DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DEL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL" - 2025

Plan N° PAIS.GTI.PLA.22-2024-MIDIS/PAIS

Versión N° 01

Plan aprobado mediante Resolución de Dirección Ejecutiva N° -2024-MIDIS/PAIS

Etapa	Responsable	Cargo	Visto Bueno y sello:
Formulado por:	Jorge Luis Távara Vallejos	Ejecutivo(a) de la Unidad de Tecnologías de la Información	Firmado digitalmente por TAVARA VALLEJOS Jorge Luis FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 26.11.2024 15:56:09 -05:00 Fecha:
Revisado por:	Irma Jennypher Cuba Araoz	Ejecutivo(a) de la Unidad de Planeamiento y Presupuesto	Firmado digitalmente por CUBA ARAOZ Irma Jennypher FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 26.11.2024 16:26:43 -05:00 Fecha:
	Igor Elías Mejía Verástegui	Ejecutivo(a) de la Unidad de Asesoría Jurídica	Firmado digitalmente por MEJIA VERASTEGUI Igor Elias FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 26.11.2024 16:57:45 -05:00 Fecha:
Aprobado por:	Fidel Pintado Pasapera	Director Ejecutivo	Firmado digitalmente por PINTADO PASAPERA Fidel FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 26.11.2024 17:12:09 -05:00 Fecha:

DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DEL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL" - 2025

ÍNDICE

1. INTRODUCCIÓN

Las Tecnologías de la Información y Comunicación (TIC) se han convertido en elementos clave para la ejecución de procesos y la prestación de servicios tanto internos como externos. Esta dependencia tecnológica implica que cualquier vulnerabilidad en los sistemas tecnológicos y/o en la infraestructura de red y comunicaciones, ya sea por errores de configuración, fallas de seguridad o posibles ataques externos, represente un riesgo significativo para cualquier entidad e institución. Estas vulnerabilidades pueden derivar en consecuencias graves, como la pérdida y/o exposición de datos confidenciales, la interrupción de servicios o daños a la reputación institucional.

En respuesta a estas necesidades y al contexto actual de creciente exposición a riesgos de ciberseguridad, se elabora el presente Plan con el fin de estructurar las actividades que permitan detectar, analizar y mitigar vulnerabilidades de manera efectiva. Además, el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" (PNPAIS) cuenta con la aprobación del Plan Multianual de Contingencia de Tecnologías de la Información y Comunicaciones del Programa Nacional "Plataformas de Acción para la Inclusión Social" 2024-2025, lo cual fortalece la implementación de este plan y asegura su alineación con otras estrategias institucionales.

A través de la ejecución del presente plan, se busca fortalecer la seguridad de la información y minimizar sus riesgos asociados, protegiendo los activos tecnológicos que sustentan los servicios digitales ofrecidos por el Programa Nacional PAIS a la población.

2. MARCO NORMATIVO

2.1. Ley N° 29158, Ley Orgánica del Poder Ejecutivo.

2.2. Ley N° 29792, Ley que creo el Ministerio de Desarrollo e Inclusión Social (MIDIS).

2.3. Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.

2.4. Ley N° 29733, Ley de Protección de Datos Personales.

2.5. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.

2.6. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733; Ley de Protección de Datos Personales.

2.7. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

2.8. Decreto de Urgencia N° 007-2020, que aprueba el marco de Confianza Digital.

2.9. Decreto Supremo N° 005-2024-MIDIS, que aprobó la Sección Primera del Reglamento de Organización y Funciones del Ministerio de Desarrollo e Inclusión Social.

2.10. Decreto Supremo N° 006-2024-MIDIS, que aprobó la Sección Primera del Reglamento de Organización y Funciones del Organismo de Focalización e Información Social (OFIS).

2.11. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas.

2.12. Resolución Ministerial N° 159-2022-MIDIS, que aprueba la Directiva N° 003-2022-MIDIS denominada "Catálogo de Documentos Oficiales del Ministerio de Desarrollo e Inclusión Social".

2.13. Resolución Directoral N° 060-2023-MIDIS/PNPAIS-DE, que aprueba el "Plan de Implementación del Sistema de Gestión de Seguridad de la Información del PNPAIS".

2.14. Resolución de Dirección Ejecutiva N° D000055-2024-MIDISPNPAIS-DE, que aprobó el Instructivo "Formulación revisión y aprobación de documentos normativos del Programa Nacional Plataformas de Acción para la Inclusión Social – PAIS" (PAIS.GPP. I.06-2024-MIDIS).

2.15. Resolución de Dirección Ejecutiva N° 0065-2024-MIDIS-PNPAIS-DE, que aprueba el Mapa de Procesos del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS".

2.16. Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Requisito 6.1 "Acciones para abordar los riesgos y oportunidades", 7.5. "Información Documentada", 8. "Operaciones".

3. ALCANCE

3.1. ÁMBITO DE APLICACIÓN

De cumplimiento obligatorio de todas las unidades de organización del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS".

3.2. ACTORES INVOLUCRADOS

a. **Director Ejecutivo:** Es la máxima autoridad administrativa de la entidad, quién aprueba el plan.

b. **Ejecutivo de la Unidad de Tecnologías de la Información:** Es responsable de ejecutar y asegurar el cumplimiento y difusión del presente plan, así como:

- Recopilar información relevante sobre las aplicaciones, sistemas y redes que serán objeto de pruebas, incluyendo direcciones IP, servicios, configuraciones y políticas de seguridad.

- Asegurar que todas las herramientas y recursos necesarios para las pruebas estén disponibles y configurados adecuadamente.

- Revisar y analizar los resultados de los escaneos y pruebas manuales para identificar vulnerabilidades, clasificándolas según su criticidad (Alta, Media, Baja).

- Elaborar informes detallados que describan las vulnerabilidades encontradas, incluyendo su descripción, impacto potencial, evidencia y recomendaciones implementadas para su mitigación.

- Realizar reescaneos y pruebas adicionales para validar que las vulnerabilidades han sido efectivamente mitigadas.

- Revisar y mejorar continuamente el proceso de pruebas de vulnerabilidades basándose en las lecciones aprendidas y las mejores prácticas emergentes en el campo de la ciberseguridad.

c. **Oficial de Seguridad y Confianza Digital:** Revisar anualmente el Plan de Detección y Evaluación de Vulnerabilidades en la Infraestructura Tecnológica, a fin de analizar e identificar las necesidades de actualización y/o adaptación, así mismo:

- Proporcionar formación semestralmente al personal de la Unidad de Tecnologías de la Información y a los usuarios finales sobre las mejores prácticas de seguridad y la importancia de la protección contra vulnerabilidades.

- Realizar campañas de concienciación para informar a todo el personal del PNPAIS sobre los resultados de las pruebas y las medidas que deben tomar para mantener la seguridad.

- Presentar los informes a los responsables de seguridad y a la alta dirección de la institución, explicando los hallazgos y sugiriendo acciones correctivas.

- Preparar y asistir en las auditorías de seguridad para demostrar el cumplimiento y la efectividad de las medidas implementadas.

4. DIAGNÓSTICO

La Unidad de Tecnologías de la Información (UTI) del Programa Nacional "Plataformas de Acción para la Inclusión Social - PAIS" aplica diversos análisis de vulnerabilidades, como ethical hacking, que se aplica una vez al año a la infraestructura en la nube; análisis de encabezados de respuesta HTTP para mejorar la seguridad de los aplicativos webs; y la gestión continua de la seguridad y monitoreo de la red utilizando herramientas especializadas.

La presente evaluación identifica diversas deficiencias de gestión en los análisis de vulnerabilidades realizados por el Programa Nacional PAIS. Si bien estos servicios cumplen una función esencial en la protección de la infraestructura y los aplicativos, existen áreas clave de mejora que pueden fortalecer la seguridad y eficiencia de los procesos. Estas deficiencias incluyen limitaciones en la frecuencia y alcance de las evaluaciones, ausencia de métricas de impacto, y un enfoque reactivo en ciertos análisis. Analizar y abordar estos aspectos permitirá optimizar

la efectividad de las medidas de seguridad, garantizando una protección integral, una respuesta proactiva y un uso óptimo de los recursos tecnológicos y humanos.

N°	Tipo de análisis	Alcance	Deficiencias	Descripción
1	Ethical hacking	Realizado al menos una vez al año y aplicado únicamente a la infraestructura y servicios desplegados en nube. Este servicio es de tipo caja gris (combinación de pruebas de caja blanca y caja negra), en el cual se realiza una búsqueda de defectos en la estructura y uso de los servicios. Al culminar el servicio, se emite un Informe Técnico Final detallando los resultados del estado de la seguridad de la infraestructura tecnológica con recomendaciones para mitigar y/o eliminar las vulnerabilidades detectadas. Posterior a ello, se realiza la implementación de estas recomendaciones, los cuales se reflejan en un Informe final de mitigación de vulnerabilidades.	Ausencia de métricas de eficacia	No se utilizan métricas para evaluar la mejora continua en la seguridad de la infraestructura ni para medir el éxito de las recomendaciones de mitigación aplicadas.
			Carencia de planificación proactiva:	No se tiene una estrategia de mejora o ajuste del servicio de ethical hacking en función de los resultados de evaluaciones previas, lo cual podría limitar su eficacia a largo plazo.
2	Análisis de encabezados de respuesta HTTP de los aplicativos webs	Realizado al menos una vez al año, utilizando herramientas gratuitas que permiten identificar funciones de seguridad modernas que no están implementadas en los aplicativos webs del Programa. Este análisis permite mejorar la protección de los aplicativos webs de ataques, intentos de rastreo, uso de API externos, entre otros. Al culminar la actividad, se elabora un Reporte con todas las deficiencias de seguridad detectadas junto con el código que debe agregarse para mitigar la vulnerabilidad. Posterior a ello, se implementa el código en el encabezado de respuesta HTTP y se elabora un Informe detallando los cambios y pruebas realizados.	Frecuencia insuficiente	Realizar el análisis solo una vez al año podría no ser suficiente para proteger los aplicativos webs contra amenazas nuevas y emergentes, especialmente si se realizan actualizaciones frecuentes en el software o la infraestructura.
			Falta de evaluación continua	No se tiene un proceso de revisión continua para verificar la efectividad de los cambios realizados ni para asegurar que las vulnerabilidades no vuelvan a surgir después de cada implementación de código.
			Alcance limitado	El análisis se centra únicamente en los encabezados de respuesta HTTP, lo que excluye otros aspectos de seguridad de los aplicativos webs, como vulnerabilidades en el código fuente, configuraciones de seguridad de servidor, o el análisis de API.

N°	Tipo de análisis	Alcance	Deficiencias	Descripción
			Ausencia de métricas de impacto	No se tiene métricas para evaluar si las modificaciones aplicadas efectivamente aumentan la seguridad de los aplicativos, ni si el riesgo de ataque se ha reducido.
			Planificación no proactiva	La implementación de recomendaciones ocurre solo después de detectar deficiencias, sin un enfoque proactivo que permita anticiparse a vulnerabilidades conocidas o comunes.
3	Gestión, seguridad y monitoreo de red	Análisis continuo, utilizando la herramienta de seguridad perimetral especializado en servicios web, la consola de administración de antivirus, la herramienta de gestión de eventos e información de seguridad, y la herramienta de monitoreo de redes y aplicaciones, permitiendo a la Unidad de Tecnologías de la Información mantener un análisis constante de los servicios web publicados, los equipos endpoint, los servidores y a la red del PNPAIS garantizando una respuesta proactiva y eficiente ante amenazas cibernéticas.	Dependencia de herramientas	La gestión se basa en un conjunto limitado de herramientas, lo cual podría dejar brechas si estas no son suficientemente actualizadas o si tienen limitaciones para detectar amenazas avanzadas o poco convencionales.
			Falta de Indicadores de Desempeño y Respuesta	No se tiene métricas claras que permitan evaluar la eficacia de la respuesta ante incidentes o la reducción de riesgos con el uso de estas herramientas, lo cual es clave para la mejora continua.
			Enfoque Limitado en la Optimización de Recursos	El enfoque en análisis y respuesta proactiva podría beneficiarse de una estrategia de optimización de recursos, que busque la eficiencia en el uso de herramientas y personal para evitar la sobrecarga operativa.

Fuente: Elaboración propia.

Si bien, como se precisó en párrafos anteriores, estos esfuerzos están alineados con las mejores prácticas de seguridad; no obstante, actualmente no cuentan con una formalización estricta en cuanto a la planificación y ejecución de sus actividades, lo que podría limitar la calidad y consistencia en la protección a largo plazo. Por ello, es crucial formalizar la gestión de estas actividades para garantizar que los análisis se realicen de manera sistemática y en

función de guías y/o pautas establecidas, mejorando así la resiliencia del Programa ante las amenazas cibernéticas.

5. MARCO ESTRATÉGICO

5.1. OBJETIVO ESTRATÉGICO / ACCIÓN ESTRATÉGICA

La formulación del presente Plan se encuentra relacionado de manera general con el objetivo estratégico institucional OEI.05 "Incrementar el acceso a infraestructura y servicios básicos de la población en centros poblados rurales, rurales dispersos, en situación de pobreza, pobreza extrema y vulnerabilidad" y a las acciones estratégicas AEI.05.01 "Servicios públicos con plataformas itinerantes accesibles a las poblaciones rurales en situación de pobreza y pobreza extrema" y AEI.05.02 "Servicios públicos con plataformas fijas accesibles a las poblaciones rurales y rurales dispersas en situación de pobreza y pobreza extrema", aprobados en el marco del Plan Estratégico Institucional 2024-2030 del Ministerio de Desarrollo e Inclusión Social, según Resolución Ministerial N° 00060-2024-MIDIS.

5.2. OBJETIVO GENERAL

Identificar, evaluar y mitigar vulnerabilidades en el hardware, software, aplicaciones, servicios digitales, sistemas de Información, entre otros; con la finalidad de asegurar que la Infraestructura de Tecnologías de la Información del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" esté protegida contra amenazas internas y externas.

6. PROGRAMACIÓN DE ACTIVIDADES

TIPOS DE ANALISIS DE VULNERABILIDADES

N°	Tipo de análisis	Descripción
1	Escaneo de Vulnerabilidades Automático	Basada en el uso de herramientas automatizadas para detectar posibles fallas de seguridad en los sistemas y redes.
2	Pruebas de Penetración (Pentesting) o Ethical hacking	Simulación de ataques reales para identificar cómo los sistemas responden a intentos de explotación de vulnerabilidades
3	Análisis de Configuración	Enfocado en revisar la configuración de sistemas, aplicaciones, redes y dispositivos para asegurar que sigan las mejores prácticas de seguridad.
4	Revisión de Código	Enfocada en identificar vulnerabilidades de seguridad en el código fuente de una aplicación.
5	Monitoreo Continuo	Enfocado en la supervisión constante de los sistemas en busca de vulnerabilidades, cambios no autorizados o incidentes de seguridad.

Fuente: Elaboración propia.

Cada tipo de análisis tiene actividades específicas diseñadas para abordar diferentes aspectos de la seguridad. El uso de estos enfoques en combinación permite una evaluación más completa de las vulnerabilidades y contribuye a una mejor defensa ante posibles ataques.

7. SEGUIMIENTO Y EVALUACIÓN

El seguimiento y evaluación del Plan de Detección y Evaluación de Vulnerabilidades en la Infraestructura Tecnológica del Programa Nacional "Plataformas de Acción para la Inclusión Social" 2025 estará a cargo del personal de la Unidad de Tecnologías de la Información, quienes remitirán de acuerdo con el Plan, los informes en cumplimiento junto con la documentación de verificación de cada actividad al Ejecutivo de la Unidad de Tecnologías de la Información.

La Unidad de Tecnologías de la Información informará trimestralmente a la Dirección Ejecutiva el cumplimiento de las actividades del Plan de Detección y Evaluación de Vulnerabilidades en la Infraestructura Tecnológica. A su vez, la recopilación de esta información permitirá elaborar el diagnóstico de la propuesta de Plan de Detección y Evaluación de Vulnerabilidades en la Infraestructura Tecnológica para el periodo 2026.

8. ANEXOS

Anexo N° 1: Matriz de programación de actividades

Anexo N° 2: Concientización del plan

ANEXO N° 1 MATRIZ DE PROGRAMACIÓN DE ACTIVIDADES

Tipo de análisis	Actividad	Descripción	Medio de verificación	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
Escaneo de vulnerabilidades automático	Definición de alcance[1]	Identificar los activos, redes, sistemas, aplicaciones y dispositivos que serán escaneados.	Documento de alcance, que incluya la lista de activos, redes, sistemas y aplicaciones a escanear.	■						■						UTI
	Selección de herramientas	Elegir la herramienta adecuada según las necesidades del entorno.	Registro de la herramienta seleccionada, con justificación técnica de la elección según las necesidades del entorno.	■						■						UTI
	Configuración del escáner	Ajustar parámetros como el rango de direcciones IP, el nivel de profundidad del análisis, y las opciones de autenticación si se requiere.	Capturas de pantalla o archivo de configuración del escáner, que incluya parámetros ajustados como rango de direcciones IP, autenticación y nivel de profundidad del análisis.	■						■						UTI
	Ejecución del escaneo	Iniciar el escaneo y permitir que la herramienta identifique vulnerabilidades, configuraciones incorrectas, puertos abiertos y servicios inseguros.	Informe preliminar generado por la herramienta de escaneo que muestre el progreso y resultados del análisis.	■						■						UTI
	Revisión de reporte / informe de resultados	Analizar el informe generado con la lista de vulnerabilidades detectadas, categorizadas por gravedad (crítica, alta, media, baja).	Informe que contenga el análisis de impacto, observaciones, y el plan de acción para solucionar las vulnerabilidades detectadas, priorizando las vulnerabilidades más críticas.	■						■						UTI
	Atención y mitigación	Ejecutar el plan de acción para solucionar las vulnerabilidades detectadas.	Reporte de acciones ejecutadas para mitigar y/o eliminar las vulnerabilidades.	■	■					■	■					UTI
	Escaneo de validación	Una vez corregidas las vulnerabilidades, realizar un nuevo escaneo para verificar que han sido mitigadas correctamente.	Informe del escaneo de validación que confirme que las vulnerabilidades corregidas ya no están presentes.		■						■					UTI

[1] De corresponder, la definición del alcance debe estar alineada a la atención de los riesgos de la "Matriz de Riesgos de Seguridad de la Información".

Tipo de análisis	Actividad	Descripción	Medio de verificación	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
	Documentación y reporte	Guardar un registro de los resultados y acciones tomadas, y reportar a las partes interesadas.	Reporte final que incluya un resumen de los hallazgos, las acciones correctivas implementadas, y los resultados del escaneo de validación.													UTI
Pruebas de Penetración (Pentesting) o Ethical hacking	Planificación y definición del alcance[2]	Identificar y definir el alcance, determinando los sistemas, aplicaciones, redes o dispositivos que serán evaluados; y establecer los objetivos de las pruebas.	Documento de alcance, que determine el sistema, aplicación, red o dispositivo a evaluar; defina el objetivo y los métodos permitidos durante la prueba.													UTI
	Reconocimiento	Recolectar información detallada sobre los sistemas y redes objetivo (recolección pasiva y/o reconocimiento activo).	Informe de reconocimiento que incluya la información recolectada (IP, servicios, nombres de dominio, etc.) y las técnicas empleadas en la recolección de datos.													UTI
	Escaneo de Vulnerabilidades	Realizar un escaneo automático y/o manual para identificar vulnerabilidades en el entorno.	Resultados de los escaneos, listando las vulnerabilidades y /o fallas detectadas con su correspondiente clasificación de criticidad.													UTI
	Explotación de Vulnerabilidades (opcional)	Intentar explotar las vulnerabilidades detectadas para comprobar su impacto.	Registro de intentos de explotación realizados (con capturas de pantalla y logs), indicando las vulnerabilidades explotadas con éxito.													UTI
	Escalación de Privilegios (opcional)	Si se consigue acceso inicial, se debe intentar elevar los privilegios para obtener un control más amplio del sistema, replicando los pasos que un atacante utilizaría para alcanzar datos sensibles o funciones administrativas.	Informe de escalación de privilegios que describa los métodos y herramientas utilizadas, junto con los permisos adicionales obtenidos en el sistema.													UTI

[2] De corresponder, la planificación y definición del alcance debe estar alineada a la atención de los riesgos de la "Matriz de Riesgos de Seguridad de la Información".

Tipo de análisis	Actividad	Descripción	Medio de verificación	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
	Análisis post-explotación (opcional)	Documentar el impacto de cada vulnerabilidad explotada, identificando la naturaleza y el alcance de los daños potenciales. Se debe evaluar el riesgo de cada vulnerabilidad en función de su impacto en el sistema.	Informe detallado de análisis post-explotación que resuma el impacto de las vulnerabilidades aprovechadas y el nivel de acceso alcanzado.													UTI
	Elaboración de informe	Crear un informe que incluya una lista completa de las vulnerabilidades encontradas, los métodos de explotación utilizados (opcional) y recomendaciones detalladas para la mitigación.	Informe final de pentesting, que incluya todas las vulnerabilidades encontradas, cómo fueron explotadas (opcional), recomendaciones para mitigación y la evaluación de riesgos.													UTI
	Atención y mitigación	Ejecutar o implementar las recomendaciones para solucionar las vulnerabilidades detectadas.	Reporte de acciones ejecutadas para mitigar y/o eliminar las vulnerabilidades.													
	Validación y revisión	Después de corregir las vulnerabilidades, realizar una nueva prueba para confirmar que ya no se pueden explotar.	Informe de validación que confirme que las vulnerabilidades ya no pueden ser explotadas, indicando los resultados de las pruebas post-mitigación.													UTI
Análisis de Configuración	Identificación de inventario de activos	Crear una lista de los sistemas y dispositivos que deben ser revisados (servidores, routers, bases de datos, etc.).	Lista de activos actualizada que incluya detalles de cada sistema y dispositivo objetivo (servidores, routers, bases de datos, etc.).													UTI
	Definición de las mejores prácticas	Consultar las guías de configuración segura y los estándares de la industria	Documento de referencia con las mejores prácticas de configuración segura, basado en guías y estándares reconocidos.													UTI
	Revisión manual y/o automatizada	Revisar las configuraciones manualmente o mediante herramientas que automatizan la auditoría de configuración.	Registro que incluya detalles de la revisión realizada en cada activo, listado de herramientas utilizadas y resultados preliminares para cada configuración revisada.													UTI
	Revisión de Permisos y Configuraciones Críticas	Revisar permisos de acceso, configuraciones de puertos, servicios innecesarios, políticas de contraseñas, entre otros.	Informe de permisos y configuraciones, documentando los accesos, servicios y políticas de contraseñas revisadas, con cualquier debilidad o desviación encontrada.													UTI

Tipo de análisis	Actividad	Descripción	Medio de verificación	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
	Identificación de problemas	Documentar configuraciones débiles o inseguras que puedan ser aprovechadas por un atacante.	Documento que liste cada configuración débil o insegura identificada, clasificada por nivel de criticidad y riesgo, aprobado por el equipo de auditoría de seguridad.		■						■					UTI
	Ajuste de configuraciones	Implementar las mejores prácticas de configuración según los problemas identificados.	Registro de cambios implementados, documentando cada ajuste realizado en la configuración de los activos para mitigar riesgos, y validado por pruebas de configuración segura.		■	■					■	■				UTI
	Documentación y reporte	Elaborar un informe con las configuraciones corregidas y las recomendaciones para mantener el entorno seguro	Informe final de configuración que resuma los problemas detectados, acciones correctivas y recomendaciones para futuros ciclos de revisión.			■						■				UTI
Revisión de Código	Definición del alcance[3]	Identificar los módulos o partes críticas del software que serán revisados	Documento de alcance detallado que indique los módulos y componentes críticos que serán revisados.				■						■			UTI
	Selección de herramientas	Utilizar herramientas de análisis estático de código (SAST)	Lista de herramientas seleccionadas (SAST) con su respectivo análisis de compatibilidad y configuración inicial.				■						■			UTI
	Revisión automatizada	Ejecutar el escaneo automatizado para identificar errores comunes, como inyecciones SQL, buffer overflow, o manejo inseguro de entradas.	Informe preliminar de escaneo automatizado que incluya vulnerabilidades identificadas y generadas por la herramienta seleccionada.				■						■			UTI
	Revisión manual	Complementar el análisis automatizado con una revisión manual para encontrar errores lógicos o vulnerabilidades difíciles de detectar.	Registro de hallazgos adicionales de la revisión manual, donde se especifiquen vulnerabilidades complejas o errores lógicos no detectados por la herramienta automatizada.				■						■			UTI

[3] En caso de nuevos desarrollos de software, aplicaciones, entre otros; el alcance de revisión debe abarcar a todo el código desarrollado. Asimismo, esta actividad debe realizar antes de dar el pasa o salida a producción.

Tipo de análisis	Actividad	Descripción	Medio de verificación	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
	Evaluación de resultados	Clasificar las vulnerabilidades por su criticidad y priorizar las correcciones.	Informe de clasificación de vulnerabilidades, priorizando las correcciones con base en criticidad.				■						■			UTI
	Corrección de vulnerabilidades	Implementar las soluciones en el código.	Registro de cambios en el código fuente donde se detalle cada corrección implementada para mitigar las vulnerabilidades encontradas.				■	■					■	■		UTI
	Revisión de correcciones	Validar que las correcciones hayan resuelto las vulnerabilidades sin introducir nuevos problemas.	Informe de validación de correcciones, mostrando que cada vulnerabilidad fue resuelta y confirmando que no se introdujeron nuevos problemas de seguridad.					■						■		UTI
	Documentación y reporte	Elaborar un informe con los hallazgos y las acciones correctivas realizadas.	Informe final de revisión de código que incluya los hallazgos, las vulnerabilidades corregidas, y las recomendaciones para el desarrollo seguro.					■						■		UTI
Monitoreo Continuo	Definición y/o actualización del entorno a monitorear	Seleccionar los sistemas, redes y aplicaciones que deben ser monitoreados de manera continua.	Documento que detalle los sistemas, redes y aplicaciones a monitorear, con una lista específica de activos críticos para la seguridad.			■						■				UTI
	Selección y/o actualización de herramientas de monitoreo	Implementar, actualizar y/o cambiar las soluciones de monitoreo continuo.	Informe de selección de herramientas con justificación sobre la elección, acompañado de las configuraciones iniciales y pruebas de integración realizadas, de corresponder.			■						■				UTI
	Establecimiento de alertas	Configurar y/o actualizar las alertas automáticas para eventos anómalos, intentos de acceso no autorizado, cambios en configuraciones críticas, entre otros.	Captura de pantallas de la configuración de alertas automáticas en el sistema de monitoreo.			■						■				UTI
	Monitoreo en tiempo real	Observar los eventos en tiempo real y reaccionar ante incidentes de seguridad conforme ocurren.	Registro de actividades de monitoreo, donde se indiquen las reacciones frente a eventos de seguridad, con evidencia de incidentes gestionados, de corresponder.	■	■	■	■	■	■	■	■	■	■	■	■	UTI

Tipo de análisis	Actividad	Descripción	Medio de verificación	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
	Análisis de logs	Revisar los registros de eventos y actividades para identificar patrones sospechosos o vulnerabilidades emergentes.	Reporte de análisis de logs, que incluyan patrones sospechosos detectados, anomalías y vulnerabilidades emergentes.	■	■	■	■	■	■	■	■	■	■	■	■	UTI
	Respuesta a incidentes	Ante la detección de una vulnerabilidad o incidente, ejecutar los pasos del Instructivo de Gestión de Incidentes de Seguridad Digital y/o de Plan de Contingencia de Tecnologías de la Información y Comunicaciones, según corresponda.	Registro detallado de cada incidente detectado, acciones de mitigación tomadas y resultados de las medidas implementadas, conforme al documento normativo utilizado.	Según corresponda												UTI
	Revisión periódica del monitoreo	Realizar auditorías periódicas para evaluar la eficacia de los sistemas de monitoreo y hacer ajustes.	Informe de auditoría evaluando la efectividad del monitoreo continuo, que incluya recomendaciones de mejora y ajustes necesarios, validado por el equipo de seguridad y TI.			■			■			■			■	UTI
	Documentación y reporte	Generar informes sobre las actividades de monitoreo, incidentes detectados y acciones correctivas realizadas.	Reporte sobre las actividades de monitoreo, con detalles de incidentes detectados y acciones correctivas realizadas.	■	■	■	■	■	■	■	■	■	■	■	■	UTI

ANEXO N° 2 CONCIENTIZACIÓN DEL PLAN

Actividad	Descripción	I TRIM			II TRIM			II TRIM			IV TRIM			Unidad Responsable
		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	
Capacitación Inicial	Reunión virtual o presencial para presentar el plan y su importancia, donde se detallarán las deficiencias detectadas y cómo los colaboradores pueden contribuir a mitigarlas.													UTI
Talleres Prácticos	Buenas prácticas en el uso de aplicaciones web y configuración de seguridad en los dispositivos													UTI
	Identificación de vulnerabilidades y pautas para una navegación segura en entornos de red.													UTI
Lecciones aprendidas	Revisión de repositorio (base de conocimiento) de vulnerabilidades detectas y acciones de mitigación.													UTI

Fuente: Elaboración propia.