EVALUACIÓN Y VERIFICACIÓN DEL PROCEDIMIENTO DE RESPALDO Y RESTAURACIÓN DE LOS SISTEMAS DE INFORMACIÓN

INFORME FINAL

Oficina de Control Interno
Junio de 2023

Tabla de contenido

1. Objetivo de la auditoría:

Evaluar y verificar el funcionamiento del procedimiento de respaldo y restauración de los sistemas de información.

2. Alcance de la auditoría:

En el marco del objetivo definido, se evaluará el procedimiento de respaldo y restauración de los sistemas de información para la vigencia 2022, definiendo acciones de verificación relacionadas con:

- Identificación de la necesidad de respaldo de las bases.
- Programación y toma de copias de seguridad y restauración.
- Traslado de las copias a disco.
- Entrega de cintas para la custodia.

3. Criterios de auditoría o parámetros normativos:

Para el desarrollo de la presente auditoría se tendrán en cuenta los siguientes criterios: procedimiento de respaldo y restauración de los sistemas de información, con código P-TI-04, versión 05 y vigencia del 30/06/2022; Guía Estrategias de Respaldo y Restauración, con código G-TI-01, versión 01 del 30 de junio de 2022; Ley 87 de 1993; Ley 1978 de 2019; ISO 27001:2013; ISO/IEC 27002:2013; Guía Técnica de Principios MinTIC versión 1.0; MGGTI.G.GEN.01 Documento Maestro del Modelo de Gestión y Gobierno de TI MinTIC versión 1.0 de 2019.

4. Metodología:

La metodología empleada por la Oficina de Control Interno (en adelante OCI), se basó en un levantamiento de información por medio de un cuestionario con cuarenta y seis (46) preguntas; por otra parte, se utilizaron métodos de evaluación tales como la constatación de información y análisis sobre la misma; adicionalmente, se adoptó un método muestral para validar información acerca de casos originados en mesad de servicio, se estableció comunicación con el área de tecnología (en adelante Tecnología), para resolver las inquietudes que se iban presentando en el desarrollo de la auditoria.

La apertura de la auditoría se realizó mediante reunión virtual el día 5 de Junio de 2023 con el Director Técnico de Tecnologías y Gestión de Información en Justicia, el Subdirector de Tecnologías y Sistemas de Información, los profesionales encargados de atender la auditoría, el jefe de la Oficina de Control Interno y la auditora de la OCI; en dicha reunión se informó el objetivo, alcance y fechas de las actividades principales para el desarrollo de la auditoría; a su vez, se realizó la socialización de la información que debe ser allegada para la auditoria.

5. Desarrollo de la Auditoría

5.1. Generalidades

La Gestión de respaldos y restauración de los sistemas de información en el Ministerio de Justicia y del Derecho (MJD) está soportada en el procedimiento de "Respaldo y Restauración de los Sistemas de Información" con código: P-TI-04 en su versión 5 del 30 de junio de 2022, siendo el responsable del procedimiento el Subdirector de Tecnologías y Sistemas de Información.

El objetivo de dicho procedimiento es "*Brindar el apoyo y actividades necesarias que permitan minimizar el riesgo de pérdida de información al igual como la restauración de información en los escenarios que así lo ameriten, esto mediante la programación de copias de seguridad y restauraciones requeridas de copias de seguridad de las bases de datos de la entidad, para conservar y recuperar los datos en caso de daño en los servidores de la Entidad o por requerimiento de los interesados y entes de control*[1]".

El alcance del procedimiento es: "*Aplica para las bases de datos de los sistemas de información de la entidad. Inicia desde la identificación de la necesidad de respaldo de las bases; continúa con la programación de la copia de seguridad y restauración en modo verificación, posteriormente se extrae la copia a disco y finaliza con la entrega del medio para la custodia*[2]".

5.2. Procedimiento de Respaldo y Restauración de los Sistemas de Información

De acuerdo con el procedimiento en mención, Tecnología realiza respaldo a las Bases de Datos de los Sistemas de Información (SI)[3] que se encuentran en producción independientemente del tipo de proceso[4] que maneje.

Esta auditoría pudo detectar -con sujeción a la información aportada por el área de tecnología- que se encuentran identificados, en el marco de los sistemas de información vigentes, los siguientes datos, a saber:

- 10 sistemas de información con categoría misional.
- 6 sistemas de información con categoría de gestión.
- 1 sistema de información con categoría de apoyo.
- Se realizan respaldos a 3 servidores físicos.
- El respaldo de un servidor relacionado con el Sistema de Información Interinstitucional de Justicia Transicional (SIIJT) lo hace directamente Cloud Azure

[1] Procedimiento de Respaldo y Restauración de los Sistemas de Información; código P-TI-04; versión 5 del 30 de junio de 2022; Pág. 1; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/3ea4528c-e44a-441c-9d81-2ba0017a582d.pdf

[2] Procedimiento de Respaldo y Restauración de los Sistemas de Información; código P-TI-04; versión 5 del 30 de junio de 2022; Pág. 1; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/3ea4528c-e44a-441c-9d81-2ba0017a582d.pdf

[3] Catálogo de sistemas de información corresponde al inventario detallado de todos los sistemas de información (misional, de apoyo, portales digitales y de direccionamiento estratégico) que tenga la entidad, con la caracterización de cada uno de ellos. La caracterización de los sistemas de información hace referencia a la descripción detallada de sus atributos o características clave, requeridas para la gestión y apoyo en la toma de decisiones.

[4] Hace referencia a los procesos misionales, estratégicos, de evaluación y apoyo.

- Se realizan respaldos a 10 servidores virtuales (Para efectos de la auditoria, se omite la información relacionada con direcciones IP proporcionadas por el área de tecnología, considerando que el presente informe será publicado en procura de guardar la confidencialidad y protección de la información al respecto).
- Los medios de Backup son: en disco de la unidad de almacenamiento y en cintas.

Dentro de la validación realizada por la auditoria, se identificó que la matriz de catálogo de sistemas de información no cuenta con la siguiente información:

- El tipo de Backup[5]
- La periodicidad de la copia[6]
- Los periodos de retención[7]
- No indica a qué sistemas le realizan copia de BD y a cuáles de la capa de aplicación

Es de agregar que, si bien es cierto que el catálogo de sistemas de información se encuentra elaborado de acuerdo a los lineamientos de MINTIC y este no estipula que se deba incluir información sobre las copias de seguridad, Tecnología no está exenta de realizar la identificación documentada de las características de las copias de respaldo; lo anterior, de acuerdo con lo mencionado en la Política de Seguridad de la información "*La STSI debe proporcionar los lineamientos para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la entidad*[8]" y la ISO:IEC 27002 en el ítem 12.3.1 que sobre respaldo de la información establece: "*cuando se diseña un plan de elaboración de copias de respaldo se deberían tener en cuenta producir registros exactos y completos de las copias de respaldo y procedimientos de restauración documentados*[9]".

Adicionalmente, el procedimiento no tiene definido cómo se realiza el respaldo de los componentes del sistema de información, diferentes a las bases de datos, tales como capa de negocio[10], capa de aplicación[11], y no toma en cuenta los requisitos de periodicidad de la información de la entidad, en cuanto a los sistemas de misión crítica, incumpliendo lo mencionado en la ISO: IEC 27002:2013 en el ítem 12.3.1 Respaldo de la información: "*cuando se diseña un plan de elaboración de copias de respaldo se deberían tener en cuenta la cobertura (por ejemplo, copias de respaldo completas o diferenciales) y la frecuencia con que*

[5] Se habla de **backup** para referirse a una copia de seguridad. Un Backup permite la restauración de todos los archivos originales, como también solo de una parte.
[6] La periodicidad de la copia hace referencia a la frecuencia con la que debe hacer copias de respaldo dependerá del tipo de datos que vaya a respaldar.
[7] El periodo de retención hace referencia al tiempo de conservación de las copias de seguridad.
[8] Política de Seguridad de la información; Código: G-IC-14; versión 3 del 19 de diciembre de 2022; en el ítem "Copias de respaldo"; pág. 21; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/73234aa5-2d8e-45b8-8f13-d19eb8723b7c.pdf
[9] ISO/IEC 27002: 2013; Ítem 12.3. Copias de respaldo; 12.3.1 Respaldo de la información versión 3 del 19 de diciembre de 2022; Pag 60.
[10] La capa de negocio expone la lógica necesaria a la capa de presentación para que el usuario, a través de la interfaz, interactúe con las funcionalidades de la aplicación.
[11] La capa de aplicación es una capa del modelo de Interconexión de Sistemas Abiertos (OSI) que se utiliza para interactuar con las aplicaciones de red. La capa de aplicación es responsable de proporcionar servicios a las aplicaciones para que puedan acceder a los recursos de la red. La capa de aplicación también proporciona una interfaz entre la aplicación y la red.

se hagan las copias de respaldo deberían reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización" y en el Dominio 6.5 Infraestructura Tecnológica en el Documento Maestro del Modelo de Gestión y Gobierno en el numeral 6.5.6. MGGTI.LI.IT.08 - Respaldo y recuperación de la infraestructura de TI "*La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con mecanismos de respaldo para la infraestructura de TI crítica que soporta los procesos de la entidad, así como con un proceso periódico de respaldo de la configuración y de la información almacenada en la infraestructura tecnológica, incluyendo la información clave de las estaciones de trabajo de los funcionarios de la entidad. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de la infraestructura de TI*[12]".

Cabe agregar que, en este sentido, el procedimiento orientado exclusivamente sobre bases de datos es susceptible de ajuste para que integre y se cumplan las normas que orientan la materia, razón por la cual se deberá adoptar un plan de mejoramiento al respecto.

A continuación, vamos a observar las características de respaldo, periodicidad de la copia y de la retención en función de los SI del MJD, las cuales son documentadas en el presente informe por la auditoria, de acuerdo a la evidencia entregada por Tecnología:

Tabla 1. Relación de sistemas de información del MJD

Nombre	Descripción	Categoría proceso	Tipo de Backup[13]	Periodicidad de la copia	Periodo de retención
SISTEMA DE INFORMACIÓN DE CONCILIACIÓN, EL ARBITRAJE Y LA AMIGABLE COMPOSICIÓN	Software para la gestión de la información relacionada con la operación de los mecanismos alternativos de solución de conflictos en Colombia.	Misional	Incremental Full[14]	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN CASAS DE JUSTICIA	Sistema que facilita la caracterización e identificación de los usuarios y la identificación de los motivos de consulta más concurrentes en centros interinstitucionales, con el fin de orientar en la toma de decisiones para una mejoría en el acceso a los servicios básicos de justicia por parte de la ciudadanía.	Misional	Incremental[15] Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN DE CONTROL DE SUSTANCIAS QUÍMICAS	Sistema que permite el control de sustancias y productos químicos, tiene como misión satisfacer las necesidades de seguridad y tranquilidad pública, mediante un efectivo servicio, fundamentado en la prevención, direccionamiento y optimización del control y fiscalización que se ejerce.	Misional	Incremental Full	Diario Semanal Mensual	Permanente

[12] Documento Maestro del Modelo de Gestión y Gobierno de TI; versión 1.0 del 31 de octubre de 2019; Pág. 2; MINTIC; https://mintic.gov.co/arquitecturati/630/articles-144767_recurso_pdf.pdf

[13] Tipo de Backup: En función de la cantidad de información a copiar, el Backup puede ser completo (toda) o incremental.

[14] **Full**: Esta clase de respaldo permite guardar una copia completa del sitio web, los emails, bases de datos y demás configuraciones del sitio de forma completa, ordenada y comprimida.

[15] **Incremental**: esta clase de Backup, como su nombre lo indica, solamente genera una copia de resguardo con todos aquellos archivos que hayan sido modificados (o aparenten haberlo sido debido a cambios en su fecha de modificación) o se hayan creado desde el último Backup realizado, ya sea este último incremental o completo

SISTEMA DE INFORMACIÓN	Sistema de Información en el cual se relaciona todo el proceso de conciliación en equidad, se registra el seguimiento del aprendizaje de los futuros conciliadores en equidad y los casos que son atendidos por éstos.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN MISIONAL - ASUNTOS INTERNACIONALES	Seguimiento a los procesos que maneja la Dirección de Asuntos Internacionales.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
MECANISMO DE INFORMACIÓN PARA EL CONTROL DE CANNABIS	Plataforma tecnológica de apoyo al ejercicio de los componentes administrativo y operativo del control del cannabis para uso médico y científico en Colombia, en su primera versión permite la solicitud y el otorgamiento de licencias de Uso de semillas para siembra, Cultivo de plantas de cannabis Psicoactivo y Cultivo de plantas de cannabis no psicoactivo, adicionalmente la solicitud y el otorgamiento de cupos.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN MISIONAL POLÍTICA CRIMINAL	Realiza el seguimiento a derechos de petición, tutelas y procesos de la Dirección de Política Criminal.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN MISIONAL ASUNTOS INTERNACIONALES	Seguimiento a los procesos que maneja la Dirección de Asuntos Internacionales.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN MISIONAL (SIM)	Sistema de Información que integra los sistemas de SICAAC, Casas de Justicia, SICEQ, Control Disciplinario, Asuntos Internacionales y Política Criminal.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN SUIN - JURISCOL (Ciclope CMS)	Sistema de Información que almacena y permite ubicar de forma rápida y gratuita, normas de carácter general y abstracto. Adicionalmente se pueden realizar consultas de jurisprudencia de control de constitucionalidad y de legalidad proferidas por las Altas Cortes.	Misional	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN DE NÓMINA Y GESTIÓN HUMANA- SIGEP	El SIGEP es un sistema de información y gestión del empleo público que gestiona los procesos de vinculación para asegurar el cumplimiento de los requisitos al momento del ingreso del personal en la entidad y el manejo de la nómina de la entidad.	Gestión	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE GESTION DOCUMENTAL - SGDEA	Sistema de información para la gestión de la correspondencia y los documentos de la entidad.	Gestión	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN CONTRACTUAL Y FINANCIERO (SICF)	Sistema que muestra la información detallada para los supervisores del estado de los contratos que supervisan e información unificada del Grupo de Gestión Contractual y el Grupo de Gestión Financiera del Ministerio, en una plataforma de fácil acceso, así como el pronto pago a los contratistas del Ministerio. Actualmente, cuenta con soporte a nivel de infraestructura por la Subdirección de Tecnología y Sistemas de Información.	Gestión	Incremental Full	Diario Semanal Mensual	Permanente
GESTIÓN DE CONTROL DISCIPLINARIO INTERNO (GCODI)	El sistema permite realizar el seguimiento y evaluación de los funcionarios del MJD, para tomar decisiones en el momento de ejercer los derechos que contempla el código disciplinario.	Gestión	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN INTEGRAL (SII)	Sistema de Información que maneja Planes, Auditorías, Indicadores, Procesos, Riesgos, Proveedores, Activos de información y Proyectos	Gestión	Incremental Full	Diario Semanal Mensual	Permanente
SISTEMA DE INFORMACIÓN PCT	Administrar de manera eficiente el almacenamiento y gestión de los bienes del Ministerio de Justicia y del Derecho.	Apoyo	Incremental Full	Diario Semanal Mensual	Permanente

Elaboración propia.

De acuerdo con lo anterior, para los periodos de retención de las copias, Tecnología informa que se realizan de forma permanente, circunstancia por la cual se recomienda validar la idoneidad del periodo de retención, ya que estos deberían estar alineados con lo mencionado en las Tablas de Retención Documental del MJD, teniendo en cuenta que los términos de retención se asignarían a las series y subseries en las cuales se encuentran los datos originales de la información.

5.2.1. Copias de seguridad

La información sobre la cual se realizan copias de seguridad[16], por parte del área de tecnología, corresponde a:

- Base de Datos de los Sistemas de Información
- Configuraciones: Hace referencia a lo que está involucrado con los sistemas de información; servidor, en caso de incidente.
- Correos institucionales, Documentos

Para realizar esta actuación, según el procedimiento auditado, se debe realizar:

1. *"El procedimiento permite restaurar información, que en el caso de una recuperación o copias de seguridad debe ser solicitada a través del único punto de contacto el cual corresponde al servicio de mesa de ayuda; dicha labor la debe realizar el usuario abriendo un caso de soporte por la mesa de ayuda. Así mismo* (sic) *se realiza la tarea de restauración en el modo de verificación programada para cada base de datos en el momento realizar la copia diaria[17]".*

En este orden de ideas, el backup de correo acredita que, para la vigencia 2022, mesa de ayuda recibió 83 solicitudes, discriminadas así:

Área solicitante	Número de solicitudes	Estado del cierre
Despacho del Viceministerio de Política Criminal y Justicia Restaurativa	7	• 1 cerrado por encuesta satisfactoria • 6 cerrados por tiempo de garantía del caso
Despacho del Viceministro de Promoción de la Justicia	1	1 cerrado por encuesta satisfactoria
Despacho Ministro de Justicia y del Derecho	3	3 cerrados por tiempo de garantía del caso
Dirección de Asuntos Internacionales	2	2 cerrados por encuesta satisfactoria
Dirección de Desarrollo del Derecho y del Ordenamiento jurídico	2	• 1 cerrado por encuesta satisfactoria • 1 cerrado por tiempo de garantía del caso
Dirección de Justicia Formal	4	4 cerrados por tiempo de garantía del caso
Dirección de Justicia Transicional	2	2 cerrados por tiempo de garantía del caso
Dirección de Métodos Alternativos de Solución de Conflictos	12	• 4 cerrado por encuesta satisfactoria • 8 cerrado por tiempo de garantía del caso
Dirección de Política Criminal y Penitenciaria	2	2 cerrados por tiempo de garantía del caso

[16] Una **copia de seguridad, respaldo, copia de respaldo o copia de reserva** (en inglés Backup y data Backup) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

[17] Procedimiento de Respaldo y Restauración de los Sistemas de Información; código P-TI-04; versión 5 del 30 de junio de 2022; Pág. 2; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/3ea4528c-e44a-441c-9d81-2ba0017a582d.pdf

Área solicitante	Número de solicitudes	Estado del cierre
Dirección de Política de Lucha Contra las Drogas	2	2 cerrados por tiempo de garantía del caso
Dirección Jurídica	3	3 cerrados por tiempo de garantía del caso
Grupo de Almacén, inventarios y transporte	6	6 cerrados por tiempo de garantía del caso
Grupo de Gestión Administrativa	2	2 cerrados por tiempo de garantía del caso
Grupo de Gestión Contractual	1	1 cerrado por tiempo de garantía del caso
Grupo de Control Disciplinario Interno	1	1 cerrado por encuesta satisfactoria
Grupo de Gestión Documental	3	3 cerrados por tiempo de garantía del caso
Grupo de Gestión Financiera y Contable	1	1 cerrado por tiempo de garantía del caso
Grupo de Gestión Humana	5	• 1 cerrado por encuesta satisfactoria • 4 cerrado por tiempo de garantía del caso
Grupo de Servicio al Ciudadano	4	4 cerrados por tiempo de garantía del caso
Oficina Asesora de Planeación	3	• 2 cerrado por encuesta satisfactoria • 1 cerrado por tiempo de garantía del caso
Oficina de Asuntos Internacionales	1	1 cerrado por tiempo de garantía del caso
Oficina de Control Interno	6	6 cerrado por tiempo de garantía del caso
Oficina de Prensa y Comunicaciones	2	2 cerrado por tiempo de garantía del caso
Secretaria General	1	1 cerrado por tiempo de garantía del caso
Subdirección de Control y Fiscalización de Sustancias Químicas y Estupefacientes	3	• 1 cerrado por encuesta satisfactoria • 2 cerrado por tiempo de garantía del caso
Subdirección de Tecnologías y Sistemas de Información	1	1 cerrado por tiempo de garantía del caso
Subdirección Estratégica y de Análisis	3	3 cerrados por tiempo de garantía del caso

83	Total

Elaboración propia

Frente a lo expuesto en el contenido de la tabla podemos inferir que:

- De las 83 solicitudes, el 9.96% han sido solicitadas por la Dirección de Métodos Alternativos de Solución de Conflictos.
- Fueron cerrados 14 casos, teniendo en cuenta la encuesta de satisfacción, condición que representa el 16,87 % de los casos.
- Fueron cerrados 69 solicitudes, con ocasión del tiempo de garantía del caso, circunstancia que representa el 83,13% de la totalidad.

Es de agregar que, la Guía de Respaldo y Restauración no tiene asociado un lineamiento que mencione el proceso de copias de respaldo para los correos y configuraciones, razón por la cual la OCI sugiere su inclusión.
Ahora bien, en lo que corresponde al backup de Bases de Datos (BD) para 2022, mesa de ayuda recibió 17 solicitudes segregadas así:

- 12 registros de solicitudes fueron atendidos de forma satisfactoria, representando el 70,58% del total registrado.
- 1 registro de solicitud, el cual exigió pedir copia de la cinta al proveedor para restablecer la BD, representando el 5,88% del total registrado.
- 3 registros de solicitudes, las cuales después de ser restauradas seguían presentado inconsistencias o errores en la información, representando el 17,64% del total registrado.

- 1 registro de solicitud, el cual no cumplió con lo solicitado por el usuario, representando el 5,88% del total registrado.

De lo anterior, podemos deducir que es importante realizar pruebas de validación de las copias de respaldo con el fin de revisar la integridad de los datos allí consignados.

Dentro de las actividades definidas por el procedimiento se encuentra la: "Creación del plan de mantenimiento y/o inclusión de datos", para lo cual se valida la evidencia allegada, encontrando información relacionada con tareas de creación de backup que se llevan a disco duro, sin presentar información asociada a la efectividad del plan. En el SSMS[18] se crea el plan de mantenimiento se incluyen las bases de datos a las cuales se les va a realizar la copia de seguridad. Así mismo, se detalla el tipo de copia, la periodicidad y destino en disco de los archivos, para lo cual se evidencia información relacionada con el origen de los archivos a respaldar; más no especifica el destino del respaldo o un log que indique que su ejecución fue exitosa.

Para generar el registro de las cintas para custodia, primero, se toma la cinta que contiene la información para revisar el código de barras con el objeto de verificarlo; se identifica la cinta para registrarla en el formato "F-TI-04-01 de entrega en custodia de Copias de Seguridad"; la cinta es protegida con sellos de seguridad se procede a firmar el formato por parte del funcionario o contratista que entrega y el funcionario del proveedor que recibe.

Todas las cintas son enviadas a custodia externa; para ello, se cuenta con los contratos: No 376 de 2019 que tuvo vigencia hasta el 30 de noviembre 2022, y el contrato de custodia 814 de 2022, el cual está vigente en la actualidad hasta el 30 de noviembre 2023.

5.2.2. Restauración de copias de seguridad

Para solicitar respaldos de información Al proveedor de la custodia externa, se le envía un correo electrónico de las custodias de los backups con los datos de las cintas a solicitar para entrega al Ministerio; el tiempo de entrega es de tres (3) horas, después de la solicitud.

Dentro del plan de mantenimiento implementado para la toma de copias de seguridad, se encuentra habilitada la opción para que se realice una restauración en modo de verificación, de cada uno de los archivos de copias de seguridad; esta tarea se ejecuta diariamente

Dentro de la evidencia allegada, no se presenta información consistente que permita evidenciar que, dentro de las pruebas determinadas para el Plan de Recuperación de

[18] SQL Server Management Studio (SSMS) es un entorno integrado para administrar cualquier infraestructura y acceder a todos los componentes de SQL Server.

Desastres (DRP), se tengan estipuladas pruebas de restauración de la información proveniente de los sistemas de información, lo cual incumple la ISO: IEC 27001: 2013 en el ítem A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información "*La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas*" y en ISO: IEC 27002 en el ítem en el ítem 12.3.1 Respaldo de la información establece " *Los medios de respaldo se deberían poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; Esto se debería combinar con una prueba de los procedimientos de restauración coma y se debería verificar contra el tiempo de restauración requerido punto seguido la prueba de la capacidad para restaurar datos de los que se ha hecho una copia de respaldo se debería hacer en medios de pruebas dedicados no sobrescribiendo el medio original en caso de que el proceso de elaboración de copias de respaldo o de restauración falle y cause daño o pérdida de datos irreparable*"

En este sentido, se deberá adoptar un plan de mejoramiento que implemente dichas condiciones.

5.3. Guía de Estrategias de Respaldo y Restauración

La Subdirección de Tecnología y Sistemas de Información, cuenta con el "Formato Guía Estrategia de Respaldo", en el cual se estipulan los pasos para la toma de copias de seguridad.

El objetivo de dicho procedimiento es "*Establecer los pasos para la realización de copias de seguridad y restauración de las bases de datos de la entidad, tanto en el almacenamiento en cinta, como en el motor de bases de datos SQL Server*[19]".

El alcance del procedimiento es: "*Inicia con el proceso de tomas de copias de seguridad en SQL Server, seguido con el traslado de las copias a disco y finaliza con la entrega de cintas para la custodia*[20]". Dentro de la validación realizada por la auditoria, se identificaron las siguientes novedades:

- En el ítem 4.1 Esquemas de respaldo, mencionan tres diferentes clases de backups (*Full, Incremental*), pero la frecuencia del backup no es un tipo de backup, sino el tiempo de configuración del tipo (en esquemas de backups, podría ser un tipo diferencial).
- En el ítem 4.2 Uso del *media pool*, se infiere que el tercer tipo de backup, es de custodia externa (no se encuentra documentado); en la imagen proporcionada no especifica qué destino de pool se encuentra configurado para las copias, ni su programación.

[19] Guía Estrategias de Respaldo y Restauración; código G-TI-01; versión 1 del 30 de junio de 2022; Pág. 1; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/04ea062c-3a86-4193-8924-835b60db53bc.pdf

[20] Guía Estrategias de Respaldo y Restauración; código G-TI-01; versión 1 del 30 de junio de 2022; Pág. 1; MINJUSTICIA; https://sig.minjusticia.gov.co/Uploads/Master/04ea062c-3a86-4193-8924-835b60db53bc.pdf

- En el ítem 4.3.1 Grupos y derechos, refieren una tabla con la definición de usuarios; es importante conocer qué usuarios se encuentran en cada grupo, tomando en cuenta los derechos asignados.
- En el ítem 4.4.3 Fase Verificar: Verificación de las Políticas de Respaldos, no especifica si se hace uso del log de tareas de data protector con el fin de verificar la ejecución adecuada del backup.
- En el ítem 4.4.4. Fase Actuar: pruebas de restauración y certificación de respaldos, indican que las pruebas de restauración se documentan en un documento Word, que se encuentra en la carpeta indicando la fecha del mes en las que se realizan las pruebas de restauración; dentro de las evidencias allegadas, no se demostró la existencia de estos documentos de prueba de restauración.
- En el ítem 4.4.4. Fase Actuar: pruebas de restauración y certificación de respaldos, indican que las pruebas de restauración se realizan dos veces al mes de las copias de respaldo de las bases de datos y de los *filesystem*, se seleccionan de las sesiones realizadas en el mes, esta actividad se debe realizar en la primera semana del mes siguiente; no se presentó evidencia de la realización de estas pruebas.
- En el ítem 4.5.1. Copias de seguridad, se indica que se crea la notificación, en la cual se señala que si el proceso se efectúa de forma satisfactoria, se debe notificar mediante correo electrónico y, en caso de ser fallida, se envíe un registro al log de Windows detallando las fallas presentadas; no se presentó evidencia de la generación de dicha notificación.
- En el ítem 4.5.2 Proceso de Restauración de Base de Datos, la restauración de bases de datos no se ejecuta con la verificación de integridad de backups, esto solo verifica que el archivo es correcto para una eventual restauración.

Dado lo anterior, la OCI sugiere validar el contenido de la guía, y corregir de ser necesario.

6. Análisis de Riesgo:

Al validar la matriz de riesgos de gestión y corrupción, se observó que la Entidad no cuenta con controles para prevenir que los datos respaldados en cintas y discos de unidad de almacenamiento de los sistemas de información presenten errores en su restauración en el caso que sean requeridos por fallas del sistema o corrupción de archivos. La OCI recomienda valorar dichos riesgos y detallar los controles que deban ejercerse periódicamente para garantizar la mitigación del riesgo.

Este posible riesgo puede provocar una presunta paralización de la actividad por indisponibilidad de la información debido a la falta de accesibilidad de los funcionarios o contratistas a los datos de los sistemas de información, paralizando el servicio y generando una falta a la continuidad del negocio de la Entidad. Adicionalmente, puede

provocar daños irreversibles a la reputación de entidad por la pérdida definitiva de datos o archivos, ya que esto implica tener que volver a recopilarlos.

7. Conclusiones, hallazgos y/ recomendaciones

Se presentan las siguientes conclusiones, hallazgos y recomendaciones para la mejora del procedimiento de respaldo y restauración de los Sistemas de Información del Ministerio de Justicia y del Derecho.

7.1. Conclusiones

Existe un procedimiento actualmente documentado, el cual no toma en cuenta el respaldo de los componentes del sistema de información, diferentes a las bases de datos, tales como capa de negocio, capa de aplicación, y los requisitos de la información de la entidad y no establece un diferenciamiento en cuanto a la periodicidad de las copias de los distintos sistemas de información. Adicionalmente, no se encuentra alineado en cuanto al establecimiento, documentación e implementación de procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

7.2. Hallazgos

Hallazgo 1:

Se evidencia incumplimiento en la documentación de las características de las copias de respaldo de los sistemas de información; lo anterior, de acuerdo a lo mencionado en la Política de Seguridad de la información "*La STSI debe proporcionar los lineamientos para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la entidad*" y la ISO:IEC 27002 en el ítem 12.3.1 que, sobre respaldo de la información, establece "*cuando se diseña un plan de elaboración de copias de respaldo se deberían tener en cuenta producir registros exactos y completos de las copias de respaldo y procedimientos de restauración documentados*".

Hallazgo 2:

Se evidencia incumplimiento, en la manera cómo se realiza el respaldo de los componentes del sistema de información, diferentes a las bases de datos, tales como capa de negocio, capa de aplicación en la definición del procedimiento de restauración y respaldo, y no toma en cuenta los requisitos de periodicidad de la información de la entidad, en cuanto a los sistemas de misión crítica, incumpliendo lo mencionado la ISO: IEC 27002:2013 en el ítem 12.3.1 Respaldo de la información "*cuando se diseña un plan de elaboración de copias de respaldo se deberían tener en cuenta la cobertura (por ejemplo, copias de respaldo completas o diferenciales)y la frecuencia con que se hagan las copias de respaldo deberían reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización*" y en el Dominio 6.5 Infraestructura Tecnológica en el Documento Maestro del Modelo de

Gestión y Gobierno en el numeral 6.5.6. MGGTI.LI.IT.08 - Respaldo y recuperación de la infraestructura de TI, que señala: "*La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con mecanismos de respaldo para la infraestructura de TI crítica que soporta los procesos de la entidad, así como con un proceso periódico de respaldo de la configuración y de la información almacenada en la infraestructura tecnológica, incluyendo la información clave de las estaciones de trabajo de los funcionarios de la entidad. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de la infraestructura de TI".*

Hallazgo 3:

Se evidencia incumplimiento en cuanto a la estipulación de pruebas sobre restauración de la información proveniente de los sistemas de información determinadas en el Plan de Recuperación de Desastres (DRP), lo cual incumple la ISO: IEC 27001: 2013 en el ítem A.17.1.3, Verificación, revisión y evaluación de la continuidad de la seguridad de la información: "*La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas*" y en ISO: IEC 27002 en el ítem 12.3.1 Respaldo de la información: "*Los medios de respaldo se deberían poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; Esto se debería combinar con una prueba de los procedimientos de restauración coma y se debería verificar contra el tiempo de restauración requerido punto seguido la prueba de la capacidad para restaurar datos de los que se ha hecho una copia de respaldo se debería hacer en medios de pruebas dedicados no sobrescribiendo el medio original en caso de que el proceso de elaboración de copias de respaldo o de restauración falle y cause daño o pérdida de datos irreparable*".

7.3. Recomendaciones

- Incluir en la matriz de catálogo de sistemas de información la siguiente información:

  - El tipo de backup.
  - La periodicidad de la copia.
  - Los periodos de retención.
  - No indica a qué sistemas le realizan copia de BD y cuáles de la capa de aplicación.

- Se recomienda validar la idoneidad del periodo de retención, ya que estos deberían estar alineados con lo mencionado en las Tablas de Retención Documental del MJD, teniendo en cuenta que los términos de retención se asignarían a las series y subseries en las cuales se encuentran los datos originales de la información.
- Elaborar pruebas de validación de las copias de respaldo con el fin de revisar la integridad de los datos allí consignados.
- La Guía de Respaldo y Restauración no tiene asociado un lineamiento que mencione el proceso de copias de respaldo para los correos y configuraciones, razón por la cual la OCI sugiere la inclusión de estos.

- Se sugiere validar el contenido de la guía y corregir de ser necesario, lo siguiente:

  - En el ítem 4.1 Esquemas de respaldo, mencionan tres diferentes clases de Backup (Full, Incremental), pero la frecuencia del Backup no es un tipo de Backup, es el tiempo de configuración del tipo (en esquemas de Backup, podría ser un tipo diferencial).
  - En el ítem 4.2 Uso del media pool, se infiere que, el tercer tipo de Backup, es de custodia externa (no se encuentra documentado), en la imagen proporcionada no especifica que destino de pool se encuentra configurado para las copias, ni su programación.
  - En el ítem 4.3.1 Grupos y derechos, refieren una tabla con la definición de usuarios, es importante conocer que usuarios se encuentran en cada grupo, tomando en cuenta los derechos asignados.
  - En el ítem 4.4.3 Fase Verificar: Verificación de las Políticas de Respaldos, no especifica si se hace uso del log de tareas de data protector con el fin de verificar la ejecución adecuada del Backup.
  - En el ítem 4.4.4. Fase Actuar: pruebas de restauración y certificación de respaldos, indican que las pruebas de restauración se documentan en un documento Word, que se encuentra en la carpeta indicando la fecha del mes en las que se realizan las pruebas de restauración; dentro de las evidencias allegadas, no se demostró la existencia de estos documentos de prueba de restauración.
  - En el ítem 4.4.4. Fase Actuar: pruebas de restauración y certificación de respaldos, indican que las pruebas de restauración se realizan dos veces al mes de las copias de respaldo de las bases de datos y de los filesystem, se seleccionan de las sesiones realizadas en el mes, esta actividad se debe realizar en la primera semana del mes siguiente; no se presentó evidencia de la realización de estas prueba.
  - En el ítem 4.5.1. Copias de seguridad, se indica que se crea la notificación, en la cual se indica que si el proceso se efectúa de forma satisfactoria se debe notificar mediante correo electrónico, y en caso de ser fallida se envíe un registro al log de Windows detallando las falla presentada; no se presentó evidencia de la generación de dicha notificación.
  - En el ítem 4.5.2 Proceso de Restauración de Base de Datos, la restauración de bases de datos no se ejecuta con la verificación de integridad de Backup, esto solo verifica que el archivo es correcto para una eventual restauración.

Mediante memorando MJD-MEM23-0004028 del día 27 de junio de 2023, se remite informe preliminar de esta auditoría, a la Dirección y Subdirección de Tecnología, mediante el cual se informa que pueden remitir sus comentarios o promover una reunión de socialización con la OCI, dentro de los tres (3) días siguientes a la recepción de este informe, conforme lo dispone el procedimiento de Auditoría Interna.

Es de agregar que el área en mención solicito reunión de aclaración de los hallazgos del informe preliminar, la cual se realizó de forma virtual el día 29 de junio de 2023; con la presencia de la Dirección de Tecnología, Subdirección de Tecnología, los profesionales encargados de atender la auditoría y la auditora de la OCI; sin embargo, no envían comentarios relacionados; por lo anterior el informe y sus respectivos hallazgos se mantienen.

Con un muy cordial saludo,

_____	_____
Cristina Alarcón Tapiero	Diego Orlando Bustos Forero
Profesional OCI	Jefe Oficina de Control Interno
Auditor Líder	