ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO

6 PLAN DE MANTENIMIENTO PARA IMPRESORAS Y PERIFERICOS

SERVICIO TÉCNICO

- **Localidades:** Las localidades incluyen la Republica Dominicana, EEUU y España.

- **Infraestructura de Soporte:** La infraestructura de Soporte consta de al menos:

- **República Dominicana:**

- Técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Hasta 15 técnicos locales del C4RD disponibles de forma presencial
- Cuatro (4) Regionales existentes en la actualidad desde donde se habilitará el servicio de manera estratégica. Allí, en la localidad, C4RD dispondrá de su estructura de soporte actual incluyendo la inclusión de personal técnico propio del fabricante cuando fuese necesario como la infraestructura de recursos en la localidad, transporte, taller y/o almacenes de repuestos debidamente equipados con las herramientas de trabajo, etc

- **EEUU:**

- 4 técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Hasta 70 técnicos locales del C4RD disponibles de forma presencial
- Regional existente en la actualidad desde donde se habilitará el servicio de manera estratégica, siendo Nueva York el punto de atención focal. Allí C4RD dispondrá de su estructura de soporte actual incluyendo, personal técnico propio del fabricante como la infraestructura de recursos en la localidad, transporte, taller y/o almacén de repuestos debidamente equipados con las herramientas de trabajo, etc.

- **España:**

- 4 técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Se contara con al menos 1 técnico local del C4RD disponibles de forma presencial
- Una (1) Region actualmente existente desde donde se habilitará el servicio de manera estratégica, incluyendo Madrid. Allí C4RD dispondrá de su estructura de soporte actual incluyendo, personal técnico propio del fabricante como la infraestructura de recursos en la localidad, transporte, taller y/o almacén de repuestos debidamente equipados con las herramientas de trabajo, etc.

- **Tiempos de Respuesta:**

- Ocho (8) horas de tiempo de respuesta en localidades lejanas; desplazamientos mayores a 2 hrs.
- Cuatro (4) horas en localidades cercanas a los centros de servicios de C4RD; desplazamientos menores a 2 horas.

- **Contingencia:**

- Cada localidad regional de servicios de C4RD contara con al menos un equipo funcional disponible y referido de este lote para sustitución inmediato además de Trick de partes y piezas para reparación.
- Todos los recursos técnicos tienen disponibles medios de comunicación con alcance mundial disponibles, entre sí, con fuentes de información centralizada para consulta técnica; algunas de estas comprenden WhatsApp, llamadas locales y/o llamadas internacionales, etc
- Las fuentes de soporte de asistencia técnica del fabricante, a nivel mundial, están disponibles con respecto al horario laborable del hemisferio occidental, cubriendo entre 8 - 19 hrs diarias entre Domingo y viernes, aprovechando el centro de soporte de Dubái en el medio oriente y el de Bogotá en América Latina.
- 8-9 hrs en ventaja con el horario de apertura de labores con NY, Santo Domingo durante el año.
- 1-2 hrs con el horario de cierre de labores con NY, Santo Domingo durante el año.

- **Registro del Incidentes:**

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.
- Incluir la siguiente información:
- Nombre de la entidad reportante (JCE.RD, JCE.EEUU o JCE.UE).
- Fecha y hora del incidente.
- Identificar como Impresora o Periférico
- Serie del equipo
- Descripción detallada del problema.
- Componentes afectados
- Nivel de urgencia del incidente

- **Protocolos de Escalamiento y Gestión de Incidentes:**

- Definición de niveles de escalamiento con tiempos de respuesta específicos según la criticidad del incidente.
- Disponibilidad de un equipo de soporte de segundo y tercer nivel para atender problemas complejos de hardware y software.

6.1 PLAN DE MANTENIMIENTO PARA PKI

6.1.1 INTRODUCCIÓN

Este documento establece los lineamientos para garantizar la continuidad y estabilidad de la infraestructura PKI-CA suministrada por el consorcio C4RD a la Junta Central Electoral (JCE). La infraestructura PKI es un pilar fundamental para la seguridad digital y la confianza en las transacciones electrónicas, permitiendo la autenticación, el cifrado y la firma digital de documentos.

Garantizar un plan de soporte técnico robusto es esencial para mantener la disponibilidad y la integridad de la plataforma. La implementación de GET Trust, junto con las mejores prácticas de mantenimiento y monitoreo, permite el cumplimiento de normativas internacionales y la continuidad operativa del sistema.

6.1.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA DEL PKI – CA

La JCE depende de la gestión técnica de C4RD para administrar la infraestructura PKI-CA, que abarca la generación y revocación de certificados, el monitoreo de riesgos y el cumplimiento de estándares globales. A través de este esquema, a la JCE se le garantiza la seguridad de sus procesos digitales, mientras que C4RD implementa además medidas para prevenir fallos y responder ante cualquier incidente.

Este programa de soporte y mantenimiento cubre los siguientes aspectos clave:

- **Infraestructura PKI-CA:** responsable de la gestión de claves, la generación y revocación de certificados, así como la administración de la Autoridad de Certificación (CA).
- **Monitoreo y gestión de incidentes:** Se implementan herramientas de auditoría y supervisión que permiten a la JCE detectar y reportar riesgos en tiempo real, mientras que C4RD ejecuta las acciones correctivas necesarias.
- **Seguridad y cumplimiento:** C4RD garantiza la adhesión a los estándares internacionales, como EAL4+, eIDAS y FIPS 140-2, asegurando la protección de la información manejada por la JCE.

El mantenimiento efectivo de la infraestructura PKI-CA es clave para preservar la autenticidad de los procesos digitales. Su robustez depende de una gestión eficiente del ciclo de vida y de la respuesta oportuna ante cualquier incidencia.

6.1.3 MODELOS DE SERVICIO Y SLA

Para garantizar tiempos de respuesta óptimos, la JCE contara con un esquema de soporte técnico proporcionado por C4RD en tres niveles: desde la resolución de consultas básicas hasta la intervención especializada. Los acuerdos de nivel de servicio (SLA) permitirán a la JCE operar sin interrupciones, asegurando que los incidentes sean atendidos según su nivel de criticidad.

Para garantizar la eficiencia y disponibilidad del sistema, C4RD ha definido tres niveles de soporte:

- **Nivel 1 (L1):** Atención inicial y resolución de consultas básicas.

- **Nivel 2 (L2):** Gestión de incidencias técnicas y soporte especializado.
- **Nivel 3 (L3):** Intervención de ingeniería avanzada y escalamiento a proveedores.

6.1.4 SLA Y TIEMPOS DE RESPUESTA

Los tiempos de atención se han definido para minimizar el impacto de las incidencias, en horario 7:00AM a 6:00PM de lunes a viernes y los sábados de 8:00 a 1:00 PM

- **Incidentes críticos (P1):** Respuesta en menos de 2 horas.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- **Incidentes mayores (P2):** Respuesta en menos de 6 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
  -
- **Incidentes mayores (P3):** Respuesta en menos de 8 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
  -
- **Incidentes menores (P4):** Respuesta en menos de 1 día.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

Estos niveles de servicio garantizan la operatividad de la infraestructura y evitan interrupciones en la emisión y validación de certificados digitales.

6.1.5 PROCEDIMIENTO PARA LA APERTURA DE INCIDENTES POR PARTE DE LA JCE

El protocolo de soporte a la JCE requiere el seguir un protocolo estructurado para reportar incidentes a C4RD, incluyendo la clasificación por nivel de urgencia y el envío de información detallada para un diagnóstico preciso. C4RD, a su vez, evalúa cada caso y asigna recursos especializados para su resolución, garantizando una comunicación fluida con la JCE hasta la solución del problema.

Este modelo de soporte robusto gestionado por C4RD, con más de 15 años de experiencia en procesos críticos de negocios del sector privado y público probado ante exigencias de trafico de alta demanda del sector financiero nacional y de servicios públicos opera 24/7 para atenderá cualquier incidencia que afecte la infraestructura PKI-CA.

Este capítulo describe la metodología de categorización y escalamiento de problemas, asegurando que la JCE cuente con un servicio confiable y eficiente en la resolución de inconvenientes técnicos. La metodología implementada por C4RD se basa en un enfoque estructurado de gestión de incidentes, que incluye la identificación, registro, clasificación por niveles de criticidad (P1 a P4), diagnóstico inicial, asignación de recursos especializados, resolución y documentación del incidente.

Además, están establecidos procedimientos de escalamiento para garantizar que, en caso de problemas complejos, los niveles de soporte superiores intervengan de manera oportuna, minimizando el impacto en las operaciones de la JCE.

6.2 CUADRO DE ESCLAMEINTO INCLUYENDO

Matriz de Escalamiento Mesa de Servicios - TIC							
Niveles	Soporte	Tiempo de Respuesta	Puesto	Nombres	Contacto	Móvil	Correo
1	L1	De 1 a 30 Minutos	Técnico Especialista 1 - CSI	Mesa de Servicio CSI	809-567-0022 Ext. 282	Técnico de Turno	ServiciosTIC@grupocsi.com.do
2		30 Minutos a 60 Minutos	Técnico Especialista 2 - CSI	Mesa de Servicio CSI	809-567-0022 Ext. 262	(849) 886 2012	jli.infante@grupcsi.com.do
3		60 Minutos (1 Horas) a 120 Minutos (2 Horas)	Gerente de Servicios TIC - CSI	Federico Norberto	809-567-0022 Ext. 281	(809) 443 1502	f.norberto@grupocsi.com.do
4		2 a 3 Horas	VP Comercial - CSI	Ruben Cordero	809-567-0022 Ext. 239	(809) 603 8696	r.cordero@grupocsi.com.do
5		3 a 4 Horas	Presidente - CSI	Manuel Infante	809-567-0022 Ext.222	(809) 430-7242	jm.infante@grupocsi.com.do
6	L2	4 Horas o Mas	Mesa de Servicios GetGroup				soportelatam@getlatamprojects.com

Cuando la JCE identifique un problema en la infraestructura PKI-CA, deberá seguir el siguiente procedimiento para reportarlo a C4RD:

1. **Registro del Incidente**

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.
- Incluir la siguiente información:

  - Nombre de la entidad reportante (JCE).
  - Fecha y hora del incidente.
  - Descripción detallada del problema.
  - Componentes afectados dentro de la infraestructura PKI-CA.
  - Capturas de pantalla o logs relevantes.
  - Nivel de urgencia del incidente.

2. **Clasificación del Incidente**

- **Máxima (P1):** El servicio de PKI-CA está completamente inoperativo.
- **Alta (P2):** Falla parcial que afecta la operación de la JCE.
- **Media (P3):** Problemas que afectan el rendimiento sin impacto inmediato.
- **Baja (P4):** Incidentes menores atendidos en la siguiente ventana de mantenimiento.

3. **Evaluación y Diagnóstico Inicial**

- C4RD realizará un análisis preliminar y solicitará información adicional si es necesario.

4. **Resolución y Seguimiento**

- C4RD asignará un técnico según la criticidad del incidente.
- Se mantendrá una comunicación constante con la JCE hasta la resolución.
- Se emitirá un informe con causas y medidas correctivas.

6.3 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

La continuidad operativa de la infraestructura PKI-CA de la JCE está respaldada por un plan de mantenimiento estructurado por C4RD. Las tareas preventivas incluyen auditorías de seguridad, actualizaciones de software y revisión de certificados, mientras que el mantenimiento correctivo aborda fallos imprevistos para minimizar el impacto en los servicios digitales de la JCE.

El mantenimiento preventivo, ejecutado por C4RD, incluye:

- Renovación y revocación programada de certificados.
- Verificación de integridad del HSM.
- Simulacros de incidentes y evaluaciones de rendimiento.
- Revisión de certificados y actualización de software.
- Pruebas de penetración y seguridad.

El mantenimiento correctivo responde a fallas imprevistas mediante:

- Atención inmediata de fallos críticos.
- Sustitución de hardware según acuerdos con proveedores.
- Monitoreo de la integridad de certificados emitidos y revocados.

6.4 SEGURIDAD Y CUMPLIMIENTO

Con la JCE, C4RD trabajaremos en conjunto para mantener la infraestructura PKI-CA alineada con estándares internacionales de seguridad, protegiendo la integridad de los datos y la identidad digital. C4RD implementara auditorías periódicas y monitoreo constante para detectar posibles vulnerabilidades, asegurando que la misma cumpla con los requisitos regulatorios en la gestión de certificados digitales.

Para garantizar la seguridad de la infraestructura PKI-CA, C4RD implementa:

- Auditorías internas propias y externas via terceros.
- Monitoreo continuo para prevenir accesos no autorizados.
- Políticas de control de acceso basado en roles.
- Procedimientos de respuesta a incidentes de seguridad.

6.5 KPIS Y MÉTRICAS DE RENDIMIENTO

Para evaluar la efectividad del soporte técnico, la JCE y C4RD dejaran definidos indicadores claves de rendimiento (KPIs) como la disponibilidad del sistema, el tiempo de respuesta ante incidentes y la satisfacción del cliente. El monitoreo constante de estos parámetros permite optimizar los procesos y garantizar la fiabilidad de la infraestructura PKI-CA.

Se emitirán informes mensuales de rendimiento del mes anterior y se ejecutarán conferencias recurrentes de análisis de estos.

Para evaluar la efectividad del soporte, se establecen los siguientes indicadores:

- **Disponibilidad del sistema:** >99.9%.
- **Cumplimiento del SLA:** >95% de los incidentes resueltos dentro del tiempo.
- **Tiempo promedio de resolución:** Optimización de respuestas según la criticidad.
- **Satisfacción del cliente:** Evaluaciones continuas para mejora del servicio.

Este programa garantizara la estabilidad, seguridad y disponibilidad de la infraestructura PKI-CA, reforzando la confianza de la ciudadanía en los servicios de la JCE

6.6 PLAN DE MANTENIMIENTO PARA TARJETA DIGITAL

6.6.1 INTRODUCCIÓN

El presente documento define el **Programa de Soporte y Mantenimiento** para la plataforma de Cédula de Identidad Digital basada en GET Mobile ID, instalada e implementada por GET Group para la JCE. Dado que esta plataforma es crítica para la gestión de identidad nacional, se establece un esquema de soporte robusto y alineado con las mejores prácticas de la industria, garantizando alta disponibilidad (99.95%), seguridad avanzada y continuidad operativa.

Este programa contempla modelos de servicio y SLA, mantenimiento preventivo y correctivo, cumplimiento con regulaciones de seguridad, y métricas de rendimiento que permitan monitorear y optimizar el funcionamiento de la plataforma.

6.6.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA

El soporte y mantenimiento de la plataforma GET Mobile ID abarca las siguientes áreas clave:

- **Infraestructura Tecnológica**: Servidores, almacenamiento, red y elementos de seguridad como NG Firewalls y WAF.
- **Software y Aplicaciones**: Mantenimiento de GET Mobile Administrator, GET Mobile ID y GET Mobile Verify.
- **Base de Datos y Firmado Digital**: Gestión del ciclo de vida de los certificados digitales, claves de firma y bases de datos vinculadas al sistema de identidad digital.
- **Monitoreo y Respuesta a Incidentes**: Supervisión proactiva de los servicios para garantizar alta disponibilidad.
- **Gestiones con la Junta Central Electoral (JCE)**: Coordinación para integraciones, actualizaciones y cambios en los procedimientos de identidad digital.

El servicio está diseñado para operar en un modelo **24/7** con distintos niveles de soporte técnico, asegurando la resolución eficiente de incidentes y la actualización continua de la plataforma.

6.6.3 MODELOS DE SERVICIO Y SLA

El servicio de soporte se estructura en distintos niveles, con acuerdos de nivel de servicio (SLA) bien definidos para cada categoría de incidencia en horario 7:00AM a 6:00PM de lunes a viernes y los sábados de 8:00 AM a 1:00 PM:

- **Nivel 1 (Soporte Básico y Atención al Cliente)**: Resolución de consultas, asistencia básica y gestión de usuarios.

- **Nivel 2 (Soporte Técnico Especializado)**: Diagnóstico avanzado de problemas, configuraciones de software y ajustes de red.
- **Nivel 3 (Soporte de Infraestructura y Seguridad)**: Resolución de incidentes críticos, recuperación ante desastres y gestión avanzada de seguridad.

6.6.4 ACUERDOS DE NIVEL DE SERVICIO (SLA):

- **4. Acuerdos de Nivel de Servicio (SLA):**
- **Incidentes críticos (P1):** Respuesta en menos de 2 horas.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- **Incidentes mayores (P2):** Respuesta en menos de 6 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- **Incidentes mayores (P3):** Respuesta en menos de 8 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

Incidentes menores (P4): Respuesta en menos de 1 día.

  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

Cuando la JCE identifique un problema en el servicio de la infraestructura Cedula Digital, deberá seguir el siguiente procedimiento para reportarlo a C4RD:

REGISTRO DEL INCIDENTE

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.

- Incluir la siguiente información:
  - Nombre de la entidad reportante (JCE).
  - Fecha y hora del incidente.
  - Descripción detallada del problema.
  - Componentes y/o servicio afectado dentro de la infraestructura Cedula Digital.
  - Capturas de pantalla o logs relevantes.
  - Nivel de urgencia del incidente.

6.6.5 CLASIFICACIÓN DEL INCIDENTE

- **Máxima (P1):** El servicio de Cedula Digital está completamente inoperativo.
- **Alta (P2):** Falla parcial que afecta los servicios o la operación de la JCE.
- **Media (P3):** Problemas que afectan el rendimiento sin impacto inmediato.
- **Baja (P4):** Incidentes menores atendidos en la siguiente ventana de mantenimiento.

5. **Evaluación y Diagnóstico Inicial**
   - C4RD realizará un análisis preliminar y solicitará información adicional si es necesario.
6. **Resolución y Seguimiento**

- C4RD asignará un técnico según la criticidad del incidente.
- Se mantendrá una comunicación constante con la JCE hasta la resolución.
- Se emitirá un informe con causas y medidas correctivas.

6.7 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

Para garantizar el funcionamiento óptimo de la plataforma, se establecen los siguientes tipos de mantenimiento:

6.7.1 ACTIVIDADES PERIÓDICAS

- **Revisión de certificados**: Verificar la validez y vigencia de los certificados emitidos, incluyendo los certificados de la Autoridad de Certificación (CA) raíz y subordinada.
- **Actualización de software y firmware**: Mantener actualizados los sistemas y aplicaciones que utilizan la solución de emisión de credenciales digitales.
- **Revisión de políticas de seguridad**: Verificar que las políticas de seguridad estén actualizadas y sean efectivas para proteger la solución de emisión de credenciales digitales.

- **Realización de copias de seguridad**: Realizar copias de seguridad regulares de la solución de emisión de credenciales digitales, incluyendo los certificados, las claves privadas y los registros de transacciones.
- **Pruebas de penetración y vulnerabilidades**: Realizar pruebas de penetración y vulnerabilidades periódicas para identificar y corregir cualquier debilidad en la solución de emisión de credenciales digitales.

6.7.2 ACTIVIDADES DE MANTENIMIENTO PREVENTIVO

- **Revisión de los registros de transacciones**: Verificar los registros de transacciones para detectar cualquier actividad sospechosa o irregular.
- **Monitoreo de la integridad de los certificados**: Verificar la integridad de los certificados emitidos y revocados.
- **Actualización de la lista de revocación de certificados (CRL)**: Actualizar la lista de revocación de certificados (CRL) para reflejar los certificados revocados.
- **Revisión de la configuración de la solución de emisión de credenciales digitales**: Verificar la configuración de la solución de emisión de credenciales digitales para asegurarse de que esté configurada correctamente y sea segura.

6.7.3 ACTIVIDADES DE RESPUESTA A INCIDENTES

Procedimientos de respuesta a incidentes: Están establecidos procedimientos de respuesta a incidentes para manejar cualquier incidente de seguridad que afecte la solución de emisión de credenciales digitales.

- **Notificación de incidentes**: Notificar a las partes interesadas relevantes en caso de un incidente de seguridad.
- **Análisis de incidentes**: Realizar un análisis detallado de cualquier incidente de seguridad para identificar la causa raíz y tomar medidas correctivas.
- **Recuperación de la solución de emisión de credenciales digitales**: Recuperar la solución de emisión de credenciales digitales después de un incidente de seguridad, incluyendo la restauración de los certificados y las claves privadas.

6.7.4 MANTENIMIENTO CORRECTIVO

- **Solución de Errores Críticos:** Reparación inmediata ante caídas del sistema.
- **Reemplazo de Componentes:** Sustitución de módulos afectados por fallos.
- **Corrección de Brechas de Seguridad:** Ajustes urgentes en respuesta a ataques o vulnerabilidades detectadas.

6.8 SEGURIDAD Y CUMPLIMIENTO

Dado que GET Mobile ID maneja información altamente sensible, el programa de mantenimiento prioriza la seguridad mediante:

- **Cifrado y Protección de Datos**: Uso de criptografía RSA y curvas elípticas.
- **Autenticación Multifactor (MFA)**: Para el acceso administrativo y operación segura se implementarán mecanismos de autenticación y autorización seguros para garantizar que solo los usuarios autorizados puedan acceder a la solución de emisión de credenciales digitales.
- **Firewall de Nueva Generación (NGFW) y WAF**: Control avanzado contra ataques cibernéticos.
- **Cumplimiento Normativo**: Asegurar que la solución de emisión de credenciales digitales cumpla con los requisitos de seguridad establecidos en la norma ISO 18013-5, ISO 27001 y regulaciones nacionales de protección de datos.
- **Monitoreo de Amenazas**: Detección temprana de intrusiones y análisis de comportamiento.
- **Gestión de claves:** Implementación de una gestión de claves segura y eficiente para proteger las claves privadas y los certificados.
- **Registros de auditoría:** Mantener registros de auditoría detallados y precisos para permitir la trazabilidad y la responsabilidad de las acciones realizadas en la solución de emisión de credenciales digitales.

6.9 KPIS Y MÉTRICAS DE RENDIMIENTO

Para evaluar la eficiencia del soporte y mantenimiento, se definen indicadores clave:

- **Disponibilidad del Sistema**: Tiempo efectivo de operación (meta: 99.95%).
- **Tiempo Medio de Resolución (MTTR)**: Promedio de tiempo para resolver incidentes.
- **Tiempo Medio entre Fallas (MTBF)**: Periodo promedio entre fallas críticas.
- **Tasa de Resolución en Primera Llamada (FCR): %** de incidencias resueltas sin escalamiento.
- **Cumplimiento de SLA: % de incidentes resueltos dentro de los tiempos acordados.**
- **Incidentes de Seguridad:** Número de alertas de seguridad atendidas y resueltas.
- **Uso de Recursos:** Análisis de carga en servidores y almacenamiento.

Estos KPIs se revisarán periódicamente, cada trimestre, para identificar oportunidades de mejora y garantizar que la plataforma opere de manera segura y eficiente.

6.10 INVENTARIO

Para garantizar la continuidad operativa y evitar interrupciones en la personalización de documentos de identidad, el Consorcio Identidad 4.0 RD mantendrá un stock de inventario equivalente a un mínimo del 3% Este inventario permitirá una respuesta inmediata en caso de fallas técnicas o necesidades de reposición, asegurando el cumplimiento ininterrumpido del servicio.