

 ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial	FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO	
	CÓDIGO: CEI-FM-022	VERSIÓN: 1
	FECHA DE APLICACIÓN: NOVIEMBRE 2023	

Tipo de trabajo	Auditoría Especial		Auditoría Regular	
Fecha trabajo	26/11/2024			
Proceso/Unidad Auditable	Auditoría Modelo de Seguridad y Privacidad de la información MSPI y pruebas de Ethical Hacking			
Equipo auditor	Ana Josefa Carreño			
Objetivo Auditoría	Evaluar los controles, riesgos y cumplimiento de la normatividad vigente para el Modelo de Seguridad y Privacidad de la Información MSPI y realizar pruebas de Ethical Hacking para verificar la efectividad de los controles de seguridad implementados en la UMV			
Alcance	Esta auditoría evaluó los riesgos y controles de los procedimientos, políticas, planes, manuales e instructivos relacionados con el MSPI desde el 01/01/2023 hasta el 30/07/2024. No se evaluaron los dominios 14, Adquisición, desarrollo y mantenimiento de sistemas y se excluye la evaluación del riesgo 9 de seguridad digital, porque ya se evaluaron en la auditoría transversal de sistemas de información. Tampoco se tuvo en cuenta el dominio que hace referencia al Plan de continuidad.			

1. ASPECTOS RELEVANTES

1.1 Fortalezas	➤ La OTI cuenta con un equipo especializado que tiene la experiencia y el conocimiento para la implementación del MSPI. ➤ La OTI acató las recomendaciones emitidas por la auditoría en la vigencia 2022 y elaboró varios instrumentos de planeación y seguimiento para el MSPI. ➤ La OTI realiza sensibilizaciones periódicas a los servidores públicos y contratistas sobre seguridad de la información y adicionalmente a través de los canales de comunicación internos emite piezas informativas para la prevención de incidentes de seguridad. ➤ Los equipos personales pueden conectarse a un segmento de red aislado sin acceso a recursos corporativos críticos, minimizando los riesgos de seguridad. ➤ Los procesos auditados cuentan con procedimientos, documentos, con inclusión de puntos de control ➤ Los procesos auditados atendieron oportuna y respetuosamente todas las pruebas de recorrido y de auditoría programadas. ➤ Los equipos auditados atendieron todas las solicitudes de información que se requirieron en el transcurso de la auditoría de manera organizada lo cual facilitó el ejercicio de auditoría.
----------------	--

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV



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

FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO

CÓDIGO: CEI-FM-022

VERSIÓN: 1

FECHA DE APLICACIÓN: NOVIEMBRE 2023

1.2 Oportunidades de mejora	❖ Debilidades en la política de control de accesos ❖ Debilidades en la aprobación y publicación de los activos de información de la vigencia 2023 en el sitio Web de la Unidad y en el portal de datos abiertos. ❖ Incumplimiento de las responsabilidades asignadas a GTHU en las políticas generales de tecnología y seguridad de la información para sensibilizar y concientizar a los servidores públicos. ❖ Inconsistencias entre el inventario de equipos tecnológicos entre GREF y la OTI ❖ Aprovechar la transición a la norma ISO 27001:2022 y revisar todos las políticas, procedimientos, instructivos y formatos en el marco de la implementación del MSPI y actualizarlos según lo que está implementado. ❖ El plan del modelo de seguridad de la información debe estar articulado con las brechas identificadas en el autodiagnóstico del MSPI. ❖ Seguimiento a los lineamientos de las diferentes políticas y procedimientos que se han elaborado en el marco de implementación del MSPI como segunda línea de defensa
1.3 Conclusiones	Evaluación de riesgos Por parte de la OCI se identificaron 11 riesgos adicionales a los 9 que fueron evaluados del proceso EGTI. Diseño de controles Se evaluaron 64 controles y 6 actividades, de los cuales 24 controles son del mapa de riesgos del proceso EGTI y 40 controles y 6 actividades fueron identificados por el equipo auditor en los documentos internos objeto de auditoría.

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV



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

FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO

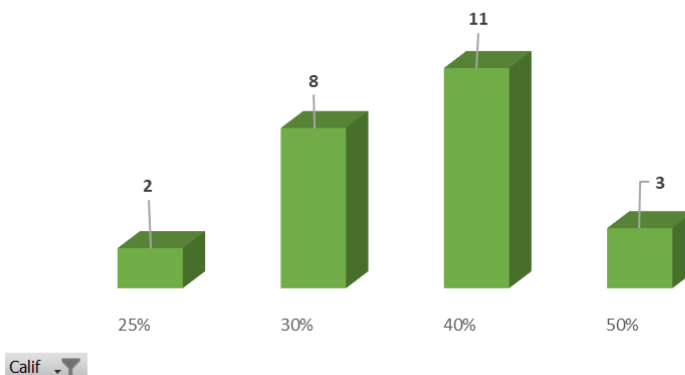
CÓDIGO: CEI-FM-022

VERSIÓN: 1

FECHA DE APLICACIÓN: NOVIEMBRE 2023

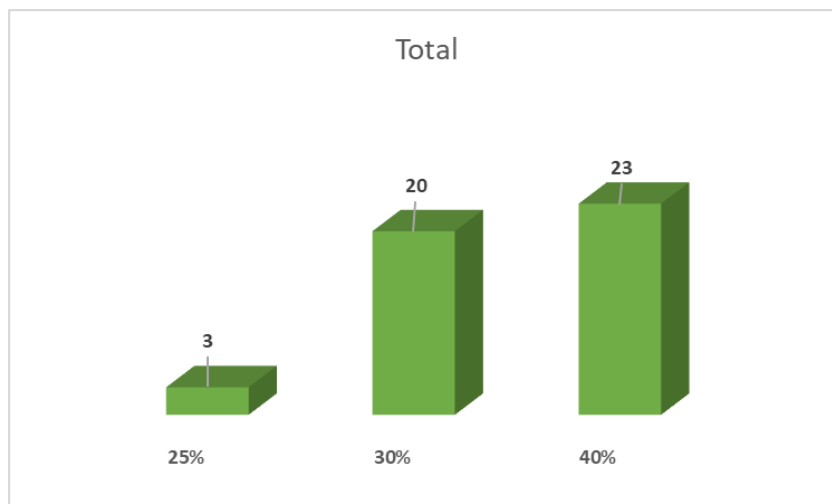
Cuenta de Control

Controles proceso EGTI



Siendo 50%, la máxima calificación para el diseño de un control, los resultados en cuanto al diseño de los controles evaluados del proceso EGTI fueron: 3 obtuvieron una calificación del diseño de 50%, once (11) de 40%, ocho (8) de 30% y dos (2) de 25%.

Total



En cuanto a los controles y actividades identificadas por el equipo auditor, 23 obtuvieron una calificación de 40%, 20 de 30% y 3 de 25%.

Las que fueron catalogadas como actividades requieren ajustarse en diseño para catalogarlas como controles.

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV



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

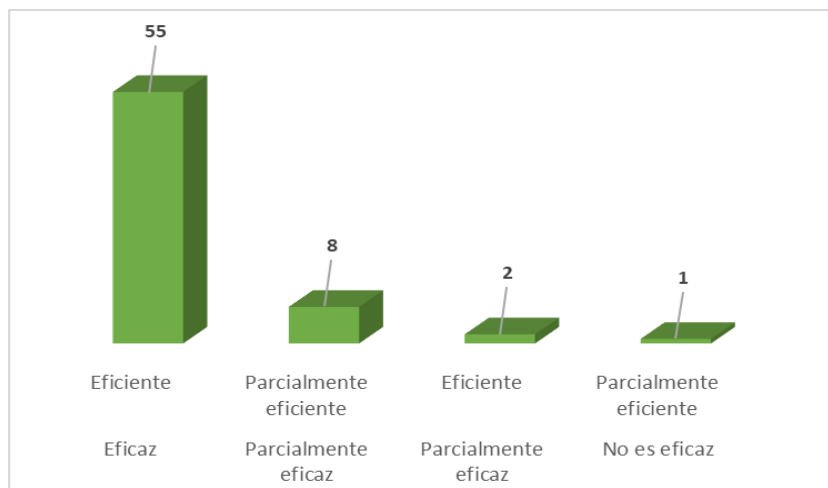
FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO

CÓDIGO: CEI-FM-022

VERSIÓN: 1

FECHA DE APLICACIÓN: NOVIEMBRE 2023

Ejecución de controles



55 controles son eficaces y eficientes dado que se ejecutan como fueron diseñados y mantienen un adecuado diseño para mitigar el riesgo asociado; 8 controles parcialmente eficientes y parcialmente eficaces, 2 controles son eficientes y parcialmente eficaces y 1 control es parcialmente eficiente y no es eficaz y pueden presentar materialización de los riesgos asociados.

2. RESUMEN DE LOS RESULTADOS

A continuación se relaciona la distribución de hallazgos por tema:

Proceso/ unidad auditable	Procedimiento	Total	%
Modelo de Seguridad y Privacidad de la Información MSPI	Controles de acceso	4	57%
	Activos de información	1	14%
	Inventario TI	1	14%
	Políticas de seguridad de la información	1	14%
TOTAL GENERAL		7	100%

Adicional a los siete (7) hallazgos se generaron tres observaciones, una relacionada con controles de acceso a office 365 y Oraclecloud, otra relacionada con la gestión de control de cambios y la otra hace referencia a la política de gestión de contraseñas y política de seguridad contra software nocivo.

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV

 ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial	FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO	
	CÓDIGO: CEI-FM-022	VERSIÓN: 1
	FECHA DE APLICACIÓN: NOVIEMBRE 2023	

3. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA

A continuación se presenta el mapa de criticidad de los hallazgos identificados:

Matriz de Calor Inherente RIESGOS OCI		Impacto					Extremo Alto Moderado Bajo
Probabilidad	Muy Alta 100%						
	Alta 80%						
	Media 60%			H7			
	Baja 40%			H1 H4 H3 H5 H6			
	Muy Baja 20%			H2			
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%	

A continuación se relaciona el nivel de riesgo de los hallazgos identificados:

Auditoría al Modelo de Seguridad y Privacidad de la Información MSPI	
Moderado	Hallazgo1: Debilidades en la ejecución de controles internos para verificar el cumplimiento de requisitos y autorizar el ingreso al Datacenter
	<i>Durante el ejercicio de auditoría para el periodo auditado se revisaron los formatos de credenciales de las personas con acceso al Datacenter, donde se evidenció lo siguiente:</i> • Para el I y II cuatrimestre de 2023, de 11 formatos revisados, en 8, que corresponden al 72% no se evidencia en la solicitud el acceso al Datacenter • Para el III cuatrimestre de 2023, adicional a los 8 solicitudes sin acceso al Datacenter, entre los usuarios autorizados se evidencia que en la sede operativa registra Leonardo Pulido Duarte, quien no aparece como contratista en Orfeo, no se encontró formato de gestión de credenciales ni se evidenció un caso de mesa de ayuda con su solicitud de acceso. • Para el I cuatrimestre de 2024, de 10 solicitudes revisadas, en 3 que corresponden al 30%, en el formato de gestión de credenciales no se evidencia la solicitud de acceso para el Datacenter. • Para el II cuatrimestre de 2024, de 10 solicitudes revisadas, en 4 que corresponden al 40%, en el formato de gestión de credenciales no se evidencia la solicitud de acceso para el Datacenter.

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV



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

FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO

CÓDIGO: CEI-FM-022

VERSIÓN: 1

FECHA DE APLICACIÓN: NOVIEMBRE 2023

Auditoría al Modelo de Seguridad y Privacidad de la Información MSPi

Moderado	Hallazgo2: Debilidades en la ejecución de controles internos para aprobar y publicar los activos de información Durante el ejercicio de auditoría se observó que entre la OTI, la OAP, Gestión Jurídica y el proceso de Gestión Documental adelantaron la actualización de los activos de información para la vigencia 2023, este proceso finalizó en el mes de julio de 2023, sin embargo no se actualizó la resolución de actualización y aprobación de los activos de información y del índice de información clasificada y por lo tanto, no se realizó la publicación en el link de transparencia de la Unidad ni el portal de datos abiertos.
Moderado	Hallazgo3: Incumplimiento de las responsabilidades establecidas en las Políticas Generales de Tecnología y Seguridad de la Información por parte de GTHU para los servidores públicos En el documento EGTI-DI-001 - Políticas Generales de Tecnología y Seguridad de la Información y Comunicaciones V5, están definidas algunas responsabilidades para Gestión del Talento Humano, las cuales no son ejecutadas por el proceso.
Moderado	Hallazgo4: Debilidades en la implementación de controles internos para el reporte oportuno de novedades a la OTI por parte de Gestión del Talento Humano Para el periodo auditado según el reporte de novedades remitido por GTHU y verificado contra el Directorio Activo se evidenció que de la muestra seleccionada (20 novedades de funcionarios de planta), el 15% que corresponde a 2 licencias por incapacidad de 14 días y una licencia de luto, no fueron reportadas a la OTI para la inactivación de credenciales.
Moderado	Hallazgo5: Debilidades en la implementación de controles internos para evitar accesos no autorizados Durante el ejercicio de auditoría se realizó un escaneo a la red corporativa donde con las credenciales del auditor se logró tener acceso a información sensible compartida en elementos activos de red sin la protección adecuada.
Moderado	Hallazgo6: Debilidades en la implementación de controles internos para restringir el acceso en los dispositivos biométricos De una muestra de 16 novedades de retiro de funcionarios de planta se evidenció que las bases de datos de los biométricos no se actualizaron oportunamente, lo mismo fue evidenciado para una muestra de 6 contratistas que finalizaron contrato durante el periodo auditado.
Moderado	Hallazgo7: Inconsistencias entre el inventario de activos tecnológicos reportado por GREF y la OTI Al cruzar el inventario de GREF con el de la OTI para una muestra de 176 elementos se identificaron las siguientes inconsistencias: Para 40 (23%) no se encontró una placa que coincida con el inventario de GREF, para 104 (59%) elementos no coincide el estado del activo en la OTI con el registrado en almacén y 152 (86%) activos difieren en el responsable asignado entre la OTI y almacén.
	Observación1: Oportunidad de mejora en el cumplimiento de requisitos de autorización para ejecutar los controles de cambio De una muestra de 25 controles de cambio realizados durante el periodo auditado se evidenciaron 4 que corresponden a cambios a nivel de software donde el formato no cuenta con la autorización del líder de desarrollo.
	Observación 2: Oportunidad de mejora en el control Depuración usuarios Office 365 y OracleCloud Según lo observado por la auditoría se evidenció que el control se ejecuta como está diseñado, se realiza la depuración de los usuarios según las novedades de ingreso y egreso y se genera la respectiva acta. Sin embargo, en las actas "Revisión Roles de Usuario Oracle Cloud", generadas para el I y II cuatrimestre de 2024, con fechas del 29 de febrero y 28 de junio, en los usuarios

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV

 ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial	FORMATO - INFORME DE AUDITORÍA INTERNA EJECUTIVO	
	CÓDIGO: CEI-FM-022	VERSIÓN: 1
	FECHA DE APLICACIÓN: NOVIEMBRE 2023	

Auditoría al Modelo de Seguridad y Privacidad de la Información MSPI	
	administradores de base de datos registra el Ing. Giovanni Sarta, quien se retiró de la entidad el 31/01/2024 y en la bitácora de infraestructura aún registra como usuario activo.
	Observación3: Oportunidad de mejora para garantizar el cumplimiento de los lineamientos de la política de contraseñas y antivirus actualizados en los equipos de cómputo de la entidad Respecto al almacenamiento de las contraseñas de la sede Administrativa 7 de 12, SI, de la sede operativa de 8, 5 tienen almacenadas las contraseñas, De la sede de producción de 8, 3 tienen almacenadas las contraseñas tanto para el correo electrónico como para los aplicativos que usan a diario. De 8 equipos revisados en la sede de producción, se evidenció que 7 equipos tienen instalado el antivirus Bitdefender pero está desactualizado y 1 equipo no tiene instalado antivirus. De los 8 equipos revisados en la sede operativa, 4 tienen instalado el antivirus Bitdefender pero está desactualizado

4. PLAN DE MEJORAMIENTO

El auditor radicó en Orfeo el informe final de auditoría a través del radicado 20241600300653 con fecha 25 de noviembre de 2024.

Los procesos auditados cuentan con 8 días hábiles para suscribir el plan de mejoramiento y remitirlo vía memorando a la Oficina de Control Interno. Una vez remitido se sube al aplicativo CHIE y se realizará seguimiento de manera periódica.

FIRMA DEL INFORME DE AUDITORÍA:		
FECHA DE APROBACIÓN:		
NOMBRE	RESPONSABILIDAD	FIRMA
Juan Hernando Lizarazo Jara	Jefe Oficina de Control Interno	
Ana Josefa Carreño Pérez	Auditor Líder	

Remitido mediante memorando 20241600302423 el 26 de noviembre de 2024

La impresión de este documento se considera Copia No Controlada La versión vigente se encuentra en la intranet SISGESTION de la UAERMV