GESTIÓN OPERATIVA DE VULNERABILIDADES Y PARCHES DEL SGI

Procedimiento que establece la secuencia operativa para la identificación, registro, análisis, priorización, tratamiento, verificación y cierre de vulnerabilidades, así como para la evaluación, aplicación, validación y seguimiento de parches dentro del Sistema de Gestión Integral de GBInfragroup S.A. de C.V., con el fin de asegurar que las debilidades técnicas u operativas que afecten activos, servicios, configuraciones o componentes dentro del alcance del SGI se gestionen de forma controlada, trazable y oportuna, evitando exposición innecesaria, correcciones improvisadas, remediaciones no verificadas, acumulación de debilidades conocidas y falsa sensación de seguridad por cambios no validados.

Contenido

1. DATOS DE IDENTIFICACIÓN

Elemento	Definición
Código del documento	SGI-PRO-VUL-01
Nombre	Gestión Operativa de Vulnerabilidades y Parches del SGI
Tipo documental	Procedimiento
Responsable del documento	Responsable del SGI
Responsable de elaboración	Responsable del SGI
Revisor	Project Manager
Aprobador	Director General
Clasificación	Interno
Versión	1.0
Estado	Vigente

Vigencia / revisión	Revisión anual o cuando existan cambios relevantes en los activos bajo control, en la forma de identificar vulnerabilidades, en los mecanismos de remediación, en la gestión de parches, en la criticidad de los servicios o en los requisitos aplicables del SGI.
Ruta maestra editable	docs/02_Procedimientos_SGI/SGI-PRO-VUL-01_Gestion_Operativa_de_Vulnerabilidades_y_Parches_del_SGI_v1.0.docx
Ruta PDF publicada	SGI_pdf/02_Procedimientos_SGI/SGI-PRO-VUL-01_Gestion_Operativa_de_Vulnerabilidades_y_Parches_del_SGI_v1.0.pdf
Documentos relacionados	SGI-POL-GOV-01 Política Integrada del SGI; SGI-POL-SI-01 Política General de Seguridad de la Información, cuando aplique; SGI-PRC-GOV-03 Gestión de Riesgos y Oportunidades del SGI; SGI-PRC-CUM-01 Cumplimiento de Requisitos Aplicables del SGI, cuando aplique; SGI-PRC-SEG-01 Gestión de Incidentes de Seguridad de la Información del SGI, cuando aplique; SGI-PRC-SEG-02 Continuidad Operativa, BCP y DRP del SGI, cuando aplique; SGI-PRC-DOC-01 Control de la Información Documentada del SGI, cuando aplique; SGI-CRT-RSI-01 Criterios y Metodología de Evaluación de Riesgos de Seguridad de la Información; SGI-CRT-RSI-02 Criterios y Metodología de Tratamiento de Riesgos de Seguridad de la Información; SGI-FOR-VUL-01 Registro de Vulnerabilidades y Parches del SGI; SGI-FOR-COM-01 Registro de Comunicaciones Relevantes, cuando aplique; SGI-FOR-NCM-01 Registro de No Conformidades y Acciones Correctivas, cuando aplique.

2. OBJETIVO

Establecer la forma operativa en que se gestionan las vulnerabilidades y los parches dentro del SGI, desde la identificación o detección inicial hasta la remediación, validación y cierre, asegurando que toda debilidad relevante y toda actualización correctiva asociada se trate con base en criticidad, impacto operativo, trazabilidad documental y verificación posterior.

3. ALCANCE

Este procedimiento aplica a vulnerabilidades y parches relacionados con activos, sistemas, componentes, configuraciones, plataformas, servicios, herramientas, repositorios, dependencias tecnológicas o elementos operativos dentro del alcance del SGI cuya exposición pueda afectar la confidencialidad, integridad, disponibilidad, continuidad, cumplimiento o control del sistema.

Este procedimiento aplica tanto a vulnerabilidades identificadas por revisión interna, monitoreo, fabricante, proveedor, auditoría, incidente, cambio, revisión técnica o cualquier otro medio legítimo, como a parches correctivos, de seguridad o de mantenimiento cuya aplicación sea necesaria para reducir exposición o restablecer una condición aceptable de control.

Este procedimiento aplica desde la identificación de la vulnerabilidad o disponibilidad del parche hasta su priorización, tratamiento, aplicación, validación, documentación y cierre, incluyendo excepciones justificadas, aplazamientos controlados y escalamiento cuando corresponda.

Este procedimiento no sustituye la gestión de riesgos, la gestión de incidentes, la continuidad operativa ni los instructivos técnicos específicos de implementación. Su función es operacionalizar el tratamiento de vulnerabilidades y parches dentro del SGI.

4. DEFINICIONES

Término	Definición
Vulnerabilidad	Debilidad, condición deficiente, exposición o falta de control que puede ser aprovechada para comprometer un activo, servicio o recurso dentro del SGI.
Parche	Corrección, actualización o ajuste emitido para remediar una vulnerabilidad, falla o condición técnica identificada.
Remediación	Acción orientada a corregir, mitigar, reducir o eliminar una vulnerabilidad o su exposición asociada.
Priorización	Determinación del orden de atención de vulnerabilidades o parches con base en impacto, criticidad, exposición, explotabilidad y efecto operativo.

Validación posterior	Verificación realizada después de una remediación o aplicación de parche para confirmar que la condición tratada quedó efectivamente corregida o controlada.
Excepción de parcheo	Decisión documentada de no aplicar un parche de inmediato, bajo justificación y control definidos.
Vulnerabilidad recurrente	Debilidad que reaparece o persiste de forma reiterada pese a acciones previas de tratamiento.

5. ROLES Y RESPONSABILIDADES

Rol	Responsabilidad dentro del procedimiento
Responsable del SGI	Controla la trazabilidad documental de vulnerabilidades y parches, valida priorización cuando corresponda, asegura vinculación con riesgos y controla el cierre formal del caso.
Project Manager	Revisa impacto operativo de la remediación, coordina ventanas de intervención, dependencias y seguimiento cuando la corrección afecte proyectos, servicios o implementaciones.
Director General	Aprueba excepciones, aplazamientos o decisiones escaladas por impacto relevante, riesgo residual significativo o necesidad de decisión superior.
Responsable del activo, sistema o servicio afectado	Aporta contexto de criticidad, valida necesidad de intervención y confirma, desde su ámbito, el resultado funcional posterior al tratamiento.
Responsable técnico o administrador del componente afectado	Analiza la condición técnica, ejecuta la remediación o el parche, conserva evidencia y reporta resultado o desviaciones.
Fuente de detección o reportante	Informa la vulnerabilidad, disponibilidad del parche o condición observada con la información inicial disponible.

6. CONDICIONES PREVIAS Y CRITERIOS DE OPERACIÓN

6.1 Condiciones previas

1. Debe existir una vulnerabilidad identificada, un aviso de seguridad, una actualización relevante o una necesidad razonable de revisión sobre un activo o componente dentro del alcance del SGI.
2. Debe poderse asociar la vulnerabilidad o el parche con al menos un activo, sistema, servicio o condición operativa identificable.
3. Debe existir un medio formal para registrar detección, priorización, tratamiento, validación y cierre.
4. Deben estar identificados responsables de análisis, ejecución y validación funcional o técnica.
5. Toda decisión de no remediar o no aplicar un parche de inmediato deberá quedar justificada y controlada.

6.2 Criterios de aplicación

1. Toda vulnerabilidad relevante para el SGI deberá registrarse y evaluarse formalmente.
2. Ningún parche o remediación deberá aplicarse como cambio permanente sin control documental y sin validación posterior razonable.
3. Toda vulnerabilidad deberá priorizarse según criticidad, exposición e impacto operativo.
4. Toda remediación deberá distinguir entre corrección efectiva, mitigación temporal y excepción controlada.
5. Todo parche que afecte servicio crítico, continuidad o estabilidad operativa deberá coordinarse con las condiciones de implementación correspondientes.
6. Toda vulnerabilidad sin tratamiento inmediato deberá mantenerse visible con estado y justificación claros.
7. Toda falla de remediación o parche que genere afectación relevante deberá documentarse y tratarse conforme a su naturaleza.

6.3 Criterios de validación o aceptación

1. Una vulnerabilidad se considera válidamente abierta solo si cuenta con descripción suficiente, activo afectado o condición asociada y estado inicial.
2. La priorización se considera válida solo si puede sostenerse frente a criticidad, impacto, exposición y urgencia razonable.
3. Una remediación o parche se considera válidamente ejecutado solo si existe evidencia de aplicación o implementación suficiente.
4. La validación posterior se considera válida solo si confirma razonablemente que la vulnerabilidad fue corregida, mitigada o controlada.
5. El cierre se considera válido solo si el estado final del caso es claro y existe evidencia suficiente del tratamiento aplicado o de la excepción aprobada.

6.4 Criterios de excepción o escalamiento

1. Toda vulnerabilidad crítica, ampliamente expuesta, explotable o asociada a activo sensible deberá escalarse de inmediato.
2. Todo parche sobre componente crítico o servicio sensible deberá coordinarse con control reforzado antes de su aplicación.
3. Toda excepción de parcheo o aplazamiento de remediación deberá aprobarse y mantenerse bajo seguimiento.
4. Toda discrepancia material sobre prioridad, suficiencia del tratamiento o cierre del caso deberá documentarse y mantenerse visible hasta su resolución.
5. Toda vulnerabilidad que derive en incidente, continuidad comprometida o incumplimiento relevante deberá vincularse con el proceso correspondiente.

7. DESARROLLO DEL PROCEDIMIENTO

7.1 Entradas o insumos

Entrada / insumo	Origen	Documento relacionado
Detección de vulnerabilidad o aviso de seguridad	Responsable técnico, proveedor, fabricante, auditoría, monitoreo o reportante autorizado	Evidencia de detección o aviso aplicable

Información del activo, sistema o servicio afectado	Responsable del activo o responsable técnico	Documento o evidencia operativa aplicable
Información de criticidad, riesgo o tratamiento	Responsable del SGI	SGI-CRT-RSI-01; SGI-CRT-RSI-02
Información sobre disponibilidad de parche o corrección	Responsable técnico, proveedor o fabricante	Evidencia técnica o aviso de actualización aplicable
Medio formal de comunicación y seguimiento	Repositorio documental del SGI	SGI-FOR-COM-01, cuando aplique

7.2 Secuencia de actividades o instrucciones

Paso	Actividad o instrucción	Responsable	Descripción operativa	Registro o evidencia generada
1	Identificar la vulnerabilidad o disponibilidad de parche	Responsable técnico, reportante autorizado o Responsable del SGI	Detectar la vulnerabilidad, el aviso de seguridad o la actualización correctiva y recopilar la información inicial disponible.	Evidencia inicial de vulnerabilidad o parche.
2	Registrar el caso	Responsable del SGI	Abrir el registro del caso identificando activo o componente afectado, descripción, origen, estado inicial y condición preliminar.	Registro inicial de vulnerabilidad o parche.
3	Analizar alcance e impacto preliminar	Responsable técnico y Responsable del SGI	Determinar qué activo, servicio o condición resulta afectada, así como el posible impacto operativo, de seguridad o de cumplimiento.	Análisis preliminar documentado.

4	Priorizar el caso	Responsable del SGI	Asignar prioridad de tratamiento con base en criticidad, exposición, impacto, explotabilidad y necesidad de intervención.	Priorización documentada del caso.
5	Definir tratamiento	Responsable del SGI y responsable técnico	Determinar si procede parche, corrección de configuración, mitigación temporal, compensación de control, excepción justificada o combinación de medidas.	Decisión documentada de tratamiento.
6	Escalar cuando corresponda	Responsable del SGI	Someter a revisión superior los casos críticos, las excepciones relevantes, los aplazamientos significativos o los tratamientos con impacto mayor.	Evidencia de escalamiento, cuando aplique.
7	Planificar la ejecución	Responsable técnico y Project Manager, cuando aplique	Definir ventana de intervención, responsables, dependencias, respaldo previo y condiciones necesarias para aplicar el tratamiento.	Plan o preparación documentada de remediación.
8	Ejecutar remediación o aplicar parche	Responsable técnico o administrador del componente afectado	Implementar la corrección, mitigación o actualización conforme a la decisión autorizada.	Evidencia de ejecución del tratamiento.
9	Validar el resultado	Responsable técnico y responsable del activo o servicio afectado	Confirmar que la vulnerabilidad quedó corregida, mitigada o controlada y que el activo o servicio sigue en condición operativa aceptable.	Evidencia de validación posterior.

10	Documentar excepciones o aplazamientos, cuando apliquen	Responsable del SGI	Registrar justificación, plazo, condiciones de seguimiento y medidas compensatorias cuando el tratamiento no se aplique de inmediato.	Evidencia de excepción o aplazamiento controlado.
11	Comunicar resultado y acciones posteriores	Responsable del SGI	Informar a las partes correspondientes el resultado del tratamiento, el estado final o las acciones pendientes.	Evidencia de comunicación del resultado.
12	Cerrar el caso	Responsable del SGI	Formalizar el cierre con estado final claro, evidencia suficiente y trazabilidad hacia riesgos, incidentes, continuidad o no conformidades, cuando aplique.	Registro de cierre del caso.

7.3 Puntos de control y validación

Punto de control	Responsable	Criterio de validación	Acción si no cumple
Validación de apertura	Responsable del SGI	El caso cuenta con descripción suficiente, activo o condición afectada identificable y estado inicial claro.	Completar información antes de avanzar a priorización.
Validación de priorización	Responsable del SGI	La prioridad asignada es coherente con criticidad, exposición e impacto.	Revaluar prioridad antes de definir tratamiento final.
Validación de tratamiento	Responsable del SGI y responsable técnico	La decisión de remediación, mitigación o excepción es congruente con el nivel de exposición y con la capacidad operativa.	Ajustar el tratamiento o escalar antes de ejecutar o cerrar.
Validación de ejecución	Responsable del SGI	Existe evidencia suficiente de que el parche o remediación fue aplicado según lo autorizado.	Completar evidencia o corregir ejecución antes de cerrar.

Validación de cierre	Responsable del SGI	El caso tiene estado final claro, validación posterior suficiente y acciones posteriores definidas cuando aplican.	No cerrar hasta corregir vacíos de evidencia, validación o trazabilidad.

7.4 Salidas

Salida	Destino	Documento relacionado
Vulnerabilidad registrada, priorizada y tratada	Repositorio documental del SGI	SGI-FOR-VUL-01 Registro de Vulnerabilidades y Parches del SGI.
Parche o remediación ejecutados	Activo, sistema o servicio afectado y control documental aplicable	Evidencia de tratamiento ejecutado
Excepción o aplazamiento documentado, cuando aplique	Repositorio documental del SGI y responsables involucrados	Evidencia de excepción controlada
Validación posterior del tratamiento	Responsable del activo, responsable técnico y Responsable del SGI	Evidencia de validación posterior
Cierre del caso o derivación a otro proceso, cuando aplique	Repositorio documental del SGI	Evidencia de cierre o de derivación correspondiente

8. REGISTROS ASOCIADOS

Código o referencia	Nombre del registro o evidencia	Uso dentro del procedimiento
SGI-FOR-COM-01	Registro de Comunicaciones Relevantes	Registro de comunicaciones formales asociadas a vulnerabilidades, parches, excepciones o resultados, cuando aplique.
SGI-FOR-NCM-01	Registro de No Conformidades y Acciones Correctivas	Registro para tratar fallas sistemáticas, recurrencias o incumplimientos relevantes asociados a vulnerabilidades o parcheo, cuando aplique.

SGI-FOR-VUL-01	Registro de vulnerabilidades y parches	Registro principal para apertura, análisis, priorización, tratamiento, validación y cierre del caso.

9. REFERENCIAS NORMATIVAS Y DOCUMENTALES

1. ISO/IEC 27001:2022.
2. ISO/IEC 27002:2022.
3. SGI-POL-GOV-01 Política Integrada del SGI.
4. SGI-POL-SI-01 Política General de Seguridad de la Información, cuando aplique.
5. SGI-PRC-GOV-03 Gestión de Riesgos y Oportunidades del SGI.
6. SGI-PRC-CUM-01 Cumplimiento de Requisitos Aplicables del SGI.
7. SGI-PRC-SEG-01 Gestión de Incidentes de Seguridad de la Información del SGI.
8. SGI-PRC-SEG-02 Continuidad Operativa, BCP y DRP del SGI.
9. SGI-PRC-DOC-01 Control de la Información Documentada del SGI.
10. SGI-CRT-RSI-01 Criterios y Metodología de Evaluación de Riesgos de Seguridad de la Información.
11. SGI-CRT-RSI-02 Criterios y Metodología de Tratamiento de Riesgos de Seguridad de la Información.
12. SGI-FOR-COM-01 Registro de Comunicaciones Relevantes.
13. SGI-FOR-NCM-01 Registro de No Conformidades y Acciones Correctivas.

SGI-FOR-VUL-01 Registro de Vulnerabilidades y Parches del SGI.

10. ANEXOS

No aplica en la emisión inicial de este procedimiento.

11. APROBACIÓN DEL DOCUMENTO

Rol	Nombre / cargo	Fecha
Elaboró	Responsable del SGI	14/04/26
Revisó	Project Manager	14/04/26
Aprobó	Director General	14/04/26

Nota: Las firmas de aprobación se incorporan en la versión PDF final controlada del documento, conforme al mecanismo de autorización vigente de GBInfragroup S.A. de C.V.

12. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1.0	14/04/26	Emisión inicial del procedimiento.

Página final de firmas y certificación digital

Referencia visible de firmas digitales y certificación documental

Certificación expresa del documento

Yo, Raúl Rodríguez Macías, en mi carácter de Responsable del Sistema de Gestión Integral, certifico de manera expresa la integridad documental del presente PDF. Este documento incorpora las firmas digitales válidas de aprobación correspondientes y la presente constancia visible de cierre documental.

Aprobación del Project Manager

Firmante Bruno Ivan Reynoso Trejo
Cargo Project Manager
Alcance Aprobación ejecutiva de la emisión documental y conformidad con el contenido del documento.

Certificado digital
Titular: Bruno Ivan Reynoso Trejo | Emisor: PDF CA Interna Intermediate CA
Serie: 2CED87417FAEA06901F739758B92197C | Vigencia: 2026-04-15 a 2029-04-14

Aprobación de Dirección General

Firmante Juan Carlos Reyes Oropeza
Cargo Director General
Alcance Aprobación final institucional del documento dentro del marco de gobierno y dirección del SGI.

Certificado digital
Titular: Juan Carlos Reyes Oropeza | Emisor: PDF CA Interna Intermediate CA
Serie: A44658F437D7B4C68381429D1D3E6ABD | Vigencia: 2026-04-15 a 2029-04-14

Certificación documental del Responsable del SGI

Firmante Raul Rodriguez Macias
Cargo Responsable del Sistema de Gestión Integral
Alcance Constancia visible de cierre documental del PDF final y de incorporación de las firmas digitales previas.

Certificado digital
Titular: Raul Rodriguez Macias | Emisor: PDF CA Interna Intermediate CA
Serie: 1006D5244EA0DF0BBA77F08906A48975 | Vigencia: 2026-04-15 a 2029-04-14