta dirección el informe de revisión de SGSI teniendo en cuenta las entradas y salidas definidas en la NormaISO 27001:2013	Acta de reunión	03/10/2022	31/12/2022	Director de TIC	C	<p>Mediante correos de fecha 20 y 21 de abril de 2023, el Proceso allega el siguiente documento en formato PDF: "Acta Reunión Revisión por la Dirección 09-11-2022", la cual incluye en su numeral 3: Revisión por la Dirección Sistema de Gestión de la Seguridad de la Información - SGSI/ Responsable del SGSI y Director de TIC.</p> <p>DTIC señala a corte de diciembre 31 de 2022, que: "El 9 de noviembre de 2022 se llevo a cabo la revisión por la alta dirección del SGSI, de acuerdo con el numeral 9.3 "Revisión por la Dirección" de la norma NTC-ISO 27001:2013.</p> <p>Por lo anterior, la Oficina de Control Interno considera dar <b>CIERRE</b> a esta No Conformidad.</p>

<b>Proceso Auditado:</b>	Sistema de Gestión de Seguridad de la Infomación-SGSI Norma ISO 27001:2013	<b>Responsable del Proceso Auditado:</b>	Edgar Martin Cubides Rojas
<b>Auditor(a):</b>	Carlos Orlando León Valenzuela- Sandra Patricia Camargo Rodriguez-Martha Cecilia Gallo Medina	<b>Fecha de Seguimiento:</b>	Abril 26 de 2023

Ítem	FUENTE	HALLAZGO	RIESGO IDENTIFICADO	ACCIÓN	INDICADOR	FECHA INICIO	FECHA FIN	RESPONSABLE	ESTADO	OBSERVACIÓN
6	Auditoría Interna	<p><b>N.C:</b> En concordancia con el Alcance del SGSI y la Declaración de Aplicabilidad código 03-FR-23, versión 2; adoptada por la entidad, se incluyen todos los procesos de la Entidad, y se indica que los requisitos como los controles del anexo A de la norma NTC/ISO 27001:2013 son aplicables en su totalidad. Sin embargo, de un total de 114 controles de la norma, la entidad clasificó 38 controles como "Control seleccionado, pero aún no está implementado", por lo tanto, llama la atención de esta auditoría como se emite una certificación del SGSI, sin implementar la totalidad de los controles del Anexo A. Objetivos de Control y Controles de Referencia, en la medida en que se deben usar en contexto con el tratamiento de riesgos de la seguridad de la información. Incumpliendo el numeral 6.1.3. literal c) y d) de la norma NTCISO-IEC 27001:2013.</p>	<p>Incumplimiento de los Objetivos de Control y Controles de Referencia establecidos para el Tratamiento de Riesgos de la Seguridad de la Información.</p>	<p>Actualizar y aprobar la declaración de aplicabilidad de acuerdo al numeral 6.1.3. literal c) y d) de la norma NTC-ISO-IEC 27001:2013.</p>	<p>Una declaración de aplicabilidad actualizada y aprobada</p>	03/10/2022	31/12/2022	Director de TIC	c	<p>Mediante correo de fecha 20 de abril de 2023, el Proceso allega el siguiente documento en formato PDF: "Declaración de Aplicabilidad SGSI Código 03-FR-23 Versión 3 del 14/04/2023.</p> <p>La DTIC señana que: "La declaración de aplicabilidad fue aprobada y firmada por el director de TIC y cuenta con 109 controles implementados y 5 sin implementar, los cuales corresponden a lineamientos y documentos que se encuentran en proceso de revisión y aprobación."</p> <p>Por lo anterior, la Oficina de Control Interno considera dar <b>CIERRE</b> a esta No Conformidad.</p>

RESPONSABLE DEL PROCESO		AUDITOR(A) QUE REALIZA EL SEGUIMIENTO		JEFE OFICINA DE CONTROL INTERNO	
Nombre:	Edgar Martin Cubides Rojas	Nombre:	Carlos Orlando León Valenzuela-Sandra Patricia Camargo Rodriguez- Martha Cecilia Gallo Medina	Nombre:	William Ospina Giraldo
Firma:		Firma:	 	Firma:	