República de Colombia Ministerio de Igualdad y Equidad INSOR Instituto Nacional para Sordos	**PROCESO EVALUACIÓN Y CONTROL**	CÓDIGO: FOEC08
		VERSIÓN: 3
	INFORME DE SEGUIMIENTO A LA GESTIÓN INSTITUCIONAL	FECHA:15/03/2024

NOMBRE DEL INFORME	**Informe de Seguimiento y Evaluación Plan de Mejoramiento Segundo Trimestre 2025**	**FECHA DE ELABORACIÓN DEL INFORME**		
		Día	**Mes**	**Año**
		30	08	2025
RESPONSABLE PROCESO AL QUE SE REALIZA EL SEGUIMIENTO	**Proceso Oficina Asesora de Planeacion y Sistemas**			
PERIODO DEL SEGUIMIENTO	**FECHA INICIAL:** 01 abril 2025			
	FECHA FINAL: 30 junio 2025			
OBJETIVO DEL SEGUIMIENTO	Realizar seguimiento y evaluación de las acciones contempladas en el Plan de Mejoramiento suscrito por el proceso Oficina Asesora de planeación y Sistemas			

DESARROLLO DEL SEGUIMIENTO

1. RESULTADO DEL SEGUIMIENTO

La oficina de Control Interno del INSOR, recibió el Plan de Mejoramiento, con corte al 30 de junio de 2025, el cual contiene 13 hallazgos.

El ejercicio de seguimiento y evaluación de las acciones de mejora propuestas para dar cumplimiento a las recomendaciones realizadas por la auditoria al proceso de Gestión de TIC, en las vigencias 2019, 2021, 2022 y 2023.

Una vez realizado el seguimiento se identificaron las siguientes fortalezas:

- Disposición del recurso humano adscrito a la Oficina Asesora de Planeación y Sistemas, para atender las reuniones y las consultas requeridas, así como la oportunidad de respuestas de las mismas.

- Diligencia para realizar las actividades del Plan de Mejoramiento

Luego de realizado el seguimiento y evaluación al plan de mejoramiento, se obtuvo el siguiente resultado sobre las acciones de mejoramiento, para los 13 hallazgos reportados.

a. Acciones de Mejora atendidas:

HALLAZGO 2022-GT-06

En atención al seguimiento del hallazgo 2022-GT-06, se realizó la verificación de las evidencias entregadas como parte de las acciones de mejoramiento comprometidas. Entre los documentos revisados se encuentran:

•ODGT03: Catálogo de Servicios de TIC
•FOGT22: Catálogo de Sistemas de Información del INSOR
•FOGT24: Matriz Catálogo de Servicios TI 2025

•FOGT20: Análisis de Impacto al Negocio (BIA) – Versión 2
•PLGT05: Plan de Continuidad del Negocio
•PRGT05: Procedimiento de Continuidad del Negocio
•Actividades documentadas de Transferencia de Conocimiento
•Encuesta de disponibilidad y recuperación de servicios tecnológicos del INSOR
•Lineamientos para el Análisis de Impacto al Negocio
•ODGT11: Dominio de los Sistemas de Información del INSOR

Con base en el análisis de estas evidencias, se concluye que las acciones de mejora han sido ejecutadas de manera satisfactoria. Se evidencia el desarrollo del Plan de Continuidad del Negocio, así como la ejecución de actividades orientadas a la actualización y fortalecimiento de la transferencia de conocimiento en el área de Tecnologías de la Información.

Estas acciones están alineadas con lo establecido en el Plan de Mejoramiento, específicamente con el compromiso de: "Desarrollar el plan de continuidad de la entidad tomando como referencia las guías del MINTIC y las plantillas entregadas por el MEN."

En consecuencia, y dado el cumplimiento verificable de las acciones correctivas, se procede a cerrar el hallazgo.

HALLAZGO 2022-GT-18

En el marco del proceso de seguimiento a las acciones de mejoramiento derivadas del hallazgo identificado como 20-22-GT-18, se evaluó el cumplimiento de las actividades correctivas establecidas, las cuales fueron:

1.Realización de mesa de trabajo con el GIT de Bienes y Servicios, con el objetivo de incluir cláusulas específicas en el contrato suscrito con el proveedor de tecnología SOLGEIN INTERNATIONAL SYSTEMS S.A.S.

2.Revisión y ajuste de la política de seguridad de la información aplicable a terceros, conforme a los lineamientos institucionales.

Como resultado del proceso de verificación, se obtuvieron las siguientes evidencias:

•Inclusión de cláusulas contractuales: Se constató, mediante comunicación oficial enviada al GIT de Bienes y Servicios, la incorporación de las obligaciones recomendadas en el informe de auditoría. Estas cláusulas fueron efectivamente integradas en el contrato vigente identificado como 131-2025, suscrito con el proveedor mencionado.

•Revisión de políticas de seguridad: Se verificó la actualización del Manual de Políticas de Seguridad y Privacidad de la Información, específicamente en el numeral 8.2, correspondiente a la política de seguridad y privacidad frente al acceso por parte de terceros. Esta revisión garantiza la alineación normativa con los riesgos identificados.

Con base en lo anterior, la Oficina de Control Interno concluye que las acciones de mejoramiento fueron implementadas de manera efectiva, cumpliendo en su totalidad con los compromisos adquiridos. Se evidencia la eliminación de la causa raíz del hallazgo, por lo cual se procede a cerrar el estado del hallazgo 20-22-GT-18.

HALLAZGO 2022-GT-20

Como parte del proceso de seguimiento al hallazgo identificado como 2022-GT-20, se realizó la verificación de las acciones de mejoramiento implementadas, con el objetivo de evaluar su efectividad frente a la mitigación de la causa raíz que originó la observación.

Las evidencias presentadas incluyen:

•Procedimiento de Seguimiento de Infraestructura
•Informes de Infraestructura correspondientes al primer y segundo trimestre de 2025
•Procedimiento de Administración y Monitoreo de Servicios de TI

Tras el análisis de la documentación y registros aportados, la Oficina de Control Interno concluye que la acción de mejoramiento ha sido cumplida de manera efectiva, evidenciando la ejecución del 100% de las actividades propuestas y la eliminación de la causa raíz del hallazgo.

En consecuencia, se determina procedente el cierre formal del hallazgo 2022-GT-20, al verificarse que los controles implementados contribuyen de manera adecuada al fortalecimiento del monitoreo y gestión de la infraestructura tecnológica, alineándose con los objetivos de control establecidos por la Entidad.

HALLAZGO 2022-GT-21

En relación con el hallazgo identificado como 2022-GT-21, correspondiente a la necesidad de configurar adecuadamente las VLAN con el fin de restringir escaneos de red hacia direcciones IP fuera del segmento asignado a cada dispositivo, se realizó la verificación de las acciones correctivas definidas en el Plan de Mejoramiento.

Las acciones contempladas incluyeron:

•Diseño del diagrama de VLANs y aplicación de la configuración correspondiente en los dispositivos de red (switches), conforme a dicho diseño.
•Ejecución de pruebas técnicas mediante herramientas especializadas para validar la efectividad de la segmentación y el aislamiento de tráfico entre VLANs.

Tras la revisión de las evidencias documentales y técnicas presentadas, se constató el cumplimiento efectivo y verificable de las medidas implementadas. En consecuencia, y conforme a los criterios establecidos para el cierre de hallazgos, se procede a cerrar formalmente el hallazgo 2022-GT-21.

HALLAZGO 2022-GT-22

En cumplimiento del proceso de seguimiento al hallazgo identificado como 2022-GT-22, se realizó la verificación de las acciones de mejoramiento implementadas, con el propósito de evaluar su efectividad frente a la mitigación de la causa raíz que originó la observación.

Las evidencias presentadas incluyen:

•Protocolo para la Custodia y Gestión de Contraseñas Críticas
•Procedimiento de Seguimiento de Infraestructura
•Informes de Infraestructura correspondientes al primer y segundo trimestre de 2025
•Procedimiento de Administración y Monitoreo de Servicios de TI

Tras el análisis de la documentación aportada, la Oficina de Control Interno concluye que las acciones de mejoramiento han sido cumplidas de manera efectiva, evidenciando la ejecución del 100% de las actividades propuestas y la eliminación de la causa raíz del hallazgo.

En consecuencia, se determina procedente el cierre formal del hallazgo 2022-GT-22, al verificarse que los controles implementados fortalecen la gestión de contraseñas críticas y el monitoreo de la infraestructura tecnológica, contribuyendo al cumplimiento de los objetivos de control definidos por la Entidad.

HALLAZGO 2022-GT-23

En seguimiento al hallazgo identificado como 2022-GT-23, relacionado con la necesidad de configurar políticas de seguridad en el firewall y en el dominio para restringir la descarga de archivos ejecutables o de instalación, se realizó la verificación de las acciones correctivas establecidas en el Plan de Mejoramiento.

Las actividades ejecutadas incluyeron:

•Implementación de políticas de restricción en el firewall, orientadas a bloquear la descarga de archivos con extensiones asociadas a ejecutables.
•Incorporación de controles adicionales en las políticas de dominio, incluyendo restricciones de seguridad complementarias en el firewall, antivirus y configuración de grupo (GPO), con el objetivo de fortalecer la postura de seguridad frente a amenazas derivadas de descargas no autorizadas.

Tras el análisis de las evidencias técnicas y documentales presentadas, se constató el cumplimiento efectivo y verificable de las acciones correctivas. En virtud de lo anterior, y conforme a los criterios establecidos para el cierre de hallazgos, se procede a cerrar formalmente el hallazgo 2022-GT-23

HALLAZGO 2022-GT-25

En seguimiento al hallazgo identificado como 2022-GT-25, se realizó la verificación del cumplimiento de las acciones de mejoramiento establecidas, con el objetivo de validar la implementación efectiva de los controles propuestos y su alineación con las políticas institucionales de seguridad de la información.

Las acciones revisadas fueron las siguientes:

1.Revisión de la política de seguridad de medios extraíbles: Se verificó la actualización y aplicación de las disposiciones contenidas

en el numeral 8.12 – Política de administración y seguridad de los medios de almacenamiento, específicamente el literal relacionado con la Administración de Medios Informáticos Removibles, incluido en el documento MNGT05: Manual de Políticas de Seguridad y Privacidad de la Información.

2.Generación del informe de configuración de políticas de seguridad para el dominio: Se constató la elaboración del informe técnico que documenta la configuración vigente de las políticas de seguridad aplicadas en el entorno de dominio, evidenciando el cumplimiento de los parámetros definidos por la organización.

3.Documentación de usuarios aprobados con privilegios: Se revisó el registro formal de usuarios con privilegios especiales, validando que se encuentra debidamente documentado y aprobado conforme a los procedimientos establecidos.

Las evidencias aportadas incluyen capturas de pantalla que demuestran la aplicación de restricciones sobre dispositivos USB, así como la implementación de directivas de seguridad específicas (Directiva de Seguridad y Directiva INSOR), las cuales respaldan la ejecución de las acciones correctivas.

Con base en la revisión documental y técnica realizada, y dado el cumplimiento verificable de las acciones de mejoramiento, se determina procedente el cierre formal del hallazgo 2022-GT-25.

b. Acciones de Mejora en proceso, para las que se recomienda mantener en estado: "Abierta".

HALLAZGO 2022-GT-13

En seguimiento a las acciones definidas para atender el hallazgo, se ha evidenciado la actualización del análisis de Impacto al Negocio (BIA), el cual ha sido alineado con los lineamientos institucionales.

Este análisis permitió establecer los tiempos de recuperación, la tolerancia a la pérdida de datos y el nivel de disponibilidad requerido para cada servicio crítico.

Asimismo, se ha logrado la articulación entre los siguientes componentes del Sistema de Gestión de Continuidad del Negocio del INSOR:

•PRGT05 – Procedimiento de Continuidad del Negocio
•FOGT20 – Análisis de Impacto al Negocio (BIA)
•PLGT05 – Plan de Continuidad del Negocio

Dicha articulación garantiza coherencia entre el análisis de impacto, los procedimientos operativos y el plan estratégico de continuidad, orientando todos los esfuerzos hacia la implementación efectiva de un sistema de continuidad del negocio institucional.

No obstante, se identificó que aún no se han ejecutado las pruebas integrales del Plan de Continuidad del Negocio, ni se han documentado los protocolos y resultados correspondientes. Esta situación fue señalada en el análisis de causa del hallazgo original, el cual indica: "Falta ejecutar las pruebas integrales al plan y documentar los protocolos y resultados, contemplar los lineamientos ISO 27001:2013, cláusula 17.1.3: Verificación, revisión y evaluación de la continuidad de la seguridad de la información."
Adicionalmente, esta acción está contemplada en el Plan de Mejoramiento bajo el compromiso de "Implementar el Plan de Continuidad del Negocio". Por lo tanto, el estado del hallazgo se mantiene abierto, y se recomienda proceder con la ejecución de las pruebas, así como la documentación formal de los resultados, con el fin de avanzar hacia una implementación integral y verificable del Plan de Continuidad del Negocio del INSOR.

HALLAZGO 2022-GT-14

En el marco del proceso de seguimiento a las acciones de mejoramiento implementadas para atender el hallazgo relacionado con la gestión de copias de seguridad, se realizó la verificación documental y técnica de las evidencias entregadas, las cuales incluyen:

•Plan de Copias de Seguridad
•Formato Único del Plan de Copias Backup
•Guía para Copias de Seguridad
•Instructivo para la Generación de Copias de Respaldo de la Información
•Formato Único de Realización de Copias de Seguridad

Si bien dichas evidencias demuestran la ejecución formal de las acciones propuestas, se identificó que actualmente no se están realizando las copias de seguridad conforme a lo establecido en la "Guía para Copias de Seguridad", específicamente en lo referente al respaldo de las ubicaciones: "Escritorio", "Mis Documentos" y "Carpetas Compartidas" de los usuarios del INSOR.

La guía establece de manera explícita en sus lineamientos generales: "Es responsabilidad de cada usuario almacenar la información institucional en las rutas establecidas por la Oficina Asesora de Planeación y Sistemas (Escritorio, Mis Documentos, carpetas compartidas)."

Asimismo, se indica:
"La Oficina Asesora de Planeación y Sistemas no se hace responsable por la pérdida de información que no sea guardada en estas ubicaciones."

Y adicionalmente:
"Se debe respaldar las carpetas de los usuarios ('Escritorio' y 'Mis Documentos'). En estas carpetas se debe respaldar únicamente la información generada por cada usuario en sus labores diarias."

Con base en el análisis realizado por la Oficina de Control Interno, se concluye que la acción de mejoramiento es inefectiva, dado que, aunque se ejecutaron en su totalidad las actividades propuestas, no se elimina la causa raíz del hallazgo, al no cumplirse el objetivo de control definido en el numeral 12.3 del Manual de Seguridad y Privacidad de la Información (MSPI): "Realizar copias de seguridad periódicas", con el propósito de asegurar que las copias se realicen de manera regular y consistente, garantizando la continuidad del negocio y la recuperación de la información mediante la implementación de mecanismos robustos y bien gestionados.

En consecuencia, se determina que el estado del hallazgo permanece abierto, hasta tanto se evidencie la ejecución efectiva de las copias de seguridad conforme a los lineamientos establecidos, permitiendo así minimizar el riesgo de pérdida de información y asegurar la continuidad operativa de la Entidad.

HALLAZGO 2022-GT-15

En el marco del proceso de seguimiento al hallazgo identificado como 2022-GT-15, se llevó a cabo la verificación de las acciones de mejoramiento implementadas, con el fin de evaluar su efectividad frente a la mitigación de la causa raíz que originó la observación.

Como evidencia de cumplimiento, se presentó el Formato Único de Realización de Copias de Seguridad, el cual contempla el control sobre la ejecución de respaldos y la realización de restauraciones aleatorias.

No obstante, se evidenció que no se están ejecutando pruebas de restauración de la información, tal como lo establece la "Guía para Copias de Seguridad", en el apartado correspondiente al "Plan de Pruebas de Restauración", donde se indica expresamente que: "Las pruebas de restauraciones se realizan al menos una cada 30 días."

La ausencia de estas pruebas representa un incumplimiento del objetivo de control definido en el numeral 12.3 del Manual de Seguridad y Privacidad de la Información (MSPI), el cual establece: "Probar los procedimientos de restauración de la información", con el propósito de asegurar que dichos procedimientos funcionen correctamente, permitiendo garantizar la continuidad del negocio y la recuperación oportuna de la información institucional.

A pesar de que la acción propuesta fue ejecutada en su totalidad desde el punto de vista documental, la Oficina de Control Interno concluye que la acción es inefectiva, dado que no se elimina la causa raíz del hallazgo. La falta de pruebas periódicas de restauración

impide validar la integridad y disponibilidad de los respaldos, lo cual compromete la capacidad de respuesta de la Entidad ante incidentes que afecten la información crítica.

En consecuencia, se determina que el estado del hallazgo permanece Abierto, hasta tanto se evidencie la ejecución efectiva y periódica de las pruebas de restauración, conforme a los lineamientos establecidos, garantizando así la robustez del proceso de respaldo y la continuidad operativa de la Entidad.

HALLAZGO 2022-GT-19

Se verificó la ejecución del procedimiento PRGT-13: Procedimiento de Seguimiento a la Infraestructura Tecnológica, el cual establece los lineamientos para la revisión del estado de los componentes tecnológicos de la entidad, incluyendo servidores, sistemas de almacenamiento y equipos de red. Este procedimiento contempla la toma de acciones correctivas y ajustes necesarios, aplicables a todos los equipos que conforman la plataforma virtual, así como el control de dispositivos y equipos activos de red del INSOR.

Durante la revisión, se evidenció la elaboración de informes periódicos de monitoreo que permiten evaluar la disponibilidad y gestión de los siguientes servicios:

•Plataforma virtual basada en VMware
•Servidores bajo sistema operativo Windows (DC, WSUS, FILESERVER, APLICACIONES)
•Equipos de red: Switch de borde y Core
•Sistemas de almacenamiento

No obstante, se identificó que aún no se ha implementado la integración del monitoreo y control de eventos provenientes de las consolas de Firewall y antivirus, ni se han definido procedimientos ni correlacionadores de eventos que permitan una gestión centralizada y proactiva de estos componentes.

Esta situación limita el alcance del monitoreo, impidiendo lograr una supervisión integral de los eventos generados por todos los sistemas de información que conforman la plataforma tecnológica de la entidad.

Como consecuencia, persiste una brecha respecto al cumplimiento de los controles establecidos en la norma ISO/IEC 27001:2013, específicamente en los dominios:

•12.4: Registrar eventos y generar evidencias
•12.7: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales

Por lo tanto, el estado del hallazgo se mantiene abierto, y se recomienda avanzar en la implementación de mecanismos de integración para el monitoreo y control de eventos, así como en el diseño de procedimientos y correlacionadores que incluyan las consolas de seguridad (Firewall y antivirus), con el fin de fortalecer el modelo de gestión de eventos y cumplir con los requisitos normativos aplicables.

HALLAZGO 2022-GT-27

En el marco del proceso de seguimiento al hallazgo identificado como 2022-GT-27 se llevó a cabo la verificación de las acciones de mejoramiento implementadas, orientadas a fortalecer la organización y trazabilidad de la infraestructura de red en el Centro de Cómputo del INSOR.

Las evidencias presentadas corresponden a la ejecución de un plan de etiquetado y generación de diagramas en los closets de comunicaciones (racks), con el objetivo de facilitar la identificación de equipos, puntos de red y la localización de fallas.

Asimismo, se contempló la instalación de organizadores de cables para mejorar el orden y la eficiencia operativa en los espacios técnicos.

Sin embargo, tras la revisión de las evidencias visuales y documentales aportadas, se constató que la acción no ha sido ejecutada en su totalidad, ya que el etiquetado y la generación de diagramas en todos los closets de comunicaciones del Centro de Cómputo no se ha completado al 100%.

En consecuencia, la Oficina de Control Interno concluye que la acción es incumplida, y determina que el estado del hallazgo permanece Abierto, al no evidenciarse la implementación completa de las medidas correctivas necesarias para eliminar la causa raíz del hallazgo.

HALLAZGO 2022-GT-28

Como parte del proceso de seguimiento al hallazgo identificado como 2022-GT-28, se realizó la verificación de las acciones de mejoramiento orientadas a fortalecer la gestión de infraestructura de red en el Centro de Cómputo del INSOR.

Las evidencias presentadas corresponden a la implementación de un diagrama de distribución de puntos, equipos y elementos activos de red en los closets de cableado, con el objetivo de facilitar la rápida referenciación por parte del personal técnico y contratistas en situaciones de contingencia, mejorando así la eficiencia en la identificación y resolución de fallas.

No obstante, tras el análisis de las evidencias visuales y documentales aportadas, se constató que la acción no ha sido ejecutada en su totalidad, ya que el diagrama de distribución mencionado no se encuentra implementado en el 100% de los closets de cableado del Centro de Cómputo.

OBSERVACIONES-RIESGOS IDENTIFICADOS

HALLAZGO 2022-GT-13

1. Ausencia de pruebas integrales del Plan de Continuidad del Negocio: A pesar de que se ha logrado una adecuada articulación documental entre el Análisis de Impacto al Negocio (BIA), el procedimiento operativo y el Plan de Continuidad del Negocio, no se han ejecutado pruebas integrales que permitan validar la efectividad real del sistema implementado. Esta omisión representa una debilidad crítica en la verificación del modelo de continuidad, con los siguientes impactos:

- Genera incertidumbre sobre la capacidad institucional para recuperar servicios ante eventos disruptivos.
- Aumenta el riesgo de fallas en la restauración de procesos críticos, afectando la operación.
- Expone a la entidad a observaciones por parte de entes de control y auditorías externas, especialmente en el marco de exigencias contractuales y normativas.

2. Falta de documentación formal de protocolos y resultados de pruebas: No se ha evidenciado la existencia de registros que documenten la ejecución de pruebas del Plan de Continuidad del Negocio, ni los resultados obtenidos. Esta carencia impide verificar la trazabilidad, la eficacia de los procedimientos y el cumplimiento del ciclo de mejora continua exigido por el MSPI. Los impactos derivados de esta situación incluyen:

- Imposibilidad de demostrar cumplimiento normativo ante instancias de control interno y externo.
- Limitación para identificar oportunidades de mejora en los procesos de recuperación.
- Riesgo reputacional institucional por ausencia de evidencia que respalde la robustez del sistema de continuidad.

3. Riesgo de falsa percepción de cumplimiento: La existencia de documentos alineados y formalmente estructurados puede inducir a una percepción errónea de cumplimiento total, cuando en realidad no se ha validado su aplicabilidad mediante pruebas operativas. Esta situación representa un riesgo estratégico, con los siguientes impactos:

- Posibilidad de tomar decisiones basadas en información no verificada, comprometiendo la gestión institucional.
- Exposición ante incidentes sin capacidad de respuesta efectiva, debido a la falta de validación práctica.
- Potencial incumplimiento contractual con entidades públicas, al no garantizar la funcionalidad del sistema de continuidad en escenarios reales.

HALLAZGO 2022-GT-14

1. Ejecución incompleta de copias de seguridad conforme a los lineamientos institucionales: Si bien se cuenta con documentación formal que define el proceso de respaldo de información, se ha evidenciado que las copias de seguridad no se están realizando en las ubicaciones establecidas por la guía institucional, específicamente en las rutas "Escritorio" y "Mis Documentos". Esta omisión representa una falla crítica en la protección de la información generada por los usuarios, comprometiendo la integridad del sistema de respaldo.

Impactos identificados:
- Pérdida irreversible de información institucional relevante para la operación.
- Afectación directa a la continuidad de los servicios misionales.
- Riesgo reputacional por deficiencias en la gestión de datos y cumplimiento normativo.

---

2. Ineficacia de la acción de mejoramiento frente a la causa raíz del hallazgo: Aunque se ejecutaron las actividades propuestas en el plan de mejoramiento, estas no abordan de manera efectiva la causa raíz del hallazgo. La acción implementada no garantiza la protección integral de la información crítica, lo que limita el cumplimiento del objetivo de control establecido en el MSPI.

Impactos identificados:
- Persistencia del riesgo operativo asociado a la pérdida de información.
- Generación de una percepción errónea de cumplimiento institucional.
- Vulnerabilidad ante auditorías externas y requerimientos de entes de control.

---

3. Falta de corresponsabilidad en la gestión de la información por parte de los usuarios: La guía institucional establece que los usuarios son responsables de almacenar la información en rutas específicas para garantizar su respaldo. Sin embargo, no se evidencia la existencia de mecanismos de control, seguimiento o sensibilización que aseguren el cumplimiento de esta directriz, lo que genera una brecha en la gestión compartida de la seguridad de la información.

Impactos identificados:
- Riesgo de pérdida de información por errores humanos o desconocimiento de los lineamientos.

- Dificultad para establecer responsabilidades en caso de incidentes de seguridad.
- Debilitamiento de la cultura organizacional en materia de seguridad digital.

HALLAZGO 2022-GT-15

1. Ausencia de ejecución periódica de pruebas de restauración de respaldos: Si bien se cuenta con documentación formal que respalda la ejecución de copias de seguridad, se ha evidenciado el incumplimiento del "Plan de Pruebas de Restauración" establecido en la guía institucional, el cual exige la realización de pruebas al menos cada 30 días. Esta omisión representa una debilidad crítica en la validación de la integridad y disponibilidad de los respaldos.

Impactos identificados:

- Incertidumbre sobre la confiabilidad de los respaldos ante eventos de pérdida de información.
- Riesgo elevado de fallas en los procesos de recuperación de datos críticos.
- Vulnerabilidad operativa frente a incidentes tecnológicos, ciberataques o fallas sistémicas.

---

2. Ineficacia de la acción de mejoramiento frente a la causa raíz del hallazgo: La acción de mejoramiento fue ejecutada desde una perspectiva documental, sin que se haya abordado de manera efectiva la causa raíz del hallazgo. La ausencia de pruebas operativas impide validar la funcionalidad real de los procedimientos de restauración, lo que limita el cumplimiento del objetivo de control definido en el MSPI.

Impactos identificados:

- Persistencia del riesgo de pérdida de información institucional.
- Generación de una percepción errónea de cumplimiento normativo.
- Exposición de la entidad ante observaciones de auditoría y requerimientos de entes de control.

---

3. Compromiso de la continuidad operativa institucional: La falta de ejecución periódica de pruebas de restauración compromete la capacidad de la entidad para responder de manera efectiva ante incidentes que afecten la disponibilidad de la información crítica. Esta situación pone en riesgo la continuidad de los servicios esenciales y la estabilidad operativa.

Impactos identificados:

- Interrupción de procesos misionales y servicios institucionales.
- Pérdida de datos relevantes para la gestión pública.
- Afectación reputacional y posible incumplimiento de obligaciones contractuales.

HALLAZGO 2022-GT-19

1. Monitoreo incompleto de la infraestructura tecnológica: La ausencia de integración de eventos de seguridad (Firewall y antivirus) limita la visibilidad sobre amenazas potenciales y vulnerabilidades activas.

2. Falta de correlación de eventos críticos: Sin correlacionadores, los incidentes pueden pasar desapercibidos o no ser tratados oportunamente, aumentando el riesgo de afectación a la disponibilidad, integridad y confidencialidad de la información.

3. Incumplimiento normativo: Persisten brechas frente a los controles definidos en la norma ISO/IEC 27001:2013, especialmente en los dominios: 12.4: Registro de eventos y generación de evidencias y 12.7: Minimización del impacto de auditorías sobre sistemas operacionales.

4. Riesgo operativo y reputacional: La falta de supervisión integral puede derivar en incidentes no detectados que afecten servicios críticos, generando pérdida de confianza institucional.

HALLAZGOS 2022-GT-27

1. Falta de trazabilidad completa en la infraestructura de red: La ausencia de etiquetado y diagramas en todos los closets de comunicaciones impide una identificación rápida y precisa de equipos y conexiones.

2. Mayor tiempo de respuesta ante fallas o incidentes técnicos: La desorganización parcial dificulta la localización de puntos críticos, lo que puede retrasar la atención de eventos que afecten la disponibilidad de servicios.

3. Riesgo operativo por errores en la manipulación de cableado o dispositivos: La falta de organización física y documental puede generar desconexiones accidentales, configuraciones incorrectas o duplicidad de conexiones.

4. Limitaciones en auditorías técnicas y mantenimiento preventivo: Sin una documentación completa y actualizada, se dificulta la verificación del estado de la infraestructura y la planificación de mejoras.

HALLAZGO 2022-GT-28

1. Falta de trazabilidad completa en la infraestructura de red del Centro de Cómputo: La ausencia de diagramas en todos los closets de cableado impide una identificación rápida y precisa de equipos, puntos de red y elementos activos.

2. Mayor tiempo de respuesta ante contingencias o fallas técnicas: La falta de referenciación visual y documental dificulta la localización de fallas, lo que puede afectar la disponibilidad de servicios críticos.

3. Riesgo operativo por errores en la manipulación de cableado o dispositivos: La desorganización parcial puede generar desconexiones accidentales, configuraciones incorrectas o duplicidad de conexiones.

4. Limitaciones en auditorías técnicas y mantenimiento preventivo: Sin documentación completa y actualizada, se dificulta la verificación del estado de la infraestructura y la planificación de mejoras.

RECOMENDACIONES

HALLAZGO 2022-GT-13

1. Ejecutar Pruebas Integrales del Plan de Continuidad del Negocio:

- Realizar simulacros que contemplen escenarios reales de interrupción de servicios críticos, pérdida de datos, fallos de infraestructura y ciberataques.

- Incluir la participación de todas las áreas involucradas en el Plan de Continuidad del Negocio, para validar la coordinación operativa y la capacidad de respuesta institucional.

2. Documentar Protocolos y Resultados de las Pruebas:

- Registrar detalladamente los procedimientos aplicados, tiempos de recuperación, incidencias detectadas y acciones correctivas.

- Consolidar los resultados en un informe técnico que sirva como evidencia de cumplimiento y base para ajustes al plan.

3. Verificar la Continuidad de la Seguridad de la Información:

- Asegurar que durante las pruebas se mantengan los controles de seguridad sobre la información.

- Validar que los datos recuperados conserven su integridad, confidencialidad y disponibilidad.

4. Actualizar el Plan de Continuidad del Negocio según los Resultados:

- Incorporar las lecciones aprendidas y hallazgos de las pruebas en el Plan de Continuidad del Negocio, ajustando procedimientos, tiempos de recuperación y recursos asignados.

5. Establecer un Cronograma de Pruebas Periódicas:

- Definir una frecuencia mínima (anual o semestral) para la ejecución de pruebas integrales del Plan de Continuidad del Negocio.

- Incluir pruebas específicas para nuevos sistemas o servicios críticos que se incorporen.

6. Sensibilizar y Capacitar al Personal Clave:

- Realizar talleres prácticos sobre activación del Plan de Continuidad del Negocio, roles y responsabilidades, y respuesta ante incidentes.

- Asegurar que el personal conozca los protocolos y pueda actuar eficazmente en situaciones reales.

7. Reportar a la Alta Dirección:

- Informar sobre el estado actual del hallazgo, las acciones pendientes y la importancia estratégica de ejecutar las pruebas para garantizar la resiliencia institucional.

- Solicitar el respaldo institucional del INSOR, para la ejecución de pruebas y asignación de recursos necesarios.

HALLAZGO 2022-GT-14

1. Implementar mecanismos automatizados de respaldo para ubicaciones críticas del usuario:

- Configurar herramientas de respaldo que incluyan de forma predeterminada las rutas "Escritorio", "Mis Documentos" y "Carpetas Compartidas".

- Validar que estas ubicaciones estén correctamente mapeadas en los scripts o configuraciones de respaldo.

2. Establecer controles de verificación periódica del cumplimiento de la guía:

- Realizar auditorías internas mensuales para verificar que las copias de seguridad incluyan las ubicaciones definidas en la guía institucional.

- Documentar los resultados de estas verificaciones y tomar acciones correctivas inmediatas ante desviaciones.

3. Sensibilizar a los usuarios sobre el uso correcto de las rutas institucionales:

- Reforzar la responsabilidad del usuario en el almacenamiento de información institucional en las rutas establecidas.

- Implementar campañas de comunicación y capacitaciones sobre buenas prácticas de respaldo y uso de carpetas institucionales.

4. Revisar y ajustar la infraestructura tecnológica si es necesario:

- Evaluar si las herramientas actuales permiten respaldos completos y confiables de las ubicaciones definidas.

- Considerar la adquisición o configuración de soluciones más robustas si se identifican limitaciones técnicas.

5. Mantener el hallazgo abierto hasta evidenciar la ejecución efectiva:

- No cerrar el hallazgo hasta que se demuestre, mediante evidencia técnica verificable, que las copias de seguridad se están realizando conforme a los lineamientos establecidos en la guía institucional.

HALLAZGO 2022-GT-15

1. Ejecutar pruebas periódicas de restauración de información:

- Cumplir con la frecuencia establecida en la "Guía para Copias de Seguridad", realizando al menos una prueba de restauración cada 30 días.

- Incluir restauraciones parciales y completas, simulando distintos escenarios de pérdida de datos.

2. Documentar formalmente los protocolos y resultados de las pruebas:

- Registrar cada prueba en el Formato Único de Realización de Copias de Seguridad, incluyendo fecha, tipo de restauración, resultado, observaciones y responsables.

- Consolidar esta documentación en informes técnicos que sirvan como evidencia de cumplimiento y base para auditorías internas.

3. Establecer indicadores de cumplimiento y alertas:

- Definir métricas que permitan monitorear el cumplimiento del plan de pruebas de restauración.

- Configurar alertas automáticas ante la omisión o retraso en la ejecución de pruebas.

4. Integrar las pruebas de restauración al ciclo de gestión de riesgos tecnológicos:

- Evaluar el impacto de no realizar pruebas en el mapa de riesgos institucionales.

- Recalcular el riesgo residual si se confirma que los respaldos no son verificables ni recuperables.

5. Sensibilizar al equipo técnico sobre la importancia de las pruebas:

- Realizar sesiones de capacitación sobre la relación entre restauración de información, continuidad operativa y cumplimiento normativo.

- Reforzar el vínculo entre el MSPI, la ISO/IEC 27001:2013 y las prácticas de respaldo efectivas.

6. Mantener el hallazgo abierto hasta evidenciar cumplimiento efectivo:

- No cerrar el hallazgo hasta que se demuestre, mediante evidencia técnica verificable, que las pruebas de restauración se están realizando conforme a los lineamientos establecidos.

HALLAZGO 2022-GT-19

1. Integrar las consolas de seguridad al sistema de monitoreo centralizado:

- Incorporar los eventos generados por el Firewall y el antivirus en la plataforma de monitoreo existente.

- Asegurar que los logs de seguridad sean recolectados, almacenados y analizados de forma continua.

2. Establecer indicadores de desempeño del monitoreo:

- Definir métricas como número de eventos críticos detectados, tiempo de respuesta, y porcentaje de cobertura de monitoreo.

- Reportar estos indicadores periódicamente a la Alta Dirección.

3. Mantener el hallazgo abierto hasta evidenciar la implementación efectiva:

- No cerrar el hallazgo hasta que se demuestre, mediante evidencia técnica verificable, que el monitoreo incluye todos los componentes críticos y que se han definido e implementado correlacionadores funcionales.

HALLAZGO 2022-GT-27

1. Completar el etiquetado físico en todos los closets de comunicaciones:

- Asegurar que cada equipo, puerto, cable y punto de red esté debidamente identificado con etiquetas legibles, normalizadas y resistentes.

2. Finalizar la generación de diagramas de red por closet:

- Elaborar diagramas detallados que representen la topología física y lógica de cada rack, incluyendo conexiones, dispositivos activos y rutas de red.

3. Establecer un procedimiento de actualización de infraestructura:

- Documentar cada cambio físico o lógico en los closets, asegurando que los diagramas y etiquetas se mantengan actualizados.

4. Realizar inspecciones técnicas periódicas:

- Programar revisiones semestrales para validar el estado del etiquetado, la organización del cableado y la coherencia entre la documentación y la infraestructura real.

5. Mantener el hallazgo abierto hasta evidenciar la implementación completa:

- No cerrar el hallazgo hasta que se verifique, mediante evidencia visual y documental, que todos los closets de comunicaciones han sido intervenidos conforme a lo establecido.

HALLAZGO 2022-GT-28

1. **Completar la implementación del diagrama de distribución en todos los closets de cableado:**

- Asegurar que cada closet cuente con un diagrama actualizado que incluya puntos de red, equipos activos, rutas de conexión y etiquetas de referencia.

2. Instalar organizadores de cables en todos los racks:

- Finalizar la instalación de organizadores físicos que permitan mantener el orden, facilitar el mantenimiento y reducir el riesgo de fallas por manipulación.

3. Realizar inspecciones técnicas periódicas:

- Programar revisiones semestrales para validar el estado del etiquetado, la organización del cableado y la coherencia entre la documentación y la infraestructura real.

4. Consolidar la documentación técnica en un repositorio institucional:

- Centralizar los diagramas, registros de etiquetado, informes de inspección y procedimientos en una ubicación accesible para auditorías y gestión operativa.

5. Mantener el hallazgo abierto hasta evidenciar la implementación completa:

- No cerrar el hallazgo hasta que se verifique, mediante evidencia visual y documental, que todos los closets de cableado han sido intervenidos conforme a lo establecido.

ASESOR DE CONTROL INTERNO
Firma. Del registro en el formato (Informe de Seguimiento a la Gestión Institucional- FOEC08), es preciso mencionar que el documento objeto del asunto no presenta firma del responsable del proceso (Asesor con funciones de Control Interno), quien presento renuncia a dicho cargo desde el 30/01/2024.
Nombre:

Informe proyectado por: Jorge Florez

Contratista Oficina Control Interno