Aproximación a un plan de mejoramiento óptimo

Formulación								
Hallazgo	**Causa Raíz**	**Acción "Objetivo general"**	**Meta "objetivos específicos"**	**Unidad de Medida de la Meta**	**Dimensión de la Meta**	**Fecha Planeada de Inicio**	**Fecha Planeada de Terminación**	**Plazo en Semanas**
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.	Número de administradores contratados y capacitados	2	01/09/2024	30/11/2024	13
			Implementar herramienta automatizada de gestión de parches y actualizaciones.	Porcentaje de implementación	100%	01/10/2024	31/01/2025	17
			Actualizar el procedimiento GT-P-03 incluyendo protocolos de actualización y priorización.	Porcentaje de actualización del procedimiento	100%	15/09/2024	15/11/2024	9
			Realizar actualizaciones de seguridad en servidores de bases de datos críticos.	Porcentaje de servidores críticos actualizados mensualmente	100%	01/12/2024	28/02/2025	13
			Implementar sistema de monitoreo y reporte de estado de actualizaciones.	Porcentaje de servidores críticos actualizados mensualmente	100%	01/11/2024	31/01/2025	13

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 actualizaciones de seguridad en los servidores críticos. El plazo de 26 semanas 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 procedimientos. Estas metas, en conjunto, abordan la causa raíz identificada (falta de 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 problemas ya existentes y detectados. En este caso, dado que el hallazgo 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 para evitar que se repita en el futuro.

Aproximación a un plan de mejoramiento NO óptimo

Formulación								
Hallazgo	**Causa Raíz**	**Acción "Objetivo general"**	**Meta "objetivos específicos"**	**Unidad de Medida de la Meta**	**Dimensión de la Meta**	**Fecha Planeada de Inicio**	**Fecha Planeada de Terminación**	**Plazo en Semanas**
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.	Porcentaje de equipos reemplazados	100%	01/09/2024	15/09/2024	2
			Instalar antivirus en todos los equipos de la Rama Judicial.	Porcentaje de equipos con antivirus instalado	100%	16/09/2024	30/09/2024	2
			Capacitar a todos los funcionarios en el uso de contraseñas seguras.	Porcentaje de funcionarios capacitados	100%	01/10/2024	07/10/2024	1

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 generales de seguridad, no en los servidores específicos mencionados en el 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 con la seguridad informática en general, las metas no contribuyen directamente 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.