Comercio, Industria y Turismo

OFICINA DE CONTROL INTERNO
OCI-037-2024

Informe Final Auditoría Interna Riesgos de Seguridad y Privacidad de la Información 2024.

Aprobó: Angela Mónica Castro Mora - Jefe Oficina de Control Interno

Elaboró: Carlos Andres Valoyes Palacios – Contratista.

Fecha emisión: 26 de Diciembre de 2024

TRD – 107-34,16

CONTENIDO

1. UNIDAD OBJETO DE AUDITORÍA, EVALUACIÓN O SEGUIMIENTO

Informe Auditoría Interna Riesgos de Seguridad y Privacidad de la Información 2024.

2. RESPONSABLE UNIDAD OBJETO DE AUDITORÍA, EVALUACIÓN O SEGUIMIENTO

Jefe Oficina de Sistemas de Información.

3. OBJETIVOS

3.1 GENERAL

Evaluar la eficacia de los controles establecidos para los riesgos de seguridad y privacidad de la información del Ministerio de Comercio, Industria y Turismo.

3.2 ESPECÍFICOS

Verificar la implementación de los controles establecidos para los riesgos de seguridad y privacidad de la información.

Revisar los informes de seguimiento a los riesgos de seguridad y privacidad de la información publicados por el proceso.

4. ALCANCE

La auditoría interna comprendió los controles asociados a los activos de información de software, infraestructura y hardware.

5. CRITERIOS DE LA AUDITORIA, EVALUACIÓN O SEGUIMIENTO

NTC ISO IEC 27001:2022
GTI-DE-002 Manual de políticas de seguridad y privacidad de la información.
GTI-DE-003 Manual del sistema de gestión de seguridad y privacidad de la información.
DE-001 Guía de Activos de Información.

GTI GTI-DE-006 Guía para el Análisis de Eventos e Incidentes de Seguridad y Privacidad de la Información.
GTI-PR-002 Gestión Operativa TI.
GTI-PR-003 Gestión de Información.
GTI-PR-004 Gestión de incidentes de seguridad y privacidad de la información.
GTI-PR-014 Control acceso servicios TI.
GTI-FM-024 Matriz riesgos de seguridad y privacidad de la información.
DE-DR-001 Política y metodología para la administración de riesgos.
Guía de Administración del Riesgo del DAFP -V6 Nov 2022.
Decreto 767 del 16 de mayo de 2022.

6. METODOLOGÍA DE LA AUDITORÍA

Para la evaluación de los controles de software, infraestructura y hardware, se utilizaron las siguientes técnicas de auditoría:

Inspección	Observación	Entrevistas
• Se verificó la documentación relacionada con las evidencias del seguimiento a los controles de los riesgos de seguridad y privacidad de la información.	• Se realizó visita al centro de cableado, Datacenter, centro de cómputo y salón de ventilación los días 4, 5 y 6 de diciembre del 2024.	• Se realizaron entrevistas con el personal para evaluar cómo se aplican y gestionan los controles.

7. RESULTADOS DE LA AUDITORÍA, EVALUACION O SEGUIMIENTO

En cumplimiento a la Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones", la Oficina de Control Interno llevó a cabo la Auditoria Interna de acuerdo a la establecido en la actividad No. 8 del

Procedimiento ES-FM-004 Informe de auditoría de gestión y demás disposiciones normativas vigentes.

Durante la verificación realizada, se evidenció lo siguiente:

Observación No. 1: Cierre de Casos.

CONDICIÓN:

El caso 38456, relacionado con la creación de usuarios y acceso a aplicaciones para un contratista y una servidora de planta, no fue documentado en la herramienta ARANDA Mesa de Ayuda, respecto a la solución implementada y el cierre del caso.

CRITERIO:

NTC ISO IEC 27001:2022:

8 Tecnología.

A. 8.15 Registros de eventos.

Control:
Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.

CAUSA:

Posible falta de control o seguimiento en la gestión de incidentes.

CONSECUENCIA:

Riesgos o fallos no identificados que pueden afectar la integridad, confidencialidad y disponibilidad de la información.

Observación No. 2: Mantenimiento Preventivo.

CONDICIÓN:

Se evidenció que el centro de cableado del piso 2, ubicado frente al Tablero UPS Tomas de energía ininterrumpida, presenta un reporte de mantenimiento preventivo con la última actividad registrada el 7 de junio de 2022. No se encontró evidencia de programación de mantenimiento posterior, ni de la renovación del contrato, el cual venció el 31 de julio de 2022.

En el Datacenter, el Tablero UPS Tomas de energía ininterrumpida - Marca SCHNEIDER, presenta la misma situación.

CRITERIO:

NTC ISO IEC 27001:2022:

7. Infraestructura

A. 7.13 Mantenimiento de los equipos

Control:
Los equipos deben recibir un mantenimiento correcto que asegure la disponibilidad, integridad y confidencialidad de la información.

CAUSAS:

El contrato de mantenimiento para el sistema UPS y el cableado venció el 31 de julio de 2022 y no se ha renovado.

CONSECUENCIAS:

Riesgo de fallos en el suministro de energía en caso de corte o fluctuaciones eléctricas.

Observación No. 3: Comunicación de los Riesgos.

CONDICIÓN:

No se evidenció registro de la socialización de los riesgos asociados a la falta de mantenimiento preventivo de los Tableros UPS tomas de energía ininterrumpida y las posibles afectaciones a los servicios críticos de información.

CRITERIO:

NTC ISO IEC 27001:2022:
7.4 Comunicación: La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) con quién comunicar;

d) cómo comunicar.

CAUSAS:

Falta de un responsable o equipo encargado de la comunicación de riesgos.

Recursos priorizados en licenciamiento y aplicaciones en lugar de actividades críticas de mantenimiento.

CONSECUENCIAS:

Fallas o problemas técnicos, afectando la operatividad de los servicios.

Fallas en los sistemas de energía.

Interrupciones o pérdidas de datos.

Observación No. 4: Gestión de Accesos.

CONDICIÓN:

Se evidenció que un contratista el 25 octubre de 2024, solicitó acceso para ingresar a la red de aplicaciones y realizar una validación de permisos en la IP 172.18.0.197 – EstudiosEconomicos. Al revisar el caso en la herramienta Mesa de Ayuda (Sistema ARANDA), se observó que no está registrada la solicitud.

CRITERIO:

Procedimiento GTI-PR-014 Control de accesos a servicios TI, define:

Actividad No. 1 (H) Solicitud Requerimiento de acceso: El registro de la solicitud de acceso se realiza en la Mesa de Ayuda por medio de:

- Mintranet> Servicios> Soporte Técnico

(http://helpdesk.mincit.gov.co/ASDKV8/Login.aspx)

- Correo electrónico soportetecnico@mincit.gov.co

- Comunicándose a la extensión número 2291

La herramienta Mesa de Ayuda genera automáticamente un número de CASO para requerimiento.

NTC ISO IEC 27001:2022:

8 Tecnología.

A. 8.15 Registros de eventos.

Control:
Se deben generar, proteger, almacenar y analizar los registros de las actividades, excepciones, fallos y otros eventos relevantes.

CAUSA:

Posible falta de control o supervisión del proceso de registro de solicitud.

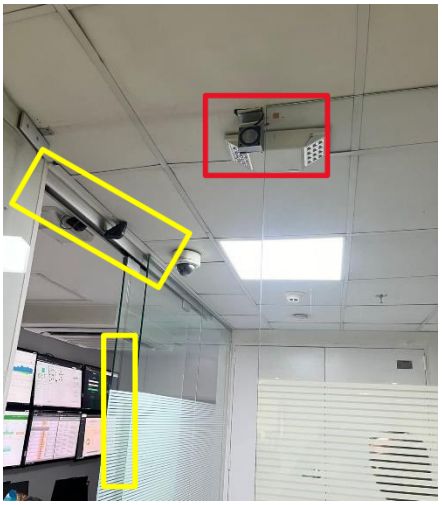
CONSECUENCIA:

Riesgos o fallos no identificados que pueden afectar la integridad, confidencialidad y disponibilidad de la información.

Observación No. 5: Controles de acceso físico en el Datacenter y Centro de Cómputo.

CONDICIÓN:

La puerta de vidrio de cierre magnético, que da acceso al Datacenter ubicada en la Oficina de Sistemas de Información en el piso 2, no funciona correctamente, permitiendo el ingreso sin restricciones. La puerta de acceso al centro de cómputo, donde se encuentran 10 pantallas de Video Walls para monitoreo de los sistemas de información y demás aplicaciones, no tiene restricción de acceso.



NOTA: La señalización en color rojo, hace referencia al dispositivo de cierre magnético, el color amarillo, puerta de acceso pantallas de Video Walls.

CRITERIOS:

NORMA NTC ISO/IEC 27001:2022:

7. Infraestructura.

A. 7.2 Controles físicos de entrada.

Control:

Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.

CAUSA:

Falta de mantenimiento en los sistemas de cierre magnético de las puertas.

Falta de monitoreo de controles de acceso físico en áreas críticas.

CONSECUENCIA:

Riesgo de acceso no autorizado a áreas críticas del Datacenter y el Centro de cómputo.

Potenciales fugas de información sensible.

Observación No. 6: Uso del Espacio en Datacenter.

CONDICIÓN:

En el centro de ventilación dentro del Datacenter, se evidenció almacenamiento de elementos no relacionados con la operación (cajas, cables, porrón de agua), bolsas tapando los sensores contra incendios y espacios con humedad.

NOTA: En la imagen No. 1 se muestra una bolsa tapando el sensor contra incendios, en la imagen No. 2 se muestra cajas, cables, etc.

CRITERIOS:

NORMA NTC ISO/IEC 27001:2022:

7. Infraestructura.

A 7.5 Protección contra las amenazas físicas y ambientales.

Control: Se debe diseñar e implementar una protección a las infraestructuras contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionadas o no.

CAUSA:

La falta de un protocolo para el almacenamiento y uso del espacio en el Datacenter.

CONSECUENCIA:

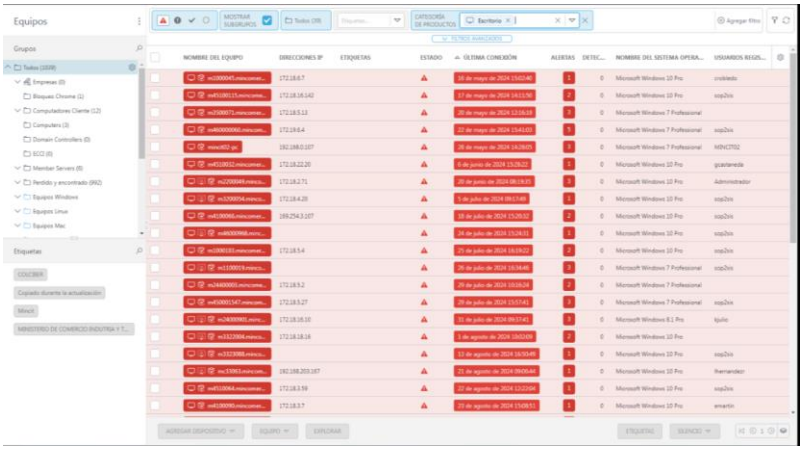
Riesgo de incendio.

Interrupción del servicio.

Observación No. 7: Alerta de Seguridad.

CONDICIÓN:

En el centro de cómputo, donde se encuentran las 10 pantallas de Video Walls, se evidenció un reporte con 73 Registros de Alertas de Seguridad por Antivirus en diferentes equipos de cómputo distribuidos en varios pisos del MINCIT. Se observó que las fechas y horas de última conexión son antiguas: 16 de mayo de 2024 a las 15:04 y 20 de junion de 2024 a las 13:18, lo que indica que no están actualizados recientemente.



Nota: La imagen muestra: Nombre equipos, Direcciones IP, estado, Última Conexión, entre otros.

CRITERIOS:

NORMA NTC ISO/IEC 27001:2022:

8. Tecnología

A 8.19 Instalación del software en sistemas en producción.

Control:
Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas en producción.

CAUSA:

El software antivirus puede no estar actualizado o correctamente configurado.

CONSECUENCIA:

Potencial interrupción de los servicios tecnológicos debido a infecciones o ataques informáticos.

8. CONCLUSIONES

En el desarrollo de la auditoría interna a los controles de los activos relacionados con software, infraestructura y hardware se identificaron controles que se deben fortalecer para garantizar la gestión de los riesgos de seguridad y privacidad de la información. Las observaciones identificadas evidencian debilidades en el seguimiento, cierre de casos, el mantenimiento preventivo de infraestructuras críticas, la gestión de accesos, los controles de acceso físico, el uso adecuado de los espacios en el Datacenter y la respuesta a alertas de seguridad.

9. RECOMENDACIONES

Reparar la puerta de acceso.

Despejar el Datacenter de elementos no operativos.

Implementar controles para asegurar el registro y cierre de casos.

10. PLAN DE MEJORAMIENTO (DE REQUERIRSE)

Formular el plan de mejoramiento para las observaciones, identificando las medidas correctivas y las preventivas.