Aproximación a un plan de mejoramiento óptimo

Formulación			
Hallazgo	**Causa Raíz**	**Acción "Objetivo general"**	**Meta "objetivos específicos"**
En la revisión del proceso de Gestión de Tecnologías de la Información de la Dirección Ejecutiva de Administración Judicial, se evidenció que 7 de los 10 servidores de bases de datos que contienen información crítica de procesos judiciales no han recibido actualizaciones de seguridad en los últimos 6 meses, contraviniendo el procedimiento GT-P-03 "Gestión de la Seguridad de la Información" del SIGCMA, que establece que estas actualizaciones deben realizarse mensualmente o tan pronto como el proveedor las publique. Esta situación se origina por la insuficiencia de personal capacitado, contando el área con solo dos administradores de bases de datos para atender más de 50 servidores en todo el país, priorizando en los últimos meses la atención de incidentes sobre las tareas de mantenimiento preventivo. Como consecuencia, la Rama Judicial se expone a riesgos significativos de seguridad de la información, incluyendo vulnerabilidades ante posibles ataques cibernéticos, potencial pérdida o alteración de datos críticos de procesos judiciales, y el incumplimiento de las políticas de seguridad establecidas por el Consejo Superior de la Judicatura, lo que podría afectar la administración de justicia, la confianza pública en el sistema judicial y resultar en hallazgos negativos en futuras auditorías.	Al indagar con el equipo de Tecnología, se identificó que la causa principal es la falta de personal capacitado para realizar las actualizaciones. El área cuenta con solo dos administradores de bases de datos para atender más de 50 servidores en todo el país, y en los últimos meses han priorizado la atención de incidentes sobre las tareas de mantenimiento preventivo.	Implementar un programa integral de fortalecimiento de la seguridad de la información en la Dirección Ejecutiva de Administración Judicial, con énfasis en la actualización y mantenimiento de servidores de bases de datos críticos.	Contratar y capacitar personal especializado en seguridad de bases de datos.
			Implementar herramienta automatizada de gestión de parches y actualizaciones.
			Actualizar el procedimiento GT-P-03 incluyendo protocolos de actualización y priorización.
			Realizar actualizaciones de seguridad en servidores de bases de datos críticos.
			Implementar sistema de monitoreo y reporte de estado de actualizaciones.

Este plan de mejoramiento aborda directamente la causa raíz identificada (falta de personal capacitado y priorización inadecuada) y establece unas meta claras y medibles para resolver el problema de las actu
permite tiempo suficiente para implementar las acciones necesarias, incluyendo la contratación y capacitación de personal, la implementación de herramientas de automatización, y la actualización de procedim
personal capacitado y priorización inadecuada) y desarrollan la acción propuesta de manera integral, cubriendo aspectos de personal, tecnología, procedimientos y monitoreo.

La acción es correctiva porque:

1. Responde directamente a un hallazgo específico que ya ha ocurrido: la falta de actualizaciones de seguridad en 7 de 10 servidores de bases de datos críticos durante los últimos 6 meses.
2. Está diseñada para corregir una no conformidad existente y prevenir que vuelva a ocurrir.
3. Aborda la causa raíz identificada: la falta de personal capacitado y la priorización inadecuada de tareas.
4. Busca eliminar la causa del incumplimiento detectado en la auditoría.
5. Se implementa después de que se ha identificado un problema específico, con el objetivo de resolverlo y evitar su recurrencia.

Las acciones correctivas se diferencian de las preventivas en que estas últimas se implementan para prevenir posibles no conformidades que aún no han ocurrido, mientras que las correctivas se aplican a
representa una situación actual de incumplimiento (servidores sin actualizaciones de seguridad), la acción propuesta se clasifica como correctiva, ya que busca resolver el problema actual y establecer medidas

Aproximación a una evaluación de la conformidad óptima

					Evaluación de la Conformidad		
Unidad de Medida de la Meta	**Dimensión de la Meta**	**Fecha Planeada de Inicio**	**Fecha Planeada de Terminación**	**Plazo en Semanas**	**Decisión sobre la Evaluación**	**Explicación Justificación o Retroalimentación de la Decisión**	**Acción a Seguir sobre la Decisión y Seguimiento**
Número de administradores contratados y capacitados	2	01/09/2024	30/11/2024	13	Conforme	Coherencia: Aborda directamente la falta de personal capacitado mencionada en la causa raíz. Pertinencia: Es crucial para resolver el problema de falta de actualizaciones. Plazos razonables: 13 semanas es un tiempo realista para procesos de contratación y capacitación inicial.	Se recomienda inciar ejecución
Porcentaje de implementación	100%	01/10/2024	31/01/2025	17	Conforme	Coherencia: Facilita la realización de actualizaciones de seguridad, que es el problema central. Pertinencia: Ayuda a priorizar y automatizar las tareas de mantenimiento. Plazos razonables: 17 semanas permiten una implementación cuidadosa y pruebas adecuadas.	Se recomienda inciar ejecución
Porcentaje de actualización del procedimiento	100%	15/09/2024	15/11/2024	9	Conforme	Coherencia: Aborda directamente la necesidad de mejorar los procesos mencionados en el hallazgo. Pertinencia: Establece guías claras para priorizar tareas de mantenimiento sobre la atención de incidentes. Plazos razonables: 9 semanas son suficientes para revisar y actualizar un procedimiento existente.	Se recomienda inciar ejecución
Porcentaje de servidores críticos actualizados mensualmente	100%	01/12/2024	28/02/2025	13	Conforme	Coherencia: Ataca directamente el problema identificado en el hallazgo. Pertinencia: Es la acción central necesaria para resolver la situación de riesgo. Plazos razonables: 13 semanas permiten un enfoque sistemático para actualizar todos los servidores críticos.	Se recomienda inciar ejecución
Porcentaje de servidores críticos actualizados mensualmente	100%	01/11/2024	31/01/2025	13	Conforme	Coherencia: Permite un seguimiento continuo del estado de las actualizaciones, abordando el problema de fondo. Pertinencia: Facilita la supervisión y el cumplimiento continuo de las políticas de seguridad. Plazos razonables: 13 semanas son adecuadas para desarrollar e implementar un sistema de monitoreo.	Se recomienda inciar ejecución

ualizaciones de seguridad en los servidores críticos. El plazo de 26 semanas
ientos. Estas metas, en conjunto, abordan la causa raíz identificada (falta de

problemas ya existentes y detectados. En este caso, dado que el hallazgo
para evitar que se repita en el futuro.

Sobre la acción en general:

Coherencia: La acción aborda directamente el problema identificado en el hallazgo: la falta de actualizaciones de seguridad en servidores de bases de datos críticos. Se enfoca en el fortalecimiento de la seguridad de la información, que es el aspecto central del hallazgo.

Pertinencia: La acción es relevante para la DEAJ y su función de gestión de tecnologías de la información. Aborda la causa raíz identificada: la falta de personal capacitado y la priorización inadecuada de tareas.

Plazos razonables: El plazo total de 26 semanas permite un tiempo adecuado para implementar cambios significativos en procesos y personal.

En conjunto, las metas forman un plan coherente que aborda todos los aspectos del hallazgo y su causa raíz, son pertinentes para la función y necesidades de la DEAJ, y tienen plazos que permiten una implementación cuidadosa y efectiva de las soluciones propuestas.

Aproximación a un plan de mejoramiento NO óptimo

Formulación			
Hallazgo	**Causa Raíz**	**Acción "Objetivo general"**	**Meta "objetivos específicos"**
En la revisión del proceso de Gestión de Tecnologías de la Información de la Dirección Ejecutiva de Administración Judicial, se evidenció que 7 de los 10 servidores de bases de datos que contienen información crítica de procesos judiciales no han recibido actualizaciones de seguridad en los últimos 6 meses, contraviniendo el procedimiento GT-P-03 "Gestión de la Seguridad de la Información" del SIGCMA, que establece que estas actualizaciones deben realizarse mensualmente o tan pronto como el proveedor las publique. Esta situación se origina por la insuficiencia de personal capacitado, contando el área con solo dos administradores de bases de datos para atender más de 50 servidores en todo el país, priorizando en los últimos meses la atención de incidentes sobre las tareas de mantenimiento preventivo. Como consecuencia, la Rama Judicial se expone a riesgos significativos de seguridad de la información, incluyendo vulnerabilidades ante posibles ataques cibernéticos, potencial pérdida o alteración de datos críticos de procesos judiciales, y el incumplimiento de las políticas de seguridad establecidas por el Consejo Superior de la Judicatura, lo que podría afectar la administración de justicia, la confianza pública en el sistema judicial y resultar en hallazgos negativos en futuras auditorías.	Al indagar con el equipo de Tecnología, se identificó que la causa principal es la falta de personal capacitado para realizar las actualizaciones. El área cuenta con solo dos administradores de bases de datos para atender más de 50 servidores en todo el país, y en los últimos meses han priorizado la atención de incidentes sobre las tareas de mantenimiento preventivo.	Fortalecer la seguridad informática de la Dirección Ejecutiva de Administración Judicial mediante la actualización de equipos de cómputo.	Reemplazar todos los equipos de cómputo de la Dirección Ejecutiva. Instalar antivirus en todos los equipos de la Rama Judicial. Capacitar a todos los funcionarios en el uso de contraseñas seguras.

Explicación de por qué este plan no cumple con los criterios necesarios:

1. Falta de coherencia: La acción general y las metas no abordan directamente el problema de falta de actualizaciones en los servidores de bases de datos. Se enfocan en equipos de cómputo y medidas g hallazgo.

2. Falta de pertinencia: Las acciones propuestas no atacan la causa raíz identificada (falta de personal capacitado y priorización inadecuada de tareas de mantenimiento en servidores). Aunque relacionadas co a resolver el problema específico de actualización de servidores de bases de datos.

3. Plazos no razonables: Los plazos propuestos son extremadamente cortos e irrealistas para las tareas descritas, especialmente considerando la escala de la Rama Judicial.

4. No aborda el riesgo específico: Las acciones no abordan el riesgo específico identificado en el hallazgo (vulnerabilidades en servidores de bases de datos críticos).

5. Uso inadecuado de recursos: Las acciones propuestas implican un uso significativo de recursos que no está justificado por el hallazgo específico.

6. No considera el procedimiento GT-P-03: El plan no hace referencia ni aborda la actualización del procedimiento GT-P-03 "Gestión de la Seguridad de la Información" mencionado en el hallazgo.

Aproximación a una evaluación de la conformidad no óptima

					Evaluación de la Conformidad		
Unidad de Medida de la Meta	**Dimensión de la Meta**	**Fecha Planeada de Inicio**	**Fecha Planeada de Terminación**	**Plazo en Semanas**	**Decisión sobre la Evaluación**	**Explicación Justificación o Retroalimentación de la Decisión**	**Acción a Seguir sobre la Decisión y Seguimiento**
Porcentaje de equipos reemplazados	100%	01/09/2024	15/09/2024	2	No Conforme	Coherencia: No es coherente porque reemplazar equipos de cómputo no resuelve el problema de falta de actualizaciones en servidores de bases de datos. Pertinencia: No es pertinente porque no aborda la causa raíz ni mejora la capacidad de actualizar los servidores. Plazos no razonables: Dos semanas para reemplazar todos los equipos de una Dirección Ejecutiva es un plazo irrealista, considerando los procesos de adquisición, configuración e implementación necesarios.	Se recomienda ajustar acción
Porcentaje de equipos con antivirus instalado	100%	16/09/2024	30/09/2024	2	No Conforme	Coherencia: No es coherente porque instalar antivirus en equipos de usuario final no resuelve el problema de actualizaciones de seguridad en servidores de bases de datos. Pertinencia: No es pertinente porque no aborda la causa raíz del problema ni mejora la capacidad de mantener actualizados los servidores. Plazos no razonables: Dos semanas para instalar antivirus en todos los equipos de la Rama Judicial es un plazo extremadamente corto, considerando la cantidad de equipos y su distribución geográfica.	Se recomienda ajustar acción
Porcentaje de funcionarios capacitados	100%	01/10/2024	07/10/2024	1	No Conforme	Coherencia: No es coherente porque la capacitación en contraseñas seguras, aunque importante, no está directamente relacionada con el problema de actualización de servidores de bases de datos. Pertinencia: No es pertinente porque no aborda la causa raíz identificada (falta de personal capacitado en mantenimiento de servidores y priorización de tareas). Plazos no razonables: Una semana para capacitar a todos los funcionarios de la Rama Judicial en el uso de contraseñas seguras es un plazo irrealista, considerando la cantidad de personal y la logística necesaria para una capacitación efectiva.	Se recomienda ajustar acción
jenerales de seguridad, no en los servidores específicos mencionados en el n la seguridad informática en general, las metas no contribuyen directamente					Frente a la acción en general: Coherencia: No es coherente porque se enfoca en la actualización de equipos de cómputo en general, mientras que el hallazgo específicamente menciona problemas con los servidores de bases de datos. Pertinencia: No es pertinente porque no aborda la causa raíz identificada (falta de personal capacitado y priorización inadecuada de tareas de mantenimiento en servidores). En resumen, este plan: 1. No es coherente porque sus acciones y metas no están alineadas con el problema específico identificado en el hallazgo (falta de actualizaciones en servidores de bases de datos). 2. No es pertinente porque no aborda la causa raíz identificada (falta de personal capacitado y priorización inadecuada de tareas de mantenimiento en servidores) y se enfoca en aspectos de seguridad general que, aunque importantes, no resuelven el problema específico. 3. Tiene plazos no razonables para todas sus metas, proponiendo tiempos extremadamente cortos para tareas que, en realidad, requerirían una planificación y ejecución mucho más extensa en una organización del tamaño y complejidad de la Rama Judicial. Este plan demuestra una falta de comprensión del problema real y propone soluciones superficiales que no abordarían efectivamente el hallazgo identificado en la auditoría.	