

**INFORME DE SEGUIMIENTO A LA SEGURIDAD DE LA INFORMACIÓN EN EL
MARCO DE LA NORMA 27001-2013 EN LA UAE CUERPO OFICIAL DE BOMBEROS
DE BOGOTÁ.
julio del 2026**

En cumplimiento a lo establecido en el Plan Anual de Auditorías basado en riesgos vigencia 2026 aprobado el 18 de diciembre de 2025 por el Comité de Coordinación de Control Interno y en cumplimiento del rol de Evaluación y Seguimiento descrito en el Decreto 1083 de 2015 modificado por el Decreto 648 de 2017, la Oficina de Control Interno OCI, realizó seguimiento a la seguridad de la información en el marco de la norma 27001-2022 en el período comprendido entre el 1 de mayo del 2025 y el 30 de junio del 2026.

ASPECTOS GENERALES

En el Manual de Políticas de Seguridad y Privacidad de la Información TIC-MN01 V3 adoptado por la Entidad establece lo siguiente:

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), es prioridad para la UAE Cuerpo Oficial de Bomberos Bogotá, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas y pertenece al habilitador transversal de Seguridad Digital y Privacidad, de la Política de Gobierno Digital.

Se procede a verificar la gestión adelantada por la Entidad con el fin de establecer si se ha venido dando cumplimiento a lo establecido en dicho manual, así como en el Plan de Tratamiento de riesgos V2, teniendo en cuenta que la finalidad de estos lineamientos es preservar la confidencialidad, integridad y disponibilidad de la información y desarrollar de manera adecuada los procesos misionales, estratégicos y administrativos.

Habida cuenta que la seguridad de la información es esencial para proteger los activos digitales, mantener las operaciones y garantizar el cumplimiento normativo, se pidió a los profesionales del área de Tecnología de la Información y las Comunicaciones-TIC responder siguiente cuestionario y allegar las evidencias que soportaran las respuestas:

No.	REQUISITOS AUDITAR (*)	Preguntas	Observaciones del auditor OCI	Evidencias
1	Política y gobernanza	Indicar en donde se puede consultar la política documentada que describan los derechos y responsabilidades de todos los empleados y/o contratistas en materia de seguridad de los datos.	Se observa publicado en el repositorio de información que dispuso la Entidad el manual de PSPI, se recomienda revisar el numeral 6.1.1. Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información pues delegan en el jefe de la OAP la responsabilidad del SIGMSPI.	https://bomberosbog.sharepoint.com/:f/s/DOMINIOA/ROSEGINF/IgCoPTZ1ua5TRJdDmKNxpfziAVXSmSe5aLjlvcdUQ4m1guk?e=jsKLwF
2		Evidencia de la formación periódicas a todo el personal de la Entidad sobre protocolos de seguridad, tratamiento de datos y procedimientos de respuesta ante incidentes.	Se observan actas y listas de asistencias a las capacitaciones dictadas por el área de TIC durante el primer semestre del 2026.	https://bomberosbog.sharepoint.com/:f/s/DOMINIOA/ROSEGINF/IgCCCSIX40cPSYJKI_TW0ugeAQroQY_VNcWv4wq_RL6MxE?e=jK1x7Q
3		Evidencia del plan de respuesta ante infracciones que detalle los pasos a seguir en caso de un incidente de seguridad.	Se evidencian publicados en la Web el procedimiento gestión de incidentes del 26/08/2022, el documento Plan de gestión de crisis, pero no se observa el documento Playbook mencionado en las evidencias; se recomienda revisar el procedimiento TIC-PR05 con el fin de armonizarlo con el plan de gestión de crisis.	https://bomberosbog.sharepoint.com/:f/s/DOMINIOA/ROSEGINF/IgAFclIWliwUSL7OdYy-3hRRAbcgqfgXOc-U3VJf_xa1ZyU?e=X6KTWG
4	Gestión de activos	Soporte del inventario actualizado de todos los activos de hardware y software de la Entidad.	Las evidencias allegadas dan cuenta del inventario del software y al hardware.	https://bomberosbog.sharepoint.com/:f/s/DOMINIOA/ROSEGINF/IgBAOMkhniLSZNPojQYd6wBAW3jxiDmj960H7ouTO3BRXk?e=IaybWg
5		¿Se tiene implementado control de acceso basado en roles (RBAC) para restringir el acceso a información confidencial en función de los roles de los usuarios? Evidenciar	Se observa el archivo en donde se evidencia la asignación de roles de los administradores de las consolas de gestión de Microsoft, estos son gestionados por los profesionales de TIC de la Entidad.	https://bomberosbog.sharepoint.com/:f/s/DOMINIOA/ROSEGINF/IgA_VhsjWHZjS65RjaW4eGUAb3Da16wpMOyGfyXZi7WxKM?e=SU2M6v
6	Seguridad de la Red	Evidencia de configuración del cortafuegos para supervisar y controlar el tráfico de red entrante y saliente.	En la imagen allegada se observa la existencia del firewall Policy monitoreado desde la consola de gestión.	https://bomberosbog.sharepoint.com/sites/DOMINIOA/ROSEGINF/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FDOMINIOA/ROSEGINF%2FShared%20Documents%2FSGSI%2DCS%2DPil%2FSGS

No.	REQUISITOS AUDITAR (*)	Preguntas	Observaciones del auditor OCI	Evidencias
				I%2F5%5F35%5FRevision%20independiente%20de%20la%20seguridad%20de%20la%20informacion%2FEvidencia%2FAuditoria%20CI%5FJunio%5F2026%2FPunto6&p=true&ga=1
7		¿Se tiene implementado sistemas de detección de intrusiones (IDS) para la supervisión del tráfico de red en tiempo real con el fin de detectar actividades sospechosas? Evidenciar	Se observa en la imagen allegada el monitoreo de intrusos.	https://bomberosbog.sharepoint.com/sites/DOMINIOAROSEGINF/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FDOMINIOAROSEGINF%2FShared%20Documents%2FSGSI%2DCS%2DP1I%2FSGSI%2F5%5F35%5FRevision%20independiente%20de%20la%20seguridad%20de%20la%20informacion%2FEvidencia%2FAuditoria%20CI%5FJunio%5F2026%2FPunto7&p=true&ga=1
8		¿Se tiene segmentada la red para separar los sistemas vitales de las áreas menos seguras de la red? Evidenciar y soportar la respuesta	Se observa en la imagen allegada que la entidad tiene segmentada por VLAN las redes IP, informan que el switch de Core actúa como Gateway (software que actúa como puerta de enlace entre dos redes o sistemas con protocolos diferentes, permitiendo la comunicación entre ellos).	https://bomberosbog.sharepoint.com/sites/DOMINIOAROSEGINF/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FDOMINIOAROSEGINF%2FShared%20Documents%2FSGSI%2DCS%2DP1I%2FSGSI%2F5%5F35%5FRevision%20independiente%20de%20la%20seguridad%20de%20la%20informacion%2FEvidencia%2FAuditoria%20CI%5FJunio%5F2026%2FPunto8&p=true&ga=1
9	Gestión de contraseñas	¿Se tiene establecida una política de contraseñas seguras que exija contraseñas complejas y actualizaciones periódicas? Evidenciar	Se observa la parametrización de la política establecida para las contraseñas seguras.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOAROSEGINF/IgA9WN_v-cviQqdTbJUA_To7AdyZB5_TlgL1YeWIRpFlt4k?e=HN5yqh
10		¿Se cuenta con la autenticación multifactorial (MFA) para acceder a sistemas críticos y mejorar la seguridad más allá de las	Se observa que se tiene configurado y funcionando el doble factor de autenticación de los usuarios de la red Institucional.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOAROSEGINF/IgCJH_8SjhsrRaMfwHUFVARGAV4QnP_Ltu4gqwppl1npVlrk?e=Gwfr4rG

No.	REQUISITOS AUDITAR (*)	Preguntas	Observaciones del auditor OCI	Evidencias
		contraseñas? Sustentar la respuesta		
11	Seguridad del sistema	Indicar cuando fue la última actualización todos los sistemas operativos con los últimos parches de seguridad. Evidenciar	Se observa el informe de vulnerabilidades, que actualizan el antivirus permanentemente con parches.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/IgDm1-8xxEHtRLn9wKFvUtyASFsyYoaowLnhrMXIVj0Ojs?e=mvTpFn
12		¿Todos los dispositivos de la Entidad cuentan con software antivirus actualizado, cada cuanto se hace la actualización? Evidenciar	Se verifica en el Secop II y se observa el contrato 782/2024 prorrogado hasta junio del 2026, con el cual se adquiere el antivirus de la Entidad.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/IgB38KfBNr05Tiyq0VjdTT5AQHJpgXrMknlipY2bjrgof8?e=zy8Ocu
13		¿Se ha realizado un análisis de vulnerabilidad internos y externos para identificar posibles puntos débiles? Evidenciar	En la evidencia allegada se observa el análisis de las vulnerabilidades, informan que lo hacen diariamente.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/IgBkcg2mzMCdTIsXpVC1sANGAUDgkQSyXNLzqKy7zOu6f08?e=0aDhw9
14	Protección de datos.	¿Se tienen cifrados los datos confidenciales tanto en reposo como en tránsito para evitar el acceso no autorizado? Evidenciar y soportar la respuesta	Las evidencias allegadas dan cuenta del cifrado en reposo de los sistemas que estimó la Entidad. Informan que se tiene cifrado en tránsito a través de certificados digitales y la plataforma Office 365 de correos electrónicos.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/IgC1hQC8ig9XTZgAD0RqQaCBAQ-JAPGrXDKNisQK6U-sJrg?e=K1Szxq
15		¿Cada cuánto se tienen programadas las copias de seguridad automáticas de los datos esenciales en ubicaciones seguras para una rápida recuperación en caso de incidente cibernético? Evidenciar	Se observa bitácora en donde registran las actividades diarias del controlador de dominio y programan las actividades de copias de seguridad.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/IgAHSod-wyYRS6en2cTya0cdAXBJfusFepkJwM2y5Lsq-lw?e=ulCTXD
16	Continuidad del negocio	¿La Entidad cuenta con el plan de continuidad del negocio en caso de presentarse una emergencia extrema? asonada, terremoto, pandemia, Etc. Evidenciar	Se observan los documentos plan de continuidad del negocio y plan de gestión de crisis publicados en la Web de la Entidad. Se observó en dos documentos que menciona al oficial de Continuidad del negocio, importante que se designe quien tendrá ese rol.	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/IgAAeYz4wyfaSrYV2j7KVv5LAZuY_mr2WqX_zKZwv3_GDk?e=29acaU

No.	REQUISITOS AUDITAR (*)	Preguntas	Observaciones del auditor OCI	Evidencias
17		¿Se cuenta con los recursos \$\$ en el PAA para implementar el plan de continuidad del negocio? Evidenciar	Se verificó en el PAA versión 13- 2026, la existencia del rubro citado para invertir en entre otros en la gestión de servicios TI y continuidad del negocio (Cloud & Backus)	https://bomberosbog.sharepoint.com/:f:/s/DOMINIOA/RQSEGINF/lqDMfnfgWzPI/SKWQYwcFtjtjAcj_4pD1Mh-60P1D2MgTh0?e=3BdL12

Se verificaron las evidencias presentadas para soportar las respuestas y se observa un resultado satisfactorio para los componentes de seguridad de la información evaluados; para los temas en los cuales se observa debilidad se dejan las sugerencias correspondientes en el acápite “Recomendaciones” de este informe.

MATRIZ DE RIESGOS DIGITALES- UAECOB

El área de tecnología tiene identificados catorce (14) riesgos digitales, en la matriz establecida describen las amenazas, vulnerabilidades, controles, plan de tratamiento de riesgos, entre otros, que responde a la metodología adoptada para la gestión de riesgos de seguridad de la información definida en la norma técnica ISO 27005 y que se articula con la guía de Gestión de riesgos sugeridas por el Departamento Administrativo de la Función Pública - DAFP dentro del marco de la implementación del Modelo Integrado de Planeación y Gestión – MIPG; de acuerdo con las evidencias revisadas se deduce que se han venido aplicando los controles establecidos con el fin de mitigar los riesgos, no obstante se observa que para los riesgos R11: Pérdida de Confidencialidad, Integridad o Disponibilidad de la información. Incumplimiento de políticas de seguridad de la información por parte de funcionarios y terceros (proveedores, contratistas, outsourcing, otros) y R23: Falta de Planificación y preparación de la gestión de incidentes de seguridad de la Información, así como tener una apropiada respuesta a incidentes de seguridad de la Información; los riesgos residuales presenta un impacto Alto después de controles, por lo que se recomienda revisar la metodología aplicada con el fin de encontrar u optimizar controles que permitan llevar el riesgo residual a un impacto aceptable para la entidad.

Una vez se revise la metodología y se compruebe que los controles son adecuados y, que el riesgo residual permanece en la misma zona en el mapa de calor, es importante que se comunique a la Alta Dirección con el fin de que estos sean tenidos en cuenta en los lineamientos que considere para el apetito del riesgo.

Lo anterior con el fin de proteger a la Entidad de cualquier tipo de pérdida o sanción por la materialización de alguno de estos riesgos.

RECOMENDACIONES

- a- En el manual de Políticas de Seguridad y Privacidad de la Información, se recomienda revisar el numeral 6.1.1. Roles y responsabilidades del SIGMSPI pues

delegan en el jefe de la Oficina Asesora de Planeación la responsabilidad de: Coordinar, orientar y promover las actividades requeridas para el mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información y Liderar e impartir lineamientos para implementar la estrategia de seguridad de la información; responsabilidad que actualmente está en cabeza de la Dirección de la Entidad delegada al profesional especializado de tecnología de la información y las comunicaciones.

- b- Para el tema de incidentes de seguridad digital se observan entre otros los documentos, procedimiento gestión de incidentes del 26/08/2022 y el documento de gestión de crisis, pero no se observa el documento Playbook que fue mencionado cuando se dio respuesta al cuestionario en el numeral 3 relacionado con el plan de respuesta ante infracciones, se recomienda publicar este documento en el repositorio de información correspondiente.
- c- En el procedimiento Gestión Incidentes de Seguridad de la Información V2 mencionan en la actividad “26. Remitirse al procedimiento de gestión de crisis”, se verificó en el repositorio de información de la Entidad y no se encontró el mencionado documento, importante revisar y armonizar los instrumentos que hacen parte del Sistema de Gestión de la Entidad.
- d- En los documentos plan de continuidad del negocio y Plan de Gestión de crisis publicados en la Web de la Entidad, se observó que menciona al oficial de Continuidad del negocio, según lo revisado no se conoce quien ejerce este rol dentro de la Entidad, por lo que se recomienda revisar esta delegación y asignarla oficialmente.
- e- Con el fin de asegurar el cumplimiento de los lineamientos impartidos desde el modelo de políticas de seguridad y privacidad de la información, se recomienda a la segunda línea de defensa de la Entidad realizar periódicamente una revisión (autorregulación) a las actividades de los procedimientos institucionales que tengan establecidas actividades de control relacionadas con la seguridad de la información.
- f- Importante que periódicamente el área de tecnología de la Entidad realice pruebas, como análisis de vulnerabilidad o pruebas de penetración, para evaluar la eficacia de los controles actuales.
- g- Para los riesgos residuales que siguen estando en nivel alto (R11 y R23) importante informar a la alta Dirección para que se tomen decisiones al respecto y se defina si estos riesgos son aceptables o no (apetito del riesgo).

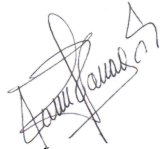
CONCLUSION

Con base en la evaluación adelantada por la Oficina de Control Interno y una vez valorados los documentos presentados por los profesionales designados por parte del proceso Tecnologías de la información y las comunicaciones, se puede concluir que la Alta Dirección se encuentra comprometida con la seguridad de la Información, en razón a que ha definido una política de Seguridad y privacidad de la Información y ha dispuesto los distintos recursos financieros, administrativos y técnicos para su implementación y mejora, así como un equipo humano profesional, calificado y comprometido en el área de tecnología, sin

embargo, se observan aspectos susceptibles de mejora que se presentaron en el capítulo precedente de recomendaciones.

Es importante que adopten las acciones de mejora pertinentes para lograr cumplir a cabalidad con el objetivo del Modelo de seguridad y privacidad de la Información MSPI, asegurar que perdure en el tiempo, blinde a la Entidad de posibles sanciones y, coadyuve al cumplimiento de sus metas y su misión.

Cordialmente,



CARLOS ANDRÉS VARGAS PUERTO
Jefe Oficina de Control Interno

Proyectó: María del Carmen Bonilla- Profesional especializada 222 grado 20 OCI
Revisó: Carlos Andrés Vargas Puerto- jefe de la OCI