1. OBJETIVO

Establecer los criterios, procedimientos y responsabilidades para identificar, clasificar, priorizar y remediar las vulnerabilidades de seguridad detectadas en la infraestructura tecnológica de la Entidad, mediante el uso de las herramientas Microsoft Intune, Microsoft Defender for Endpoint y Microsoft Defender for Cloud, así como la gestión de los hallazgos reportados por el COLCERT, DNI o el SOC sobre activos expuestos en internet, con el propósito de reducir la superficie de ataque y mantener un nivel de riesgo aceptable para la Entidad.

2. ALCANCE

La presente guía aplica desde la detección de vulnerabilidades hasta su cierre mediante remediación, mitigación, aceptación de riesgo o clasificación como falso positivo.

El alcance comprende los siguientes activos y entornos:

- Dispositivos finales (endpoints) gestionados mediante Microsoft Intune y Microsoft Defender for Endpoint, incluyendo equipos de cómputo, portátiles y servidores con agente instalado.
- Infraestructura en la nube y servidores monitoreados por Microsoft Defender for Cloud.
- Aplicaciones y servicios expuestos en internet, sujetos al análisis del COLCERT. DNI.
- Infraestructura de red y sistemas en todas las sedes donde la Entidad gestione activos tecnológicos.
- Monitoreo e inteligencia de amenazas del SOC o de los administradores de infraestructura a través de boletines oficiales de los fabricantes o del entorno mundial.
- Activos identificados y no identificados

Quedan excluidos de esta guía los activos de terceros sobre los cuales la Entidad no tiene capacidad de gestión directa, salvo cuando los contratos de servicio establezcan obligaciones específicas de remediación.

3. RESPONSABLE

El responsable de la ejecución y cumplimiento de esta guía es la Coordinación de Seguridad e informática Forense.

La siguiente tabla describe los roles y sus responsabilidades en el proceso:

Cargo / Dependencia	Responsabilidad
Coordinador de Seguridad e informática Forense	Realizar el seguimiento y control al proceso de gestión de vulnerabilidades, asegurando la identificación, análisis, priorización y tratamiento oportuno de las debilidades de seguridad detectadas en los activos de información. Lo anterior incluye la revisión sistemática de los reportes generados por el Centro de Operaciones de Seguridad (SOC), a través de la herramienta de gestión de vulnerabilidades de Microsoft Defender, con el propósito de evaluar la exposición al riesgo y verificar la efectividad de las acciones de remediación implementadas. Adicionalmente, se deberá efectuar el monitoreo a los planes de tratamiento definidos, garantizando su adecuada ejecución, así como la escalación oportuna de hallazgos críticos a la alta dirección, conforme a los lineamientos de gestión de riesgos de la organización. De igual manera, se contempla la gestión, análisis y seguimiento de los reportes emitidos por el COLCERT.
Funcionario del grupo de seguridad e Informática Forense	Ejecutar el ciclo integral de gestión de vulnerabilidades, que comprende la detección, análisis, priorización y seguimiento, mediante el uso de herramientas del ecosistema Microsoft. Coordinar con los equipos técnicos la implementación de acciones de remediación, asegurando su adecuada ejecución dentro de los tiempos establecidos. Asimismo, documentar los hallazgos identificados, mantener la trazabilidad de su tratamiento y generar los reportes correspondientes, con el fin de apoyar la mejora continua de la postura de seguridad y el cumplimiento de los lineamientos.
Administrador de Infraestructura / TI	Implementar los parches, actualizaciones y controles de remediación definidos, asegurando su ejecución dentro de los plazos establecidos y conforme a los procedimientos de gestión de cambios de la organización. Asimismo, informar de manera oportuna al responsable de Seguridad de la Información e Informática Forense sobre la ejecución de las actividades realizadas, garantizando la trazabilidad y el adecuado registro de los cambios efectuados.
Propietario del Activo	Autorizar los cambios en los sistemas bajo su responsabilidad, en cumplimiento de los procedimientos de gestión de cambios establecidos. Asimismo, evaluar y aceptar formalmente el riesgo residual derivado de vulnerabilidades que no puedan ser remediadas de manera inmediata, dejando constancia documentada de dicha decisión, junto con su justificación, nivel de riesgo y las medidas de tratamiento o mitigación definidas.

Oficial de Seguridad de la Información / CISO	Aprobar excepciones y aceptaciones de riesgo. Recibir informes periódicos del estado de vulnerabilidades, realizar reporte a terceros sobre el avance en las remediaciones.

4. DEFINICIONES

Activo Crítico: Aquel componente cuya indisponibilidad o compromiso afecta gravemente la operación del negocio o el cumplimiento de la misión de la Entidad.

Activo de información: Cualquier componente tecnológico (hardware, software, servicio o dato) que tenga valor para la Entidad y requiera protección.

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño a un sistema o a la organización.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Encargado de coordinar la ciberseguridad del Estado colombiano y emitir informes de vulnerabilidades a entidades del sector público.

Control compensatorio: Medida de seguridad alternativa implementada cuando no es posible aplicar la remediación principal, con el fin de reducir el riesgo de explotación de una vulnerabilidad.

CVSS (Common Vulnerability Scoring System): Sistema estándar de puntuación de vulnerabilidades que permite evaluar su severidad en una escala de 0 a 10, considerando factores como vector de ataque, complejidad e impacto.

CVE (Common Vulnerabilities and Exposures): Sistema de identificación pública de vulnerabilidades de seguridad conocidas, mantenido por el MITRE Corporation, que asigna un identificador único a cada vulnerabilidad.

Excepción de remediación: Autorización formal que permite no aplicar la corrección de una vulnerabilidad dentro del plazo estándar, sujeta a aprobación y controles compensatorios.

Exploit: Fragmento de software, comando o metodología utilizado para aprovechar una vulnerabilidad y causar un comportamiento no deseado.

Falso positivo: Reporte de vulnerabilidad generado por una herramienta que, tras análisis técnico, se determina que no representa un riesgo real en el contexto específico de la Entidad.

Microsoft Defender for Cloud: (MDFC) Plataforma de Microsoft para la gestión de postura de seguridad en la nube (CSPM) y protección de cargas de trabajo en la nube (CWP), que identifica configuraciones inseguras y vulnerabilidades en infraestructura Azure.

Microsoft Defender for Endpoint: (MDE) Solución de seguridad empresarial de Microsoft que proporciona detección y respuesta en endpoints (EDR), incluyendo capacidades de gestión de amenazas y vulnerabilidades (TVM).

Microsoft Intune: Plataforma de gestión unificada de endpoints de Microsoft que permite la administración de dispositivos móviles (MDM), aplicaciones (MAM) y políticas de seguridad, facilitando la distribución de parches y actualizaciones.

Parche de seguridad: Actualización de software emitida por el fabricante para corregir una o más vulnerabilidades de seguridad en un producto.

Remediación: Acción correctiva aplicada a un activo para eliminar o mitigar una vulnerabilidad identificada, que puede incluir la aplicación de parches, cambios de configuración o actualizaciones de software.

Riesgo aceptado: Decisión formal y documentada de no remediar una vulnerabilidad, asumiendo conscientemente el riesgo residual, previa autorización de los responsables competentes.

Secure Score: Puntuación en Microsoft Defender for Cloud que mide la postura de seguridad de la Entidad en la nube, basada en el cumplimiento de controles y recomendaciones de seguridad.

Superficie de ataque: Conjunto de puntos de entrada o vulnerabilidades en un sistema o red que pueden ser explotados por un agente de amenaza.

TVM (Threat & Vulnerability Management): Módulo de Microsoft Defender for Endpoint que proporciona visibilidad en tiempo real del inventario de software, configuraciones y vulnerabilidades en los endpoints de la Entidad.

Vulnerabilidad: Debilidad en un activo de información (software, hardware o configuración) que puede ser explotada por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de la información.

5. CONTENIDO

- La instalación oportuna de parches de seguridad permite reducir la exposición a vulnerabilidades conocidas, amenazas cibernéticas y explotación de debilidades técnicas en estaciones de trabajo y dispositivos administrados.
- La postergación de dichas actividades para procesos extensivos de aprobación manual podría incrementar el riesgo residual y afectar la postura de seguridad de la organización.
- Los parches son emitidos directamente por el fabricante, poseen soporte oficial, son distribuidos mediante una plataforma corporativa centralizada y se implementan de manera controlada y automatizada.
- Se realiza monitoreo continuo del despliegue y se mantiene evidencia de cumplimiento y resultados.
- Las actividades de parchado estándar no representan modificaciones arquitectónicas, cambios funcionales mayores ni alteraciones significativas en procesos de negocio, por lo que no requieren evaluación individual en la reunión de aprobación de cambios, salvo excepciones definidas.
- La Entidad aplica un enfoque basado en riesgo conforme al SGSI, determinando que: el riesgo de no aplicar oportunamente los parches es superior, mientras que el riesgo operativo del despliegue se mantiene mitigado mediante controles preventivos y detectivos.

5.1. Herramientas de Gestión de Vulnerabilidades

La Entidad dispone de un ecosistema unificado de soluciones Microsoft, diseñado para articular la detección, el análisis y la gestión de vulnerabilidades de manera integral. A continuación, se detalla el alcance y la funcionalidad de cada componente:

Herramienta	Ámbito de Detección	Función Principal
Microsoft Intune	Endpoints (dispositivos gestionados)	Gestión de parches del sistema operativo y aplicaciones en dispositivos Windows. Provee visibilidad de dispositivos no conformes y estado de actualización.
Microsoft Defender for Endpoint	Endpoints y red interna	Detección y respuesta en endpoints (EDR). Identifica vulnerabilidades del sistema operativo, software instalado y configuraciones inseguras mediante Threat & Vulnerability Management (TVM).
Microsoft Defender for Cloud	Infraestructura cloud y servidores	Gestión de postura de seguridad en la nube (CSPM). Identifica configuraciones inseguras, vulnerabilidades en máquinas virtuales y recursos de Azure. Genera recomendaciones con puntuación de seguridad (Secure Score).
Microsoft Defender Vulnerability	Activos de usuario final y su configuración de seguridad	Comprende la identificación continua de vulnerabilidades, configuraciones inseguras y debilidades de seguridad en dispositivos finales (endpoints), incluyendo estaciones de trabajo, servidores y equipos portátiles. Asimismo, permite detectar software desactualizado, aplicaciones con vulnerabilidades conocidas (CVE), configuraciones que no cumplen con las líneas base de seguridad y posibles exposiciones derivadas de malas prácticas de configuración.
Análisis COLCERT	Superficie externa (internet)	Análisis periódico de vulnerabilidades en aplicaciones y servicios expuestos a internet. Cubre CVEs conocidos, configuraciones inseguras, puertos expuestos y hallazgos de seguridad en la capa de aplicación.
Inteligencia de Amenazas – SOC	Infraestructura tecnológica	Reportar de acuerdo con los análisis e inteligencia de amenazas las vulnerabilidades identificadas y determinar la superficie de ataque y las implicaciones sobre la Tecnología de la Entidad

Adicionalmente, de manera semestral el COLCERT remite un informe con los resultados del análisis de vulnerabilidades sobre las aplicaciones e infraestructura expuesta en internet, el cual debe integrarse al proceso de gestión de vulnerabilidades como una fuente de detección externa complementaria.

5.2 Clasificación y Priorización de Vulnerabilidades

La priorización considera toda vulnerabilidad que se identifique, debe clasificarse según la puntuación del sistema CVSS v3.1. La siguiente tabla establece los niveles de severidad y los tiempos máximos de remediación aplicables a la Entidad:

Nivel de Severidad	Puntuación CVSS	Tiempo de Remediación	Descripción
Crítica	9.0 – 10.0	15 días calendario	Vulnerabilidades con alto impacto, explotables de forma remota y sin autenticación.
Alta	7.0 – 8.9	30 días calendario	Vulnerabilidades con impacto significativo que requieren intervención prioritaria.
Media	4.0 – 6.9	60 días calendario	Vulnerabilidades con impacto moderado; pueden requerir condiciones específicas para explotarse.
Baja	0.1 – 3.9	90 días calendario	Vulnerabilidades con impacto limitado; se gestionan en ciclos de mantenimiento regular.
Informativa	0.0	Próximo ciclo de mantenimiento	Hallazgos informativos o buenas prácticas recomendadas sin riesgo inmediato.

En caso de que la herramienta de detección no proporcione una puntuación CVSS, el funcionario de Seguridad e Informática Forense asignará un nivel de severidad con base en el impacto potencial sobre la confidencialidad, integridad y disponibilidad del activo afectado, documentando la justificación de la clasificación asignada.

Para la priorización de la remediación, además de la severidad CVSS se considerarán los siguientes factores adicionales:

- Criticidad del activo afectado para la operación de la Entidad.
- Disponibilidad de un exploit público conocido (KEV – Known Exploited Vulnerabilities de CISA).
- Exposición del activo a redes no confiables o a internet.
- Volumen y sensibilidad de los datos procesados por el sistema afectado.

5.3 Ciclo de Gestión de Vulnerabilidades Internas (Herramientas Microsoft)

El ciclo de gestión de vulnerabilidades internas comprende las siguientes fases:

5.3.1 Detección y Descubrimiento:

La detección y descubrimiento de vulnerabilidades se realiza de manera continua mediante herramientas automatizadas y fuentes externas de información, con una frecuencia mínima de revisión semanal. Este proceso garantiza la identificación oportuna de vulnerabilidades técnicas, configuraciones inseguras, software desactualizado y activos no inventariados dentro de la infraestructura tecnológica de la Entidad.

La detección incluye vulnerabilidades conocidas (CVE), configuraciones que no cumplen con las líneas base de seguridad, exposición de servicios y posibles debilidades identificadas a través de inteligencia de amenazas.

Las actividades de detección se ejecutan a través de las siguientes herramientas:

- **Microsoft Defender for Endpoint – TVM**: ejecuta análisis continuos sobre endpoints gestionados, identificando vulnerabilidades de software instalado, configuraciones del sistema operativo y ausencia de parches. La revisión del portal se realiza como mínimo con frecuencia semanal.
- **Microsoft Defender for Cloud**: monitorea continuamente la postura de seguridad de los recursos en la nube. El Analista de Seguridad revisa las recomendaciones activas y las alertas del Secure Score con frecuencia mínima semanal.
- **Microsoft Intune**: Detecta e identifica dispositivos con actualizaciones pendientes, políticas de cumplimiento no satisfechas y software no autorizado. La revisión de cumplimiento se realiza semanalmente.
- **Fuentes externas (COLCERT, SOC e inteligencia de amenazas):** se integran reportes de vulnerabilidades, alertas de seguridad, boletines de fabricantes y análisis de superficie expuesta en internet, con el fin de complementar la detección interna y ampliar la visibilidad del riesgo.

Adicionalmente, este proceso contempla la identificación de activos no registrados (Shadow IT), mediante el análisis del inventario de dispositivos y software reportado por las herramientas de seguridad, con el fin de asegurar la cobertura completa del proceso de gestión de vulnerabilidades.

5.3.2 Registro y Documentación

Cada vulnerabilidad identificada con severidad media o superior es generada a través de un reporte de Vulnerabilidades, Remediaciones, Eventos MDE generada por Defender el cual incluye la siguiente información:

- CVE asociado (cuando aplique).
- Nivel de severidad CVSS y puntuación.
- Fecha Publicación
- Fue Explotado
- Amenazas conocidas
- Software relacionado
- Maquinas expuestas

- Estatus
- Herramienta o fuente de detección.
- Activo(s) afectado(s) con su clasificación de criticidad.
- Fecha de detección y fecha límite de remediación.
- Responsable de la remediación
- Estado: Abierta / En gestión / Cerrada / Aceptada / Falso positivo.

5.3.3 Análisis y Asignación

El funcionario de Seguridad e Informática Forense evalúa cada vulnerabilidad registrada, y si no tiene prioridad la determina conforme a los criterios establecidos en la sección 5.2 y asigna formalmente las actividades de remediación al equipo responsable, definiendo la acción requerida y el plazo de ejecución.

Para la ejecución de las acciones de remediación, las vulnerabilidades asociadas a servidores e infraestructura tecnológica serán gestionadas por el grupo GSAT o GIIDA, mientras que aquellas relacionadas con endpoints o estaciones de trabajo serán atendidas por el responsable de la administración de Microsoft Intune. En todos los casos, se deberá garantizar la coordinación entre las áreas involucradas, así como el seguimiento y la trazabilidad de las acciones implementadas hasta su cierre.

5.3.4 Remediación

La remediación de vulnerabilidades se ejecuta mediante mecanismos técnicos y administrativos, definidos según la herramienta de detección, el tipo de vulnerabilidad y la criticidad del activo afectado, garantizando la reducción efectiva del riesgo.

Las acciones de remediación incluyen:

- Aplicación de parches del sistema operativo y software de terceros mediante Microsoft Intune, a través de perfiles de actualización, políticas de cumplimiento y despliegues controlados.
- Remediación guiada en Microsoft Defender for Endpoint: las recomendaciones de TVM pueden generar tareas de remediación que se envían directamente al grupo GSAT a través del CST.
- Aplicación de recomendaciones de seguridad en Microsoft Defender for Cloud, incluyendo correcciones de configuración en recursos Azure.
- Cambios de configuración, restricción de accesos, des habilitación de servicios innecesarios o implementación de controles compensatorios cuando el parche no está disponible.
- En escenarios donde el parche no está disponible o existe una incompatibilidad operativa, se aplicarán cambios de configuración, restricción de accesos mediante Acceso Condicional, des habilitación de servicios innecesarios o implementación de reglas en controles de protección perimetral.

- En entornos de nube pública y servicios externos, la remediación se gestiona bajo el modelo de responsabilidad compartida, aplicando los mecanismos y recomendaciones del proveedor. Cuando la remediación inmediata no es posible, se aplican controles compensatorios como parches virtuales, reglas en firewalls de nueva generación y configuraciones en balanceadores de carga para reducir la exposición y proteger los activos.
- La implementación de parches de seguridad y calidad liberados por fabricantes autorizados y desplegados mediante herramientas corporativas administradas (ej. Microsoft Intune) se considera un Cambio Estándar preaprobado, debido a su naturaleza repetitiva, bajo riesgo controlado y necesidad operativa de remediación oportuna.
- Se determinan los siguientes controles para el cambio estándar:
  - Validación Previa e informada
  - Grupo piloto previo.
  - Criterios de exclusión.
  - Métricas de éxito/falla.
  - Plan de reversa.
  - Evidencia de monitoreo.

  Excepción: Las remediaciones que afecten los ambientes productivos deben seguir las actividades establecidas en el GTI-PR-006 GESTION DE CAMBIOS AMBIENTE PRODUCTIVO cuando:

  - El parche es crítico y urgente y afecta sistemas Core
  - Requiere reinicio masivo
  - Cambia configuraciones sensibles
  - Tiene antecedentes de incompatibilidad
  - Despliegues extraordinarios fuera del ciclo estándar

5.3.5 Verificación y Cierre

Una vez ejecutada la remediación, el funcionario del grupo de seguridad e informática forense verifica su efectividad mediante la herramienta correspondiente (re-escaneo o validación en el portal), genera el reporte y cierra formalmente el hallazgo con fecha de cierre y evidencia del resultado. Las vulnerabilidades críticas y altas requieren verificación técnica obligatoria antes del cierre.

5.3.6 Seguimiento y Reporte

El funcionario del grupo de seguridad e informática Forense genera un informe del resumen de seguridad mensual que contiene la puntuación de seguridad de Microsoft de estado de vulnerabilidades dirigido al Coordinador de Seguridad e Informática Forense, que incluye:

Número de vulnerabilidades detectadas por severidad, porcentaje de cumplimiento en plazos de remediación, tendencias y excepciones activas. El Coordinador de Seguridad de Informática Forense realiza la medición de los indicadores correspondientes para reporte mensual.

5.4 Gestión de Hallazgos del COLCERT (Superficie Externa)

El COLCERT realiza análisis periódicos (mínimo anualmente) de la superficie expuesta en internet de la Entidad, reportando vulnerabilidades en aplicaciones web, servicios expuestos, configuraciones inseguras y otros hallazgos visibles desde redes externas. Estos hallazgos tienen carácter oficial y deben gestionarse con la máxima prioridad.

El proceso de gestión de los hallazgos del COLCERT es el siguiente:

Paso	Actividad	Descripción
1	**Recepción del informe**	El director de Tecnología recibe el informe semestral del COLCERT con los hallazgos de vulnerabilidades sobre activos expuestos en internet.
2	**Registro en la bitácora**	El Coordinador de Seguridad e informática Forense registra todos los hallazgos en una bitácora para definir el plan de mejoramiento, fecha de recepción, actividades para su mitigación.
3	**Análisis y priorización**	Se evalúa el impacto de cada hallazgo considerando: criticidad CVSS, exposición del activo, facilidad de explotación y datos procesados por el sistema afectado.
4	**Notificación a Administradores de TI**	Se notifica formalmente a los administradores de cada uno de los activos afectados sobre los hallazgos y los plazos de remediación requeridos.
5	**Ejecución de remediación**	El Administrador de Infraestructura aplica los controles correctivos: parches, cambios de configuración, restricción de accesos o implementación de controles compensatorios.
6	**Verificación y cierre**	El Oficial de Seguridad de la Información realiza seguimiento trimestral al estado de la remediación y verifica la efectividad de la remediación. Si el COLCERT realizó el hallazgo, se documenta la subsanación para evidencia ante el siguiente ciclo de análisis.
7	**Reporte a Alta dirección**	El Oficial de Seguridad presenta un informe en el Comité Institucional de Gestión y desempeño con el estado de remediación, hallazgos pendientes y riesgos aceptados.

Los plazos de remediación para los hallazgos del COLCERT se rigen por los tiempos definidos en la tabla de clasificación CVSS (sección 5.2). En ningún caso los hallazgos críticos o altos reportados por el COLCERT podrán quedar sin plan de remediación activo al momento del siguiente ciclo de análisis semestral.

5.5 Gestión de Excepciones y Aceptación de Riesgo

Cuando no sea posible remediar una vulnerabilidad dentro del plazo establecido, o cuando la remediación no sea técnicamente viable, se deberá gestionar formalmente mediante uno de los siguientes mecanismos:

Tipo	Condición	Requisito
Excepción temporal	La remediación no puede realizarse en el plazo definido por razones técnicas o de negocio justificadas.	Aprobación del Oficial de Seguridad de la Información. Plazo máximo de extensión: 30 días adicionales con controles compensatorios activos.
Aceptación de riesgo	La vulnerabilidad no puede remediarse por incompatibilidad técnica o costo desproporcionado frente al riesgo.	Aprobación del director de la Dirección de Tecnologías de la Información y las Comunicaciones y el Oficial de Seguridad de la información. Revisión obligatoria Cada 6 meses.
Falso positivo	La herramienta reporta una vulnerabilidad que tras análisis técnico se determina que no aplica al contexto.	Documentación técnica del análisis que justifica el descarte. Aprobación de los coordinadores de los grupos de infraestructura, seguridad y desarrollo.

Toda excepción o aceptación de riesgo debe documentarse en la matriz de seguimiento de vulnerabilidades e incluir: justificación técnica o de negocio, controles compensatorios implementados, plazo de revisión y firmas de los autorizadores competentes. No se aceptarán riesgos de vulnerabilidades críticas sin controles compensatorios activos y documentados.

5.6 Indicadores de Gestión (KPIs)

El proceso de gestión de vulnerabilidades se medirá mediante los siguientes indicadores:

Indicador	Meta	Frecuencia de Medición
Vulnerabilidades críticas remediadas o solucionadas vulnerabilidades criticas mitigadas / vulnerabilidades criticas identificadas	**20%**	Mensual

Los resultados de los indicadores serán revisados por el Coordinador de Seguridad e Informática Forense y reportados mensualmente como parte de los indicadores del plan estratégico sectorial y en el comité institucional de gestión y desempeño, y formarán parte de los insumos para la revisión del Sistema de Gestión de Seguridad de la Información (SGSI).

5.7 Integración con la Gestión de Cambios y Continuidad

La aplicación de parches y controles de remediación sobre sistemas productivos (core) debe coordinarse con el procedimiento GTI-PR-006 GESTION DE CAMBIOS AMBIENTE PRODUCTIVO, garantizando que las ventanas de mantenimiento no excedan los plazos de remediación

establecidos y que estos cambios no afecten la disponibilidad de servicios críticos evaluando el impacto y estableciendo los planes de rollback.

5.8 Comunicación y Notificación de Incidentes

Cuando se detecte que una vulnerabilidad activa ha sido explotada o existe evidencia razonable de intento de explotación, el hallazgo debe escalarse inmediatamente de acuerdo con lo establecido en la GTI-GU-006 GUIA DE GESTION DE INCIDENTES.

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	30/06/2026	Versión inicial del documento.

Elaboró	Revisó	Aprobó
Nombre: Jeny Díaz Cargo: Profesional Fecha: 14/04/2026	Nombre: Rocio Pedrozo Cargo: Coordinador Grupo de Seguridad e informática Forense Fecha:20/4/2026 Nombre: Iván Alexis Ontibon Rojas Cargo: Contratista OAP Fecha: 20/4/2026	Nombre: Ricardo Ríos Fernelix Cargo: director de Tecnología de la información y las comunicaciones Fecha:16/06/2026