

ANEXO 1
CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS

SOLICITUD DE ACCIÓN CORRECTIVA		No. 1 de 3		
<input type="checkbox"/> No - Conformidad Mayor <input checked="" type="checkbox"/> No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	<table border="1"> <tr> <td>Requisito(s):</td> </tr> <tr> <td>9.3</td> </tr> </table>	Requisito(s):	9.3
Requisito(s):				
9.3				
Descripción de la no conformidad: En la revisión por la dirección no se evidencia la retroalimentación de todas las partes interesadas (9.3.d) ni el estado de los planes de tratamiento de riesgos (9.3.e).				
Evidencia: Revisión por la Dirección, Periodo 2023, Aprobada el 31 de octubre de 2023 en el Acta No. 12.				
Corrección	Evidencia de Implementación	Fecha		
1. Realizar retroalimentación adecuada para la elaboración del informe de Revisión por la Dirección mediante la generación previa de un informe estructurado con enfoque en los riesgos del proceso de Gestión TICs.	Registro de retroalimentación.	31/10/2024		
Descripción de la (s) causas (s) <i>(5M: Mano de Obra, Maquinaria, Método, Medio Ambiente, Materia Prima)</i> <u>Materia prima:</u> insuficiente información de retroalimentación del proceso de Gestión TICs al procedimiento de elaboración del informe por la Dirección. <u>Método:</u> Estructura compleja de la matriz de riesgos.				
Acción correctiva	Evidencia de Implementación	Fecha		
1. Participar de manera activa en la actualización de la versión 4 a la versión 6 de la matriz de riesgos	Evidencia de participación	28/06/2024		
2. Generar un informe de la gestión en TICs relacionado con los riesgos de seguridad de la información, como insumo para la Revisión por la Dirección.	Informe de riesgos de seguridad de la información en la Gestión TICs.	31/10/2024		

SOLICITUD DE ACCIÓN CORRECTIVA		No. 2 de 3		
<input type="checkbox"/> No - Conformidad Mayor <input checked="" type="checkbox"/> No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	<table border="1"> <tr> <td>Requisito(s):</td> </tr> <tr> <td>A.12.6.1</td> </tr> </table>	Requisito(s):	A.12.6.1
Requisito(s):				
A.12.6.1				
Descripción de la no conformidad: No se realizó verificación de cierre de las vulnerabilidades técnicas.				
Evidencia: Test de vulnerabilidades técnicas realizado en el año 2022, a la fecha existe un plan de trabajo, pero no se realizó el re-test para verificar el cierre efectivo de las vulnerabilidades.				
Corrección	Evidencia de Implementación	Fecha		
1. Identificar el mismo universo de objetivos de activos de información que se alcanzaron en el ejercicio de escaneo inicial.	Lista de objetivos de escaneo.	15/03/2024		
2. Realizar el re-test a los objetivos identificados en el punto anterior, validando la remediación de vulnerabilidades técnicas.	Informe de re-test.	28/05/2024		
Descripción de la (s) causas (s) <i>(5M: Mano de Obra, Maquinaria, Método, Medio Ambiente, Materia Prima)</i> <u>Método:</u> Incompleta documentación para gestionar el análisis de vulnerabilidades que no incluye la validación de los objetivos y el debido acompañamiento al contratista prestador del servicio. <u>Mano de Obra:</u> Insuficiente capacitación a los funcionarios que acompañan al contratista en el ejercicio de análisis de vulnerabilidades técnicas.				
Acción correctiva	Evidencia de Implementación	Fecha		
1. Elaborar un instructivo para la gestión de vulnerabilidades técnicas que incluya el paso a paso de cómo realizar la selección de direcciones y/o aplicaciones a ser revisadas, el proceso de cierre y re-test, incluyendo que deben ser los mismos objetivos del test inicial.	Instructivo para la gestión de vulnerabilidades técnicas	8/03/2024		
2. Socializar a los funcionarios de GIT de Apoyo Informático acerca del instructivo para la gestión de vulnerabilidades técnicas.	Registro de socialización.	11/03/2024		

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



SOLICITUD DE ACCIÓN CORRECTIVA		No. 3 de 3		
<input type="checkbox"/> No - Conformidad Mayor <input checked="" type="checkbox"/> No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	<table border="1"> <tr> <td>Requisito(s):</td> </tr> <tr> <td>A.16.1.6</td> </tr> </table>	Requisito(s):	A.16.1.6
Requisito(s):				
A.16.1.6				
Descripción de la no conformidad: No se evidencia el aprendizaje obtenido de los incidentes de seguridad de la información.				
Evidencia: Incidentes de seguridad de la información registrados en la plataforma GLPI durante el año 2023.				
Corrección	Evidencia de Implementación	Fecha		
1. Registrar en el formato de incidentes de seguridad las lecciones aprendidas en el respectivo campo, con la información relativa al conocimiento de la solución de los incidentes de seguridad durante el año 2024.	Campo de lecciones aprendidas en el formato de incidentes de seguridad	01/03/2024		
2. Socializar el formato con las lecciones aprendidas y conservarlo como información documentada en el servicio correspondiente de GLPI.	Registro de socialización y registro en GLPI.	15/02/2024		
Descripción de la (s) causas (s) <i>(5M: Mano de Obra, Maquinaria, Método, Medio Ambiente, Materia Prima)</i> <u>Método:</u> Deficiente documentación en el campo de lecciones aprendidas del formato de incidentes de seguridad de la información para completar su registro. <u>Maquinaria:</u> Incompleta documentación del registro en la solicitud GLPI por falta de gestión.				
Acción correctiva	Evidencia de Implementación	Fecha		
1.Revisar y ajustar el flujograma y el instructivo de gestión de incidentes, incluyendo la gestión del registro en el campo de lecciones aprendidas	Flujograma ajustado.	15/02/2024		
2. Gestionar el campo de lecciones aprendidas en el formato de gestión de incidentes de seguridad	Compleitud del Campo de lecciones aprendidas en el Formato de incidentes de seguridad.	15/02/2024		