ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
Nancy Liliana Garzon Piratique **Roger Alfonso Gonzalez Herrera**	**Gestión de TICS-OTIC (Seguridad de la Información)**	**Gestión de TICS-OTIC (Seguridad de la Información)**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
5. Liderazgo 5.1 Liderazgo y compromiso 5.2 Política 6.2 Objetivos de seguridad de la información y planificación para cumplirlos Control A.5.4 Responsabilidades de gestión	5. Liderarzgo. 5.1 Liderazgo y Compromiso. La alta dirección lidera, apoya y demuestra activamente la responsabilidad del SGSI mediante la integración de la seguridad de la información en los procesos de negocio, la garantía de los recursos necesarios y la promoción de la mejora continua. Exige una participación ejecutiva visible y sostenida como prueba de su compromiso, mediante actas, paneles de control, presupuestos y comunicaciones. Evidencia consistente y de múltiples capas, todos convergiendo en seguridad. Mediante: -Actas de la Junta: La seguridad de la información presente en todas las agendas, con puntos estratégicos desde los altos ejecutivos. -Revisiones de gestión: Directores no sólo firman, dan forma, desafían y escalan los objetivos del SGSI en tiempo real. -Asignaciones presupuestarias: aprobación ejecutiva, rastreable desde la asignación de recursos hasta la inversión en habilidades. - Respaldos y mensajes públicos: Liderazgo transmitido al personal y a las partes interesadas, asumiendo visiblemente las prioridades y los resultados. La brecha entre la política y la evidencia se cierra solo cuando se incluye la rendición de cuentas - liderazgo: nombrar, rastrear y revisar cada acción y cada resultado. Mejora continua. Enfoque de auditoría: - Responsabilidades ejecutivas hasta el director: propietarios explícitos. - Rendición de cuentas entre departamentos a través de matrices RACI y organigramas transparentes. - Evidencia de comités ejecutivos directos y grupos de dirección donde los cuadros de mando, las métricas y la respuesta a incidentes permanecen	X			Se evidencia el compromiso y liderazgo de la alta dirección frente al SGSI a través de la conformación y operatividad del comité de seguridad. Se constata que el comité mantiene una periodicidad de reuniones mensual, con capacidad de sesiones extraordinarias ante eventualidades. Como evidencia objetiva del involucramiento de la dirección y la supervisión del sistema (Control A.5.4), se revisó el documento acta_cigd_10-03-2026. Dicha acta incluye un anexo en formato PDF que documenta formalmente la presentación de eventos de seguridad, la evaluación de resultados del SGSI y la aprobación directiva de las estrategias y planes de acción a ejecutar.
5. Liderazgo 5.1 Liderazgo y compromiso 5.2 Política 6.2 Objetivos de seguridad de la información y planificación para cumplirlos Control A.5.4 Responsabilidades de gestión	5.2 Politica de seguridad de la información La alta dirección establece, aprueba y comunica una política de seguridad de la información alineada con la dirección estratégica, la postura de riesgo y las obligaciones de cumplimiento de la organización. Esta política debe documentarse, mantenerse, ser accesible a las partes interesadas y revisarse periódicamente para garantizar su idoneidad y eficacia. Enfoque de auditoría: Registro de auditoría visible: debates de la junta directiva, decisiones de riesgo y seguimiento documentados. Señales de liderazgo: Ejecutivos que comparten logros de políticas y las "lecciones aprendidas" con sus equipos y la cadena de suministro. Acción receptiva: actualizaciones de políticas inmediatas después de incidentes de la vida real, no solo "esperar hasta la próxima revisión anual". Cláusula 5.2 exige que cada obligación esté directamente vinculada a su política y a quienes la gestionan. Esto incluye el RGPD, la CCPA, el NIS 2, los mandatos específicos del sector y todas las cláusulas contractuales de clientes o proveedores que afecten a la seguridad de la información. Vigencia de su política: campañas de correo electrónico, preguntas y respuestas sobre políticas, estadísticas de aprendizaje electrónico, informes posteriores a incidentes y cuestionarios de rendimiento. Revise las tasas de finalización, la retención de conocimientos y los informes posteriores a incidentes para detectar (y subsanar) deficiencias. ISMS.online integra la interacción y la verificación en cada paso, para que los auditores vean la política vigente en su empresa, no solo en papel.	X			Se constata la existencia, formalización y disponibilidad del documento PA04-PO1V-03 Política General de Seguridad de la Información. La política establece las directrices de alto nivel y demuestra la intención de la dirección de apoyar la seguridad de la información.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
5. Liderazgo 5.1 Liderazgo y compromiso 5.2 Política 6.2 Objetivos de seguridad de la información y planificación para cumplirlos Control A.5.4 Responsabilidades de gestión	6.2, Objetivos de seguridad de la información y planificación para alcanzarlos, exige que la Entidad establezca objetivos en las funciones y niveles pertinentes que sean coherentes con la política de seguridad, medibles (cuando sea factible), basados en el riesgo, monitorizados, comunicados, actualizados y documentados. Al planificar cómo alcanzar estos objetivos, la Entidad debe definir las acciones a realizar, los recursos necesarios, los responsables, los plazos de finalización y los métodos de evaluación para garantizar que los objetivos sean viables y estén alineados con los riesgos del negocio. Enfoque de auditoría: La cláusula 6.2 exige cuatro preguntas importantes: ¿Qué es exactamente lo que estás intentando lograr? ¿Cómo sabrás, objetivamente, cuándo has llegado allí? ¿Quién es responsable del progreso y de las pruebas? ¿Está claro cómo esto reduce el riesgo de la Entidad en este momento? Sin estos, los objetivos de seguridad quedan relegados a un segundo plano. Los objetivos concretos y medibles se convierten en palancas que impulsan la reducción de incidentes, la protección de los ingresos y la credibilidad de la junta directiva. Cada objetivo debe cumplir tres estándares: Operacional — ¿Puedes mostrarnos exactamente qué está cambiando y quién lo está haciendo posible? Mensurable —¿Existe algún número, un récord o un acontecimiento que puedas demostrarle a otra persona? Alineado — ¿Este objetivo está vinculado con el apetito de riesgo a nivel de directorio o con los imperativos regulatorios?	X			Se verificó la definición y establecimiento de los objetivos de seguridad de la información. Se evidencia que dichos objetivos son claros, medibles, coherentes con la política de seguridad y se encuentran alineados con el alcance documentado y definido del SGSI. Adicionalmente, como evidencia de la planificación estratégica para mitigar riesgos y cumplir con la disponibilidad de los servicios críticos, se observa en estado de ejecución la implementación de un Plan de Recuperación ante Desastres (DRP) focalizado en el Sistema de Gestión Documental 'Orfeo' y el aplicativo 'Fénix'.
5. Liderazgo 5.1 Liderazgo y compromiso 5.2 Política 6.2 Objetivos de seguridad de la información y planificación para cumplirlos Control A.5.4 Responsabilidades de gestión	Anexo A 5.4 Responsabilidades de gestión. Liderazgo apoye activamente la seguridad proporcione los recursos necesarios y garantice que el personal cumpla con las políticas establecidas. Exige que la alta dirección garantice activamente que todo el personal cumpla con las políticas y los procedimientos de seguridad de la información de la organización. proporcione los recursos, la supervisión y los marcos legales necesarios para garantizar el cumplimiento de las normas de protección de datos. Requisito Cumplimiento obligatorio: La dirección debe exigir a todo el personal y a los contratistas que apliquen las normas de seguridad de la información de acuerdo con las políticas establecidas. No es opcional. Asignación de recursos: Los líderes deben proporcionar los recursos adecuados (presupuesto, tiempo y herramientas) para implementar y mantener el SGSI . Competencia y habilidades: La gerencia garantizar que el personal sea competente para sus funciones de seguridad. Esto implica mantener una matriz de competencias para hacer un seguimiento de la capacitación, la experiencia y las certificaciones. Cumplimiento contractual: Los requisitos de seguridad deben estar estipulados explícitamente en los contratos de trabajo y en los acuerdos con terceros para garantizar su exigibilidad legal. Proceso de denuncia: La dirección debe implementar un proceso que permita a los empleados denunciar problemas o infracciones de seguridad de forma anónima y sin temor a represalias. Enfoque de auditoría Pruebas directas: “Muéstrenme las actas de la reunión donde la alta dirección revisó el registro de riesgos y aprobó el presupuesto de	X			Se verificó la definición, planificación y el seguimiento estructurado de los objetivos del SGSI. A través de la plataforma de gestión 'Daruma', se constató la formalización de cinco (5) objetivos de seguridad. La trazabilidad operativa de los mismos se encuentra respaldada en el documento PA04-P01-F01 Plan de cumplimiento de objetivos 2026, el cual se articula mediante un plan operativo anual. Se evidencia que la organización realiza y reporta el seguimiento de estos objetivos de manera trimestral. A modo de muestra (sampling), se verificó la medición del objetivo de 'Gestión de Activos', evidenciando que el reporte de activos se extrae de Daruma y se resguarda en el repositorio 'Drive', garantizando la conservación de la evidencia objetiva de su cumplimiento.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**
Nombre del responsable del proceso auditado:	**Proceso:**	**Depedencia :**
	Gestión de TICS-OTIC (Seguridad de la Información) **Gestión Del Talento Humano**	**Gestión de TICS-OTIC (Seguridad de la Información)** **Gestión Del Talento Humano**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencia 7.3 Toma de conciencia Dominio A.6 Controles de personas A.5.2 Roles y responsabilidades de seguridad de la información A.5.5 Contacto con las autoridades	5.3 Roles organizativos, Roles, responsabilidades y autoridades de la Entidad, exige que la alta dirección garantice que los roles de seguridad de la información estén claramente definidos, asignados, comunicados y respaldados con la autoridad necesaria. Responsabiliza a la dirección de asegurar que las responsabilidades se comprendan y se cumplan, evitando lagunas o solapamientos y proporcionando evidencia auditable de la rendición de cuentas en todo el SGSI. Enfoque de auditoría: -Definir roles y responsabilidades en materia de seguridad de la información: quién es responsable de qué, no solo a un alto nivel, sino de cada aspecto significativo del SGSI. -Asignar autoridades: Otorgar la facultad de tomar decisiones, implementar controles y escalar asuntos. -Documentar y comunicar: La documentación refleje estas asignaciones. comunique estas responsabilidades para que todas las partes conozacan dónde están los límites y las vías de escalamiento. -Demostrar el compromiso de la alta dirección: Los líderes ejecutivos no han renunciado a sus responsabilidades. Deben asignar y apoyar estas funciones, haciéndose responsables. Roles, responsabilidades y la autoridad son determinará el resultado. Los auditores no solo buscan políticas escritas, sino también evidencia operativa. Los auditores buscan evidencia viva de que su SGSI no es sólo un ejercicio en papel. Los tipos clave de documentación y evidencia incluyen:	X			Se constata la asignación, comunicación y formalización de los roles y responsabilidades pertinentes al SGSI mediante la Resolución 323207 expedida el 31 de octubre de 2023. Esta resolución evidencia la directriz formal de la organización para establecer las autoridades y obligaciones en materia de seguridad de la información, alineándolas plenamente con los requisitos del sistema de gestión.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencia 7.3 Toma de conciencia Dominio A.6 Controles de personas A.5.2 Roles y responsabilidades de seguridad de la información A.5.5 Contacto con las autoridades	7.2 Competencia La cláusula 27001 de la norma ISO 2022:7.2 requiere que las organizaciones determinen la competencia necesaria de las personas cuyo trabajo afecta la seguridad de la información, se aseguren de que sean competentes a través de educación, capacitación o experiencia, tomen medidas para llenar cualquier vacío, evalúen la eficacia y conserven evidencia documentada de la competencia. El peor escenario un incidente y se dé cuenta de que su personal clave nunca tuvo las habilidades requeridas para sus funciones. La cláusula 7.2 fusiona la capacitación, la realidad laboral y el riesgo con un principio: debe definirlo, medir, y conservar evidencia de competencia real, rol por rol. ¿Qué se exige? Requisitos de habilidades *vinculados al riesgo* y a las prioridades del negocio. Seguimiento en vivo de credenciales y desempeño en el trabajo, sin necesidad de “configurar y olvidar”. Prueba auditable de que las capacidades de cada persona cierran brechas documentadas. Planes de desarrollo y revisiones periódicas para mantener sus habilidades actualizadas a medida que su negocio evoluciona. Los reguladores y equipos de auditoría exigencias? Habilidades definidas y basadas en roles que coinciden visiblemente con el nivel de riesgo de cada trabajo. Prueba actualizada de que el personal ha adquirido (o mantiene activamente) esas capacidades. Vínculos claros entre las inversiones en formación y resultados reales.	X			Para garantizar la idoneidad del personal que afecta el desempeño del SGSI, particularmente frente a la tercerización de servicios tecnológicos, se verificó la definición de competencias de los proveedores. Se revisó el documento 'Anexo 1: Ficha técnica / Especificaciones técnicas mínimas', evidenciando la definición rigurosa de los perfiles mínimos requeridos para los ingenieros del SOC (Security Operations Center) y demás recursos humanos asignados a la ejecución y finalización de los proyectos de TI.
5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencia 7.3 Toma de conciencia Dominio A.6 Controles de personas A.5.2 Roles y responsabilidades de seguridad de la información A.5.5 Contacto con las autoridades	7.3, Toma de concienccia : Todo el personal dentro del alcance del SGSI (incluidos empleados, contratistas y directivos) conozca las políticas de seguridad de la información de la organización, su función en el apoyo al SGSI y las consecuencias de las no conformidades. Hace hincapié en integrar la seguridad en el comportamiento diario, no solo en realizar una formación puntual. Los organismos reguladores exigen cada vez más pruebas de que su personal "vive" su comprensión de la seguridad, no solo de que aprueba el aprendizaje electrónico. La cláusula 7.3 le permite demostrarlo, con la evidencia necesaria de que todos conocen: La política y los objetivos de seguridad de la información Su contribución al SGSI, incluidos sus beneficios Qué podría salir mal y qué significa la no conformidad con el SGSI, a nivel personal y para la empresa ¿El punto clave? La concientización debe ser relevante, actualizada y verificable. Requisitos en materia de concientización y por qué la capacitación no es suficiente? La cláusula 7.3 de la norma ISO 27001:2022 exige que cada persona bajo el SGSI comprenda tres aspectos: la política de seguridad de la información, su función y las consecuencias de las fallas. Si se omite cualquier aspecto, la auditoría será vulnerable, incluso si sus políticas son una fortaleza en el papel.	X			La organización demuestra un enfoque sistemático para el mantenimiento de la competencia y la toma de conciencia a través de la estructuración anual del Plan Institucional de Capacitación (PIC) - Plan de Acción 2026. Se evidencia que este plan está reforzado por un programa de sensibilización complementario. Así mismo, se verificó la ejecución de procesos formales de inducción y reinducción orientados al personal nuevo y existente de la Secretaría, validando la eficacia de estas acciones formativas mediante exámenes recurrentes de conocimiento. Adicionalmente, se constató la implementación de una plataforma LMS (Moodle) dedicada a la formación y capacitación de contratistas. El sistema garantiza la trazabilidad y legitimidad de las competencias adquiridas mediante la emisión de certificados que incorporan un código de validación, facilitando así la auditoría y autenticación de las credenciales operativas del personal externo.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencia 7.3 Toma de conciencia Dominio A.6 Controles de personas A.5.2 Roles y responsabilidades de seguridad de la información A.5.5 Contacto con las autoridades	Anexo A 6 controles de personas 6.1 Selección. Verificar los antecedentes de todos los candidatos antes de su contratación. Este control mitiga las amenazas internas al garantizar que los empleados, contratistas y proveedores sean confiables e idóneos para sus funciones. Exige verificaciones proporcionales a la clasificación de la información a la que se accederá, asegurando que se realice la debida diligencia antes del acceso. Anexo A 6.2 Términos y condiciones de empleo. Establecer obligaciones contractuales claras en materia de seguridad de la información. Este control garantiza que los empleados y contratistas comprendan sus responsabilidades legales en cuanto a confidencialidad y protección de datos antes de que se les conceda acceso. Refuerza la posición legal de la organización y establece expectativas explícitas sobre el comportamiento aceptable y los requisitos de no divulgación. Anexo A 6.3 Sensibilización, educación y formación en seguridad de la información. Capacitar al personal sobre sus funciones específicas en materia de seguridad y las amenazas en constante evolución. Este control exige una formación periódica y pertinente para reducir el error humano, a menudo el eslabón más débil de la seguridad. Al fomentar una cultura de seguridad, las organizaciones garantizan que el personal esté capacitado para reconocer el phishing, gestionar los datos correctamente y cumplir con las políticas. Anexo A 6.4 Proceso disciplinario. Implementar un proceso disciplinario formal para las infracciones de seguridad. Este control proporciona un marco estructurado para abordar las filtraciones de datos causadas por negligencia o mala fe. Actúa como un elemento disuasorio fundamental.	X			En articulación con la revisión de competencias técnicas del personal tercerizado (Anexo 1), se constató la implementación de controles legales para la protección de la información. Se verificó la suscripción formal de Acuerdos de Confidencialidad o No Divulgación (NDA) por parte del proveedor tecnológico. Se evidencia que los ingenieros y analistas asignados a la operación del SOC (Security Operations Center) se encuentran sujetos a estos acuerdos legalmente vinculantes, garantizando el resguardo, la no divulgación y el manejo idóneo de los activos de información a los que tienen acceso durante la prestación del servicio.
5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencia 7.3 Toma de conciencia Dominio A.6 Controles de personas A.5.2 Roles y responsabilidades de seguridad de la información A.5.5 Contacto con las autoridades	Anexo A 5.2 Funciones y responsabilidades en materia de seguridad de la información. tareas de seguridad específicas a personas concretas. Este control evita lagunas en la rendición de cuentas al garantizar que las responsabilidades sobre los activos y los procesos de seguridad estén claramente definidas y asignadas. Establece un enfoque estructurado para la gestión de riesgos, asegurando que cada aspecto de la seguridad tenga un responsable designado. Garantizar que exista una estructura definida, aprobada y comprendida para la implementación y el funcionamiento del sistema de gestión de la seguridad de la información. Requisito Definición explícita: Debe documentar claramente las funciones de cada puesto de seguridad. Esto se suele lograr mediante una matriz de roles y responsabilidades o incluyendo las tareas de seguridad en las descripciones de puestos estándar. Asignación a personal competente: Los roles deben asignarse a personas que posean las habilidades y la autoridad necesarias para desempeñarlos. En organizaciones pequeñas, es común (y aceptable) que una persona ocupe varios roles. Supervisión de la dirección: La alta dirección es responsable de garantizar que estas funciones estén correctamente establecidas y cuenten con los recursos adecuados, incluyendo las herramientas, el tiempo y la formación necesarios.	X			Se constata la asignación, comunicación y formalización de los roles y responsabilidades pertinentes al SGSI mediante la Resolución 323207 expedida el 31 de octubre de 2023. Esta resolución evidencia la directriz formal de la organización para establecer las autoridades y obligaciones en materia de seguridad de la información, alineándolas plenamente con los requisitos del sistema de gestión.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencia 7.3 Toma de conciencia Dominio A.6 Controles de personas A.5.2 Roles y responsabilidades de seguridad de la información A.5.5 Contacto con las autoridades	Anexo A 5.5 Contacto con las autoridades. Canales de comunicación con los organismos reguladores y las fuerzas del orden. Este control garantiza que la organización esté preparada para informar sobre incidentes de seguridad o solicitar asesoramiento legal en caso de una brecha de seguridad. Permite una respuesta rápida y conforme a la ley ante incidentes de seguridad importantes y garantiza el cumplimiento de las obligaciones de notificación. Entidad establezca y mantenga contacto con las autoridades pertinentes para garantizar un flujo de información adecuado en relación con incidentes de seguridad, requisitos normativos y obligaciones legales. Aunque pueda parecer obvio, este control es fundamental para la gobernanza. Garantiza que, ante una crisis, como una filtración de datos importante o un incendio, su equipo sepa exactamente a quién contactar, cómo informar del problema y cuáles son los plazos legales para la notificación. Requisito Identificación de autoridades: Debe enumerar todos los organismos reguladores, legales y de supervisión pertinentes para su negocio. Esto incluye a los organismos de protección de datos (como la ICO en el Reino Unido), las fuerzas del orden y los proveedores de servicios públicos. Procesos de notificación definidos: Debe documentar cómo y cuándo se debe contactar a estas autoridades. Por ejemplo, el RGPD exige notificar al organismo regulador en un plazo de 72 horas tras una violación de datos personales. Integración de la respuesta a incidentes: Su lista de contactos debe ser accesible para sus equipos de gestión de incidentes y continuidad del negocio, de modo que puedan actuar de inmediato durante un evento. Registro reglamentario: Debe demostrar que se ha registrado ante las	X			Se evidenció la existencia y formalización de un procedimiento definido para el contacto con las autoridades pertinentes. El proceso establece claramente los protocolos de actuación, los canales de comunicación y designa los roles específicos autorizados para interactuar, notificar y coordinar de manera oportuna con entidades regulatorias y de orden público (tales como autoridades de protección de datos como la SIC, el CSIRT Nacional o el CAI Virtual de la Policía) en caso de materializarse incidentes de seguridad de la información, garantizando el cumplimiento normativo y legal de la organización.
A.6 Controles de personas		X			Se rigen por la ley: ley 1952 de 2019 para la toma de acciones correctiva.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Inteligencia para la MovilidadGestión de Trámites y Servicios a la CiudadaníaGestión de Tránsito Y Control de Tránsito y TransporteControl DisciplinarioIngenieria de TránsitoGestión SocialGestión Contravencional y Transporte PúblicoGestión FinancieraSeguridad VialPlaneación de Transporte e Infraestructura	**Inteligencia para la MovilidadGestión de Trámites y Servicios a la CiudadaníaGestión de Tránsito Y Control de Tránsito y TransporteControl DisciplinarioIngenieria de TránsitoGestión SocialGestión Contravencional y Transporte PúblicoGestión FinancieraSeguridad VialPlaneación de Transporte e Infraestructura**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
6.1 acciones para tratar riesgos y oportunidades 6.1.1 Generalidades 6.1.2 Evaluación de riesgos de seguridad de la información 6.1.3 Tratamiento de los riesgos de seguridad de la información 7.3Toma de conciencia	6.1 Acciones para abordar riesgos y oportunidades. 6.1.1 Generalidades. La entidad planifica e implementa acciones para abordar los riesgos y las oportunidades, integrándolos en los procesos del SGSI, garantizando así que el sistema logre los resultados previstos, prevenga efectos no deseados y fomente la mejora continua. Esto incluye la realización de evaluaciones de riesgos para identificar, analizar y priorizar los riesgos para la confidencialidad, la integridad y la disponibilidad, así como la evaluación de la eficacia de los tratamientos elegidos. Demostrar a la junta directiva y a las partes interesadas que la Entidad reacciona a las amenazas, anticipa y aprovecha activamente todas las ventajas que esconde el riesgo. Esta cláusula saca la seguridad de la información de las rutinas de TI aisladas y la convierte en una fuerza visible y operativa, directamente vinculada a la estrategia, el crecimiento y la confianza de las partes interesadas. La Entidad que adoptan la Cláusula 6.1 como un proceso dinámico convierten la gestión de riesgos y oportunidades en una conversación a nivel directivo, acortando la distancia entre los equipos técnicos y los resultados empresariales. 6.1.2. Evaluación de riesgos de seguridad de la información. -Proceso que establezca y mantenga criterios de aceptación del riesgo y la realización de evaluaciones de riesgos. - Evaluaciones periódicas de riesgo produzcan resultados coherentes, válidos y comparables. - Riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del SGSI. - Se identifiquen a los propietarios de los riesgos. - Probabilidad de materialización. - Consecuencias - Impacto en la materialización de riesgos. - Niveles de riesgo. - Valorar los riesgos y comparación de resultados. - Priorizar los riesgos analizados para determinar trratamiento			X	Se constató que la organización cuenta con una metodología formal y documentada para la apreciación de riesgos, sustentada en el documento 'Guía para la Gestión de Riesgo de la SDM PE01'. Se verificó que el proceso inicia con la identificación de los activos de información a través del módulo de gestión de la plataforma 'Daruma'. La metodología establece criterios de valoración claros basados en la estimación de Probabilidad e Impacto. Asimismo, define los umbrales de aceptación, estipulando que los activos con criticidad alta exigen tratamiento obligatorio, mientras que los riesgos valorados como 'Bajos' son documentados, pero no requieren planes de tratamiento adicionales, en coherencia con el apetito de riesgo de la organización. Oportunidad de Mejora (OM) - Relacionada con 6.1.2 a (Identificación de Riesgos/Amenazas) Durante la revisión del análisis de riesgos del aplicativo 'Observatorio' (específicamente el riesgo de indisponibilidad), se recomienda a la organización reevaluar la inclusión de 'Falta de mantenimiento' como una amenaza dentro de la matriz. Dado que el mantenimiento preventivo y correctivo es una obligación operativa respaldada por un cronograma preestablecido, su omisión constituye un incumplimiento de los procesos internos o una falla de control, más que una amenaza probabilística externa o interna. Ajustar este enfoque permitirá una valoración más precisa de los riesgos reales que afectan la plataforma.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
	7.3, Toma de conciencia : Todo el personal dentro del alcance del SGSI (incluidos empleados, contratistas y directivos) conozca las políticas de seguridad de la información de la organización, su función en el apoyo al SGSI y las consecuencias de las no conformidades. Hace hincapié en integrar la seguridad en el comportamiento diario, no solo en realizar una formación puntual. - Evidencia necesaria de que todos conocen: La política y los objetivos de seguridad de la información Su contribución al SGSI, incluidos sus beneficios Qué podría salir mal y qué significa la no conformidad con el SGSI, a nivel personal y para la empresa ¿El punto clave? La concientización debe ser relevante, actualizada y verificable. Requisitos en materia de concientización y por qué la capacitación no es suficiente? cada persona bajo el SGSI comprenda tres aspectos: la política de seguridad de la información, su función y las consecuencias de las fallas. Si se omite cualquier aspecto, la auditoría será vulnerable, incluso si sus políticas son una fortaleza en el papel. Características clave para la excelencia en la concientización Centralizar la evidencia: Conecte cada actividad de concientización con la política, el riesgo y el rol con unos pocos clics: ya no es necesario buscar pruebas en el momento de la auditoría. Automatizar recordatorios: Los avisos incorporados alertan a los usuarios antes de que la conciencia decaiga, no después. Alinear mensajes: Dirija la información correcta a los puestos adecuados. Ventas, TI y la junta directiva ven lo que les importa.	X			Se verificó la implementación de los planes de tratamiento de riesgos dentro del aplicativo 'Daruma', donde se declaran y gestionan los controles de seguridad aplicables. Mediante un ejercicio de trazabilidad (sampling) sobre el proceso de 'Gestión de Tránsito', se revisó el riesgo de 'Pérdida de disponibilidad del Centro de Datos', el cual afecta directamente a los sistemas de información críticos SUANET y ATULAA. Se evidenció que este riesgo se encuentra en estado 'Aprobado y en supervisión', y se le han aplicado cinco (5) controles específicos para su mitigación. Adicionalmente, como parte del tratamiento de riesgos y las acciones operativas del sistema, se evidenció el registro estructurado de las actualizaciones de seguridad implementadas en los aplicativos y portales web de la organización. La organización demuestra un enfoque sistemático para el mantenimiento de la competencia y la toma de conciencia a través de la estructuración anual del Plan Institucional de Capacitación (PIC) - Plan de Acción 2026. Se evidencia que este plan está reforzado por un programa de sensibilización complementario. Así mismo, se verificó la ejecución de procesos formales de inducción y reinducción orientados al personal nuevo y existente de la Secretaría, validando la eficacia de estas acciones formativas mediante exámenes recurrentes de conocimiento.

	SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG	
ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	Versión 2.0

Fecha:	Nombre(s) equipo auditor y Rol:	Sistema de Gestión auditado :
22/07/2026	Oscar Alberto Barragán León - OABL Sergio Eduardo Reyes Trillos - SERT	SGSI

Nombre del responsable del proceso auditado:	Proceso:	Dependencia :
	Gestión de TICS-OTIC (Seguridad de la Información)	Gestión de TICS-OTIC (Seguridad de la Información)

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
8. Operación 8.1 Planificación y contro operacional 8.2 Evaluación de los riesgo para la seguridad de la información 8.3 Tratamiento de los riesgos para la seguridad de la información	8. Operación. Los controles deben estar en funcionamiento, ser monitoreados y demostrables en el mundo real. 8.1 – Planificación y Control Operativo, exige que la Entidad planifique, implemente y controle los procesos necesarios para cumplir con los requisitos de seguridad de la información, transformando las políticas y los planes de gestión de riesgos en prácticas operativas consistentes, demostrables y responsables. Ënfasis en ejecución medible, la responsabilidad asignada y la capacidad de generar evidencia en tiempo real del cumplimiento y la eficacia, incluso durante cambios, crisis o auditorías. Cada rutina, desde el análisis de vulnerabilidades hasta la verificación de proveedores, debe tener un responsable designado, un cronograma y un registro de evidencias repetible. - La información documentada debe estar disponbile para tener confinza que los procesos han sido ejecutados según lo planificado. - Control de cambios planificdos y de emergencia. - Control de procesos, productos y servicios suministrados externamente relativos al SGSI. 8.2. Evaluación de los riesgos para la seguridad de la información. - Evaluación de los riesgos de seguridad a intervalos planificados o cuando se presenten cambios significativos en los procesos, productos o servicios. - Información documentada de los resultados de las evaluciones de riesgos de seguridad de la información. 8.3. Tratamiento de riesgos de seguridad de la información.	X			Se evidencia una adecuada planificación y control operacional del SGSI mediante la estructuración del mapa de procesos de la organización. A través de la plataforma 'Daruma', se constató que la documentación está metódicamente dividida y alineada, vinculando cada proceso con sus respectivos procedimientos, manuales y políticas de seguridad aplicables. Se verificó el uso del repositorio 'Drive' como sistema de almacenamiento de archivos, destacándose que el personal auditado demuestra un amplio conocimiento, apropiación y control sobre la documentación allí resguardada. En estricto cumplimiento con el requisito de controlar los procesos contratados externamente (tercerizados), se constató la gestión operativa sobre los proveedores de servicios tecnológicos críticos, los cuales abarcan: el Centro de Operaciones de Seguridad (SOC), soluciones SIEM y SOAR, servicios de infraestructura en la Nube y ejecución de ejercicios de Ethical Hacking. Como parte de los controles técnicos operacionales base, se validó la operatividad e implementación de sistemas Antivirus y plataformas Firewall (arquitectura Palo Alto).
8. Operación 8.1 Planificación y contro operacional 8.2 Evaluación de los riesgo para la seguridad de la información 8.3 Tratamiento de los riesgos para la seguridad de la información	8. Operación. Los controles deben estar en funcionamiento, ser monitoreados y demostrables en el mundo real. 8.1 – Planificación y Control Operativo, exige que la Entidad planifique, implemente y controle los procesos necesarios para cumplir con los requisitos de seguridad de la información, transformando las políticas y los planes de gestión de riesgos en prácticas operativas consistentes, demostrables y responsables. Ënfasis en ejecución medible, la responsabilidad asignada y la capacidad de generar evidencia en tiempo real del cumplimiento y la eficacia, incluso durante cambios, crisis o auditorías. Cada rutina, desde el análisis de vulnerabilidades hasta la verificación de proveedores, debe tener un responsable designado, un cronograma y un registro de evidencias repetible. - La información documentada debe estar disponbile para tener confinza que los procesos han sido ejecutados según lo planificado. - Control de cambios planificdos y de emergencia. - Control de procesos, productos y servicios suministrados externamente relativos al SGSI. 8.2. Evaluación de los riesgos para la seguridad de la información. - Evaluación de los riesgos de seguridad a intervalos planificados o cuando se presenten cambios significativos en los procesos, productos o servicios. - Información documentada de los resultados de las evaluciones de riesgos	X			Como parte de las actividades continuas de identificación y apreciación de riesgos a intervalos planificados y ante cambios en el entorno técnico, se constató la ejecución estructurada de análisis de seguridad técnica. Como evidencia objetiva, se revisó el 'Informe de Implementación', el cual consolida los registros y resultados de los servicios tercerizados de detección de vulnerabilidades, incluyendo los datos arrojados por las herramientas de escaneo de aplicaciones web (WAS - Web Application Security) y los reportes derivados de las pruebas de Ethical Hacking."

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
8. Operación 8.1 Planificación y contr operacional 8.2 Evaluación de los riesgo para la seguridad de la información 8.3 Tratamiento de los riesgos para la seguridad de la información	8. Operación. Los controles deben estar en funcionamiento, ser monitoreados y demostrables en el mundo real. 8.1 – Planificación y Control Operativo, exige que la Entidad planifique, implemente y controle los procesos necesarios para cumplir con los requisitos de seguridad de la información, transformando las políticas y los planes de gestión de riesgos en prácticas operativas consistentes, demostrables y responsables. Ënfasis en ejecución medible, la responsabilidad asignada y la capacidad de generar evidencia en tiempo real del cumplimiento y la eficacia, incluso durante cambios, crisis o auditorías. Cada rutina, desde el análisis de vulnerabilidades hasta la verificación de proveedores, debe tener un responsable designado, un cronograma y un registro de evidencias repetible. - La información documentada debe estar disponbile para tener confinza que los procesos han sido ejecutados según lo planificado. - Control de cambios planificdos y de emergencia. - Control de procesos, productos y servicios suministrados externamente	X			Se verificó la materialización del plan de tratamiento de riesgos a través de la implementación de controles técnicos avanzados. La organización evidencia el despliegue de medidas mitigantes proporcionales a las amenazas identificadas, operando de manera orquestada a través del SOC tercerizado. Esto incluye la aplicación de controles preventivos y de monitoreo continuo (SIEM) y la automatización de la respuesta (SOAR), apoyados en la infraestructura perimetral (Firewall Palo Alto) y de punto final (Antivirus) para garantizar la contención técnica frente a la materialización de riesgos de seguridad de la información.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
Hernan Rodolfo Lopez Ahumada	**Gestión Administrativa**	**Gestión Administrativa**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.9 Inventario de activos y otros activos asociados A.5.10 uso aceptable de activos y otros activos asociados A 5.11 Devolución de activos A.5.12 Clasificación de la información A.5.13 Etiquetado de la información	Anexo A 5.9 Inventario de información y otros activos asociados Identifique y enumere todos los activos críticos. Este control sienta las bases para la evaluación de riesgos al requerir un inventario detallado de la información y los activos físicos. Garantiza que todos los elementos valiosos sean conocidos, propiedad de sus dueños y estén protegidos según su importancia y criticidad para las operaciones comerciales. Desarrollar y mantener un inventario de toda la información y demás activos asociados, incluyendo la asignación de propietarios. Este control se basa en un principio de seguridad sencillo pero fundamental: «No se puede proteger lo que se desconoce». Al identificar cada dispositivo físico, aplicación de software y conjunto de datos dentro de su ámbito de aplicación, se sientan las bases para la gestión de riesgos, la respuesta a incidentes y la gestión del ciclo de vida. Objetivo El objetivo del Anexo A 5.9 de la norma ISO 27001 es garantizar que se identifique la información de la organización y otros activos asociados para preservar su seguridad y asignar la propiedad adecuada. Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios. Requisito - Identificación de 3 tipos de activos: Debe inventariar tres categorías específicas: Activos físicos: Ordenadores portátiles, servidores, equipos de red y soportes extraíbles. Activos de información/datos: Bases de datos de clientes, propiedad	X			Se verificó la gestión, identificación y mantenimiento del inventario de activos. Para los activos de información (físicos e intangibles), la organización utiliza el sistema 'Daruma', el cual se descarga y somete a un proceso de auditoría mensual. Por su parte, el control de activos físicos e infraestructura tecnológica se administra a través del aplicativo web 'SI CAPITAL', complementado por el sistema 'SAI' para el control de ingresos y la herramienta de mesa de ayuda 'Aranda'. Como evidencia de control y seguimiento, se constató la ejecución de un cierre y auditoría de inventario mensual (corte al día 30), garantizando la integridad y actualización de los registros.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.9 Inventario de activos y otros activos asociados A.5.10 uso aceptable de activos y otros activos asociados A 5.11 Devolución de activos A.5.12 Clasificación de la información A.5.13 Etiquetado de la información	Anexo A 5.10 Uso aceptable de la información y otros activos asociados. Normas estrictas para el uso de los activos. Este control establece políticas claras sobre cómo los empleados y terceros pueden utilizar la tecnología y los datos de la organización. Protege los activos contra el uso indebido, los daños o el acceso no autorizado, al establecer límites y expectativas claras sobre el comportamiento profesional. El objetivo del Anexo A 5.10 de la norma ISO 27001 es establecer un control preventivo que garantice que la información y otros activos asociados estén protegidos, utilizados y gestionados adecuadamente. Requisito Implementación formal de la Política de Uso Aceptable (PUA): Debe contar con una Política de Uso Aceptable (PUA) documentada , aprobada por la gerencia y reconocida explícitamente por todos los usuarios. Gestión integral del ciclo de vida: El uso aceptable se aplica desde el momento en que se asigna un activo hasta que se devuelve o se destruye. Esto incluye normas para la clasificación de datos, el almacenamiento seguro y la eliminación correcta. Nube y dispositivos personales: Las normas deben extenderse a los activos que no son propiedad de la empresa, como los servicios en la nube (SaaS) y los dispositivos personales (BYOD) , si se utilizan para procesar información de la empresa. Divulgación de la supervisión: La política debe indicar claramente qué tipo de supervisión realiza la organización (por ejemplo, filtrado de correos electrónicos o de páginas web) para garantizar la transparencia y el cumplimiento legal. Expectativas de comportamiento: Debe definir los “comportamientos prohibidos”, como instalar software pirateado, compartir contraseñas o	X			Se evidenció el control sobre la asignación y responsabilidad de los activos de la organización de acuerdo con el Procedimiento de Gestión de Bienes v5. La organización mantiene trazabilidad de todo el ciclo de vida del activo (ingreso, movimiento y salida). Se constató que la entrega de activos a los colaboradores se formaliza mediante la firma de un acuse de recibo, documento que actúa como evidencia de la aceptación de las responsabilidades y el compromiso de uso aceptable por parte del usuario final.
A.5.9 Inventario de activos y otros activos asociados A.5.10 uso aceptable de activos y otros activos asociados A 5.11 Devolución de activos A.5.12 Clasificación de la información A.5.13 Etiquetado de la información	Anexo A 5.11 Devolución de activos. Devolución del equipo al finalizar la relación laboral. Este control garantiza la devolución de todos los activos e información de la organización cuando un empleado o contratista se marcha. Previene la fuga de datos y el acceso no autorizado, asegurando que el hardware y la propiedad intelectual permanezcan bajo el control de la organización. El objetivo del Anexo A 5.11 de la norma ISO 27001 es garantizar la protección de los activos de la organización como parte del proceso de modificación o rescisión de un contrato de trabajo, un acuerdo o una relación laboral. Requisito Proceso formal de recuperación de activos: Debe contar con un procedimiento documentado para la recuperación de activos. Este proceso debe ser activado automáticamente por el departamento de Recursos Humanos cada vez que se reciba una notificación de renuncia o despido. Aplicación de la ley: Los contratos laborales y de contratistas deben incluir cláusulas explícitas que exijan la devolución de todos los activos. Sin esto, no tendrá ninguna base legal para recuperar los bienes de la empresa. Recuperación digital del acceso: La recuperación de los activos no es solo física. Debe revocar el acceso al correo electrónico, las VPN y las aplicaciones SaaS (por ejemplo, Salesforce, Slack) inmediatamente después de la salida del empleado. Eliminación de datos de dispositivos personales: Si los empleados utilizan dispositivos personales para trabajar (BYOD), debe asegurarse de que los datos de la empresa se eliminen de dichos dispositivos. Esto se suele hacer mediante borrado remoto o una declaración formal de eliminación firmada por el empleado que deja la empresa.	X			Se evaluó el procedimiento para la devolución, retiro y baja de activos, evidenciando un proceso estructurado y documentado. Se constató que cualquier solicitud de baja tecnológica por obsolescencia debe estar respaldada obligatoriamente por un concepto técnico formal y un memorando de solicitud. Adicionalmente, como evidencia del control directivo sobre la disposición final de los activos, se revisó el acta de reunión mediante la cual se aprueba y oficializa qué bienes son retirados del inventario corporativo para ser destinados a procesos de subasta.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.9 Inventario de activos y otros activos asociados A.5.10 uso aceptable de activos y otros activos asociados A 5.11 Devolución de activos A.5.12 Clasificación de la información A.5.13 Etiquetado de la información	Anexo A 5.12 Clasificación de la información. Clasificación de los datos según su valor y sensibilidad. Este control requiere que la información esté clasificada para garantizar la aplicación de los niveles de protección adecuados. Optimiza los recursos de seguridad al concentrar las defensas en los datos críticos y confidenciales, cumpliendo al mismo tiempo con los requisitos legales y normativos. El objetivo del Anexo A 5.12 de la norma ISO 27001 es garantizar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización. Requisito Esquema de clasificación simple: Debe definir un esquema claro para los niveles de datos. Si bien el estándar sugiere hasta cuatro niveles, la mayoría de las implementaciones exitosas utilizan un enfoque simple de 3 niveles: Público, Interno y Confidencial. Propietarios de la información asignados: Cada conjunto de datos o activo de información debe tener un "Propietario" asignado. El propietario es responsable de determinar el nivel de clasificación y de garantizar que los datos se gestionen correctamente a lo largo de su ciclo de vida. Coherencia en toda la organización: La clasificación debe ser un lenguaje universal. Ya sea un documento en papel o una base de datos digital, todos en la empresa deben clasificar y gestionar el mismo tipo de datos de la misma manera. Etiquetado visual o metadatos: La información clasificada debe estar claramente marcada. Esto puede ser visual (por ejemplo, una marca de agua que indique "Confidencial") o técnico (por ejemplo, etiquetas de metadatos utilizadas por el software de prevención de pérdida de datos (DLP)).	X			Se verificó el establecimiento y aplicación de un esquema estructurado de clasificación basado en el documento 'Instructivo para la Clasificación de Activos de Información PA04-IN03 V4'. Durante las entrevistas de auditoría, el personal demostró un claro entendimiento, apropiación y competencia respecto a los criterios del procedimiento de clasificación. El inventario clasificado de los activos de información de la SDM se encuentra centralizado y resguardado en la plataforma 'Daruma'.
A.5.9 Inventario de activos y otros activos asociados A.5.10 uso aceptable de activos y otros activos asociados A 5.11 Devolución de activos A.5.12 Clasificación de la información A.5.13 Etiquetado de la información	Anexo A 5.13 Etiquetado de la información Marcar los datos para evitar su manipulación indebida. Este control garantiza que la información esté claramente etiquetada según su esquema de clasificación. Las etiquetas visuales y electrónicas ayudan al personal y a los sistemas automatizados a identificar datos sensibles, evitando la divulgación accidental o el acceso no autorizado a registros confidenciales. El propósito del Anexo A 5.13 de la norma ISO 27001 es garantizar que se facilite la comunicación de la clasificación de la información y se respalde la automatización del procesamiento y la gestión de la información. Requisito Alineación con la clasificación: Las etiquetas deben coincidir directamente con sus niveles de clasificación (por ejemplo, Público, Interno, Confidencial). Si aún no tiene un esquema de clasificación, no podrá cumplir con este control. Etiquetado independiente del formato: Los procedimientos deben abarcar los datos en todas sus formas: físicas (papel, memorias USB), digitales (documentos de Office, PDF) y comunicaciones electrónicas (correos electrónicos, Slack). Introducción de metadatos: La actualización de 2022 hace especial hincapié en los metadatos . Idealmente, los archivos digitales deberían estar "etiquetados" con etiquetas de seguridad ocultas que los sistemas automatizados (como DLP o pasarelas de correo electrónico) puedan leer y sobre las que puedan actuar. Gestión de excepciones: Debe definir cuándo no se requiere el etiquetado (por ejemplo, para información "pública") para reducir la carga administrativa del personal. Capacitación del personal: El personal debe recibir capacitación sobre cómo	X			En concordancia con el esquema de clasificación, se constató la implementación técnica de los procedimientos de etiquetado. La organización ha determinado un enfoque de etiquetado digital, el cual se ejecuta y visualiza de manera exclusiva a través de los sistemas corporativos 'Daruma' (para el inventario y gestión de mesa de ayuda) y 'Orfeo' (como sistema de gestión documental), asegurando que la información sea tratada de acuerdo con su nivel de clasificación dentro de dichas plataformas.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Operador TecnológicoGestión Jurídica	**Gestión de TICS-OTIC (Seguridad de la Información)Operador TecnológicoGestión Jurídica**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
6.3 Planificación de los cambios 9.1 Monitoreo, medición, análisis y evaluación Control A.8.32 Gestión del cambio Control A.5.31 Requisitos legales, reglamentarios y contractuales, A.5.32 Derechos de propiedad intelectual, A.5.33 Privacidad y protección de la información, A.5.34 protección de registros, A.5.35 revisiones independientes de seguridad de la información, A.5.36 Cumplimiento de políticas reglas y estándares de Seguridad de la	6.3. Planificación de los cambios. Cuando la entidad determine la necesidad de realizar cambios al Sistema de Gestión de Seguridad de la Información SGSI - compruebe que se realice de forma planificada. 9.1 Seguimiento, medición, análisis y evaluación La entidad establezca un proceso estructurado para la monitorización, medición, análisis y evaluación de su SGSI, a fin de garantizar su eficacia y su alineación con los objetivos y riesgos del negocio. Hace hincapié en la selección de métricas relevantes, su revisión periódica y el uso de los resultados para impulsar la toma de decisiones informadas y la mejora continua. Decidir qué es lo más importante para ver: No todos los registros o listas de verificación aportan valor. Debe determinar qué controles, eventos o resultados de aprendizaje revelan la salud de su SGSI o resaltan la desviación del riesgo. Establecer una frecuencia inteligente y rendición de cuentas: ¿Se realizan revisiones en tiempo real, mensualmente o trimestralmente? La respuesta debe ajustarse a su perfil de amenaza, no al calendario del auditor. Análisis exigente, no solo registro: Las cifras no significan mucho hasta que las tendencias incitan a la investigación y la acción. Combine las métricas cuantitativas con revisiones cualitativas: entrevistas, relatos de incidentes o cambios en el apetito de riesgo de la gerencia. Hacer que la medición sea operativa y no ornamental: Los KPI y los paneles de control deberían revelar los problemas antes de que se produzca un incidente o un auditor, no después. Cuando se aplica correctamente la Cláusula 9.1, sus métricas:	X			Se verificó la planificación, control y seguimiento de los cambios que afectan la seguridad de la información. El registro, trazabilidad y gestión del ciclo de vida de los cambios se ejecuta de manera centralizada en la plataforma 'Aranda', utilizando como soporte documental el formato PA04-PR04-F01-V2-RFC (Request for Change). A través de un ejercicio de muestreo técnico, se auditó un cambio de emergencia correspondiente a la actualización de servidores Apache. Se evidenció de manera satisfactoria que dicho cambio fue gatillado como respuesta a una notificación oficial de ciberseguridad emitida por el COLCERT, demostrando una articulación eficaz entre la inteligencia de amenazas externas y el control de cambios interno. Así mismo, se constató que cualquier modificación a nivel de bases de datos debe surtir, de manera obligatoria, este mismo flujo de aprobación institucional. Se constató que la organización ejecuta procesos continuos de monitoreo y análisis sobre los componentes de su SGSI. Esto se evidencia de manera objetiva a través de la revisión sistémica de la Matriz Legal, el seguimiento estructurado de los tickets de cambios en la plataforma Aranda y la supervisión de la infraestructura de bases de datos, garantizando que el sistema produce resultados válidos y permite evaluar el desempeño de la seguridad de la información.
6.3 Planificación de los cambios 9.1 Monitoreo, medición, análisis y evaluación Control A.8.32 Gestión del cambio Control A.5.31 Requisitos legales, reglamentarios y contractuales, A.5.32 Derechos de propiedad intelectual, A.5.33 Privacidad y protección de la información, A.5.34 protección de registros, A.5.35 revisiones independientes de seguridad de la información,	Anexo A 8.32 Gestión del cambio. Controlar los cambios en la infraestructura de TI. Este control exige un proceso formal para gestionar los cambios en los sistemas e instalaciones de procesamiento de información. Garantiza que todos los cambios se evalúen, autoricen, prioricen, planifiquen y prueben para minimizar el riesgo de interrupciones o incidentes de seguridad causados por modificaciones no gestionadas. cualquier cambio en las instalaciones de procesamiento de información (sistemas informáticos, redes, software) o en el propio Sistema de Gestión de la Seguridad de la Información (SGSI) se gestione de forma planificada, no improvisada. Su objetivo es evitar que las buenas intenciones provoquen incidentes de seguridad, garantizando que cada actualización, parche o ajuste de configuración se evalúe en cuanto a riesgos antes de su implementación. El objetivo del Anexo A 8.32 de la norma ISO 27001 es establecer un control preventivo para preservar la seguridad de la información al realizar cambios. Requisito La regla de "Detenerse y verificar": Antes de cambiar una regla de firewall, actualizar un servidor o migrar a un nuevo proveedor de nube, debe preguntarse formalmente: "¿Esto comprometerá nuestra seguridad?". Separación de funciones: Lo ideal es que la persona que escribe el código o solicita el cambio no sea la misma que lo aprueba. Se necesita una segunda opinión. Procedimientos de respaldo: Debe tener un "Plan B". Si el cambio falla (por	X			Se verificó la planificación, control y seguimiento de los cambios que afectan la seguridad de la información. El registro, trazabilidad y gestión del ciclo de vida de los cambios se ejecuta de manera centralizada en la plataforma 'Aranda', utilizando como soporte documental el formato PA04-PR04-F01-V2-RFC (Request for Change). A través de un ejercicio de muestreo técnico, se auditó un cambio de emergencia correspondiente a la actualización de servidores Apache. Se evidenció de manera satisfactoria que dicho cambio fue gatillado como respuesta a una notificación oficial de ciberseguridad emitida por el COLCERT, demostrando una articulación eficaz entre la inteligencia de amenazas externas y el control de cambios interno. Así mismo, se constató que cualquier modificación a nivel de bases de datos debe surtir, de manera obligatoria, este mismo flujo de aprobación institucional.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
6.3 Planificación de los cambios 9.1 Monitoreo, medición, análisis y evaluación Control A.8.32 Gestión del cambio Control A.5.31 Requisitos legales, reglamentarios y contractuales, A.5.32 Derechos de propiedad intelectual, A.5.33 Privacidad y protección de la información, A.5.34 protección de registros, A.5.35 revisiones independientes de seguridad de la información, A.5.36 Cumplimiento de políticas reglas y estándares de Seguridad de la	Anexo A 5.31 Identificación de los requisitos legales, estatutarios reglamentarios y contractuales. Documentar todas las obligaciones de cumplimiento. Este control exige la identificación y documentación explícita de todas las leyes y regulaciones pertinentes. Previene sanciones por incumplimiento al garantizar que la organización comprenda sus obligaciones legales específicas en materia de protección de datos, propiedad intelectual y estándares del sector. El objetivo del Anexo A 5.31 de la norma ISO 27001, relativo a los requisitos legales, reglamentarios y contractuales, es garantizar el cumplimiento de dichos requisitos en materia de seguridad de la información. Las responsabilidades de una organización en materia de seguridad de la información se rigen por leyes, reglamentos y requisitos contractuales. Las organizaciones deben comprender claramente sus obligaciones y estar preparadas para incluirlas en sus prácticas de seguridad de la información. Requisito Registro Legal: Debe crear un documento centralizado (un “Registro Legal”) que enumere todas las leyes, reglamentos y cláusulas contractuales aplicables a su seguridad. Este es el elemento principal de este control. Responsabilidad específica: No basta con enumerar una ley; debe asignarse a una persona específica (por ejemplo, "Jefe de Recursos Humanos") la responsabilidad de supervisar dicha ley. Controles criptográficos: Debe identificar específicamente las leyes relativas al cifrado, especialmente si opera a nivel internacional, ya que algunos países restringen la importación/exportación de software criptográfico. Revisión periódica: Las leyes cambian. Debe revisar su registro a intervalos	X			Se constató la identificación y documentación de los requisitos legales y regulatorios aplicables al SGSI. La organización administra una Matriz Legal de Cumplimiento, cuyo marco de gestión se encuentra definido en el 'Instructivo Normatividad y Conceptos PA05-IN02 V12'. Se auditó el procedimiento de actualización de dicha matriz, validando mediante trazabilidad de correos electrónicos el flujo de notificación hacia el área de Calidad para la integración y completitud de nuevas normativas. En el ámbito contractual, se consultó el repositorio 'Daruma' (categoría 'Estudios Previos'), revisando el documento de 'Obligaciones generales contractuales para las personas jurídicas y naturales', el cual establece y formaliza las exigencias de seguridad y cumplimiento normativo exigidas por la SDM hacia sus contratistas.
6.3 Planificación de los cambios 9.1 Monitoreo, medición, análisis y evaluación Control A.8.32 Gestión del cambio Control A.5.31 Requisitos legales, reglamentarios y contractuales, A.5.32 Derechos de propiedad intelectual, A.5.33 Privacidad y protección de la información, A.5.34 protección de registros, A.5.35 revisiones independientes de seguridad de la información, A.5.36 Cumplimiento de políticas reglas y estándares de Seguridad de la	Anexo A 5.32 Derechos de propiedad intelectual. Garantizar el cumplimiento de las leyes de propiedad intelectual. Este control protege a la organización de litigios relacionados con la piratería de software o la infracción de derechos de autor. Asimismo, asegura el cumplimiento de las restricciones legales sobre el uso de material de terceros y salvaguarda los activos propios y la propiedad intelectual de la organización. Anexo A 5.33 Protección de registros. Proteja los registros contra pérdidas falsificaciones. Este control salvaguarda los registros de la organización contra la destrucción y el acceso no autorizado. Garantiza el cumplimiento de los requisitos legales, reglamentarios y contractuales de conservación y eliminación segura de registros, preservando así la memoria y la reputación jurídica de la organización. Anexo A 5.34 Privacidad y protección de la información personal identificable (PII, por sus siglas en inglés). Proteger la información de identificación personal. Este control garantiza el cumplimiento de las leyes de privacidad como el RGPD o la CCPA. Exige medidas técnicas y organizativas para proteger los datos personales, respetando los derechos de los titulares de los datos y previniendo violaciones de la privacidad que podrían acarrear multas cuantiosas y daños a la reputación. Anexo A 5.35 Revisión independiente de la seguridad de la información. Realizar evaluaciones de seguridad objetivas. Este control requiere una revisión imparcial del enfoque de la organización respecto a la seguridad de la información. Mediante auditores independientes, la organización verifica que sus controles se implementen de manera efectiva y sigan siendo adecuados para el panorama de riesgos en constante evolución.	X			Se verificó el cumplimiento de las directrices para la protección de la propiedad intelectual. A través de la revisión del documento de obligaciones contractuales previamente mencionado, se evidenció la existencia de cláusulas legales explícitas que garantizan y reafirman que todos los derechos de propiedad intelectual derivados de la prestación de servicios o desarrollos pertenecen íntegramente a la SDM, previniendo riesgos legales o disputas de autoría. Se evaluaron los controles técnicos implementados para garantizar la integridad, privacidad y protección de los registros de la organización. Se evidenció la utilización de modelos de bases de datos relacionales desplegados en entornos de Nube. Para asegurar la consistencia y blindar la información contra modificaciones no autorizadas, la arquitectura de datos emplea restricciones lógicas (constraints). Además, se constató que los privilegios y permisos de escritura en las bases de datos se encuentran estrictamente controlados, aplicando el principio de mínimo privilegio.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Operador TecnológicoGestión Jurídica	**Gestión de TICS-OTIC (Seguridad de la Información)Operador TecnológicoGestión Jurídica**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
9.2 Auditoría interna 10.1 Mejora continua 10.2 No conformidad y acción correctiva 9.3 Revisión por la Dirección	9.2 Auditoría interna. Entidad establezca un programa estructurado de auditoría interna para evaluar periódicamente la eficacia de su Sistema de Gestión de la Seguridad de la Información (SGSI). Ënfasis en la imparcialidad, la evidencia documentada y la aplicación oportuna de medidas correctivas para garantizar que el SGSI se mantenga conforme, sea eficaz y responda a los riesgos. La mayoría de los equipos ven la auditoría interna como una tarea rutinaria. Las empresas de alto rendimiento la reconocen como el motor que marca su ritmo de riesgo y transmite confianza a todas las partes interesadas. Si opera a un ritmo digital y sabe que las amenazas reales no esperan a las revisiones anuales, necesita que la Cláusula 9.2 funcione a pleno rendimiento. La Cláusula 9.2 pone fin a la era de las auditorías superficiales. Exige un programa integral que abarque la Declaración de Aplicabilidad completa, relacione cada hallazgo con una acción real y documente cada cierre. ISMS.online integra estas exigencias: formalizando la independencia, detallando su alcance en tiempo real y persiguiendo la rendición de cuentas hasta su finalización. Así es como los SGSI promedio superan la adecuación y crean un registro en el que sus auditores externos pueden confiar sin pestañear.	X			Se verificó la planificación, ejecución y objetividad del programa de auditorías del SGSI. La organización demostró la estructuración de este proceso mediante el documento 'Plan de Auditorías Internas 2026' y el lineamiento aplicable PV01-IN. Se evidenció que la entidad ha optado por ejecutar este ejercicio a través de proveedores externos independientes, garantizando la imparcialidad del proceso. Para validar la idoneidad del equipo evaluador, se auditaron las hojas de vida de los dos auditores asignados, constatando que ambos profesionales cumplen a cabalidad con la competencia, formación y experiencia exigidas por el procedimiento de auditoría interna del sistema.
9.2 Auditoría interna 10.1 Mejora continua 10.2 No conformidad y acción correctiva 9.3 Revisión por la Dirección	10.1 Mejora continua La cláusula 10.1 de la norma ISO 27001:2022 exige que las organizaciones implementen un proceso de mejora continua para su Sistema de Gestión de Seguridad de la Información (SGSI), garantizando su evolución con el tiempo en respuesta a auditorías, incidentes, retroalimentación y riesgos cambiantes. En lugar de una tarea puntual, exige un progreso continuo y basado en la evidencia que demuestre aprendizaje, adaptación y una mejora medible de la seguridad. Para que la mejora sea real, hay que basarla en tres prácticas repetibles: 1. Análisis de desencadenantes de rutina Cada auditoría, incidente, cuasi accidente o incluso sugerencia del personal debería dar lugar a una minirevisión. Capacite a los equipos para que se pregunten: ¿Qué aprendimos y qué debemos cambiar? En la práctica, esto significa analizar los hallazgos de las auditorías, los registros de incidentes y los informes de turno con una mirada crítica y orientada al futuro. Incluso una sola vulnerabilidad detectada puede impulsar una actualización de procesos o tecnología. 2. Cerrar brechas con acciones documentadas La cláusula 10.1 exige que las brechas no solo se identifiquen, sino que se aborden sistemáticamente, cada una con una responsabilidad clara, plazos y una solución visible. Aquí es donde muchas organizaciones tropiezan: actividad sin pruebas o actualizaciones perdidas en semanas de mucha actividad. Los líderes ideales de SGSI adquieren el hábito de rastrear cada				Se evaluó la eficacia de la organización para gestionar las salidas de las auditorías y promover la mejora continua del sistema. Se constató que durante el ciclo de auditoría inmediatamente anterior no se materializaron No Conformidades; sin embargo, el equipo auditor documentó tres (3) Oportunidades de Mejora (OM). Mediante un ejercicio de trazabilidad, se auditó el registro y tratamiento del hallazgo referenciado como '003-2026', evidenciando que la organización realiza el seguimiento pertinente y aplica acciones para optimizar la conveniencia, adecuación y eficacia del SGSI.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
9.2 Auditoría interna 10.1 Mejora continua 10.2 No conformidad y acción correctiva 9.3 Revisión por la Dirección	10.2 No conformidad y acciones correctivas La cláusula 27001 de la norma ISO 2022:10.2 exige que las organizaciones tomen medidas rápidas y estructuradas cuando se produzcan no conformidades. Esto incluye identificar la causa raíz, implementar acciones correctivas eficaces, verificar su éxito y asegurar que se evite su recurrencia. Hace hincapié en el cierre documentado y basado en la evidencia para apoyar la mejora continua y la preparación para auditorías. La transformación ya no es opcional: es el precio del liderazgo La cláusula 10.2 no solo pone a prueba el cumplimiento, sino que también expone su capacidad de adaptación. Los equipos que desarrollan memoria institucional y hábitos de mejora visibles obtienen más que certificados: se ganan la confianza de la junta directiva, la aprobación de las regulaciones y la lealtad de los clientes. Mejore antes de imponerse. Lidere el cumplimiento normativo de su mercado con acciones y pruebas, no con declaraciones de crisis y excusas.			X	Se evaluó la eficacia de la organización para gestionar las salidas de las auditorías y promover la mejora continua del sistema. Se constató que durante el ciclo de auditoría inmediatamente anterior no se materializaron No Conformidades; sin embargo, el equipo auditor documentó tres (3) Oportunidades de Mejora (OM). Mediante un ejercicio de trazabilidad, se auditó el registro y tratamiento del hallazgo referenciado como '003-2026', evidenciando que la organización realiza el seguimiento pertinente y aplica acciones para optimizar la conveniencia, adecuación y eficacia del SGSI.
9.2 Auditoría interna 10.1 Mejora continua 10.2 No conformidad y acción correctiva 9.3 Revisión por la Dirección	9.3 Revisión por la dirección La cláusula 27001 de la norma ISO 2022:9.3 exige que la alta dirección realice revisiones proactivas y basadas en la evidencia del SGSI para evaluar su rendimiento, abordar los riesgos emergentes e impulsar la mejora continua. Esta cláusula cambia el enfoque de la supervisión pasiva a la participación estratégica del liderazgo, garantizando que la seguridad se convierta en una función esencial del negocio, no solo en una cuestión de cumplimiento. La cláusula 9.3 de la norma ISO 27001:2022 no es una modificación burocrática de las viejas rutinas, es una Reinicio completo de cómo el liderazgo se relaciona con el SGSIEl nuevo plan exige una revisión continua basada en evidencia, sin lugar a ambigüedades sobre quién hace qué, qué se discute o cómo se generan los resultados. Pasar por los obstáculos mínimos no es suficiente. Los organismos de certificación ahora cuestionan tanto su “proceso” como su “prueba”. Una revisión de gestión conforme debe examinar: Estado de las acciones de revisión de gestión anteriores: – ¿Tu equipo actuó o sólo tomó nota del punto? Cambios en el panorama de riesgos: – Tanto internos (fusiones, reestructuraciones, rotación de personal, incidentes) como externos (nuevas leyes, evolución de actores de amenazas, tendencias regulatorias). Objetivos y desempeño del SGSI: – ¿Habéis alcanzado vuestros objetivos de seguridad? ¿Y cuáles son las pruebas? KPI, métricas de incidentes y hallazgos de auditoría: – Los datos, no la esperanza, impulsan los próximos pasos. Comentarios de las partes interesadas: – Clientes, cadena de suministro,	X			Se constató que la alta dirección revisa el SGSI a intervalos planificados para asegurar su conveniencia, adecuación y eficacia continuas. Como evidencia objetiva del cumplimiento de los elementos de entrada y salida exigidos por la norma, se referencia el acta_cigd_10-03-2026 (comité mensual), en la cual se aprueban las acciones de mejora, se evalúan los resultados del sistema y se asignan los recursos necesarios para el desarrollo del SGSI.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN
	Lista de verificación
	Código: PV01-IN03- F02 / **Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Direccionamiento Estratégico-OAPI	**Gestión de TICS-OTIC (Seguridad de la Información)Direccionamiento Estratégico-OAPI**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
4. Contexto de la organización 4.1 Comprensión de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información 4.4 Sistema de gestión de la seguridad de la información 7.1 Recursos	Contexto (Cláusula 4): Obliga a una evaluación real de su entorno operativo. ¿Quiénes son importantes? ¿Qué está en riesgo? ¿Dónde están los puntos de presión? El cumplimiento empieza por mapear su territorio, no por copiar las políticas de sus vecinos. 4.1 Comprensión de la organización y el contexto La cláusula 27001 de la norma ISO 2022:4.1 exige que las organizaciones identifiquen y supervisen los problemas internos y externos que podrían afectar los resultados previstos de su Sistema de Gestión de la Seguridad de la Información (SGSI). Esto garantiza que el SGSI esté alineado con la dirección estratégica de la organización, el entorno de riesgos y el contexto empresarial en constante evolución. La cláusula 4.1 de la norma ISO 27001:2022 existe porque la seguridad de la información no opera de forma aislada, sino que está integrada en las realidades de su negocio, los mercados y los riesgos regulatorios. Si omite este paso fundamental, todos los controles que implemente se asientan sobre una base inestable. Los riesgos que no puedes ver suelen ser los más importantes. Reconocer el contexto significa no solo implementar controles adicionales, sino construir un SGSI alineado directamente con sus activos clave, su tolerancia al riesgo y el valor de las partes interesadas. Con un aumento interanual de más del 38% en los ciberataques. (Investigación de Check Point, 2023), y los reguladores imponen multas récord en todo el mundo (DLA Piper, 2023)Comprender las amenazas inherentes a su sector y geografía no es opcional. Es la única manera de defender la confianza y la reputación.	X			Se constató que la organización ha determinado de manera adecuada las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos del SGSI. La definición general del contexto organizacional se encuentra formalizada, documentada y disponible para las partes interesadas a través de la página web institucional. Como evidencia objetiva del análisis estratégico, se auditó la Matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas). Resulta imperativo destacar que, en estricto cumplimiento con las recientes resoluciones y enmiendas armonizadas de la ISO sobre el cambio climático, la organización evaluó y documentó explícitamente la pertinencia de los factores derivados del cambio climático, integrándolos como variables formales dentro de su análisis de amenazas y contexto operacional.
4. Contexto de la organización 4.1 Comprensión de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información 4.4 Sistema de gestión de la seguridad de la información 7.1 Recursos	4.2 Comprensión de los requisitos de las partes interesadas La cláusula 27001 de la norma ISO/IEC 2022:4.2 exige que las organizaciones identifiquen, comprendan y monitoreen continuamente las necesidades y expectativas de las partes interesadas —como reguladores, clientes, socios y partes interesadas internas— cuyos requisitos podrían afectar al Sistema de Gestión de Seguridad de la Información (SGSI). Esta participación proactiva garantiza que las obligaciones legales, contractuales y reputacionales, en constante evolución, se registren y reflejen en la planificación y los controles del SGSI. La cláusula 4.2 está diseñada para sistemas vivos, lo que requiere una visión de futuro, no solo registros retrospectivos. Los mejores equipos de SGSI: Monitorear las actualizaciones regulatorias (ICO, NIST, la autoridad de su sector) Aproveche los comentarios de los clientes, las tendencias del mercado e incluso la escucha social. Revisar sistemáticamente las modificaciones de los contratos y las directivas de la junta ejecutiva. La revisión trimestral es su punto de partida, pero el liderazgo implica actuar con mayor rapidez al detectar señales. Las herramientas modernas de SGSI establecen alertas, automatizan el mapeo y señalan cambios inusuales para que no se pierda la próxima gran ola. Muéstrelo en sus registros de auditoría: cambios, quién los generó, cómo se evaluaron, qué medidas tomó. Si improvisa, estará expuesto: la detección y	X			Se constató que la organización ha determinado de manera adecuada las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos del SGSI. La definición general del contexto organizacional se encuentra formalizada, documentada y disponible para las partes interesadas a través de la página web institucional. Como evidencia objetiva del análisis estratégico, se auditó la Matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas). Resulta imperativo destacar que, en estricto cumplimiento con las recientes resoluciones y enmiendas armonizadas de la ISO sobre el cambio climático, la organización evaluó y documentó explícitamente la pertinencia de los factores derivados del cambio climático, integrándolos como variables formales dentro de su análisis de amenazas y contexto operacional.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
4. Contexto de la organización 4.1 Comprensión de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información 4.4 Sistema de gestión de la seguridad de la información 7.1 Recursos	4.3 Determinación del alcance del sistema de gestión de seguridad de la información La cláusula 4.3 de la norma ISO 27001:2022 exige que las organizaciones definan y documenten el alcance de su Sistema de Gestión de la Seguridad de la Información (SGSI) considerando el contexto interno y externo, los requisitos de las partes interesadas y las interfaces/dependencias. Este alcance debe ser claro, estar justificado y alineado con las operaciones reales del negocio, ya que establece los límites para todas las actividades, controles y auditorías del SGSI. Todo CISO, responsable de cumplimiento y CEO se enfrenta a una simple verdad: ni los auditores ni los atacantes se conforman con límites "suficientemente buenos". Si no tiene claro qué cubre realmente su SGSI —no solo los puntos fuertes, sino también los puntos débiles—, está arriesgando su reputación y resiliencia operativa. Los mejores líderes anticipan este escrutinio y lo convierten en una señal de confianza. El alcance de su SGSI debe ser independiente de la terminología y estar basado en la realidad. Detalle qué está protegido, qué no y, crucialmente Por qué se tomó cada decisión En un lenguaje que los	X			El alcance del SGSI se encuentra definido y documentado, tomando en consideración las cuestiones referenciadas en el contexto organizacional (DOFA) y los requisitos de las partes interesadas. Asimismo, mediante la revisión integral de los procesos (gestión de riesgos, operaciones, infraestructura tecnológica y cumplimiento legal), se evidencia que la organización ha establecido, implementado, mantenido y mejorado continuamente un Sistema de Gestión de la Seguridad de la Información robusto (4.4), soportado en herramientas de centralización documental como Daruma y orquestado a nivel técnico a través de sus proveedores tercerizados.
4. Contexto de la organización 4.1 Comprensión de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información 4.4 Sistema de gestión de la seguridad de la información 7.1 Recursos	4.4 Sistema de gestión de la seguridad de la información La cláusula 4.4 de la norma ISO 27001:2022 exige que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de la seguridad de la información (SGSI) plenamente integrado con las operaciones del negocio. Este SGSI debe documentarse sistemáticamente, gestionarse activamente y demostrar su eficacia en todas las funciones, activos y riesgos dentro del alcance definido. Un SGSI conforme no se construye en el vacío. Los mayores fallos ocurren no por la ausencia de controles, sino porque nadie es responsable de los resultados ni impulsa la mejora continua. La cláusula 4.4 señala: Si se busca seguridad y una reputación sólida, la responsabilidad debe ser... everywhere, desde la sala de juntas hasta las sucursales, desde los arquitectos de políticas hasta los ejecutores de procesos. Un SGSI fragmentado es un caldo de cultivo para el riesgo invisible: la complejidad camufla el fracaso hasta que es demasiado tarde. Mapear el territorio. Empiece por definir qué está realmente dentro del alcance: cada oficina, dispositivo, aplicación, proceso, asociación y punto de contacto con el mercado. En cuanto "deja algo fuera", invita a problemas o, al menos, contraria a su auditor. Establecer una rendición de cuentas explícita. Si no está claro quién es dueño de cada riesgo, proceso y control, la auditoría de rutina de hoy se convierte en el simulacro de incendio de mañana. Lo esencial: Un alcance del SGSI claramente definido e inequívoco: cada activo, cada sitio, cada proceso de alto valor. Procesos y procedimientos actuales, meticulosamente documentados:	X			El alcance del SGSI se encuentra definido y documentado, tomando en consideración las cuestiones referenciadas en el contexto organizacional (DOFA) y los requisitos de las partes interesadas. Asimismo, mediante la revisión integral de los procesos (gestión de riesgos, operaciones, infraestructura tecnológica y cumplimiento legal), se evidencia que la organización ha establecido, implementado, mantenido y mejorado continuamente un Sistema de Gestión de la Seguridad de la Información robusto (4.4), soportado en herramientas de centralización documental como Daruma y orquestado a nivel técnico a través de sus proveedores tercerizados.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
4. Contexto de la organización 4.1 Comprensión de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas□ 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información 4.4 Sistema de gestión de la seguridad de la información 7.1 Recursos	7.1 Recursos La cláusula 27001 de la norma ISO 2022:7.1, Recursos, exige que las organizaciones identifiquen, asignen y mantengan los recursos adecuados (que abarcan personal, infraestructura, tecnología y apoyo financiero) necesarios para establecer, implementar, operar y mejorar continuamente el SGSI. Garantiza que el liderazgo proporcione y demuestre los recursos necesarios para que el SGSI se mantenga eficaz y preparado para auditorías. La desatención de recursos no solo sobrecarga su SGSI, sino que lo sabotean silenciosamente. La norma ISO 27001:2022, cláusula 7.1, no se logra con papeleo ni suposiciones; se construye con pruebas diarias y respaldadas por datos de que su personal, presupuesto y sistemas están realmente preparados para el escrutinio y las dificultades. Para muchos, la brecha no es el esfuerzo, sino la omisión de detalles. Puede creer que está listo para una auditoría, pero una sola inconsistencia en la cobertura de recursos o una evidencia de liderazgo poco clara pueden desmantelar todo su sistema de cumplimiento, dañando la confianza desde la junta directiva hasta los líderes. Los auditores actuales esperan evidencia con múltiples capas, mucho más completa que los expedientes de personal o los gráficos de gastos genéricos: Propietarios de SGSI designados con mandatos vigentes: No sólo líderes nominales, sino líderes multifuncionales con tiempo, financiación y apoyo siempre rastreables para una reducción de riesgos mensurable. Compromiso de liderazgo sostenible: La participación práctica de su junta directiva y de los altos ejecutivos (revisiones registradas, aprobaciones,	X			Se constató que la organización determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. Esto se evidencia de manera transversal a lo largo de la auditoría mediante la asignación de plataformas tecnológicas especializadas (Daruma para gestión documental y riesgos; Aranda para mesa de ayuda y cambios; Orfeo; SI CAPITAL), la provisión de infraestructura en la Nube y la inyección de presupuesto para la tercerización de servicios críticos de ciberseguridad, como el SOC, SIEM, SOAR y herramientas de escaneo de vulnerabilidades.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Comunicaciones y Cultura para la Movilidad	**Gestión de TICS-OTIC (Seguridad de la Información)Comunicaciones y Cultura para la Movilidad**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
7.4 Comunicación 7.5 Información Documentada A.5.1 Políticas de seguridad de la información.	7.4 Comunicación La cláusula 27001 de la norma ISO 2022:7.4, Comunicación, exige que Entidad establezca, implemente y documente un proceso de comunicación que garantice qué se comunica, a quién, cuándo y cómo, con evidencia verificable. El objetivo es facilitar una comunicación consistente, adaptada a la audiencia y auditable que respalde la eficacia del SGSI. La cláusula 7.4 significa que debe: Definir con precisión Lo que estás comunicando: desde incidentes hasta políticas internas, desde capacitación hasta estrategia. Decidir que Debes escucharlo, dentro y fuera de tus muros. Especificar cuándo, Con qué frecuencia, y sobre cual canales y respaldarlo todo con registros. Pasar de la extinción de incendios a la resiliencia requiere más que una simple intención: exige una comunicación sistematizada, adaptativa y con enfoque en los roles. Así es como los líderes de cumplimiento de alto rendimiento la estructuran: Comience con el mapeo de mensajes Cada mensaje, detonante y público se mapea. Sin ambigüedades ni confusiones. ¿Está identificando los puntos débiles ocultos (capacitación, infracciones, avisos a proveedores) que rara vez se monitorean? Enlace a roles, no a nombres Deje de depender de la memoria o de las transferencias informales. Automatice la asignación de roles para que la rotación no implique pérdida de información.	X			Se constató la planificación, estructuración y eficacia de las comunicaciones pertinentes al SGSI. La organización ha formalizado sus directrices a través del 'Plan estratégico de comunicaciones y cultura para la movilidad 2026' y el 'Manual de comunicaciones y cultura para la movilidad', documentos que dan cumplimiento integral a los requisitos normativos (qué comunicar, cuándo, a quién, quién comunica y los procesos por los cuales se efectúa). Como canales oficiales y de uso continuo, se evidenció la operatividad del boletín institucional 'Movilidad al día' y un canal corporativo de WhatsApp destinado a la gestión diaria de novedades de los sistemas. En alineación con los objetivos de seguridad, se revisó el PA04-P01-F04-V1 Cronograma de Sensibilización en Seguridad de la Información. Como evidencia objetiva de su ejecución (sampling), se verificó el despliegue de una campaña específica sobre el uso del Doble Factor de Autenticación (2FA), difundida exitosamente el 23 de julio de 2026. Para garantizar que el sistema produce resultados válidos y permite evaluar el nivel de comprensión, se constató que la organización aplica encuestas de conocimiento posteriores a las campañas, midiendo así la eficacia real de las comunicaciones y la apropiación de los temas por parte del personal.
7.4 Comunicación 7.5 Información Documentada A.5.1 Políticas de seguridad de la información.	7.5 Información documentada La Entidad establezca un control estricto sobre la información documentada, garantizando que todos los documentos del SGSI se creen, revisen, aprueben y versionen correctamente, sean accesibles solo al personal autorizado y se conserven o eliminen de acuerdo con las políticas definidas. Esto transforma la documentación, que pasa de ser una simple formalidad a una evidencia operativa de liderazgo, responsabilidad y preparación para auditorías. es el centro neurálgico para cualquier empresa que se proclame líder en seguridad de la información. La junta directiva espera respuestas en segundos. Los reguladores quieren ver pruebas, no promesas. Cuando sus documentos son meticulosos, están versionados y funcionan correctamente en su SGSI, usted lidera. Cuando se pierden, su autoridad se desmorona. Ganarse la confianza de la auditoría comienza en el momento en que trata la documentación como el motor de la defensa de su empresa. La mayoría de los fallos de auditoría no empiezan por deficiencias técnicas. Empiezan con documentos que no se pueden encontrar o, peor aún, que no son fiables. Intentar pasar una auditoría sin estos requisitos es pedir que se suspenda: Declaración del alcance del SGSI: — es su “lo que protegemos” en blanco y negro (Cláusula 4.3) Políticas y objetivos de seguridad: — evidencia de que usted establece las reglas y vive de acuerdo con ellas (cláusulas 5.2, 6.2) Registros de competencias, concientización y capacitación: — a prueba de	X			Se verificó el establecimiento de lineamientos formales para la creación, actualización y control de la información documentada del SGSI, sustentados rigurosamente en el 'PE01-PR04 V20 Procedimiento de Control de Documentos'. Este procedimiento transversal asegura la idoneidad, revisión, aprobación, disponibilidad y control de versiones de toda la documentación normativa y operativa de la entidad (tales como manuales, instructivos y políticas), integrándose de manera coherente con los sistemas centralizados de gestión documental.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
7.4 Comunicación 7.5 Información Documentada A.5.1 Políticas de seguridad de la información.	Anexo A 5.1 Políticas de seguridad de la información. Definir y aprobar las políticas de seguridad a nivel directivo. Este control establece la dirección estratégica de la seguridad de la información, garantizando su alineación con los objetivos empresariales. Asimismo, exige que las políticas se comuniquen a todos los empleados y a las partes externas pertinentes para asegurar el cumplimiento y la concienciación sobre los objetivos de seguridad de la organización. Las políticas son la piedra angular de un sistema de gestión de la seguridad de la información. Aprobadas por la alta dirección, definen el enfoque de la organización para salvaguardar los datos confidenciales. Además, incluyen directrices tanto generales como específicas, lo que garantiza que todos los empleados comprendan sus responsabilidades en el mantenimiento de la confidencialidad, la integridad y la disponibilidad de los datos. Por consiguiente, las revisiones de políticas, la comunicación con las partes interesadas y un proceso formal de gestión del cambio son cruciales para mantener la eficacia de este elemento fundamental del sistema de gestión de la seguridad de la información de la organización. Básicamente, su objetivo es garantizar la idoneidad, la adecuación y la	X			Se evidenció que el conjunto de políticas de seguridad de la información se encuentra alineado con los objetivos del negocio y el entorno de amenazas. Además de su aprobación y publicación formal, se constata que estas políticas son un elemento vivo dentro de la organización, al estar integradas activamente en el Plan Estratégico de Comunicaciones y en el Cronograma de Sensibilización, garantizando su difusión continua y asegurando que las partes interesadas comprendan sus directrices.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Comunicaciones y Cultura para la Movilidad	**Gestión de TICS-OTIC (Seguridad de la Información)Comunicaciones y Cultura para la Movilidad**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.3 Segregación de funciones. A.5.5 Contacto con las autoridades A.5.6 Contacto con grupos de interés especial, A.5.7 Inteligencias de amenazas, A.5.8 Seguridad de la información en la gestión de proyectos A.8.1 Dispositivos de punto final	Anexo A 5.3 Separación de funciones. Separar las responsabilidades contradictorias para prevenir el fraude. Este control mitiga el riesgo de error o mal uso al garantizar que ninguna persona tenga el control total de un proceso crítico. Exige la división de las tareas de ejecución, autorización y verificación para crear un sistema interno de controles y equilibrios. El objetivo del Anexo A 5.3, Separación de Funciones, es reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información. Requisito Identificación de conflictos: Es necesario analizar los procesos de la empresa para determinar dónde una sola persona ejerce demasiado control. Algunas áreas comunes de conflicto incluyen la gestión de cambios, los pagos financieros y la gestión del acceso de los usuarios. Control de acceso basado en roles (RBAC): Implementar RBAC es la forma más práctica de garantizar la segregación. Al definir roles con permisos específicos y no superpuestos, se asegura que "la persona que solicita" sea técnicamente diferente de "la persona que aprueba". Independencia de la auditoría: La persona responsable de un control de seguridad nunca debe ser quien lo audite. Este es un error común entre los gerentes de seguridad de la información que intentan realizar sus propias auditorías internas. Revisiones de acceso periódicas: Debe realizar revisiones periódicas (idealmente mensuales) para asegurarse de que las funciones no hayan cambiado y de que los empleados no hayan acumulado permisos "conflictivos" con el tiempo. Adaptabilidad para pequeñas empresas: Si su equipo es demasiado pequeño para separar físicamente las tareas, debe implementar controles	X			
A.5.3 Segregación de funciones. A.5.5 Contacto con las autoridades A.5.6 Contacto con grupos de interés especial, A.5.7 Inteligencias de amenazas, A.5.8 Seguridad de la información en la gestión de proyectos A.8.1 Dispositivos de punto final	Anexo A 5.6 Contacto con grupos de interés especial Participe en foros seguridad y comunidades profesionales. Este control fomenta la participación en grupos del sector para mantenerse al día sobre las amenazas emergentes y las mejores prácticas. De esta manera, la organización se beneficia de la inteligencia colectiva y las alertas tempranas sobre los riesgos específicos del sector y los avances tecnológicos. El objetivo del Anexo A 5.6 de la norma ISO 27001 es garantizar que se produzca un flujo de información adecuado en lo que respecta a la seguridad de la información. Requisito Identificar grupos relevantes: Debes determinar qué grupos externos son más relevantes para tu conjunto de tecnologías y tu sector. Esto incluye foros de seguridad de proveedores (por ejemplo, blogs de seguridad de Microsoft o AWS), organismos profesionales (por ejemplo, ISACA o ISC2) y grupos específicos del sector (por ejemplo, FS-ISAC para finanzas). Documenta tu participación: Debes mantener un registro de los grupos con los que colaboras y cómo interactúas con ellos. Esto puede abarcar desde suscribirte a un boletín informativo hasta participar activamente en las secciones locales de seguridad. Manténgase al día: El objetivo principal de estos contactos es garantizar que reciba avisos tempranos sobre alertas, notificaciones y actualizaciones. Este flujo de información externo le ayuda a anticipar los riesgos antes de que afecten a su organización. Demuestra tu compromiso: No basta con simplemente marcar una casilla registrándote. Debes poder explicar cómo se utiliza la información que recibes de estos grupos para mejorar tu postura de seguridad (por	X			Se constató la formalización de los canales de comunicación externos para la respuesta ante eventos cibernéticos. La organización cuenta con una 'Matriz de contacto con las autoridades' debidamente integrada en la Guía de Gestión de Incidentes de Seguridad de la Información. Se evidenció un relacionamiento continuo, proactivo y bidireccional con autoridades competentes y grupos de interés especial (foros de seguridad y redes de confianza nacional e internacional), facilitando el intercambio de información sobre posibles eventos y el panorama de amenazas del sistema.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.3 Segregación de funciones. A.5.5 Contacto con las autoridades A.5.6 Contacto con grupos de interés especial, A.5.7 Inteligencias de amenazas, A.5.8 Seguridad de la información en la gestión de proyectos A.8.1 Dispositivos de punto final	Anexo A 5.7 Inteligencia sobre amenazas Recopilar y analizar datos sobre amenazas a la seguridad. Este control exige la recopilación de información sobre vectores y motivaciones de ataque para fundamentar las decisiones de riesgo. Al comprender la evolución del panorama de amenazas, las organizaciones pueden ajustar sus defensas de forma proactiva para mitigar riesgos específicos antes de que sean explotados por los atacantes. s un nuevo control introducido en la actualización de 2022 que exige a las organizaciones recopilar y analizar información sobre las amenazas a la seguridad de la información. El objetivo es pasar de una gestión reactiva de crisis a una defensa proactiva. Al recopilar información sobre quién, cómo y cuándo se producen los ciberataques modernos, las organizaciones pueden implementar medidas de mitigación específicas antes de que se produzca una brecha de seguridad. Este control es esencial para la gestión de riesgos moderna, ya que garantiza que las defensas se basen en datos reales en lugar de suposiciones genéricas. Existen numerosas fuentes de información sobre inteligencia de amenazas, muchas de ellas gratuitas	X			Se validó la capacidad de la organización para recopilar, analizar y aplicar inteligencia de amenazas para proteger su entorno. A través de la revisión operativa del SIEM (FortiSIEM), se auditaron las reglas de correlación implementadas. Se evidenció la recepción sistemática de boletines de seguridad emitidos por el FIRST (Forum of Incident Response and Security Teams), permitiendo la ingesta proactiva de Indicadores de Compromiso (IoCs) como direcciones IP, URLs y hashes maliciosos. Adicionalmente, se constató que el SOC tercerizado analiza esta inteligencia y emite reportes periódicos con recomendaciones accionables para mitigar vulnerabilidades y prevenir ataques.
A.5.3 Segregación de funciones. A.5.5 Contacto con las autoridades A.5.6 Contacto con grupos de interés especial, A.5.7 Inteligencias de amenazas, A.5.8 Seguridad de la información en la gestión de proyectos A.8.1 Dispositivos de punto final	Anexo A 5.8 Seguridad de la información en la gestión de proyectos Inte los riesgos de seguridad en los ciclos de vida de los proyectos. Este control garantiza que la seguridad de la información se aborde desde el inicio de cualquier proyecto, evitando costosas modificaciones posteriores. Exige definir los requisitos de seguridad con anticipación para asegurar que todos los entregables del proyecto sean seguros desde el diseño y estén alineados con los estándares de la organización. El objetivo del Anexo A 5.8 de la norma ISO 27001 es garantizar que los riesgos de seguridad de la información relacionados con los proyectos y los entregables se aborden de manera efectiva en la gestión de proyectos a lo largo de todo el ciclo de vida del proyecto. Requisitos Integración de la metodología: Debe contar con un proceso de gestión de proyectos documentado (Agile, Waterfall, etc.) que incluya hitos de seguridad explícitos. Evaluación temprana de riesgos: Los riesgos de seguridad de la información deben identificarse y tratarse durante la fase inicial. Esto incluye considerar el impacto en la confidencialidad, la integridad y la disponibilidad . Protección de la propiedad intelectual: Los proyectos suelen crear o utilizar propiedad intelectual de alto valor. Es fundamental definir cómo se protege esta propiedad intelectual a lo largo de todo el ciclo de vida del proyecto. Roles de seguridad asignados: Cada proyecto debe tener roles definidos para la seguridad de la información. Esto garantiza la rendición de cuentas respecto a los entregables de seguridad (por ejemplo, pruebas de penetración, configuración de cifrado). Seguimiento del progreso: La eficacia del tratamiento de riesgos debe	X			Se evaluó la integración sistemática de la seguridad de la información dentro del ciclo de vida de la gestión de proyectos. Mediante un ejercicio de trazabilidad sobre la sustentación interna de un proyecto, se evidenció que la organización analiza, define y documenta formalmente la aplicabilidad de los requisitos de seguridad desde las fases iniciales. Este proceso contempla y evalúa transversalmente aspectos legales y contractuales, asegurando la protección de la propiedad intelectual y exigiendo la aplicación de Acuerdos de Confidencialidad (NDA) antes de la ejecución.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.3 Segregación de funciones. A.5.5 Contacto con las autoridades A.5.6 Contacto con grupos de interés especial, A.5.7 Inteligencias de amenazas, A.5.8 Seguridad de la información en la gestión de proyectos A.8.1 Dispositivos de punto final	Anexo A 8.1 Dispositivos de punto final del usuario Proteja los dispositivos utilizados para acceder a la información. Este control establece los requisitos para proteger portátiles, smartphones y tabletas, evitando así el acceso no autorizado. Garantiza que los dispositivos finales estén reforzados, cifrados y supervisados, reduciendo el riesgo de robo de datos o entrada de malware a través de dispositivos de usuario vulnerables. Requisitos básicos para el cumplimiento Inventario completo de activos: No se puede proteger lo que se desconoce. Es imprescindible mantener una lista actualizada de todos los dispositivos proporcionados por la empresa y los dispositivos personales (BYOD) utilizados para el trabajo. La “Trilogía de la Seguridad”: Como mínimo, los auditores esperan ver cifrado de disco completo (BitLocker/FileVault), protección de endpoints (antivirus/EDR) y aplicación de parches gestionada en cada dispositivo. Administración de puntos finales (MDM/UEM): utilice herramientas como Microsoft Intune o Jamf para aplicar medidas de seguridad básicas, como temporizadores de bloqueo automático, complejidad de contraseñas y la capacidad de borrar de forma remota un dispositivo perdido. Capacitación en seguridad física: Los usuarios deben recibir capacitación sobre "etiqueta en espacios públicos", nunca dejar una computadora portátil desatendida y usar pantallas de privacidad para evitar que personas ajenas vean la pantalla en áreas abiertas. Gobernanza de BYOD: Si permite el uso de teléfonos o portátiles personales, debe utilizar la "contenedorización" (como los perfiles de trabajo de Outlook) para mantener los datos de la empresa separados y que se puedan eliminar sin borrar las fotos personales del usuario.	X			Se verificó la implementación de controles técnicos y administrativos rigurosos para proteger la información tratada en dispositivos de punto final (equipos propios y arrendados). Se constató la política de restricción absoluta frente al uso de dispositivos personales (BYOD no permitido) para acceder a la red privada. A nivel técnico, el endurecimiento (hardening) de los equipos incluye el despliegue del agente Cortex XDR para el monitoreo continuo y protección antimalware, así como el bloqueo lógico de puertos USB y conectividad Bluetooth. Se constató la aplicación del principio de mínimo privilegio mediante la asignación de cuentas de usuario básico. Finalmente, la organización demostró capacidad de respuesta ante incidentes (pérdida o robo) mediante la ejecución de comandos de bloqueo y borrado remoto (Wipe). La trazabilidad de instalación y configuración de estos equipos se soporta mediante actas en la plataforma 'Aranda', operando en sinergia con el inventario en 'Daruma'.

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico	**Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.15 Control de acceso, A.5.16 gestión de identidades, A.5.17 Derechos de acceso, A.5.18 Información de autenticación, A.8.2 Derechos de acceso privilegiado, A.8.3 restricción de acceso a la información, A.8.4 acceso al código fuente A.8.5 autenticación segura, A.8.17 Sincronización de relojes, A.8.18 uso de programas de utilidad privilegiados, A.8.24 uso de la criptografía	Anexo A 5.15 Control de acceso. Restringir el acceso según las necesidades del negocio. Este control requiere una política formal para gestionar los derechos de acceso a la información y las instalaciones. Al aplicar el principio del mínimo privilegio, se garantiza que los usuarios solo accedan a los datos necesarios para sus funciones, minimizando así las amenazas internas y la exposición de datos. Anexo A 5.16 Gestión de identidades. Gestiona el ciclo de vida completo de las identidades de usuario. Este control abarca el registro, el aprovisionamiento y la desactivación de los ID de usuario. Garantiza que solo los usuarios válidos y autorizados tengan identidades dentro del sistema y que estas identidades estén vinculadas de forma unívoca a personas específicas para garantizar la rendición de cuentas. Anexo A 5.17 Información de autenticación. Proteja los secretos utilizados para verificar la identidad. Este control rige la gestión de contraseñas, tokens y datos biométricos. Exige una estricta confidencialidad para las credenciales de autenticación y requiere controles del sistema, como la complejidad y la rotación, para prevenir el acceso no autorizado mediante el robo de credenciales. Anexo A 5.18 Derechos de acceso Revise y revoque los permisos de usuario periódicamente. Este control abarca la asignación, modificación y eliminación de derechos de acceso. Garantiza que los permisos se ajusten cuando cambien las funciones y se revoquen inmediatamente al finalizar la relación laboral, evitando así la acumulación de permisos y el acceso no autorizado por parte de exempleados.			X	Se verificó la estructuración e implementación de lineamientos formales para la solicitud, creación, modificación y revocación de usuarios. El ciclo de vida completo de las identidades corporativas es administrado y trazado a través de la plataforma 'Aranda'. Como mecanismo de control y mejora continua, se evidenció la ejecución de auditorías trimestrales sobre los tickets y formatos de acceso. Adicionalmente, se constató la gestión centralizada de identidades mediante la revisión del Directorio Activo de usuarios. En relación con la restricción de acceso a la información (A.8.3), se auditó la matriz de roles y perfiles implementada en los sistemas misionales 'Fénix' y 'Orfeo', evidenciando la aplicación de controles lógicos alineados con las necesidades operativas de la organización. Se verificó la implementación de controles lógicos y administrativos para restringir, gestionar y proteger el acceso al código fuente de la organización. Se evidenció la utilización de las plataformas Azure DevOps y GitLab como repositorios centralizados para el alojamiento, control de versiones y gestión del ciclo de vida del desarrollo de software. A través de estas herramientas, se constató que el acceso a los repositorios se encuentra estrictamente controlado bajo el principio de mínimo privilegio, asignando permisos específicos (lectura, escritura o revisión) de acuerdo con el rol de cada desarrollador. Asimismo, las plataformas garantizan
A.5.15 Control de acceso, A.5.16 gestión de identidades, A.5.17 Derechos de acceso, A.5.18 Información de autenticación, A.8.2 Derechos de acceso privilegiado, A.8.3 restricción de acceso a la información, A.8.4 acceso al código fuente A.8.5 autenticación segura, A.8.17 Sincronización de relojes, A.8.18 uso de programas de utilidad privilegiados, A.8.24 uso de la criptografía	Anexo A 8.2 Derechos de acceso privilegiado. Restrinja el acceso de alto nivel únicamente a usuarios autorizados. Este control exige la asignación y revisión de los derechos de acceso privilegiado según el principio del mínimo privilegio. Al gestionar estrictamente quién puede eludir los controles del sistema, las organizaciones minimizan el impacto de las amenazas internas y las cuentas de administrador comprometidas. Anexo A 8.3 Restricción del acceso a la información. Limite la disponibilidad de datos según las necesidades del negocio. Este control garantiza que el acceso a la información y a las funciones de la aplicación esté restringido de acuerdo con la política de control de acceso establecida. Previene la visualización o manipulación no autorizada de datos confidenciales mediante la aplicación de reglas de acceso granulares alineadas con las responsabilidades laborales específicas. Anexo A 8.4 Acceso al código fuente. Garantizar la propiedad intelectual y la integridad del software. Este control limita estrictamente el acceso de lectura y escritura al código fuente del programa y a los elementos asociados. Previene modificaciones no autorizadas, el robo de algoritmos patentados y la introducción de código malicioso o puertas traseras en los activos de software de la organización. Anexo A 8.5 Autenticación segura. Verifique la identidad del usuario con mecanismos robustos. Este control requiere la implementación de tecnologías de autenticación sólidas, como la autenticación multifactor (MFA), para validar a los usuarios antes de otorgarles acceso. Esto reduce el riesgo de robo de credenciales y garantiza que solo los usuarios legítimos puedan acceder a sistemas y datos críticos.	X			Para proteger el acceso a los recursos tecnológicos y mitigar riesgos de suplantación de identidad, se constató la implementación de mecanismos de autenticación robustos. La organización despliega un Segundo Factor de Autenticación (2FA) soportado en la infraestructura de Azure, exigido para el acceso a los recursos y plataformas de información. Se evidenció que la organización establece restricciones y controles sobre los perfiles de los equipos de cómputo mediante el 'Instructivo de configuración y aislamiento de equipos de cómputo'. Esto garantiza que las configuraciones privilegiadas se encuentren aisladas y estandarizadas, limitando el uso no autorizado de utilidades que puedan alterar los controles del sistema.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.15 Control de acceso, A.5.16 gestión de identidades, A.5.17 Derechos de acceso, A.5.18 Información de autenticación, A.8.2 Derechos de acceso privilegiado, A.8.3 restricción de acceso a la información, A.8.4 acceso al código fuente A.8.5 autenticación segura, A.8.17 Sincronización de relojes, A.8.18 uso de programas de utilidad privilegiados, A.8.24 uso de la criptografía	Anexo A 8.17 Sincronización de relojes. Sincronice los relojes del sistema con una única hora de referencia. Este control garantiza que los relojes de todos los sistemas de procesamiento de información relevantes estén sincronizados con una fuente de tiempo confiable. El registro preciso de la hora es fundamental para el análisis de registros, las investigaciones forenses y el correcto funcionamiento de protocolos de seguridad dependientes del tiempo, como Kerberos. Anexo A 8.18 Uso de programas de utilidad privilegiados. Restringir el uso de potentes herramientas del sistema. Este control limita y supervisa estrictamente el uso de programas de utilidad que pueden eludir los controles del sistema y de las aplicaciones. Al controlar estas herramientas, las organizaciones evitan modificaciones no autorizadas de datos o software y reducen el riesgo de escalada de privilegios. Anexo A 8.24 Uso de la criptografía Cifra los datos para garantizar confidencialidad e integridad. Este control define las reglas para el uso eficaz de la criptografía, incluida la gestión de claves. Garantiza que la información confidencial sea ilegible para terceros no autorizados y protege los datos, tanto en reposo como en tránsito, contra la interceptación y la manipulación.	X			Se verificó la estandarización y precisión de las marcas de tiempo dentro del ecosistema tecnológico, respaldada por el 'Manual de políticas específicas de seguridad de la información PA04-M01-VER-004' y el 'Instructivo de Sincronización de Relojes SMD-SW-I-003'. A través de una revisión técnica (sampling) sobre servidores operativos con sistemas operativos Windows y Linux, se constató la correcta configuración del protocolo NTP (Network Time Protocol). Se evidenció que todos los servidores sincronizan su reloj de manera centralizada tomando la hora exacta del Controlador de Dominio, garantizando así la fiabilidad, validez forense e integridad de los registros de auditoría (logs). Se evaluó la gestión del ciclo de vida de las claves criptográficas y los certificados digitales de la organización. Se evidenció la existencia de un inventario estructurado que controla y alerta sobre el vencimiento de las llaves de encriptación y los certificados, los cuales se encuentran formalmente registrados en el inventario de activos. Se

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)	**Gestión de TICS-OTIC (Seguridad de la Información)**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
Control A.5.37 Procedimientos operativos documentados, Control A.8.6 Gestión de la capacidad, A.8.7 Protección contra malware, A.8.8 Gestión de vulnerabilidades técnicas, A.8.9 Gestión de la configuración, A.8.10 Eliminación de información	Anexo A 5.37 Procedimientos operativos documentados. Estandarizar las operaciones mediante la documentación. Este control requiere la creación de procedimientos detallados para las instalaciones de procesamiento de información. Garantiza la coherencia, reduce el riesgo de errores humanos durante las operaciones y proporciona una referencia fundamental para la capacitación del personal y la resolución eficiente de incidentes. Requisitos básicos para el cumplimiento Procedimientos Operativos Estándar (POE): Debe documentar los "procedimientos" para las tareas críticas (por ejemplo, la baja de usuarios, la gestión de parches y el manejo de errores). Accesibilidad: Los procedimientos deben estar fácilmente disponibles para los miembros del personal específicos que los necesiten; no pueden estar ocultos en una carpeta de políticas genérica. Gestión del cambio: Los documentos deben tratarse como registros vivos. Requieren revisión (al menos anualmente) y deben actualizarse cada vez que cambien los sistemas. Verificación de auditoría: Los auditores comprobarán que estos documentos no solo estén escritos, sino que se utilicen activamente y que sean precisos en relación con el entorno técnico actual. La implementación del Anexo A 5.37 de la norma ISO 27001 garantiza que su organización mantenga operaciones de procesamiento de información consistentes, seguras y confiables. Como auditor líder de ISO 27001, busco evidencia técnica de que los procedimientos no solo estén escritos, sino que se utilicen y rijan activamente. Siga estos diez pasos técnicos para formalizar sus procedimientos operativos documentados y cumplir con los rigurosos requisitos de auditoría.	X			Se verificó la existencia y formalización de los procedimientos operativos necesarios para garantizar el correcto y seguro funcionamiento de las instalaciones de procesamiento de información. Como evidencia objetiva de este control, se constató la implementación y disponibilidad del procedimiento documentado para la ejecución y gestión de copias de seguridad (backup), asegurando que las actividades operativas críticas se realicen de manera estandarizada y repetible.
	Anexo A 8.6 Gestión de la capacidad. Supervise el uso de recursos para prevenir fallos del sistema. Este control garantiza que las instalaciones de procesamiento de información cuenten con la capacidad suficiente para satisfacer las necesidades empresariales actuales y futuras. Al proyectar los requisitos y optimizar los sistemas, las organizaciones evitan interrupciones del servicio causadas por sobrecargas, asegurando así una alta disponibilidad y la continuidad del rendimiento. Anexo A 8.7 Protección contra el malware Implemente mecanismos defensa contra software malicioso. Este control exige la implementación de medidas de detección, prevención y recuperación para protegerse contra el malware. Esto incluye el uso de software antivirus, la sensibilización y el análisis de los archivos entrantes para prevenir infecciones y la consiguiente pérdida o corrupción de los datos de la organización. Anexo A 8.8 Gestión de vulnerabilidades técnicas. Identificar y corregir rápidamente las vulnerabilidades del sistema. Este control requiere obtener información sobre las vulnerabilidades técnicas existentes y evaluar la exposición para aplicar las medidas adecuadas (parches). De esta forma, se cierran de manera proactiva las brechas de seguridad antes de que los atacantes puedan explotarlas, manteniendo así la integridad y la seguridad de la infraestructura de TI. Anexo A 8.9 Gestión de la configuración Estandarice la configuración seguridad en todos los sistemas. Este control garantiza que las configuraciones de hardware, software y redes estén definidas, documentadas y se apliquen correctamente. Al prevenir cambios no autorizados y desviaciones en la configuración, las organizaciones mantienen una postura de seguridad coherente y reducen la superficie de	X			Se verificó la implementación de controles técnicos en diferentes capas de la arquitectura para prevenir, detectar y mitigar la ejecución de código malicioso. A nivel perimetral, la organización opera con soluciones Firewall de Palo Alto, mientras que a nivel de punto final (endpoint), se constató el despliegue activo de la solución de seguridad Cortex, la cual se encarga del filtrado, monitoreo y bloqueo efectivo de malware en los equipos de la infraestructura. Se evaluó el proceso de identificación y tratamiento de vulnerabilidades técnicas. Se evidenció que la organización gestiona adecuadamente las vulnerabilidades detectadas y ejecuta pruebas de penetración (Pen-Testing) periódicas para validar la seguridad de los sistemas de información. Se constató el establecimiento de parámetros seguros y estandarizados para los sistemas tecnológicos. La organización administra una Matriz de Configuración documentada que define las líneas base (baselines) de seguridad. Asimismo, para garantizar la disponibilidad y resiliencia ante incidentes operacionales, se verificó que las configuraciones de los servidores y de los equipos de red son respaldadas continuamente mediante copias de seguridad (backups) almacenadas en la plataforma de Nube Azure. Se verificó la aplicación de controles técnicos y procedimentales para prevenir la fuga de datos confidenciales durante la disposición final de los activos

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC Gestión Administrativa	**Gestión de TICS-OTIC Gestión Administrativa**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.7.1 Perímetros de seguridad física, A.7.2 Entrada física, A.7.3 Asegurar oficinas, habitaciones e instalaciones, A.7.4 Monitoreo de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.7 Escritorio y pantalla limpios, A.7.8 Emplazamiento y protección de equipos, A.7.9 Seguridad de los activos fuera de las instalaciones, A.7.10 Medios de almacenamiento, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.14 Disposición o reutilización segura de los equipos	Anexo A 7.1 Perímetro de seguridad física. Establezca barreras de seguridad para proteger la información confidencial. Este control requiere definir y construir perímetros robustos —como muros, puertas o puntos de acceso controlados con tarjeta— para impedir el acceso físico no autorizado a las instalaciones donde se almacenan datos y activos críticos, creando así la primera línea de defensa contra intrusiones. Anexo A 7.2 controles de acceso físico Restringir el acceso a áreas segu mediante mecanismos de autenticación. Este control exige la implementación de sistemas de acceso, como credenciales, sistemas biométricos o recepciones atendidas, garantizando que solo el personal autorizado pueda ingresar a zonas específicas y manteniendo un registro de los movimientos físicos. Anexo A 7.3 Garantizar la seguridad de oficinas, habitaciones e instalaciones. Refuerce la seguridad de los espacios de trabajo para prevenir el acceso no autorizado y proteger los activos. Este control se centra en la seguridad física de oficinas y salas de servidores, e incluye medidas como puertas con cerradura, protección para ventanas y un diseño estratégico de la distribución para salvaguardar la información contra robos, daños o escuchas ilegales. Anexo A 7.4 Vigilancia de seguridad física Detectar accesos físicos autorizados mediante vigilancia continua. Este control requiere la implementación de sistemas de monitoreo, como cámaras de CCTV, alarmas de intrusión y sensores de movimiento, para proporcionar visibilidad en tiempo real y registros de auditoría de todas las actividades físicas dentro de los perímetros de seguridad.	X			Se verificó la implementación de controles estrictos en los perímetros y accesos a las instalaciones de la organización. Se evidenció la presencia de personal de vigilancia controlando los puntos de entrada físicos, respaldado por procedimientos formales que incluyen: requisa sistemática de maletines, registro detallado de equipos portátiles, verificación de identidad mediante número de cédula y la asignación obligatoria de etiquetas (stickers) de identificación visual para los visitantes.
A.7.1 Perímetros de seguridad física, A.7.2 Entrada física, A.7.3 Asegurar oficinas, habitaciones e instalaciones, A.7.4 Monitoreo de la seguridad física, A.7.5 Protección contra amenazas fisicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.7 Escritorio y pantalla limpios, A.7.8 Emplazamiento y protección de equipos, A.7.9 Seguridad de los activos fuera de las instalaciones, A.7.10 Medios de almacenamiento, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.14 Disposición o reutilización segura de los equipos	Anexo A 7.1 Perímetro de seguridad física. Establezca barreras de seguridad para proteger la información confidencial. Este control requiere definir y construir perímetros robustos —como muros, puertas o puntos de acceso controlados con tarjeta— para impedir el acceso físico no autorizado a las instalaciones donde se almacenan datos y activos críticos, creando así la primera línea de defensa contra intrusiones. Anexo A 7.2 controles de acceso físico Restringir el acceso a áreas segu mediante mecanismos de autenticación. Este control exige la implementación de sistemas de acceso, como credenciales, sistemas biométricos o recepciones atendidas, garantizando que solo el personal autorizado pueda ingresar a zonas específicas y manteniendo un registro de los movimientos físicos. Anexo A 7.3 Garantizar la seguridad de oficinas, habitaciones e instalaciones. Refuerce la seguridad de los espacios de trabajo para prevenir el acceso no autorizado y proteger los activos. Este control se centra en la seguridad física de oficinas y salas de servidores, e incluye medidas como puertas con cerradura, protección para ventanas y un diseño estratégico de la distribución para salvaguardar la información contra robos, daños o escuchas ilegales. Anexo A 7.4 Vigilancia de seguridad física Detectar accesos físicos autorizados mediante vigilancia continua. Este control requiere la implementación de sistemas de monitoreo, como cámaras de CCTV, alarmas de intrusión y sensores de movimiento, para proporcionar visibilidad en tiempo real y registros de auditoría de todas las actividades físicas dentro de los perímetros de seguridad.			X	OB 1 Durante el recorrido por las instalaciones, específicamente en el Centro de Cableado 1 (SDM Piso 2), se observó el almacenamiento inadecuado de materiales de red, equipos tecnológicos antiguos y cajas de cartón en condiciones de desorden. El espacio está siendo utilizado de manera análoga a una bodega. Adicionalmente, se encontraron equipos de cómputo almacenados en este cuarto sin etiquetas de identificación que clarifiquen su estado (si están destinados para baja o reutilización). Recomendación: Se sugiere a la organización adecuar espacios óptimos y exclusivos para el almacenamiento transitorio de hardware, e implementar controles visuales (etiquetado) para los equipos en tránsito, garantizando que los cuartos de telecomunicaciones permanezcan despejados y libres de materiales ajenos a su función principal.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.7.1 Perímetros de seguridad física, A.7.2 Entrada física, A.7.3 Asegurar oficinas, habitaciones e instalaciones, A.7.4 Monitoreo de la seguridad física, A.7.5 Protección contra amenazas fisicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.7 Escritorio y pantalla limpios, A.7.8 Emplazamiento y protección de equipos, A.7.9 Seguridad de los activos fuera de las instalaciones, A.7.10 Medios de almacenamiento, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.14 Disposición o reutilización	Anexo A 7.1 Perímetro de seguridad física. Establezca barreras de seguridad para proteger la información confidencial. Este control requiere definir y construir perímetros robustos —como muros, puertas o puntos de acceso controlados con tarjeta— para impedir el acceso físico no autorizado a las instalaciones donde se almacenan datos y activos críticos, creando así la primera línea de defensa contra intrusiones.□ Anexo A 7.2 controles de acceso físico Restringir el acceso a áreas segu mediante mecanismos de autenticación. Este control exige la implementación de sistemas de acceso, como credenciales, sistemas biométricos o recepciones atendidas, garantizando que solo el personal autorizado pueda ingresar a zonas específicas y manteniendo un registro de los movimientos físicos. Anexo A 7.3 Garantizar la seguridad de oficinas, habitaciones e instalaciones. Refuerce la seguridad de los espacios de trabajo para prevenir el acceso no autorizado y proteger los activos. Este control se centra en la seguridad física de oficinas y salas de servidores, e incluye medidas como puertas con cerradura, protección para ventanas y un diseño estratégico de la distribución para salvaguardar la información contra robos, daños o escuchas ilegales.			X	Se constató la existencia de un procedimiento estructurado para la baja y disposición de equipos tecnológicos, enmarcado en el documento 'PA01-PR12 Procedimiento general de ingresos, egresos y traslados'. El flujo operativo garantiza que los equipos son remitidos al almacén tras la emisión de un diagnóstico técnico. Posteriormente, el equipo técnico documenta sus recomendaciones en un acta, la cual escala a través de la Jefatura de la OTIC hasta obtener la autorización formal de la Subdirectora Administrativa.
A.7.1 Perímetros de seguridad física, A.7.2 Entrada física, A.7.3 Asegurar oficinas, habitaciones e instalaciones, A.7.4 Monitoreo de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.7 Escritorio y pantalla limpios, A.7.8 Emplazamiento y protección de equipos, A.7.9 Seguridad de los activos fuera de las instalaciones, A.7.10 Medios de almacenamiento, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.14 Disposición o reutilización segura de los equipos	Anexo A 7.1 Perímetro de seguridad física. Establezca barreras de seguridad para proteger la información confidencial. Este control requiere definir y construir perímetros robustos —como muros, puertas o puntos de acceso controlados con tarjeta— para impedir el acceso físico no autorizado a las instalaciones donde se almacenan datos y activos críticos, creando así la primera línea de defensa contra intrusiones.□ Anexo A 7.2 controles de acceso físico Restringir el acceso a áreas segu mediante mecanismos de autenticación. Este control exige la implementación de sistemas de acceso, como credenciales, sistemas biométricos o recepciones atendidas, garantizando que solo el personal autorizado pueda ingresar a zonas específicas y manteniendo un registro de los movimientos físicos. Anexo A 7.3 Garantizar la seguridad de oficinas, habitaciones e instalaciones. Refuerce la seguridad de los espacios de trabajo para prevenir el acceso no autorizado y proteger los activos. Este control se centra en la seguridad física de oficinas y salas de servidores, e incluye medidas como puertas con cerradura, protección para ventanas y un diseño estratégico de la distribución para salvaguardar la información contra robos, daños o escuchas ilegales. Anexo A 7.4 Vigilancia de seguridad física Detectar accesos físicos autorizados mediante vigilancia continua. Este control requiere la implementación de sistemas de monitoreo, como cámaras de CCTV, alarmas de intrusión y sensores de movimiento, para proporcionar visibilidad en tiempo real y registros de auditoría de todas las actividades físicas dentro de los perímetros de seguridad.	X			En relación con los servicios de telecomunicaciones que soportan las operaciones de la entidad, se evidenció que la solución de telefonía IP se encuentra completamente externalizada y gestionada a través de la infraestructura en la Nube del proveedor ETB, garantizando así la disponibilidad y continuidad del servicio fuera de las instalaciones físicas locales. Tambien se cuenta con generadores eléctricos y UPS que garantizan la continuidad del flujo eléctrico ante interrupcion del proveedor.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
			X		NC 1 - Incumplimiento de controles A.7.12 Seguridad del cableado y A.7.11 Servicios públicos de apoyo Declaración del Hallazgo: Se evidencia una deficiencia sistemática en la protección física del cableado de telecomunicaciones y en las instalaciones eléctricas, exponiendo a la organización a riesgos de intercepción de datos, pérdida de disponibilidad por daños accidentales y riesgos eléctricos para el personal. Evidencia Objetiva: En la Sala de Juntas Jiménez, se observan cables de red desprovistos de canalización adecuada, colgados y sujetos de manera improvisada con abrazaderas plásticas. Existen múltiples puntos eléctricos y de red sin las tapas de protección (faceplates) correspondientes. En el Cuarto de Control, se identificó cableado por fuera de la línea de protección (canaleta/tubería), presencia de cables cortados con aislamiento en cinta, empalmes de cable UTP realizados con soldadura (práctica no estandarizada que degrada la señal) y cables UTP con el blindaje físico comprometido. En los Puestos de Trabajo QT80, JM63 y JM59, se evidenció la conexión de equipos mediante extensiones y adaptadores tipo 'T' colocados sobre la superficie de trabajo, práctica que

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico	**Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.8.11 Enmascaramiento de datos, A.8.12 Prevención de fugas de datos, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.16 Actividades de seguimiento, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos.Control A.5.14 Transferencia de información, A.8.20 Seguridad de redes, A.8.21 Seguridad de los servicios de red, A.8.22 Segregación de redes, A.8.23 Filtrado web	8.15 Registro Enfoque de auditoría La prueba del "administrador": "¿Cómo se asegura de que su gerente de TI no pueda eliminar el registro de auditoría de sus propias acciones?" Prueba forense: “Muéstrame los registros de un día específico de hace tres meses. ¿Siguen siendo accesibles y precisos?” Revisión práctica: “Muéstrenme pruebas de que alguien realmente revisa estos registros. ¿Dónde está el informe mensual de revisión de registros?” A.8.16 Actividades de seguimiento. Enfoque de auditoría El detonante: "Muéstrame la alerta que se activó durante tu última prueba de seguridad". La respuesta: “¿Quién investigó esa alerta? ¿Cuál fue el resultado?” El equilibrio: Comprueban que no estés registrando todo (lo que provoca fatiga por exceso de alertas), sino que te centres en los desencadenantes de alto riesgo. A.8.17 Sincronización de reloj, Enfoque de auditoría Verificación de configuración: Le pedirán que muestre la configuración NTP en un servidor aleatorio. La prueba: “Demuéstrame que la hora de tu servidor coincide con la hora actual de tu región”. La Cadena: Si operas a nivel global, ¿cómo gestionas las zonas horarias? (Normalmente, los sistemas deben configurarse en UTC para mantener una base de referencia universal). A.8.19 Instalación de software en sistemas operativos.	X			Se verificó la implementación de técnicas criptográficas y de ofuscamiento para proteger la información de identificación personal y datos sensibles. Mediante la revisión del documento técnico aplicable, se constató que la organización ejecuta procedimientos de enmascaramiento de datos (nombres, direcciones, teléfonos, correos, entre otros) al momento de replicar o migrar bases de datos productivas hacia entornos de pruebas, garantizando la confidencialidad de la información. Se constató el despliegue de controles técnicos orientados a la Prevención de Fuga de Datos (DLP). Se evidenció la configuración de reglas específicas en el servicio de correo electrónico y restricciones lógicas que impiden compartir carpetas de la plataforma 'Drive' con dominios u organizaciones externas. Se verificó que las excepciones (ej. compartición con la Contraloría) son gestionadas temporalmente bajo autorización. Adicionalmente, se evidenció que el proveedor Xertica ejecuta un monitoreo activo de la red, encargado de alertar ante posibles eventos de exfiltración de información.
A.8.11 Enmascaramiento de datos, A.8.12 Prevención de fugas de datos, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.16 Actividades de seguimiento, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos.Control A.5.14 Transferencia de información, A.8.20 Seguridad de redes, A.8.21 Seguridad de los servicios de red, A.8.22 Segregación de redes, A.8.23 Filtrado web	Anexo A 5.14 Transferencia de información. Protección de datos en tránsito. Este control establece políticas formales para la transferencia de información a terceros. Previene la interceptación, copia o modificación al exigir el uso de cifrado, protocolos seguros y acuerdos estrictos siempre que los datos confidenciales salgan del perímetro de seguridad de la organización. El objetivo del Anexo A 5.14 de la norma ISO 27001 es garantizar que se mantenga la seguridad de la información en la transfrencia dentro de la Entidad y con cualquier parte interesada externa. Requisito - Reglas para 3 métodos de transferencia: Debe abordar tres modos de transferencia específicos: 1. Medios electrónicos: correo electrónico, SFTP, uso compartido en la nube y aplicaciones de mensajería. 2. Formato físico: Documentos en papel, unidades USB y soportes de almacenamiento extraíbles. 3. Voz: Llamadas telefónicas, videoconferencias y conversaciones presenciales. - Protección proporcional: Los controles deben coincidir con la clasificación de los datos (según el Anexo A 5.12). Por ejemplo, los datos “públicos” pueden enviarse por correo electrónico estándar, pero los datos “confidenciales” requieren cifrado y enlaces de acceso restringido. - Trazabilidad y no repudio: Para transferencias confidenciales, debe poder demostrar quién envió la información, quién la recibió y que no fue modificada durante el tránsito. Esto suele requerir registros y comprobantes de entrega. - Prevención de malware: Los sistemas de transferencia electrónica deben	X			Se evidenció el establecimiento de reglas formales para el intercambio seguro de datos con terceros. La organización dispone de un formato modelo estandarizado para los acuerdos de transferencia de información. Se constató que los requisitos técnicos de integración y seguridad quedan debidamente definidos en los anexos técnicos de dichos acuerdos.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.8.11 Enmascaramiento de datos, A.8.12 Prevención de fugas de datos, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.16 Actividades de seguimiento, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos.Control A.5.14 Transferencia de información, A.8.20 Seguridad de redes, A.8.21 Seguridad de los servicios de red, A.8.22 Segregación de redes, A.8.23 Filtrado web	8.15 Registro Enfoque de auditoría La prueba del "administrador": "¿Cómo se asegura de que su gerente de TI no pueda eliminar el registro de auditoría de sus propias acciones?" Prueba forense: “Muéstrame los registros de un día específico de hace tres meses. ¿Siguen siendo accesibles y precisos?” Revisión práctica: “Muéstrenme pruebas de que alguien realmente revisa estos registros. ¿Dónde está el informe mensual de revisión de registros?” A.8.16 Actividades de seguimiento. Enfoque de auditoría El detonante: "Muéstrame la alerta que se activó durante tu última prueba de seguridad". La respuesta: “¿Quién investigó esa alerta? ¿Cuál fue el resultado?” El equilibrio: Comprueban que no estés registrando todo (lo que provoca fatiga por exceso de alertas), sino que te centres en los desencadenantes de alto riesgo. A.8.17 Sincronización de reloj, Enfoque de auditoría Verificación de configuración: Le pedirán que muestre la configuración NTP en un servidor aleatorio. La prueba: “Demuéstrame que la hora de tu servidor coincide con la hora actual de tu región”. La Cadena: Si operas a nivel global, ¿cómo gestionas las zonas horarias? (Normalmente, los sistemas deben configurarse en UTC para mantener una base de referencia universal). A.8.19 Instalación de software en sistemas operativos.	X			Se evidenció una gestión madura, probada y documentada de las copias de seguridad, sustentada en el documento 'SDM-M-T03 Manual de respaldo y restauración de información', el cual define tipos de backup, ventanas de tiempo, retenciones y alcance. La administración de políticas se ejecuta a través de la herramienta Veritas NetBackup. Para validar la eficacia del control (capacidad de recuperación), se auditaron los informes de restauración de mayo, junio y julio. De manera objetiva, se evidenciaron pruebas de restauración exitosas de bases de datos desde almacenamiento en cinta, trazadas mediante los tickets de Aranda 724032 y 708737. Se verificó la existencia de controles estrictos sobre la instalación de software en los sistemas de la organización. Cualquier requerimiento de software adicional debe ser escalado por el jefe del área (incluyendo la justificación y/o contrato) y someterse a un flujo de aprobación formal para validar su licenciamiento y compatibilidad con las políticas de seguridad de la SDM.
Pruebas. A.8.11 Enmascaramiento de datos, A.8.12 Prevención de fugas de datos, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.16 Actividades de seguimiento, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos.Control A.5.14 Transferencia de información, A.8.20 Seguridad de redes, A.8.21 Seguridad de los servicios de red, A.8.22 Segregación de redes, A.8.23 Filtrado web	8.11 Enmascaramiento Enfoque de auditoría Las pantallas: “Muéstrame la vista que tiene un usuario estándar de la base de datos de clientes. ¿Están ocultos los campos confidenciales, como los números de la Seguridad Social?” Entornos de desarrollo/prueba: "¿Cómo se garantiza que los desarrolladores no vean nombres reales de clientes mientras depuran el código?" La reversibilidad: “Si se utiliza la seudonimización, ¿cómo se protege la 'clave' para desbloquear los datos reales?” 8.12 Prevención de fugas Enfoque de auditoría Datos en reposo: ¿Cómo protege los archivos que se encuentran en discos duros o en repositorios en la nube? (por ejemplo, mediante cifrado). Datos en tránsito: ¿Cómo protege los datos mientras se transmiten? (por ejemplo, mediante filtrado de correo electrónico o TLS). Datos en uso: ¿Cómo se evita que los datos se "filtren" mientras alguien trabaja con ellos? (por ejemplo, restricciones de portapapeles/copiar y pegar). 8.13 Copias de seguridad Enfoque de auditoría El cronograma: “Muéstrame tu política de copias de seguridad. ¿Especifica con qué frecuencia realizas copias de seguridad de los datos críticos frente a los no críticos?” El RTO/RPO: "¿Cuál es su objetivo de pérdida de datos (RPO)? Demuestre que su frecuencia de copias de seguridad permite alcanzar ese objetivo."	X			Para software adicionales el jefe de área debe enviar solicitud de instalación incluyendo contrato y suple un proceso de aprobación para verificar si es compatible con las políticas de la SDM.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
Pruebas. A.8.11 Enmascaramiento de datos, A.8.12 Prevención de fugas de datos, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.16 Actividades de seguimiento, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos.Control A.5.14 Transferencia de información, A.8.20 Seguridad de redes, A.8.21 Seguridad de los servicios de red, A.8.22 Segregación de redes, A.8.23 Filtrado web	8.15 Registro Enfoque de auditoría La prueba del "administrador": "¿Cómo se asegura de que su gerente de TI no pueda eliminar el registro de auditoría de sus propias acciones?" Prueba forense: “Muéstrame los registros de un día específico de hace tres meses. ¿Siguen siendo accesibles y precisos?” Revisión práctica: “Muéstrenme pruebas de que alguien realmente revisa estos registros. ¿Dónde está el informe mensual de revisión de registros?” A.8.16 Actividades de seguimiento. Enfoque de auditoría El detonante: "Muéstrame la alerta que se activó durante tu última prueba de seguridad". La respuesta: “¿Quién investigó esa alerta? ¿Cuál fue el resultado?” El equilibrio: Comprueban que no estés registrando todo (lo que provoca fatiga por exceso de alertas), sino que te centres en los desencadenantes de alto riesgo. A.8.17 Sincronización de reloj, Enfoque de auditoría Verificación de configuración: Le pedirán que muestre la configuración NTP en un servidor aleatorio. La prueba: “Demuéstrame que la hora de tu servidor coincide con la hora actual de tu región”. La Cadena: Si operas a nivel global, ¿cómo gestionas las zonas horarias? (Normalmente, los sistemas deben configurarse en UTC para mantener una base de referencia universal). A.8.19 Instalación de software en sistemas operativos.	X			Se verificó la generación y protección de los registros de auditoría (logs). A nivel de bases de datos (Oracle), se constató la activación de registros sobre cambios estructurales, así como auditoría sobre operaciones DML en tablas críticas (eventos Update y Delete). La organización ha definido y cumple con periodos de retención escalonados para la información de auditoría, resguardando los registros por rangos de 60, 90 y hasta 180 días. El monitoreo continuo de la infraestructura y el comportamiento de la red se ejecuta mediante la plataforma NagiosXI, la cual supervisa un inventario de 352 máquinas, analizando tráfico, capacidades y latencia. Se evidenció una correcta articulación entre el monitoreo y la gestión de incidentes/capacidad; al detectar dos (2) equipos en estado Offline en la consola, se validó la trazabilidad de la respuesta operativa, la cual se encuentra en gestión de repuestos (contactores) bajo el caso RFns7289.
Pruebas. A.8.11 Enmascaramiento de datos, A.8.12 Prevención de fugas de datos, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.16 Actividades de seguimiento, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos.Control A.5.14 Transferencia de información, A.8.20 Seguridad de redes, A.8.21 Seguridad de los servicios de red, A.8.22 Segregación de redes, A.8.23 Filtrado web	A.8.20 Seguridad de redes, Enfoque de auditoría Visibilidad: “Muéstrame tu diagrama de red. ¿Refleja con precisión lo que está conectado actualmente?” Control de configuración: “Muéstrame los registros de la última vez que se modificó una regla del firewall. ¿Quién lo autorizó?” Autenticación: "¿Cómo gestiona el acceso administrativo a sus conmutadores? ¿Sigue utilizando la contraseña 'admin' predeterminada de fábrica?" A.8.21 Seguridad de los servicios de red, Enfoque de auditoría El contrato: “Muéstrame las cláusulas de seguridad de tu contrato con el proveedor de servicios de Internet (ISP) o el proveedor de servicios gestionados (MSP)”. Prueba de disponibilidad: “Muéstrame el informe que demuestre que tu proveedor de red cumplió con su objetivo de disponibilidad del 99,9% el mes pasado”. Garantía de terceros: "¿Cómo sabe que su proveedor es seguro? Muéstreme su certificado ISO 27001 más reciente o el resumen de su auditoría." A.8.22 Segregación de redes, Enfoque de auditoría Los límites: “Muéstrame dónde termina la red de invitados y dónde comienza la red corporativa”. Los Gateways: “Muéstrame el cortafuegos que se encuentra entre estas dos zonas”. La evidencia: Es posible que te pidan que intentes hacer "ping" a un			X	Se auditó la arquitectura lógica y física de las comunicaciones, evidenciando una organización estructurada en la distribución de las topologías de red (se revisó específicamente la topología de la Sede Calle 13). La organización aplica principios de segregación para proteger los servicios críticos, lo cual se evidenció a través de la configuración y aislamiento de la red de invitados, ajustada con políticas de seguridad restrictivas. OB: Durante el recorrido y revisión de puestos de trabajo, se evidenció que el equipo de cómputo asignado al contratista externo (Ing. Ubolmester) se encuentra operando con el sistema operativo Windows sin activación (licencia inactiva). Recomendación: Se sugiere fortalecer los controles de validación en la mesa de servicios durante el aprovisionamiento o conexión de equipos pertenecientes a contratistas, garantizando el cumplimiento de requisitos de licenciamiento y mitigando riesgos asociados a la falta de actualizaciones de seguridad en sistemas operativos no legítimos o inactivos. Relacionada con A.5.22 (Seguridad de los proveedores) y A.8.19 (Instalación de software / Licenciamiento)

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico	**Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento de información.	Anexo A 8.25 Ciclo de vida de desarrollo seguro. Integre la seguridad en cada fase del desarrollo de software. Este control exige que las normas de seguridad de la información se apliquen a lo largo de todo el ciclo de vida del desarrollo de software (SDLC). Garantiza que la seguridad se diseñe desde el principio, en lugar de añadirse posteriormente, reduciendo así las vulnerabilidades en el producto final. Anexo A 8.26 Requisitos de seguridad de la aplicación. Defina las necesidades de seguridad antes de desarrollar o adquirir software. Este control exige identificar, especificar y aprobar los requisitos de seguridad de la información al desarrollar o adquirir aplicaciones. Garantiza que el software cumpla con los estándares de seguridad de la organización en cuanto a autenticación, validación de entrada y protección de transacciones. Anexo A 8.27 Principios de arquitectura e ingeniería de sistemas seguros. Construya sistemas sobre una base segura. Este control establece principios para el diseño de sistemas seguros y los aplica a todas las actividades de desarrollo de sistemas de información. Garantiza un enfoque coherente en materia de defensa en profundidad, privilegios mínimos y gestión de fallos en toda la infraestructura tecnológica de la organización. Anexo A 8.28 Codificación segura. Código resistente a ataques. Este control exige la aplicación de principios de codificación segura al desarrollo de software. Su objetivo es prevenir vulnerabilidades comunes como la inyección SQL y el cross-site scripting (XSS), garantizando que los desarrolladores sigan las mejores prácticas y validen las entradas durante el proceso de codificación. Anexo A 8.29 Pruebas de seguridad en el desarrollo y la aceptación. Validar los controles de seguridad antes del despliegue. Este control requiere definir e implementar procesos de pruebas de seguridad dentro del ciclo de vida del desarrollo. Incluye pruebas de estrés, pruebas de penetración y revisión de código para verificar que los nuevos sistemas o cambios no introduzcan vulnerabilidades de seguridad en el entorno de producción.	X			Se verificó la adopción y formalización de metodologías para el desarrollo de software seguro. La organización cuenta con un 'Manual de Arquitectura de Desarrollo Seguro para la Secretaría Distrital de Movilidad' y lineamientos de código seguro que actúan como documentos rectores. Se evidenció un diagrama de flujo estructurado del ciclo de vida del desarrollo. Como estándar de seguridad en las aplicaciones (A.8.26), la entidad ha adoptado rigurosamente la metodología OWASP Top 10, garantizando que la codificación prevenga las vulnerabilidades más críticas del mercado. Se constató la segregación lógica y operativa de los entornos de software. El control de versiones se administra a través de GitLab, implementando una arquitectura de ramas (branching): se utiliza una rama exclusiva de 'Desarrollo' para ajustes de funcionalidad, la cual, tras ser probada, se transfiere al entorno de 'QA' para pruebas funcionales, manteniendo la rama 'Main' estrictamente para producción. La validación de seguridad está automatizada e integrada en el ciclo (DevSecOps) a través de Azure DevOps, herramienta que ejecuta pruebas de seguridad dinámicas y estáticas, estableciendo una barrera técnica (gate) que impide realizar despliegues hacia producción si no se han mitigado todas las vulnerabilidades detectadas.
A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento de información.	Anexo A 8.30 Desarrollo externo. Supervisar la creación de software de terceros. Este control garantiza que la organización dirija, supervise y revise las actividades relacionadas con el desarrollo de sistemas subcontratados. Asimismo, garantiza que los proveedores externos cumplan con los mismos estándares de seguridad y prácticas de codificación que los equipos internos, previniendo así vulnerabilidades en la cadena de suministro. Anexo A 8.31 Separación de los entornos de desarrollo, prueba y producción. Aísle los entornos para evitar cambios accidentales. Este control requiere la separación de los entornos de desarrollo, pruebas y producción. Impide que el código no probado dañe los sistemas en producción y garantiza que los datos reales no se utilicen de forma insegura en los entornos de pruebas, manteniendo así la estabilidad del sistema y la confidencialidad de los datos. Anexo A 8.33 Información de la prueba. Proteja los datos operativos durante las pruebas. Este control requiere la selección, protección y gestión cuidadosas de la información de prueba. Generalmente, prohíbe el uso de información personal identificable (PII) o datos operativos confidenciales para las pruebas, a menos que se hayan anonimizado o enmascarado adecuadamente, garantizando así que las actividades de prueba no provoquen filtraciones de datos. Anexo A 8.34 Protección de los sistemas de información durante las pruebas d auditoría. Minimizar las interrupciones durante las auditorías de seguridad. Este contr garantiza que las pruebas de auditoría y otras actividades de aseguramiento se planifiquen y acuerden para minimizar el impacto en las operaciones comerciales. Evita que las auditorías provoquen accidentalmente tiempos de inactividad o comprometan la disponibilidad e integridad de los sistemas que se están probando.	X			Se evaluó el control sobre el desarrollo de software ejecutado por terceros. Se evidenció un contrato (vigente desde diciembre) cuyo anexo técnico establece y pacta explícitamente los requisitos de seguridad para la recepción de los productos finales. Durante el ciclo de liberación, se constató que los planes de pruebas reposan de forma centralizada en la Wiki del proyecto. Para la aceptación final del código, el proveedor tecnológico debe diligenciar un checklist de requisitos y tramitar un ticket RFC (Request for Change). Se evidenció que el formato de aceptación integra la completitud de las pruebas, y en el RFC quedan debidamente registradas y trazadas las pruebas de seguridad ejecutadas antes de autorizar el paso a producción. Como complemento a la gestión de vulnerabilidades técnicas y pruebas de validación, se constató en el alcance contractual con el proveedor la inclusión formal de tres (3) ejercicios de Ethical Hacking y tres (3) ejercicios de Pen-Testing (incluyendo modalidades de Caja Negra y pruebas internas). Se evidenció la programación de pruebas de intrusión orientadas tanto al acceso físico como lógico, demostrando un enfoque ofensivo proactivo.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento de información.	Anexo A 5.29 Seguridad de la información durante las interrupciones. Mantenga los controles de seguridad durante desastres. Este control garantiza que las medidas de seguridad de la información sigan funcionando o se sustituyan por controles equivalentes durante una crisis. Previene las brechas de seguridad mientras la organización opera en modo de emergencia o mientras los planes de continuidad del negocio están activos. El objetivo de la cláusula 5.29 de la norma ISO 27001 es proteger la información y otros activos asociados durante una interrupción. Requisito Integración de la seguridad en BCP/DR: Debe incluir explícitamente los requisitos de seguridad de la información en sus planes de continuidad del negocio (BCP) y procedimientos de recuperación ante desastres (DR) . Mantenimiento de los controles: Debe procurar mantener el mismo nivel de seguridad durante una interrupción que en las operaciones normales. Si falla un control principal (por ejemplo, SSO), debe estar listo un control de respaldo previamente aprobado. Continuidad de la confidencialidad e integridad: Si bien el enfoque de la BCP suele estar en la disponibilidad , este control exige que la confidencialidad y la integridad no se sacrifiquen para que los sistemas vuelvan a estar en línea. Pruebas y validación: No basta con tener un plan; hay que ponerlo a prueba. Los simulacros de continuidad del negocio deben incluir un paso para verificar que los controles de seguridad funcionan correctamente en el entorno de respaldo. Lecciones aprendidas: Después de cualquier interrupción o prueba, debe realizar una revisión para identificar dónde se vio comprometida la seguridad y actualizar sus planes en consecuencia (Anexo A 5.27). Enfoque de auditoría Coherencia del plan: “Muéstrame tu plan de continuidad del negocio. ¿Dónde se describen los controles de seguridad que permanecen activos durante una conmutación por error?”	X			La organización demuestra un nivel de resiliencia excepcional, respaldado por la Certificación en la norma ISO 22301 (Sistema de Gestión de Continuidad de Negocio). Se verificó la alineación del Plan de Recuperación Tecnológica (DRP) con el Análisis de Impacto al Negocio (BIA). La entidad ha identificado claramente sus procesos críticos, determinando métricas de recuperación exigentes para su aplicativo misional 'ORFEO', con un RPO (Punto de Recuperación) inmediato y un RTO (Tiempo de Recuperación) de 2 horas. Se evidenció un plan estructurado para cada actividad de los procesos críticos. Como prueba de eficacia y viabilidad de los planes de contingencia (operación en modo degradado), se auditaron las pruebas de envío manual de documentos de ORFEO, las cuales se ejecutaron exitosamente bajo distintas circunstancias en coordinación con el proveedor de correspondencia '4-72'. Como respuesta al análisis de riesgos sobre la disponibilidad del Datacenter físico, la organización se encuentra ejecutando su plan de tratamiento mediante la migración y despliegue del DRP hacia la Nube de Azure, empleando la herramienta Azure Migrate. Plan de Acción en Curso: En paralelo a la estrategia de Nube, se evidenció que la entidad está gestionando activamente la adquisición de un nuevo canal de fibra óptica, lo cual garantizará la redundancia en telecomunicaciones requerida
Pruebas A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento	8.25 Desarrollo seguro Requisito Defina las reglas: Debe contar con una política escrita (o "reglas de uso") para el desarrollo. Esto establece el estándar sobre cómo se escribe, prueba y aprueba el código. Puntos de control de seguridad: No basta con comprobar la seguridad al final. Se necesitan "puertas" en etapas clave (diseño, codificación, pruebas) donde el proyecto no pueda avanzar hasta que se cumplan los requisitos de seguridad. Separación de entornos: Debe establecerse una estricta separación entre los entornos de desarrollo, pruebas y producción. Por lo general, los desarrolladores no deben tener acceso de escritura al entorno de producción en vivo. Control de versiones: Debes gestionar tu código en un repositorio seguro (como GitHub o GitLab) con estrictos controles de acceso, garantizando que no se introduzcan cambios no autorizados. Enfoque de auditoría La política: “Muéstrame tu política de desarrollo seguro”. Los puntos de control: “Muéstrame el plan del proyecto para tu última función. ¿Dónde revisaste los riesgos de seguridad?” La Separación: “Muéstrame que un desarrollador no puede modificar directamente el código del sitio web en producción”. 8.26 Seguridad aplicaciones Requisito El enfoque de la "lista de la compra": Antes de escribir una línea de código o firmar un contrato, debe crear una lista de características de seguridad no negociables (por ejemplo, "Debe admitir la autenticación multifactor", "Debe cifrar los datos en reposo", "Debe tener registros de auditoría"). Comprar vs. Construir: Este control se aplica a ambos . Desarrollo: Los desarrolladores necesitan requisitos de seguridad en sus tickets/historias de usuario (por ejemplo, "Como usuario, mi contraseña debe estar cifrada con sal y hash").	X			

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
Pruebas A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento	8.30 Desarrollo externo Requisito Seguridad contractual: El contrato debe indicar explícitamente sus expectativas de seguridad (por ejemplo, "Debe seguir las directrices OWASP Top 10", "No debe utilizar bibliotecas GPL", "Debe cifrar todos los datos"). Supervisión y monitoreo: Es necesario contar con un proceso para verificar su trabajo durante el proyecto, no solo al final. Esto podría incluir revisiones periódicas del código o la presentación de informes de análisis de vulnerabilidades con cada hito. Pruebas/Aceptación: Debe probar usted mismo el código subcontratado (o contratar a un tercero para que lo haga) antes de su lanzamiento. Nunca implemente sin antes verificar el código enviado por un proveedor. Propiedad intelectual y licencias: Aclare quién es el propietario del código y asegúrese de que el proveedor no utilice componentes de código abierto pirateados o restrictivos que puedan poner en peligro legalmente su producto. Enfoque de auditoría El contrato: Comprobarán si su “Acuerdo de servicios” incluye un calendario o cláusula de seguridad. La evidencia: Le pedirán el informe de la prueba de penetración o el análisis de código que realizó en el producto del proveedor antes de pagar la factura final. La cadena de suministro: Comprobarán si usted realizó la "debida diligencia" (por ejemplo, un cuestionario) antes de contratar al estudio de desarrollo. 8.31 Separacion de entornos desarrollo, calidad-prueba, producción Requisito La regla de la "calle de sentido único": El código debe fluir en una sola dirección: Desarrollo a Pruebas a Producción. Nunca se deben aplicar correcciones urgentes directamente en el servidor de producción. Separación de funciones: idealmente, la persona que escribe el código no debería ser la misma que lo implementa en producción. Esto evita que código malicioso (o errores	X			
A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento de información.	Anexo A 5.29 Seguridad de la información durante las interrupciones. Mantenga los controles de seguridad durante desastres. Este control garantiza que las medidas de seguridad de la información sigan funcionando o se sustituyan por controles equivalentes durante una crisis. Previene las brechas de seguridad mientras la organización opera en modo de emergencia o mientras los planes de continuidad del negocio están activos. El objetivo de la cláusula 5.29 de la norma ISO 27001 es proteger la información y otros activos asociados durante una interrupción. Requisito Integración de la seguridad en BCP/DR: Debe incluir explícitamente los requisitos de seguridad de la información en sus planes de continuidad del negocio (BCP) y procedimientos de recuperación ante desastres (DR) . Mantenimiento de los controles: Debe procurar mantener el mismo nivel de seguridad durante una interrupción que en las operaciones normales. Si falla un control principal (por ejemplo, SSO), debe estar listo un control de respaldo previamente aprobado. Continuidad de la confidencialidad e integridad: Si bien el enfoque de la BCP suele estar en la disponibilidad , este control exige que la confidencialidad y la integridad no se sacrifiquen para que los sistemas vuelvan a estar en línea. Pruebas y validación: No basta con tener un plan; hay que ponerlo a prueba. Los simulacros de continuidad del negocio deben incluir un paso para verificar que los controles de seguridad funcionan correctamente en el entorno de respaldo. Lecciones aprendidas: Después de cualquier interrupción o prueba, debe realizar una revisión para identificar dónde se vio comprometida la seguridad y actualizar sus planes en consecuencia (Anexo A 5.27). Enfoque de auditoría Coherencia del plan: “Muéstrame tu plan de continuidad del negocio. ¿Dónde se describen los controles de seguridad que permanecen activos durante una conmutación por error?”	X			Se esta trabajando en la aplicación del DRP, ORFEO es la aplicación principal que se montara en el DRP. Se logro la migración de los servicios a azure. Usando la herramienta azure migrate para llevar la infraestructura BIAS. Dentro del plan de recuperación tecnológica están los BIA para identificar los procesos críticos y los procesos que tienen ciertas actividades criticas, los RTO y RPO. Los RPO de orfeo es inmediato y el RTO es de 2h. Debido al análisis de riesgos sobre la disponibilidad de los servicios de Datacenter se está trabajando en establecer el DRP en la nube. Actualmente se esta trabajando en adquirir un nuevo canal de fibra para poder tener la redundancia necesaria para atender la interrupción. Se hicieron pruebas de envío manual de documentos de ORFEO con el proveedor de correspondencia 472 en distintas circunstancias. Se tiene un plan para cada actividad de los procesos críticos.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio, A.8.14 redundancia de las instalaciones de procesamiento de información.	Anexo A 5.30 Preparación de las TIC para la continuidad del negocio. Asegurar que lo sistemas de TI respalden los objetivos de recuperación. Este control requiere que los sistemas de TIC tengan la resiliencia suficiente para respaldar los objetivos de continuidad del negocio. Garantiza que los sistemas redundantes, las copias de seguridad y los mecanismos de conmutación por error se prueben y estén disponibles para cumplir con los objetivos definidos de tiempo de recuperación (RTO) y punto de recuperación (RPO). El objetivo del Anexo A 5.30 de la norma ISO 27001, Preparación de las TIC para la continuidad del negocio, es garantizar la disponibilidad de la información de la organización y otros activos asociados durante una interrupción. Requisito Evaluación del impacto en el negocio (EIM): No se puede planificar la recuperación si no se sabe qué es importante. Es necesario realizar una EIM para identificar qué sistemas son críticos (por ejemplo, «El correo electrónico es la prioridad 1, las redes sociales son la prioridad 3»). Objetivos definidos (RTO y RPO): Debe definir objetivos exactos para la recuperación. ¿Cuánto tiempo puede estar sin conexión (RTO)? ¿Cuántos datos puede perder (RPO)? Estas no son decisiones de TI; son decisiones de negocio. Pruebas y ejercicios: Un plan en papel no es suficiente. Debes probar periódicamente la continuidad de tus sistemas TIC (por ejemplo, una prueba de conmutación por error a un servidor de respaldo) para comprobar que funcionan correctamente. Redundancia: Implementación de medidas de resiliencia técnica, como hardware duplicado, líneas de internet de respaldo o almacenamiento en la nube multirregión, para cumplir con sus objetivos de disponibilidad. Enfoque de auditoría Alineación: ¿Su plan de recuperación ante desastres (DR) coincide con su análisis de impacto empresarial (BIA)? (Por ejemplo, si el BIA dice "La nómina debe estar disponible en	X			Se incluyen 3 ethical hacking y 3 pen testing. 1 de caja negra y 1 prueba interna que se define con el proveedor. Se han realizado programaciones de pruebas de acceso físico y lógico.
A.8.25 Ciclo de vida de desarrollo seguro, A.8.26 Requisitos de seguridad de las aplicaciones, A.8.27 Arquitectura de sistemas seguros y principios de Ingeniería A.8.28 Codificación segura, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo extemalizado, A.8.31 Separación de entornos de desarrollo, evidencia y producción, A.8.33 Información de las pruebas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría. A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad del negocio,	Anexo A 8.14 Redundancia de las instalaciones de procesamiento de información. Garantizar la alta disponibilidad mediante sistemas de conmutación por error. Este control requiere identificar los requisitos de disponibilidad del negocio e implementar componentes o arquitecturas redundantes. Al eliminar los puntos únicos de fallo, las organizaciones garantizan que los sistemas críticos permanezcan operativos incluso durante fallos de componentes o ventanas de mantenimiento. Requisitos básicos para el cumplimiento Elimine los puntos únicos de fallo (SPOF): debe identificar cualquier componente individual que, si falla, provocaría la caída de todo su servicio (por ejemplo, una sola línea de Internet, una sola fuente de alimentación o un solo servidor de base de datos). Duplicación técnica: Dependiendo del riesgo, esto puede incluir fuentes de alimentación duales, bases de datos replicadas, balanceadores de carga o proveedores de servicios de Internet (ISP) redundantes. Conmutación por error automática frente a manual: Debe definir cómo el sistema cambia al componente redundante. Para sistemas críticos, esto debe ser automático; para sistemas menos críticos, un proceso manual documentado es aceptable. Pruebas: La redundancia es una teoría hasta que se pone a prueba. Es necesario simular regularmente un fallo (por ejemplo, desconectar un cable de alimentación o provocar la conmutación por error de una base de datos) para demostrar que los sistemas de respaldo funcionan correctamente. Enfoque de auditoría Análisis de SPOF: “Muéstrame tu lista de sistemas críticos. ¿Alguno de ellos depende de un único servidor o enlace a Internet?”	X			

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Secretaría de Movilidad	**SISTEMA INTEGRADO DE GESTIÓN DISTRITAL BAJO EL ESTÁNDAR MIPG**	
	PROCESO CONTROL Y EVALUACIÓN A LA GESTIÓN	
	Lista de verificación	
	Código: PV01-IN03- F02	**Versión 2.0**

Fecha:	**Nombre(s) equipo auditor y Rol:**	**Sistema de Gestión auditado :**
22/07/2026	**Oscar Alberto Barragán León - OABL** **Sergio Eduardo Reyes Trillos - SERT**	**SGSI**

Nombre del responsable del proceso auditado:	**Proceso:**	**Dependencia :**
	Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico	**Gestión de TICS-OTIC (Seguridad de la Información)Operador Tecnológico**

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
A.5.19 Seguridad de la información en la relación con los proveedores, A.5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores, A.5.21 gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC), A.5.22 Seguimiento, revisión y gestión de cambio de los servicios de los proveedores, A.5.23 , Seguridad de la información para los servicios en la nube. A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, A.5.25 evaluación de la decisión sobre eventos de seguridad de la información, A.5.26 respuesta de incidentes de Seguridad de la información, A.5.27 aprender de los incidentes de seguridad de la información, A.5.28 Recopilación de evidencias.	Anexo A 5.19 Seguridad de la información en las relaciones con lo proveedores Implementar estándares de seguridad con socios externos Este control garantiza que los proveedores acepten y cumplan con los requisitos de seguridad de la organización. Mitiga el riesgo en la cadena de suministro al establecer un nivel mínimo de seguridad que los proveedores deben cumplir antes de poder acceder a los datos o sistemas de la organización. Anexo A 5.20 Abordar la seguridad de la información en los acuerdos co proveedores. Incorpore las obligaciones de seguridad en los contratos formales. Este control exige que los requisitos de seguridad de la información se documenten en los acuerdos con los proveedores. Proporciona un marco legal para su cumplimiento, que abarca la protección de datos, el derecho a auditoría y la notificación de incidentes, para proteger a la organización legal y operativamente. Anexo A 5.21 Gestión de la seguridad de la información en la cadena d suministro de TIC. Garantizar la seguridad de la cadena de suministro tecnológico. Este control aborda los riesgos asociados a los productos y servicios de TIC. Requiere acuerdos con los proveedores para asegurar la integridad de los componentes de hardware y software, evitando la introducción de tecnología comprometida o maliciosa en la infraestructura crítica. Anexo A 5.22 Supervisión, revisión y gestión de cambios de los servicios d los proveedores Audite periódicamente el desempeño de sus proveedores Este control requiere la revisión continua de la prestación de servicios por parte de los proveedores en función de los acuerdos de seguridad. De esta manera, se garantiza que los cambios en los servicios se gestionen	X			La revisión y evaluación de la gestión de seguridad de la información en la relación con los proveedores, la cadena de suministro de TIC y los servicios en la nube fue ejecutada y validada en su totalidad por el Auditor Líder. Tras la auditoría de los acuerdos contractuales, la inclusión de cláusulas de seguridad, los procesos de seguimiento a los niveles de servicio y la gestión de cambios en las plataformas tercerizadas, se dictamina la conformidad total de este bloque normativo. El proceso opera de manera eficaz, garantizando la protección de los activos de la organización en manos de terceros. No se identificaron hallazgos, desviaciones ni No Conformidades durante la revisión de estos controles.
A.5.19 Seguridad de la información en la relación con los proveedores, A.5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores, A.5.21 gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC), A.5.22 Seguimiento, revisión y gestión de cambio de los servicios de los proveedores, A.5.23 , Seguridad de la información para los servicios en la nube. A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, A.5.25 evaluación de la decisión sobre eventos de seguridad de la información, A.5.26 respuesta de incidentes de Seguridad de la información, A.5.27 aprender de los incidentes de seguridad de la información, A.5.28 Recopilación de evidencias.	Anexo A 5.23 Seguridad de la información para el uso de servicios en nube. Establecer criterios para el uso seguro de la nube. Este control define los requisitos para seleccionar, usar y abandonar los servicios en la nube. Garantiza que se comprenda el modelo de responsabilidad compartida y que los proveedores de servicios en la nube ofrezcan controles adecuados para proteger los datos de la organización en entornos multiusuario. Anexo A 5.24 Planificación y preparación para la gestión de incidentes de seguridad de la información. Prepararse para las brechas de seguridad. Este control requiere establecer procedimientos y responsabilidades para la gestión de incidentes de seguridad de la información. Garantiza que la organización esté preparada para detectar, reportar, evaluar y responder a los incidentes de manera efectiva, minimizando los daños y el tiempo de inactividad operativa. Anexo A 5.26 Respuesta ante incidentes de seguridad de la información. Ejecutar los procedimientos de respuesta a incidentes. Este control exige que los incidentes confirmados se aborden según los planes documentados. Garantiza que las acciones de contención, erradicación y recuperación se implementen con prontitud para limitar el impacto en la confidencialidad, la integridad y la disponibilidad de los datos. Anexo A 5.27 Aprender de los incidentes de seguridad de la información. Analizar los incidentes para prevenir su recurrencia. Este control requiere una revisión posterior al incidente para identificar las causas raíz y mejorar las respuestas futuras. Convierte las fallas de seguridad en oportunidades para fortalecer las defensas, actualizar las políticas y evitar que el mismo tipo de ataque tenga éxito nuevamente.	X			El dominio correspondiente a la gestión de incidentes y eventos de seguridad de la información fue auditado de manera exhaustiva por el Auditor Líder. Se constató que la organización mantiene un marco operativo maduro y documentado para la planificación, evaluación, toma de decisiones y respuesta ante incidentes cibernéticos. Así mismo, los protocolos para aprender de las brechas pasadas y la recolección con validez técnica y forense de evidencias digitales (A.5.28) se encuentran operando bajo los estándares exigidos. Se declara la conformidad total del proceso, sin presentarse Oportunidades de Mejora ni No Conformidades en el actual ciclo de auditoría.

Criterio	Descripción del aspecto a verificar	C	NC	OM	Descripción detallada de las situaciones y las evidencias encontradas
Pruebas A.5.19 Seguridad de la información en la relación con los proveedores, A.5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores, A.5.21 gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC), A.5.22 Seguimiento, revisión y gestión de cambio de los servicios de los proveedores, A.5.23 , Seguridad de la información para los servicios en la nube. A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, A.5.25 evaluación de la decisión sobre eventos de seguridad de la información, A.5.26 respuesta de incidentes de Seguridad de la información, A.5.27 aprender de los incidentes de seguridad de la información,	5.19 Seguridad relacion proveedores Requisito Verificación y diligencia debida de proveedores: Antes de firmar un contrato, debe evaluar la postura de seguridad del proveedor. Esto generalmente se realiza mediante cuestionarios de seguridad o verificando su certificación ISO 27001 . Clasificación por niveles según el riesgo: No todos los proveedores son iguales. Debe clasificar a los proveedores en diferentes niveles según la sensibilidad de los datos que manejan o su importancia para sus operaciones. Obligatoriedad contractual: Los requisitos de seguridad deben ser legalmente exigibles. Esto incluye cláusulas de "Derecho a auditar", términos de protección de datos (RGPD) y plazos para la notificación de incidentes. Registro de proveedores: Debe mantener un inventario centralizado de todos los proveedores externos, sus datos de contacto y su estado de seguridad actual. Gestión de accesos: Debe definir cómo acceden los proveedores a sus sistemas, asegurándose de que solo tengan el acceso mínimo necesario (principio de mínimo privilegio) y que este acceso se revoque inmediatamente cuando finalice el proyecto. Supervisión continua: La seguridad de los proveedores no es una verificación puntual. Debe revisar periódicamente a los proveedores críticos para asegurarse de que no hayan dejado caducar sus certificaciones ni que sus estándares de seguridad se hayan desviado. Enfoque de auditoría Pruebas directas de verificación: “Muéstrenme la evaluación de seguridad de su proveedor de alojamiento en la nube o de su empresa de nóminas.	X			
Pruebas A.5.19 Seguridad de la información en la relación con los proveedores, A.5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores, A.5.21 gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC), A.5.22 Seguimiento, revisión y gestión de cambio de los servicios de los proveedores, A.5.23 , Seguridad de la información para los servicios en la nube. A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, A.5.25 evaluación de la decisión sobre eventos de seguridad de la información, A.5.26 respuesta de incidentes de Seguridad de la información, A.5.27 aprender de los incidentes de seguridad de la información,	5.24 Incidentes de seguridad Requisito Proceso de gestión de incidentes: Debe contar con un proceso documentado que abarque la detección, priorización, clasificación, análisis, comunicación y coordinación de incidentes. Roles y responsabilidades definidos: Debe establecer un Equipo de Respuesta a Incidentes (ERI) con roles claramente definidos. Estos roles deben comunicarse a toda la organización para que todos sepan a quién contactar durante una crisis. Procedimientos de notificación: Debe existir un método común y bien comunicado para que los empleados y terceros informen sobre incidentes de seguridad (por ejemplo, una dirección de correo electrónico específica o un sistema de gestión de incidencias). Capacitación y competencia: El personal que gestiona incidentes debe ser competente y recibir capacitación periódica. La norma recomienda identificar certificaciones específicas o itinerarios de desarrollo para el equipo de respuesta a incidentes (IRT). Objetivos de nivel de servicio: Debe definir niveles de prioridad (por ejemplo, de P1 a P4) con tiempos de respuesta y resolución específicos acordados con la gerencia. Planificación de escenarios: Su plan de gestión de incidentes debe contemplar diversos escenarios, como filtraciones de datos, infecciones de malware o desastres naturales. Enfoque de auditoría Sensibilización del personal: Es probable que un auditor pregunte a cualquier empleado al azar: "¿Si cree que su computadora portátil ha sido pirateada o ha perdido una unidad USB, cómo debe informarlo?". Verificación del proceso: “Muéstrenme su Plan de Gestión de Incidentes .	X			