BOGOTÁ | SECRETARÍA GENERAL	**OFICINA DE CONTROL INTERNO**
	INFORME EJECUTIVO **AUDITORIA DE GESTION AL PROCESO ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TRATAMIENTO DATOS PERSONALES Y SEGURIDAD DIGITAL)**

PERIODO DE EJECUCION

Entre el 17 de agosto y el 28 de septiembre de 2022, se realizó auditoría al proceso de Estrategia de Tecnologías de la Información y las comunicaciones, en sus dimensiones de Tratamiento de Datos Personales y Seguridad Digital, de acuerdo con lo aprobado en el Plan Anual de Auditoría para el 2022.

OBJETIVO GENERAL

Establecer la adecuada aplicación de los controles claves y el cumplimiento de lineamientos establecidos en los documentos contentivos del proceso Estrategia de Tecnologías de la Información y las Comunicaciones en lo que respecta a la Guía de riesgos de Seguridad Digital, Política y Manual de Tratamiento de Datos Personales, para el período objeto de evaluación comprendido entre septiembre de 2021 y agosto 2022.

ALCANCE

Evaluar la aplicación de controles establecidos según directrices y lineamientos señalados en los siguientes documentos del Sistema Integrado de Gestión, para el periodo de evaluación comprendido desde el 1 de septiembre 2021 a 31 de agosto 2022:

- Política General para el Tratamiento de Datos Personales de la SG (4204000-OT082 Versión 02 del 12/07/2022.
- Manual de políticas y procedimientos para el tratamiento de datos personales (4204000-MA-033) Versión 1 del 20/12/2019.
- Guía metodológica para la gestión de riesgos de seguridad digital (4204000-GS-096) versión 3 del 29/04/2022.

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 sobre tratamiento de datos personales y seguridad digital, se aplicaron las técnicas de auditoría 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) Versión 2 del 12/10/2021

- ✓ Guía metodológica para la gestión de riesgos de seguridad digital (4204000-GS-096) versión 3 del 29/04/2022
- ✓ Política General para el Tratamiento de Datos Personales de la SG (4204000-OT082 Versión 02 del 12/07/2022
- ✓ Manual de políticas y procedimientos para el tratamiento de datos personales (4204000-MA-033) Versión 1 del 20/12/2019
- ✓ Ley 1581 de 2012 – Disposiciones Generales para la Protección de Datos Personales

CONCLUSION

Como resultado de la evaluación de auditoría realizada al proceso de Estrategia de Tecnologías de la Información y las Comunicaciones, en sus dimensiones de Tratamiento de Datos Personales y Seguridad Digital, para el periodo objeto de evaluación comprendido entre el 1 de septiembre 2021 y el 31 de agosto 2022, se estableció que en términos generales se viene cumpliendo con los lineamientos definidos en los documentos contentivos del proceso y se ajustan a las necesidades de la entidad.

Se encontró que a través de los lineamientos dados en los documentos establecidos del proceso Estratégico de Tecnología, se está dando cumplimiento a la normatividad sobre tratamiento de datos personales, resaltando los siguientes aspectos:

- A través de la herramienta FT-367– Activos de Información, cada una de las dependencias de la Entidad ha identificado los Activos de Información bajo su responsabilidad. En esta herramienta Excel, se observó la existencia y diligenciamiento de información relacionada con aspectos de protección de datos personales como son: Categoría de Titulares Almacenados, Tipos de Datos Generales Almacenados y Tipos de Datos Sensibles Almacenados.

- El Sistema de Información Bogotá Te Escucha, por medio del cual se atienden los requerimientos y peticiones del Ciudadano, y por medio del cual se registran datos del ciudadano, cuenta con mensajes de protección de datos, controles de acceso y trazabilidad que permite concluir sobre la seguridad razonable para la protección de datos personales y sensibles registrados y almacenados en dicho Sistema de Información.

- El Sistema de Administración de Turnos (SAT) por medio del cual se atiende al ciudadano tanto en ventanilla de atención Manzana Liévano como en los CADEs y Supercades, a través de los cuales se registra información de datos personales como: identificación, nombres y apellidos, fecha de nacimiento, teléfono, sexo y pertenencia étnica, cuenta con controles de acceso y trazabilidad para dar seguridad razonable para la protección de los datos personales y sensibles registrados y almacenados en dicho Sistema de Información.

- Se cuenta con un Sistema de Control de Acceso a través de la tecnología de Biometría, en algunos puntos tanto en las instalaciones de Manzana Liévano como en los Cades y Supercades, el cual es administrado de manera central y remotamente por la OTIC (Sistema de Control de Acceso y Biometría de Manzana Liévano) y por la Dirección del Sistema Distrital de Servicio a la Ciudadanía, respectivamente.

- Desde la OTIC se han realizado análisis de vulnerabilidad a la infraestructura de red donde se conectan los servidores críticos y sensibles que almacenan información personal y sensible como por ejm: bases de datos que soportan los sistemas de información Sivic, Bogota Te Escucha, Siab, Sistema de Gestión Contractual, Sistema de Liquidación de Nómina Perno, de acuerdo con los resultados obtenidos se generan planes de remediación o se asume el riesgo, cuando es mínimo el impacto de la remediación es mayor en riesgo en la afectación del funcionamiento del servidor.

- Se realizan copias de respaldo de los registros de acceso de los dieciocho (18) biométricos que se encuentran en uso (ocho en Manzana Liévano y diez en Cades), gestionadas por los Administradores Funcionales de los servidores que soportan estos equipos, específicamente por la OTIC (Oficina de Tecnologías de la Información y Comunicaciones) para el Servidor Andover y la DSDSC (Dirección del Sistema Distrital de Servicio a la Ciudadanía) para el servidor de biométricos de los Cades.

- La OTIC con apoyo de la DTH, ha realizado cuatro (4) sesiones de capacitación durante el año 2022, las cuales se realizan periódicamente a los funcionarios de la Secretaría General, donde se socializan temas relacionados con la Protección de Datos Personales.

Sin perjuicio de lo anterior, se identificaron algunas observaciones, oportunidades de mejora y recomendaciones que al ser gestionadas propenderán por fortalecer la seguridad digital para garantizar confidencialidad e integridad de la información personal administrada en la Entidad.

A continuación, se relacionan algunas de las situaciones observadas y objeto de mejora:

- Es necesario poner en funcionamiento los siete (7) equipos biométricos instalados (6 de Manzana Liévano y 1 del Cade Gaitana) y un (1) botón de salida Push Outdoor ubicado en la Oficina Jurídica, los cuales se encuentran sin uso o sin reprogramación para administración remota (Liévano y Cade La Gaitana), que aún no han sido reactivados luego de su desactivación debido a la emergencia sanitaria por la pandemia Covid19.

- Revisar los mensajes de autorización y/o información sobre el tratamiento de datos personales que se tiene en el Sistema de Información BTE e implementar mensajes sobre autorización y uso de datos personales en el aplicativo SAT, con el propósito de dar cumplimiento a lo establecido en la ley 1581 de 2012. Se recomienda extender este análisis para todos los Sistemas de Información que manejen información de datos personales.

- Las matrices de Activos de Información, cuentan con columnas de información para tratamiento de datos personales, se diligencian aspectos asociados a almacenamiento de información, es decir, activos relacionados con Bases de Datos. Al respecto, la OTIC indicó que estos Activos de Información corresponden a medios de recolección de datos, pero al no conformar una Base de Datos no se evalúan como Protección de Datos Personales (PDP); no obstante, esta Oficina de Control considera recomendable que los otros activos de información como documentos, formatos y herramientas tecnológicas para las que no se ha considerado la necesidad de contar con esta información, se logre identificar y definir su diligenciamiento.

- Es importante evaluar los procedimientos que se llevan a cabo para la toma de copias de respaldo de la base de datos de los equipos biométricos (sistema Andover y sistema ZKTeco), para que en lo posible se realicen bajo las políticas y lineamientos ya establecidos en los procedimientos de la OTIC y se implemente el almacenamiento en medio magnético y envío a ubicación física externa.

OBSERVACIONES, OPORTUNIDADES DE MEJORA Y RECOMENDACIONES PRODUCTO DE LAS PRUEBAS PRACTICADAS

Para el desarrollo de la evaluación de los controles claves y el cumplimiento de lineamientos establecidos en los documentos contentivos del proceso Estrategia de Tecnologías de la Información y las Comunicaciones, en lo que respecta a la Guía de Riesgos de Seguridad Digital, Política y Manual de Tratamiento de Datos Personales, se realizaron verificaciones a las Matrices de Activos de Información, pruebas a los sistemas de información Bogotá Te Escucha (BTE), Sistema de Administración de Turnos (SAT) y Equipos Biométricos.

A continuación, se describen los principales aspectos identificados como observaciones, oportunidades de mejora y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Normatividad, Acuerdos de Confidencialidad y Capacitaciones

La entidad cuenta con normatividad interna debidamente publicada y actualizada en el Sistema Integrado de Gestión (SIG), relacionada con Tratamiento de Datos Personales y Seguridad Digital.

Referente a las cláusulas de confidencialidad de los contratos, en los Estudios Previos se encuentran obligaciones para los contratistas referente al manejo de la información confidencial, así mismo, se cuenta con una cláusula en el anexo de Condiciones del Contrato, ambos documentos soporte registrados en Secop2.

Observación No. 1 – Acuerdos de Confidencialidad

Analizada la información relacionada con las responsabilidades de los funcionarios con respecto al manejo y confidencialidad de la información, se establece la existencia del formato FT-1186 Acuerdo de Confidencialidad y Reserva de Manejo de Información Versión 1, con fecha de publicación en el SIG (Sistema Integrado de Gestión) del 4 de julio 2022, sin obtener evidencia de su utilización en la entidad para la celebración de contratos ni la firma del documento por parte de los servidores públicos al posesionarse en su cargo público.

Lo anterior genera riesgo de incumplimiento de la normatividad interna (PR-187 Activos de Información) que dice en la sesión 5. Condiciones Generales: "*Los servidores públicos que tengan un vínculo laboral con la Entidad deberán cumplir con el acuerdo de confidencialidad que se encuentra detallado en el documento 4204000-FT-1186 Acuerdo de Confidencialidad y Reserva de Manejo de la Información y por ende se abstendrán de hacer mal uso de la información que conocen, administran, manejan, modifican y custodian durante la ejecución de sus actividades en la Entidad.*" Y del mismo formato FT-1186 que en la consideración No.3 dice: "..*Que, en Cláusula (número de cláusula del contrato Contratista/Funcionario que indique la firma de confidencialidad),*

Obligaciones del (EL CONTRATISTA/FUNCIONARIO/PROVEEDOR) - Obligaciones Generales, numeral xxx del Contrato No. XXX, las Partes estipularon: "Suscribir simultáneamente a la firma del contrato el acuerdo de confidencialidad y manejo de la información que suministre Secretaría General de la Alcaldía Mayor de Bogotá."

Recomendación

En respuesta recibida de la OTIC, se informó que el documento no aplica, de manera que será eliminado del Sistema Integrado de Gestión y el Procedimiento PR-187 será actualizado eliminando este documento.

Recomendación No. 1 – Sensibilización sobre Protección de Datos Personales

Se evidenció que, en los meses de abril, junio y agosto de 2022, la OTIC en coordinación con la Dirección de Talento Humano, realizaron cuatro (4) charlas de sensibilización relacionadas con el tema de Seguridad, Privacidad y Protección de Datos Personales. Las fechas en las que se dictaron estas charlas de sensibilización son: 22/04/2022, 22/06/2022, 11/08/2022 y 25/08/2022. Se observó la participación de cincuenta y ocho funcionarios en total para las cuatro (4) charlas, de un total aproximado de 600 funcionarios de planta, es decir, la cubertura de las charlas llego a un 10% de los funcionarios.

Desde esta Oficina se sugiere a la Dirección de Talento Humano que incluya en estas charlas como en las sesiones de inducción y reinducción que se dictan a los funcionarios, de tal manera que se logre cubrir la totalidad de funcionarios de la Entidad y determinar la participación de un gran porcentaje de los funcionarios en las mismas, sin que esto constituya obligatoriedad de participación por parte de los funcionarios.

2. Registro, Almacenamiento y Administración de Datos Personales

Realizada la revisión del registro y almacenamiento de los Datos Personales en los Sistemas de Información SAT y BTE, se evidenció que se cuenta con controles de acceso controlado y se deja trazabilidad de la información registrada.

El Sistema Bogotá Te Escucha cuenta con mensaje relacionado a uso de datos personales y se cuenta con la funcionalidad para atención a niños o adolescentes, cumpliendo con lo establecido en la Política de Tratamiento de Datos de la SG publicada en la página Web de la Entidad y en la ley 1581 de 2012.

Observación No. 2 - Mensajes Relacionados con Tratamiento de Datos Personales

Revisados los mensajes de autorización y/o informativos sobre el Tratamiento de Datos Personales, según lo establecido en la Ley Estatutaria 1581 de 2012 – Disposiciones Generales para la protección de Datos Personales, específicamente para los Sistemas de Información Bogotá Te Escucha (BTE), Sistema de Asignación de Turnos (SAT) y los formatos de Asistencia donde se registra información personal, se estableció que:

- ✓ En el Sistema SAT no se cuenta con mensajes sobre la autorización que el ciudadano debe dar sobre el tratamiento de datos (artículo 6 literal a) de la ley 1581 de 2012, que dice: "*El titular haya dado su autorización explícita a dicho tratamiento…*" , tampoco mensaje informativo sobre el uso de sus datos como lo indica el articulo 8 literal c) de la mima ley que indica: "*ser informado por el Responsable del*

Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales"

- ✓ El Sistema BTE cuenta con el mensaje de autorización de uso de datos que dice: "He leído y estoy de acuerdo con los términos y condiciones de uso de datos, implementados por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. resolución 777 de 2019…"; sin embargo, no se observó explícitamente una autorización y/o información sobre el tratamiento de dichos datos personales.

Recomendación

Es importante que la Dirección del Sistema Distrital de Servicio a la Ciudadanía revise, actualice e implemente los mensajes de autorización e información sobre el manejo y tratamiento de datos que la Entidad da a la información que el ciudadano registra o entrega a través de los diferentes medios de recolección de información, para este caso específicamente en los Sistemas de Información BTE y SAT.

Recomendación No.2 - Matrices Activos de Información

Se recomienda a la OTIC que, en conjunto con las diferentes Dependencias de la entidad, realice la revisión de las matrices de Activos de Información que actualmente se encuentran en proceso de actualización para la vigencia 2022, en especial con las dependencias que Administran los siguientes Sistemas de Información, donde se registran y almacenan Datos Personales: Bogotá Te Escucha, Sistema de Gestión Contractual, Sistema Perno.

Analizadas las matrices de Activos de Información recientemente actualizadas para la vigencia 2022, se identificaron las siguientes situaciones:

1. Existen Sistemas de Información y/o Bases de Datos que no cuentan con el detalle de identificación de Datos Personales en la matriz FT-367 de Activos de Información. Las Bases de Datos que no se observan en las matrices de la Dependencia responsable o que no cuentan con la identificación de Datos Personales para su tratamiento son: Bogotá Te Escucha de la Dirección del Sistema Distrital de Servicio a la Ciudadanía y SAT (Sistema de Administración de Turnos) de la Dirección del Sistema Distrital de Servicio a la Ciudadanía.

2. Las dependencias a cargo de los Sistemas de Información mencionadas identificaron sus Activos de Información para la vigencia 2022 y, en la matriz FT-367 con la relación de dichos Activos de Información se observó que las áreas relacionaron detalladamente la información requerida sobre Tratamiento de Datos Personales almacenados, tanto de Bases de Datos como de otros tipos de Activos de Información. Sin embargo, según lineamientos de la OTIC esto aplica únicamente para las bases de datos, razón por la cual, se considera conveniente revisar el lineamiento para que se consideren los registros diferentes a Tipo Base de Datos como sujetos de Tratamiento de Datos Personales.

Asimismo, consultada la Información Clasificada y Reservada vigencia 2021 (Archivo: Inventario de la información ft-1136_indice_informacion_clasificada_y_reservada_2021.xlsx), publicada en el sitio Web de la Entidad, no se encontró activo de información relacionado con el Sistema de Información de Liquidación de Nómina (Perno), lo cual de acuerdo con lo informado por la OTIC quedará solucionado en el proceso de actualización que se llevará a cabo para los próximos meses de la vigencia 2022.

3. Sistema de Control de Acceso con equipos Biométricos

Recomendación No. 3 – Equipos biométricos Manzana Liévano

Teniendo en cuenta que los elementos que integran el Sistema de Control de Acceso de la Manzana Liévano, fueron recibidos e ingresados al almacén bajo una única placa de inventario (No. 68359) e incluso algunos elementos fueron registrados como de consumo y otros como devolutivos, se recomienda para un mayor control que futuras ocasiones que este tipo de elementos se ingresen al almacén con placas de inventario independientes y que los elementos de la misma clase se registren bajo el mismo tipo de ingreso, ya sea de Consumo o Devolutivo.

La situación identificada, corresponde a elementos ingresados como de Consumo (comprobante de ingreso No. 110-2017 del 26/12/2017 y soporte en Folio 3 – 409 del contrato), los cuales no fueron incluidos como parte del Sistema de Control de Acceso identificados con la placa de inventario No. 68359 aun cuando corresponden al mismo tipo de elemento de otros que si hacen parte integral de este registro de inventario, como se detalla a continuación:

- Cuatro (4) equipos Outdoor Single-Gang (botón de salida de cuartos) que no hacen parte de la placa de inventario No. 68359, pero allí, si se identifican catorce (14) de los dieciocho (18) referenciados en los folios 3-387 y 3-399 de la documentación del contrato.

- Cuarenta y tres (43) lectores de Proximidad registrados que no hacen parte de los equipos inventariados bajo la placa mencionada, en la cual si se registraron cuatro (4) de los cuarenta y siete (47) referenciados en los folios 3-387 y 3-399 de la documentación del contrato.

- Nueve (9) equipos denominados “Controladora ACX5740, 8 reader 12in, 4Do”, que no hacen parte de los equipos inventariados bajo la placa mencionada y que siendo elementos de cómputo inteligentes que en nuestro concepto deben ser controlados como parte de los activos (bienes devolutivos) de la entidad.

En tal sentido, se deja a consideración de la OTIC como área responsable del activo y de la Subdirección de Servicios Administrativos como área responsable del inventario de la entidad, que se revisen las situaciones reportadas por esta auditoría y determinen si aplica la realización de ajustes al inventario de los mencionados elementos del Sistema de Control de Acceso.

Oportunidad de Mejora No. 1

Revisados los treinta y tres (33) equipos biométricos para registro de ingreso, existentes en el inventario de activos, recibido de la Subdirección de Servicios Administrativos, se identificaron algunas situaciones de equipos sin uso, fuera de servicio o sin conexión, que se mencionan a continuación:

- De catorce (14) biométricos identificados bajo una única placa de inventario No. 68359, se observó que todos se encuentran instalados. Sin embargo, debido a las medidas tomadas por la emergencia sanitaria Covid-19, algunos fueron desactivados y aún se encuentran sin uso o sin conexión para administración remota, por lo que se considera necesario que la OTIC evalúe y defina su reconexión y puesta en funcionamiento. Son seis (6) biométricos de ingreso denominados “Multifactor Biométrico Bio/Card/Pin” y un (1) botón de salida denominado “Push Outdoor”:

- Dos (2) equipos biométricos instalados en los Cades no están en funcionamiento y que, de acuerdo con lo informado por el Administrador de estos equipos no se cuenta con software vigente para su uso. Por lo tanto, se recomienda que desde la Subdirección de Servicios Administrativos en conjunto con la Dirección del Sistema Distrital de Servicio a la Ciudadanía realizar el proceso de evaluación para definir si se deben dar de baja o poner en servicio. Las placas de los equipos son: 24073 en el SuperCade 20 de Julio y 9093 en el Supercade Suba.

- Un (1) biométrico identificado con placa No. 34179 ubicado en Cade la Gaitana se encuentra instalado y pendiente de ponerlo en línea para su administración remota desde la Dirección del Sistema Distrital de Servicio a la Ciudadanía.

Recomendación

Se recomienda a la OTIC y a la Dirección del Sistema Distrital de Servicio a la Ciudadanía, realizar las gestiones encaminadas a poner en funcionamiento los equipos biométricos y/o configurarlos para permitir su conexión en línea con el servidor y la administración centralizada remota, tanto para los biométicos Manzana Liévano a cargo de la OTIC y de los Cades a cargo de la DSDSC.

Para los equipos obsoletos o inservibles que se encuentran en los Supercades, se recomienda a la Dirección del Sistema Distrital de Servicio a la Ciudadanía realizar las gestiones correspondientes con la Subdirección de Servicios Administrativos para evaluar la obsolescencia de los equipos y seguir el procedimiento para darlos de baja del inventario de la Entidad.

En tal sentido, se sugiere evaluar la posibilidad de reasignar los equipos que no están en uso por parte de la OTIC hacia la DSDSC para su uso en los Cades.

Oportunidad de Mejora No. 2 – Copias de Respaldo información equipos biométricos

Una vez revisadas las copias de respaldo que se realizan de la información de los equipos biométricos, se observa que los Administradores Funcionales de las áreas OTIC y DSDSC realizan las copias de respaldo; sin embargo, no se realizan bajo los lineamientos establecidos en la Guía de Gestión y Administración de Copias de Respaldo (4204000-GS-036 Versión 7). Situación que genera riesgo de pérdida de información

y/o dificultad de recuperar los datos antes daños de los servidores o de los equipos donde se conservan las copias de respaldo, al igual, que incumplimiento de los lineamientos internos establecidos en la Guía de Gestión de Administración de Copias de Respaldo.

Recomendación

Con el fin de fortalecer las medidas de seguridad de la información que se registra y se almacena en los Sistemas de la entidad, se recomienda a la Oficina de Tecnologías de Información y las Comunicaciones gestionar la toma de backups bajo los lineamientos establecidos en la guía de Gestión y Administración de Copias de Respaldo para que las copias de respaldo se conserven y almacenen en medios magnéticos y en ubicación externa diferente a la ubicación del servidor.

Es necesario que la Dirección del Sistema Distrital de Servicio a la Ciudadanía analice la guía de Gestión y Administración de Copias de Respaldo vigente e implementar los controles de periodicidad y almacenamiento en medio magnético y externo, cumpliendo con los lineamientos establecidos en la mencionada guía de Gestión y Administración de Copias de Respaldo.

4. Control de Acceso Sistema de Información y Análisis de Vulnerabilidades

Observación No. 3 - Usuarios Genéricos Sistema de Información Bogotá Te Escucha

Analizada la relación de usuarios con acceso al Sistema de Información BTE, se identificó que:

- Existen dos (2) usuarios genéricos con perfil de consulta (consultapqrs y linea195), a los cuales no es factible asociarles un funcionario según el UserID, incumpliendo lo definido en el Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (MA031 V4), que en su numeral 10.4.5 Control de Acceso dice:
  "…

  ▪ *Todos los funcionarios, contratistas y terceros tendrán un identificador único (ID del usuario) para su uso personal e intransferible que les permita acceder y hacer buen uso de los datos e información, sistemas de información e instalaciones.*
  ▪ *En caso de que existan identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente individualizados los responsables, validados y gestionados los respectivos riesgos de seguridad de la información y de esta manera, encontrarse aprobados los controles respectivos por la Oficina de Tecnologías de la Información y las Comunicaciones.*

  …"
- Dos (2) usuarios activos en el Sistema de Información BTE, asignados a funcionarios ya retirados de la entidad y que requieren ser inactivados para evitar accesos no autorizados a la información sensible de los ciudadanos, y para dar cumplimiento a lo definido en el Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (MA031 V4), que en su

numeral 10.4.5.6 Gestión de Acceso de Usuarios dice: "*Los derechos de acceso de todos los funcionarios, contratistas, proveedores y aliados para acceder a los datos e información y a los servicios de procesamiento de información se retiran al terminar el vínculo laboral y/o se deben ajustar cuando existan cambios de dependencias y/o responsabilidades*." Los usuarios son: Nubia Elsy Gomez Meza con id 24364502 y Ennis Esther Jaramillo Mora con id 32140655

Recomendación

Desde la Dirección del Sistema Distrital de Servicio a la Ciudadanía revisar y depurar los usuarios activos con acceso al aplicativo que ya no laboran en la entidad, al igual que realizar un análisis de los usuarios genéricos existentes con el fin de asignar un responsable y en caso de ser absolutamente necesario continuar con su uso, realizar la validación y gestión de los respectivos riesgos de seguridad de la información para que sean aprobados los controles respectivos por la Oficina de Tecnologías de la Información y las Comunicaciones, según se indica en el Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (MA031 V4), que en su numeral 10.4.5 Control de Acceso.

Análisis de Vulnerabilidad para la protección de servidores donde se almacenan Datos Personales

Verificados los resultados del análisis de vulnerabilidad realizado por la OTIC para la vigencia 2022 sobre la infraestructura de red, se identificó que se incluyeron las direcciones IP de los servidores donde residen las bases de datos de los Sistemas de Información BTE, SIVIC, SGC, Perno y Siab, y que para los servidores donde reposan las bases de datos del SGC y Perno se encontraron dos vulnerabilidades para las que según el concepto técnico recibido se concluye que: "*Se ha revisado la documentación y encontramos que en el sistema operativo que estamos utilizando no se afecta por la vulnerabilidad ya que los protocolos de conexión no usan 3DES para las conexiones. https://access.redhat.com/es/articles/2621311. Por lo tanto, se asume el riesgo (el cual es mínimo) ya que no implica un peligro de explotación y si puede traer desventajas en el funcionamiento del producto instalado el cual es de muy alta demanda en la Entidad*."

Política de Tratamiento de Datos Personales publicada en el sitio Web de la Entidad

Se evidenció que en el sitio Web de la Secretaría General (https://secretariageneral.gov.co/transparencia-y-acceso-la-informacion-publica/politicas-y-lineamientos-sectoriales/politicas), al momento del cierre del trabajo de campo de la auditoría se encontraban publicados dos documentos relacionados con la Política de Tratamiento de Datos, uno denominado "Política General de Tratamiento de Datos Personales" y otro "Política para el Tratamiento de Datos Personales" sin diferenciación de versionamiento. De acuerdo con la respuesta recibida al informe preliminar y reunión realizada con la gestora de calidad de la OTIC el día 10 de octubre 2022, se concluye que en el sitio Web deben quedar publicadas las diferentes versiones que han existido sobre la Política para el Tratamiento de Datos Personales.

En tal sentido, la OTIC ajustó los documentos publicados manteniendo ambas Políticas y diferenciando las versiones correspondientes.

A continuación la evidencia del ajuste realizado por la OTIC como resultado del informe preliminar, donde se evidencia en el Sitio Web la publicación de ambas versiones de la Política de Tratamiento de Datos claramente identificadas en su versionamiento, con lo cual se concluye que la Política vigente es la versión 2 publicada, en la cual ya no se mencionan los temas asociados a tablas de retención documental para la la vigencia y conservación de las bases de datos donde se registran Datos Personales.

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 y la Dirección del Sistema Distrital de Servicio a la Ciudadanía, definieron 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