ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

FORMATO PLAN DE MEJORAMIENTO

CÓDIGO: CEM-FM-004 | **VERSIÓN: 8**

FECHA DE APLICACIÓN: MAYO DE 2022

PROCESO / UNIDAD AUDITADA:	**MSPi-Modelo de Seguridad y Privacidad de la Información y PGDi-Política de Gobierno Digital UAERMV 2022**	**AÑO:**	**2022**
RESPONSABLE DEL PROCESO / UNIDAD AUDITADA:	**Martha Patricia Aguilar Copete - Secretaria General UAERMV**	**FECHA DE DILIGENCIAMIENTO:**	**8/03/2023**

ÍTEM	DESCRIPCIÓN DEL HALLAZGO DE AUDITORÍA /OPORTUNIDAD DE MEJORA/ NO CONFORMIDAD/ OBSERVACIÓN	ORIGEN (1)	CAUSA (2)	TIPO DE ACCIÓN A IMPLEMENTAR (3)	DESCRIPCIÓN DE LA ACCIÓN A IMPLEMENTAR (4)	INDICADOR (5)	FORMULA INDICADOR (6)	META DEL INDICADOR (7)	RESPONSABLE DE LA ACCIÓN A IMPLEMENTAR (8)	FECHA INICIO (9)	FECHA FIN (10)	AVANCE REPORTADO DE LA ACCIÓN A IMPLEMENTAR (11)					SEGUIMIENTO (12)				
												FECHA DE CORTE	RESULTADO DEL INDICADOR A LA FECHA DE CORTE	ESTADO	DESCRIPCIÓN DE LAS ACTIVIDADES REALIZADAS EN EL PERIODO	EVIDENCIA(S) SOPORTADA(S)	FECHA	RESULTADO DEL INDICADOR A LA FECHA DE CORTE	ESTADO	OBSERVACIONES
1	DOMINIO Políticas de Seguridad de la Información La política general y las políticas específicas de la Seguridad de la Información, no tienen definidos lineamientos que orienten de manera completa los aspectos relacionados con el control de acceso a las aplicaciones de computador, al uso de controles criptográficos, a la gestión de dispositivos móviles y al	Auditoria Externa	Falta de seguimiento de las políticas MSPI especificas vigentes y de revisión de las políticas MSPI requeridas a documentar, para ser divulgadas e implementadas en la Entidad.	Acción Correctiva	Actualizar y/o documentar siete (7) políticas MSPI: Actualizar dos (2) políticas MSPI existentes y Documentar cinco (5) políticas del MSPI complementarias, consolidadas para su implementación.	Políticas del MSPI vigentes y consolidadas	([(Número de políticas MSPI actualizadas) + (Número de políticas MSPI documentadas)] / (Número de Políticas MSPI programadas para actualizar-documentar y consolidar))x100	Siete (7) políticas MSPI documentadas vigentes y consolidadas	**CISO designado (Chief Information Security Officer: es el director de seguridad de la información)**	2023-03-15	2023-10-30			Sin Iniciar							
2	DOMINIO Organización de la Seguridad de la Información En los documentos revisados por parte de la Auditoría, se observó que el gobierno y la gestión de la Seguridad de la Información se concentra en la Secretaría General.	Auditoria Externa	Inadecuada segregación de las funciones y responsabilidades para la Gobernanza y la Gestión de la Seguridad de la Información dentro de la Entidad.	Acción Correctiva	Documentar un (1) "Manual del SGSI-Sistema de Gestión de Seguridad de la Información", que contenga los roles y perfiles para su implementación. Aprobado y divulgado.	Documentación del Manual del SGSI-Sistema de Gestión de Seguridad de la Información	% de documentación del Manual SGSI-Sistema de Gestión de Seguridad de la Información	Un (1) Manual del SGSI documentado	CISO	2023-04-15	2023-07-30			Sin Iniciar							
3	DOMINIO Seguridad de los Recursos Humanos La Auditoría no evidenció programas de capacitación y concienciación dirigida a los contratistas que manejan los	Auditoria Externa	No se tiene un análisis de los riesgos sobre la información que manejan los contratistas y proveedores...*por falta de capacitaciones del MSPI*	Acción Correctiva	Desarrollar dos (2) sensibilizaciones de seguridad y privacidad de la información, y de datos personales.	Sensibilizaciones MSPI desarrolladas	[(Número de sensibilizaciones MSPI desarrolladas) /(Número Total de sensibilizaciones MSPI programadas)]x100	Dos (2) sensibilizaciones MSPI desarrolladas	CISO	2023-05-15	2023-11-15			Sin Iniciar							
4	DOMINIO Gestión de Activos No se identificó que la UMV cuente con lineamientos y procedimientos que permitan dar un adecuado uso a medios removibles, cuando en estos se almacena información de la entidad.	Auditoria Externa	No se ha definido un análisis de los riesgos relacionados con la utilización de medios extraíbles/removibles, que permita definir, implementar y hacer seguimiento de las políticas requeridas en el MSPI, relacionadas con el uso de	Acción Correctiva	Documentar un (1) "procedimiento de Gestión de medios extraíbles/removibles", de acuerdo con el esquema de clasificación adoptado por la Entidad. Aprobado y divulgado.	Documentación del procedimiento de Gestión de medios extraíbles/removibles	% de documentación del procedimiento de Gestión de medios extraíbles/removibles	Un (1) procedimiento de Gestión de medios extraíbles/removibles documentado	CISO	2023-07-15	2023-08-30			Sin Iniciar							
5	DOMINIO Control de Acceso En la política general y específicas de Seguridad de la Información, no se identificaron reglas de control relacionadas con el acceso y restricciones a los activos de información para las aplicaciones que apoyan los	Auditoria Externa	No se ha definido, por parte de la entidad, las matrices de roles y responsabilidades asignadas a los usuarios de las aplicaciones institucionales y sus accesos.	Acción Correctiva	Actualizar una (1) "política de control de acceso" incorporando directrices que apunten a definir los límites de acceso de usuarios y perfiles a la información y funciones de los sistemas y/o aplicaciones institucionales. Aprobada y divulgada.	Actualización de la política de control de acceso	% de documentación de la política de control de acceso	Una (1) política de control de acceso de usuarios y perfiles actualizada	CISO	2023-07-30	2023-08-30			Sin Iniciar							
6	DOMINIO Criptografía La verificación de la documentación aportada por la Unidad no permite evidenciar una adecuada implementación de los controles relacionados con la protección criptográfica de información sensible, no se encontró una política y procedimientos documentados, que orienten la implementación de los controles sobre	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el modelo de Seguridad y Privacidad de la Información... en cuanto a la protección criptográfica.	Acción Correctiva	Documentar una (1) "política de criptografía" relacionada con el uso de controles criptográficos para la protección de la información. Aprobado y divulgado.	Documentación de la política de Criptografía	% de documentación de la política de Criptografía	Una (1) política de Criptografía documentada	CISO	2023-07-30	2023-08-30			Sin Iniciar							
7	DOMINIO Seguridad Física y del Entorno No se pudo identificar si la Unidad maneja áreas especiales para despacho y carga de activos de información y si este requerimiento aplica dentro de la entidad o si se requiere excluir del alcance de los controles del Modelo de Seguridad y Privacidad. Así mismo no se encontraron políticas o procedimientos relacionados con el retiro de activos de la entidad, o instructivos de borrado de información de equipos fuera	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el modelo de Seguridad y Privacidad de la Información, en cuanto a la declaración de aplicabilidad.	Acción Correctiva	Documentar una (1) "política de Declaración de aplicabilidad" relacionada con el control en áreas especiales como: de despacho y carga y/o retiro de activos de información de la Entidad, que incluya el borrado seguro de información. Aprobada y divulgada.	Documentación de la política de Declaración de aplicabilidad	% de documentación de la política de Declaración de aplicabilidad	Una (1) política de Declaración de aplicabilidad documentada	CISO	2023-03-30	2023-11-30			Sin Iniciar							
8	DOMINIO Seguridad de las Operaciones Los documentos aportados por la Unidad, no evidenciaron que se estén realizando revisiones periódicas a las actividades de los usuarios, excepciones, fallas y eventos	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el modelo.	Acción Correctiva	Actualizar una (1) "Política de seguridad para la gestión de logs" la cual incluya la revisión periódica, para garantizar la seguridad a nivel de los administradores de TI. Aprobada y divulgada.	Actualización de la Política de seguridad para la gestión de logs	% de actualización de la Política de seguridad para la gestión de logs	Una (1) política de gestión de logs actualizada	CISO	2023-04-30	2023-08-30			Sin Iniciar							
9	DOMINIO Seguridad de las Comunicaciones No se evidenciaron planes de trabajo e informes relacionados con la revisión de los acuerdos de confidencialidad o no divulgación de la información.	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el MSPI... por la ausencia de acuerdos de confidencialidad que cuenten con la normatividad de seguridad y privacidad de la información y datos personales	Acción Correctiva	Documentar un (1) documento interno de "Acuerdos de confidencialidad y transferencia de información" que contenga la normatividad e información clasificada o sensible para la Entidad. Aprobado y divulgado.	Documentación de la política de Acuerdos de confidencialidad y transferencia de información	% de documentación de Acuerdos de confidencialidad y transferencia de información	Una (1) Acuerdos de confidencialidad y transferencia de información documentado	CISO	2023-04-30	2023-08-30			Sin Iniciar							
10	DOMINIO Adquisición, Desarrollo y Mantenimiento de Sistemas No se identificó una política y procedimientos que guíen el desarrollo seguro de las aplicaciones	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el MSPI... por la ausencia de una política de desarrollo seguro de aplicaciones y software en la entidad	Acción Correctiva	Documentar una (1) "política de Desarrollo Seguro" relacionada con el uso de controles criptográficos para la protección de la información. Aprobada y divulgada	Documentación de la política de Desarrollo Seguro	% de documentación de la política de Desarrollo Seguro	Una (1) política de control de Desarrollo Seguro documentada	CISO	2023-07-30	2023-08-30			Sin Iniciar							
11	DOMINIO Relaciones con los Proveedores En la documentación aportada por la Unidad, no se pudo evidenciar que se tiene una adecuada identificación de los proveedores, los contratos que tiene asociados y categorizados por tipo de relevancia y criticidad, así mismo, no se pudo evidenciar la planeación y ejecución del monitoreo de la política de seguridad de la relación	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el modelo, para la identificación de proveedores y de la información que manejan y a la que tienen acceso.	Acción Correctiva	Documentar un (1) documento interno "catalogo de proveedores tecnológicos" por importancia de continuidad tecnológica, donde se identifiquen a los proveedores, los contratos asociados y categorizados por tipo de relevancia y criticidad. Aprobado y divulgado.	Documentación del DI-Catálogo de proveedores TI	% de documentación del DI-Catálogo de proveedores TI	Un (1) DI-Catálogo de proveedores TI documentado	PROFESIONAL UNIVERSITARIO DEL PROCESO DE TI	2023-07-30	2023-08-30			Sin Iniciar							
12	DOMINIO Gestión de Incidentes de Seguridad de la Información No se evidenciaron registros de la aplicación de los procedimientos para la identificación, recolección, adquisición y preservación de información relacionada con los análisis de vulnerabilidades en sistemas y servicios.	Auditoria Externa	Falta de un plan de hacking ético que permita revisar las vulnerabilidades que puedan tener los sistemas, aplicativos y bases de datos de la Entidad.	Acción Correctiva	Documentar un (1) "procedimiento de Análisis de vulnerabilidades de sistemas y servicios" de alto impacto, que permitan identificar si la plataforma tecnológica de la entidad, se encuentra debidamente protegidas contra ataques externos. Aprobado y divulgado.	Documentación del procedimiento de Análisis de vulnerabilidades de sistemas y servicios	% de documentación del procedimiento de Análisis de vulnerabilidades de sistemas y servicios	Un (1) procedimiento de Análisis de vulnerabilidades de sistemas y servicios documentado	CISO	2023-05-30	2023-12-30			Sin Iniciar							
13	DOMINIO Aspectos de Seguridad de la Información de la Continuidad del Negocio En la documentación relacionada por parte de la Unidad, no se pudo evidenciar que se cuente con un plan formal que permita dar continuidad a las operaciones, cuando	Auditoria Externa	Falta de definición y seguimiento a la implementación de las políticas requeridas en el modelo de Seguridad y Privacidad de la Información, en cuanto a la ausencia de mecanismos de continuidad del negocio y continuidad tecnológica	Acción Correctiva	Documentar un (1) Plan de Continuidad de Negocio UAERMV, que contenga la definición de los recursos mínimos necesarios (financieros, humanos, técnicos-tecnológicos y físicos) para su sostenibilidad y poder continuar con la operación de la Entidad en caso de crisis. Aprobado y divulgado	Documentación del Plan de Continuidad de Negocio UAERMV	% de documentación del Plan de Continuidad de Negocio UAERMV	Un (1) Plan de Continuidad de Negocio UAERMV documentada	CISO- gobierno de TI	2023-05-30	2023-12-30			Sin Iniciar							

14	DOMINIO Cumplimiento No se evidenciaron documentadas las pruebas técnicas realizadas a los sistemas de información, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.	Auditoria Interna	Falta de definicion y seguimiento a la implementacion de las políticas requeridas en el modelo, por la falta identificación, priorización de atención, ejecución de pruebas, Instalación y seguimiento de parches de vulnerabilidades de alto impacto sobre las plataformas tecnológicas de la Entidad.	Acción Correctiva	Actualizar un(1) "Procedimiento actualizaciones de software" que incluya la gestión de vulnerabilidades de alto impacto. Aprobado y divulgado.	Actualización del procedimiento actualizaciones de software	% de actualización del procedimiento actualizaciones de software	Un (1) procedimiento de actualizaciones de software actualizado	CISO- gobierno de TI	2023-07-30	2023-11-30			Sin Iniciar						

HALLAZGO: Registre el hallazgo (/OPORTUNIDAD DE MEJORA/NO CONFORMIDAD/ OBSERVACIÓN) completo, contenido en el informe de auditoria
(1): ORIGEN: El origen pueden ser: Auditoría Interna, Auditoría Externa, Revisión por la Dirección, Tratamiento del Producto y/o Servicio No Conforme, Medición de Indicadores, Mapa de Riesgos, Autoevaluación del Proceso, Sistema de Gestión, Quejas y Reclamos, Normograma, OTRO: describa
(2): CAUSAS: Registre la causa del hallazgo o riesgo materializado, que originó la situación detectada (formato: Análisis de Causa) , sobre la cual se enfocará la acción.
(3) TIPO DE ACCIÓN A IMPLEMENTAR: acción que subsana la causa que dio origen al hallazgo identificado, con el fin de solucionar las causas identificadas, para que no vuelvan a suceder.
(4): DESCRIPCIÓN DE LA ACCIÓN A IMPLEMENTAR: Registre la(s) acción(es) que realizará descriptivamente, para corregir definitivamente la causa del hallazgo de Auditoría, Oportunidad de Mejora, No Conformidad u Observación. Inicie con un verbo en infinitivo.
(5): INDICADOR: Registre el nombre del indicador a través de la cual se pueda observar el cumplimiento de la acción determinada . (Ej.: informes, jornadas de capacitación, actas, etc.)
(6): FORMULA INDICADOR: Determine las variables y la correspondiente fórmula del indicador que permite medir el cumplimiento de la acción determinada a implementar.
(7): META DEL INDICADOR: registre la cantidad asociada a las actividades realizables y verificables de la acción correctiva que se espera alcanzar en el tiempo definido, teniendo en cuenta la realidad Institucional y recursos disponibles (Ej.: 5 informes, 10 jornadas de capacitación, 3 actas, etc.).
(8): RESPONSABLE: DE LA ACCIÓN A IMPLEMENTAR: Señale el responsable Directivo o Jefe de Dependencia del proceso o unidad auditada, a la cual le corresponde ejecutar la acción correctiva a implementar.
(9): FECHA DE INICIO: Indique la fecha en que comienza cada acción a implementar registrada. El formato debe ser (AAAA/MM/DD)
(10): FECHA FIN: Señale la fecha en que finaliza cada acción implementada. El formato debe ser (AAAA/MM/DD) . Esta fecha **NO PODRÁ SUPERAR 12 MESES** contados a partir de la fecha de formulación del respectivo plan de mejoramiento.
(11): AVANCE REPORTADO DE LA ACCIÓN A IMPLEMENTAR: En esta sección se deberá diligenciar los siguientes campos: Fecha de corte, Resultado del Indicador a la fecha de corte, Estado, Descripción de las actividades realizadas en el periodo, Evidencia (s) soportada (s)
Los procesos deben autoevaluarse calificando el estado de las acciones, de acuerdo al resultado del avance teniendo en cuenta los siguientes criterios:
-Sin iniciar: Indica que aún no ha iniciado el plazo para realizar la implementación de la acción
-En ejecución: Indica que la acción se está desarrollando en los plazos establecidos y se encuentra en términos.
-Cumplida: Indica que la acción está cerrada y se adelantaron todas las acciones propuestas-
-Vencida: Indica que la acción se está desarrollando fuera del plazo establecido.
(12) SEGUIMIENTO: En esta sección se deberá diligenciar los siguientes campos: Fecha, resultado del indicador a la fecha de corte, estado y observaciones.