Orden de Trabajo 9 – Contrato Abierto UOC 16/2022 - MITIC

Orden de Trabajo (OT)	
Nro. de Orden de Trabajo	9
Contrato:	Contrato abierto UOC Nº 16 /2022 MITIC
Proveedor:	Grupo Horus S. A
Cantidad de Horas/Hombre	263 horas
Costo	50.496.000 Gs.
Título	Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria.

Plan de trabajo acordado	
Fecha de pedido de la OT	13/11/2023
Acuse de recibo de la OT por parte del proveedor *(Máximo de 5 días hábiles posteriores al acuse de recibo)*	13/11/2023
Aceptación de la OT por parte del proveedor *(Máximo de 5 días hábiles posterior al acuse de recibo)*	14/11/2022
Fecha de entrega al MITIC para inicio de las verificaciones *(Código fuente, Documentación adicional solicitada en OT, Evidencia de Control de calidad, Informe Final)*	07/12/2023
Verificación, ciclo de pruebas y correcciones *(Máximo de 40 días hábiles posterior a la entrega al MITIC para verificaciones)*	06/02/2024
Fecha tope para emisión de Constancia de Recepción Satisfactoria *(Máximo de 50 días hábiles posterior a la entrega al MITIC para verificaciones)*	20/02/2024

GRUPO HORUS
GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

CONTENIDO

1. OBJETIVO GENERAL 3
2. OBJETIVOS ESPECÍFICOS 3
3. MARCO LEGAL 3
4. GLOSARIO DE TÉRMINOS 3
5. REQUERIMIENTOS FUNCIONALES 4
6. REQUERIMIENTOS NO FUNCIONALES 5
7. ANEXOS 7
7.1. FLUJO DE FUNCIONAMIENTO 7
7.1.1. FLUJO GENERAR QR 7
7.1.2. FLUJO - VALIDAR QR 8
8. ESTIMACIÓN DE ESFUERZO 9

GRUPO HORUS
GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

Introducción

En el Contexto de la Ley Nº 7177 / DE VALIDEZ DEL FORMATO DIGITAL DE LOS DOCUMENTOS DE PORTACIÓN OBLIGATORIA, el MITIC, como ente responsable de su aplicación, se encuentra en proceso de realizar los ajustes tecnológicos a las aplicaciones oficiales para permitir que los ciudadanos puedan generar y portar la representación digital de los documentos establecidos en la ley.

1. Objetivo General

Modificaciones, adaptaciones y desarrollo de funcionalidades a la aplicación móvil (Portal Paraguay), para la generación y validación de los documentos de portación obligatoria en formato digital.

2. Objetivos Específicos

- Generar documentos de representación digital para:
  - Cédula de Identidad Policial.
  - Cédula Verde Vehicular.
  - Licencia de Conducir.
- Generar códigos (QR) de validación de los documentos digitales desplegados en la aplicación.
- Permitir realizar validaciones de los códigos (QR) de los documentos digitales dentro de la aplicación.
- Realizar bloqueos para evitar realizar impresiones de pantallas desde los dispositivos que generan los documentos digitales.
- Implementar mecanismos de seguridad a la aplicación para asegurar que los códigos del documento generado sólo puedan ser utilizados una sola vez y sean autodestruidos una vez validados.
- Realizar las modificaciones necesarias a aplicación para generar autorías de generación y validación de los documentos digitales.

3. Marco Legal

El presente documento abarca la descripción de los requisitos funcionales y no funcionales que deberán ser considerados en el proceso de implementación de la portación digital de documentos en la aplicación móvil Portal Paraguay, contemplados en la LEY N° 7177 DE VALIDEZ DEL FORMATO DIGITAL DE LOS DOCUMENTOS DE PORTACIÓN OBLIGATORIA.

4. Glosario de Términos

OEE: Organismo o Entidad del Estado
MITIC: Ministerio de Tecnologías de la Información y Comunicación
RF: Requisito Funcional
RNF: Requisito No Funcional
Agente verificador o Agente validador o Validador: Usuario de la aplicación Portal Paraguay que escanea el código QR generado por el *"Ciudadano"*, para su validación.
Ciudadano: Usuario de la aplicación Portal Paraguay que genera un documento digital portable y un código QR del mismo para su uso en formato digital.
Online: Característica de la conectividad a Internet de un usuario que utiliza la aplicación Portal Paraguay en la cual se cuenta con conexión a los servicios gubernamentales proveídos por el MITIC.

GRUPO HORUS
GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

Orden de Trabajo 9 – Contrato Abierto UOC 16/2022 - MITIC

5. **Requerimientos Funcionales**

A continuación, se presenta la lista de Requerimientos Funcionales que componen la presente orden de trabajo:

ID	Requerimientos Funcionales	DESCRIPCIÓN
RF1	Análisis y Diseño de Solución	Realizar un análisis técnico de la aplicación móvil (Android e iOS), para confirmar la factibilidad de las modificaciones solicitadas en esta OT.
RF2		Elaborar documentación de la arquitectura de solución implantada.
RF3	Modificación de la aplicación Backend "documentos-core"	Realizar las adaptaciones a backend de la aplicación para la generación de los documentos digitales. • Obtención de datos de CI, RUA y OPACI desde SII • Servicios para la aplicación móvil de Generación y Verificación para ambos tipos de documentos • Persistencia en base de datos no relacional • Protocolo de generación de QR y sus validaciones
RF4		Desarrollar las funcionalidades para la generación de códigos de seguridad (QR), que sean de un solo uso y un tiempo de vida limitado.
RF5		Realizar las modificaciones a las entidades y colecciones necesarias para el concepto de "documentos_digitales"
RF6		• Desarrollar las modificaciones necesarias a aplicación para generar auditorías de generación y validación de los documentos digitales. • Se deberá generar entidades dentro del backend y las tablas de la Base de datos. • La misma deberá permitir hacer una trazabilidad de las generaciones y validaciones realizadas por y entre los ciudadanos
RF7		Desarrollar los WS, de generación de documentos digitales (en caso de ser necesarios), para otros documentos de portación obligatoria establecidos en la Ley.
RF8	Modificación de la Aplicación Móvil	• Desarrollar las funcionalidades para la generación de documentos digitales, las cuales deben poder generarse estando OnLine y que el ciudadano se encuentre autenticado en la Aplicación con su Identidad Electrónica. • El Documento digital generado deberá incorporar un código (QR) de validación, de utilización única y temporal, que deberá generarse cada vez que se genera el documento digital.
RF9		• Desarrollar las funcionalidades de validación de los documentos digitales por medio de un lector de (QR), dentro de la aplicación, que deberá levantar la cámara del dispositivo y permitir su lectura. • La validación del código (QR), deberá confirmar que los datos obtenidos desde el (QR) provienen de la aplicación oficial (no apócrifa), y deberá enviar al validador la confirmación correspondiente, desplegando datos básicos del (QR) validado. (*definir datos de respuesta*).

		• (El lector de QR debe ser de la propia aplicación Portal Paraguay y el usuario debe estar logueado. • El agente validador o verificador podrá ser cualquier ciudadano logueado con su Identificación Electrónica. • Validar que la información enviada por la aplicación sea confiable e inmutable. Para tal efecto, se deberá implementar mecanismos de encriptación de datos. (AES256).
RF10		Implementar mecanismos de seguridad a la aplicación para asegurar que los códigos del documento generado sólo puedan ser utilizados una sola vez y sean autodestruidos una vez validados.

6. Requerimientos No Funcionales

ID	Requerimientos No Funcionales
RNF1	Detalle de la representación del documento digital generado: 1080x1350 o estándar de aplicaciones móviles.
RNF2	Los documentos digitales sólo podrán ser generados y/o validados para Credenciales de Identidad Electrónica con conexión a Internet y estando logueados.
RNF3	No se deberá permitir la captura de pantalla ni el almacenado de los documentos digitales generados en la aplicación. ***Obs: En caso de ser posible con las versiones actuales del Stack de desarrollo de la aplicación (Flutter), no obstante, se deberá declarar esta imposibilidad en el informe de finalización de la OT.***
RNF4	Deberán emitirse notificaciones de errores contextuales en caso de no poder generarse alguno de los documentos digitales.
RNF5	El desarrollo deberá estar contemplado para dispositivos con Android y iOS.
RNF6	El desarrollo y publicación de la App deberá realizarse en ambas tiendas (PlayStore y Apple Store).
RNF7	Motor de base de datos: Todas las persistencias de información (para los actuales RFs, deberán ser realizados sobre MongoDB
RNF8	**Servicios Datos de Cédula de identidad (PN)** http://devsii.mitic.gov.py/frontend-identificaciones/api/persona/obtenerPersonaPorCedula/{cédula}
RNF9	- **Servicio de Consulta del Registro Único del Automotor (RUA)** http://devsii.mitic.gov.py/rua-csj/api/automotor/consultarRua?tipoCriterio=T&criterio1=1&criterio2=123456 - **Proyectos y ramas a ser modificados para el desarrollo:** https://gitlab.mitic.gov.py/senatics/documentos-core/tree/2023-ot9 https://gitlab.mitic.gov.py/senatics/portal-py-app/tree/2023-ot9 - **Proyectos auxiliares (rama master solo de lectura):**

	https://gitlab.mitic.gov.py/senatics/portal-py-backend-core/tree/master https://gitlab.mitic.gov.py/ie/oauth2-server/tree/master https://gitlab.mitic.gov.py/ie/oauth2-frontend/tree/master/login_app
RNF10	- **Deberá realizarse un escaneo de vulnerabilidades del tipo "Caja Negra" para las siguientes "URLs base" que tengan un servicio expuesto:** o **https://www.paraguay.gov.py/docsapi/app/documento/** o **https://www.paraguay.gov.py/docsapi/documento/** o **https://identidad.paraguay.gov.py/login**
RNF11	**El escaneo realizado será mediante la utilización de una herramienta** ***no intrusiva.***

Observaciones:

- Esta OT no contempla realizar pruebas de concepto en el caso de potenciales vulnerabilidades encontradas, que, en caso afirmativo, se generará una OT, específica para el efecto.
- Esta OT, no contempla lanzar simulaciones o explorar mecanismos que exploren 'denegación de servicios', las mismas se generarán en una OT, específica para el efecto.

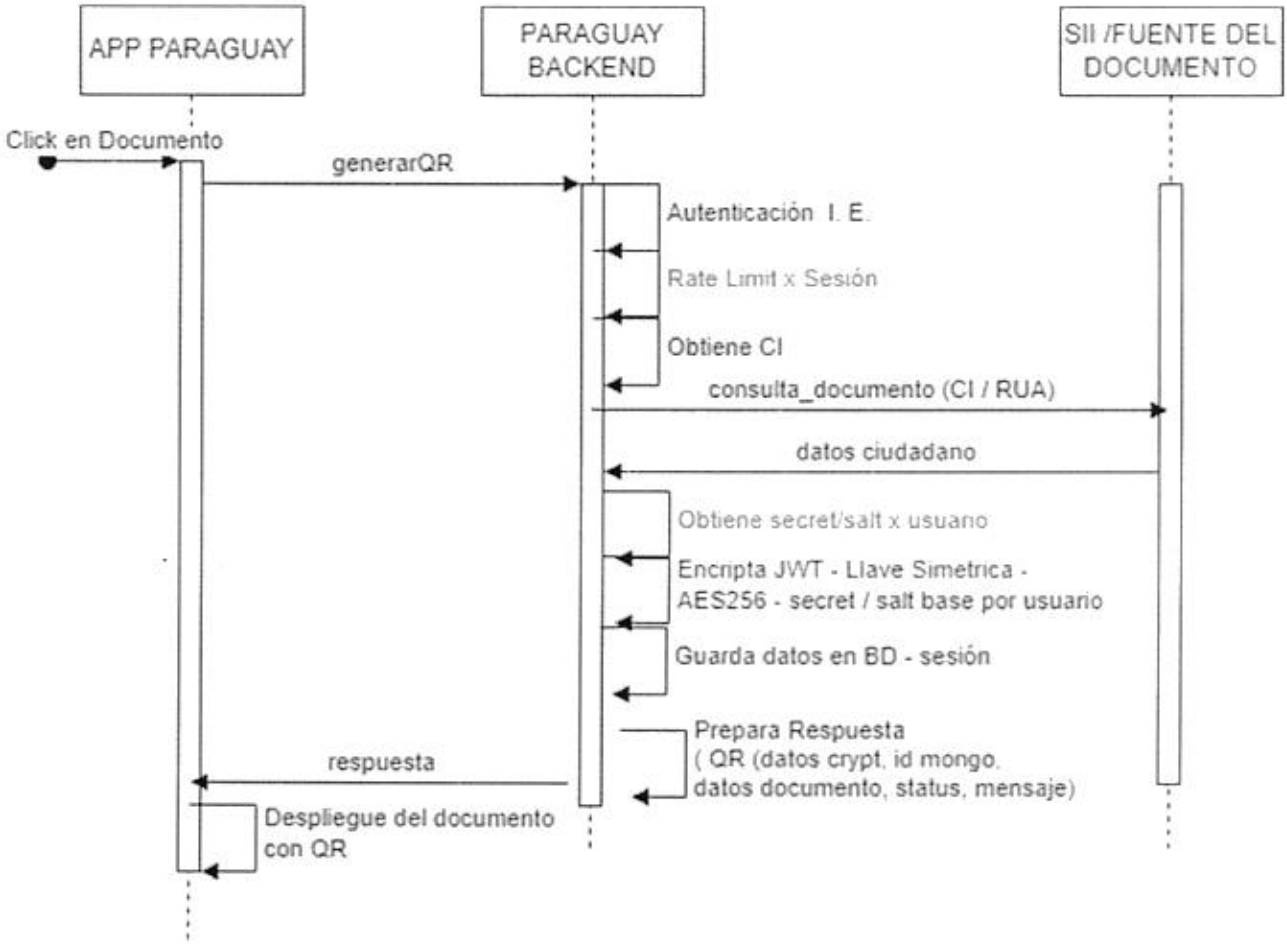
GRUPO HORUS
GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

7. Anexos

7.1. Flujo de Funcionamiento

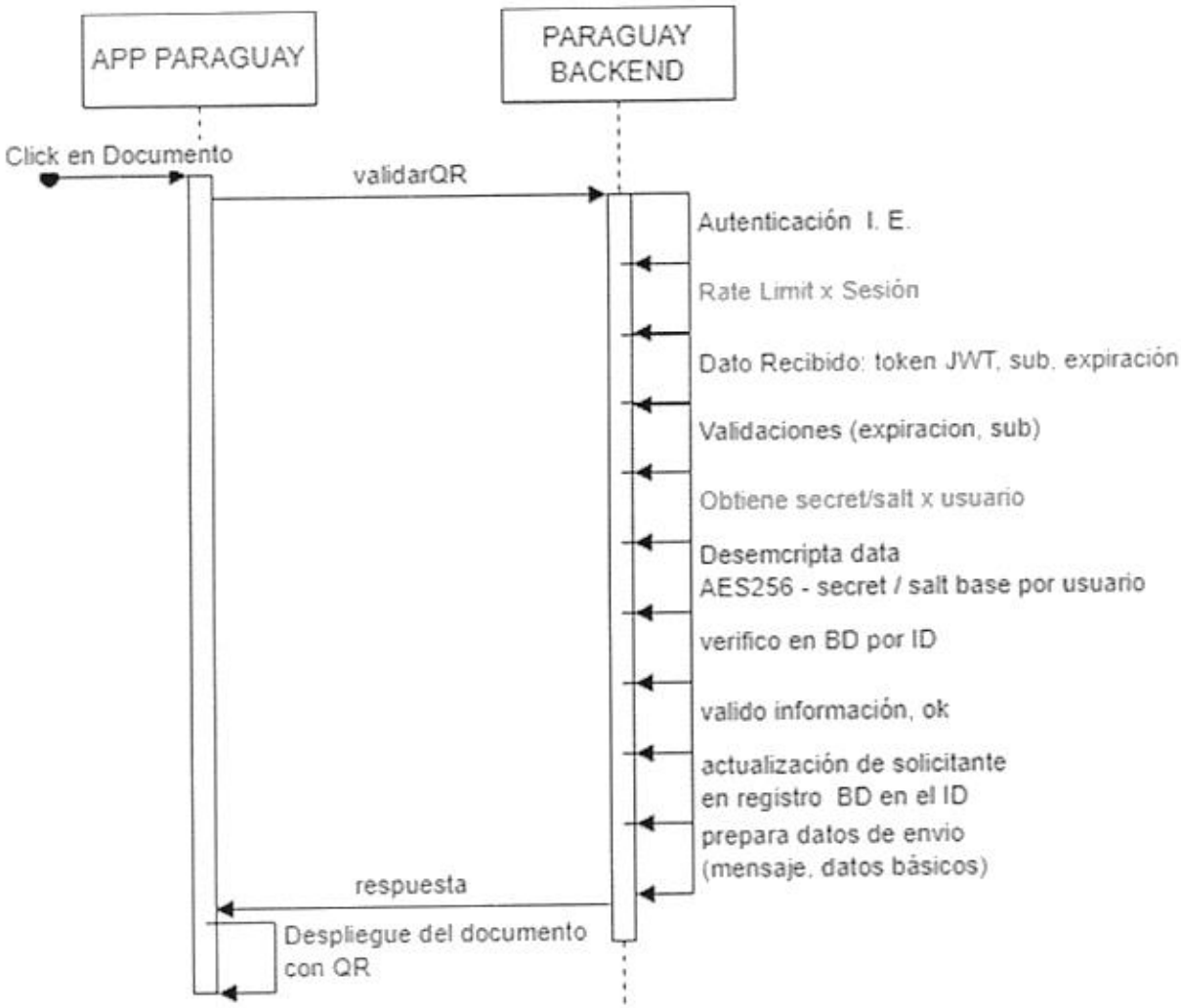
7.1.1. Flujo Generar QR



GRUPO HORUS
GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

7.1.2.Flujo - Validar QR



GRUPO HORUS
GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

8. Estimación de Esfuerzo

Complejidad	Horas x Etapa					Costo por Hora	192,000
	Análisis y Diseño	Desarrollo	Testing	Documentación	Total Horas-Hombre (H/H)		
CU - Simple (CU-S)	4	2	4	2	12		
CU - Mediana (CU-M)	4	5	8	2	19		
CU - Compleja (CU-C)	7	27	30	2	66		
CU - Muy Compleja (CU-MC)	10	40	50	5	105		
CU - Súper Compleja (CU-SC)	21	50	80	5	156		
Modificación CU-S	0.5	2	3	0.5	6		
Modificación CU-M	1.5	4	6	0.5	12		
Modificación CU-C	2.5	14	28	0.5	45		
Margen Ajustes / Corrección Errores %	0						

Orden de Trabajo	Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria.									
Casos de Uso	CU-S	CU-M	CU-C	CU-MC	CU-SC	MCU-S	MCU-M	MCU-C	TOTAL HORAS	COSTO
Gestión y Planificación										
Relevamiento, análisis y diseño de la arquitectura	0.5								6	1.152.000
Planificación	0.5								6	1.152.000
Gestión	0.5								6	1.152 000
Hacking ético en los portales vinculados a la app móvil	0.5								6	1.152.000
Prototipado	1								12	2.304.000
Modificación y puesta a punto del Rate limit por tipo de documento y nro de cédula	1								12	2.304.000
Aplicación Móvil										
Sección de documentos digitales	0.5								6	1.152.000
Botón de Generación de código QR Documentos Digitales		1							19	3.648.000
Botón de Generación de código QR para Validación QR	0.5								6	1.152.000
Diseño de interfaces de acuerdo al mockup enviado por MITIC para la generación de QR de Cédula Policial, Licencia de conducir y Cédula del Automotor	0.5								6	1.152.000
Actualización de enlaces rotos de redirección a Crear Identidad, Reportes y Sugerencias, Olvide mi contraseña.	0.5								6	1.152.000
Core del módulo de Documentos Digitales										
Cliente REST para consumir datos de Documentos Digitales	1								12	2.304.000
Api REST para generar código QR de acuerdo al tipo de documento solicitado: Cédula Policial, Licencia de Conducir, Cédula del Automotor.		1							19	3.648.000
Api REST para validar código QR		1							19	3.648.000

Orden de Trabajo 9 – Contrato Abierto UOC 16/2022 - MITIC

Implementación de modelo caché para la generación de código QR según el tipo de documento digital.		1							19	3.648.000
Integración de reglas de validación a fin de controlar posibles casos de servicios intermitentes/inestables.	1								12	2.304.000
Integración de reglas de validación de acuerdo al resultado recibido al consultar los servicios	1								12	2.304.000
Validación de acceso vía Identidad Electrónica	0.5								6	1.152.000
Integración de servicio para limpiar documentos temporales	1								12	2.304.000
Cifrado simétrico para el caché de los datos respondido por los distintos servicios.		1							19	3.648.000
Implementación de modelo cache en todos los tipo de documentos	1								12	2.304.000
Adecuación de campos visibles en la función validar QR	0.5								6	1.152.000
Pruebas	0.5								6	1.152.000
Documentación de pruebas	0.5								6	1.152.000
Implementación: Instalación, Publicación										
Implantación, instalación, publicación	0.5								6	1.152.000
Documentación técnica										
Elaboración de informe final	0.5								6	1.152.000

Total horas sin margen	**263**	**50.496.000**
Total	**263**	**50.496.000**

Acuse de recibo Orden de Trabajo 9			
Proveedor		**Fecha**	**Firma**
Luis Cordoza	Coordinador Especialista TIC	14/11/2023	GRUPO HORUS S.A.

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

Orden de Trabajo 9 – Contrato Abierto UOC Nº 16 /2022 MITIC

Aceptación de Orden de Trabajo (OT) por el Proveedor

Orden de Trabajo (OT)	
Nro. de Orden de Trabajo	9
Contrato:	Contrato abierto UOC Nº 16 /2022 MITIC
Proveedor:	Grupo Horus S. A
Cantidad de Horas/Hombre	263 horas
Costo	50.496.000 Gs.
Título	Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria.

Plan de trabajo acordado	
Fecha de pedido de la OT	13/11/2023
Acuse de recibo de la OT por parte del proveedor *(Máximo de 5 días hábiles posteriores al acuse de recibo)*	13/11/2023
Aceptación de la OT por parte del proveedor *(Máximo de 5 días hábiles posterior al acuse de recibo)*	14/11/2023
Fecha de entrega al MITIC para inicio de las verificaciones *(Código fuente, Documentación adicional solicitada en OT, Evidencia de Control de calidad, Informe Final)*	07/12/2023
Verificación, ciclo de pruebas y correcciones *(Máximo de 40 días hábiles posterior a la entrega al MITIC para verificaciones)*	06/02/2024
Fecha tope para emisión de Constancia de Recepción Satisfactoria *(Máximo de 50 días hábiles posterior a la entrega al MITIC para verificaciones)*	20/02/2024

Aceptación de Orden de Trabajo 9			
Proveedor		**Fecha**	**Firma**
Grupo Horus S.A	Coordinador Especialista TIC	14/11/2023	GRUPO HORUS GRUPO HORUS S.A.

PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY
MINISTERIO DEL INTERIOR
DECRETO N° 802.-

POR EL CUAL SE DECLARA ASUETO EL DÍA JUEVES 7 DE DICIEMBRE DE 2023 PARA LOS FUNCIONARIOS DE LA ADMINISTRACIÓN PÚBLICA CENTRAL Y DE LOS ORGANISMOS Y ENTIDADES DESCENTRALIZADAS.

Asunción, 6 de diciembre de 2023

VISTO: El artículo 1° de la Ley N° 08/1990 que establece como feriado nacional el 08 de diciembre de cada año, en conmemoración al Día de la Virgen de Caacupé, feriado fijo acorde a lo previsto en la Ley N° 1723/2001; y

CONSIDERANDO: Que el artículo 238, numeral 1) de la Constitución Nacional faculta a quien ejerce la Presidencia de la República a dirigir la administración general del país.

Que la conmemoración del Día de la Virgen de Caacupé es una celebración espiritual que tiene profundas raíces en la tradición popular de nuestro país, y conlleva la realización de peregrinaciones desde distintos puntos del país hasta Caacupé en los días previos, siendo además de una ocasión de peregrinación estrictamente religiosa, una oportunidad de gran impacto para el turismo interno, el comercio en general y el movimiento de paraguayos que han migrado a la capital o centros urbanos para volver al terruño o bien visitar a familiares.

N° 277.-

Que en consecuencia, se trata de un feriado de características peculiares, que ocasiona un impacto económico directo e indirecto de gran significancia, por la posibilidad de consumo de bienes y servicios relacionados con el movimiento de personas hacia el interior del país, lo que da vigor a la extensa actividad comercial y turística nacional originada, además de la festividad religiosa para quienes profesan la religión católica apostólica y romana,

PODER EJECUTIVO
SANTIAGO PEÑA
2023-2028

PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY
MINISTERIO DEL INTERIOR
DECRETO Nº 802.-

POR EL CUAL SE DECLARA ASUETO EL DÍA JUEVES 7 DE DICIEMBRE DE 2023 PARA LOS FUNCIONARIOS DE LA ADMINISTRACIÓN PÚBLICA CENTRAL Y DE LOS ORGANISMOS Y ENTIDADES DESCENTRALIZADAS.

cuyo protagonismo en la formación histórica y cultural es reconocida en el artículo 82 de la Constitución.

Que en consecuencia es tradicional, y justificado, establecer un asueto para la función pública en la víspera de dicho feriado, no solo por su impacto espiritual sino también por su impacto positivo en el turismo interno, la economía y en la circulación de paraguayos en su tierra, debiéndose sin embargo prever en forma irrestricta la continuidad de los servicios públicos imprescindibles para la comunidad, excluyéndose a los funcionarios públicos afectados a la prestación de dichos servicios.

Nº_____

POR TANTO, en ejercicio de sus atribuciones constitucionales,

EL PRESIDENTE DE LA REPÚBLICA DEL PARAGUAY

DECRETA:

Art. 1º.- Declárase asueto el día jueves 7 de diciembre de 2023, para los funcionarios de la administración pública central y de los organismos y entidades descentralizadas.

Art. 2º.- Exclúyase del asueto declarado en el artículo 1º de este decreto a los funcionarios y empleados públicos que prestan servicios médicos de urgencia y en horarios especiales, a los funcionarios afectados a los servicios públicos imprescindibles para la comunidad, comercio exterior y percepción de tributos.

Art. 3º.- Refréndese por el Ministro del Interior.

Art. 4º.- Comuníquese, publíquese e insértese en el Registro Oficial.

PODER EJECUTIVO
SANTIAGO PEÑA
2023-2028
PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY | TETÃ MBURUVICHA GUASU RENDA

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria"

Informe Final

1. Resumen del Proyecto

Orden de Trabajo Nro.	9
Proyecto: Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria	
Plan de Trabajo acordado	
Fecha de Pedido	13/11/2023
Fecha de acuse de recibo del Proveedor	13/11/2023
Aceptación de la OT por parte del Proveedor *(máximo de 5 días hábiles posterior al acuse de recibo)*	14/11/2023
Fecha de entrega al MITIC para inicio de las verificaciones (Código Fuente, Documentación adicional solicitada en la OT, evidencia de control de calidad, Informe final)	07/12/2023
Verificación, ciclo de pruebas y correcciones *(máximo de 40 días hábiles posterior a la entrega al MITIC para verificaciones)*	06/02/2024
Fecha Tope para emisión de Constancia de Recepción Satisfactoria	20/02/2024
Equipo de Proyecto Ejecutor	
Equipo Grupo Horus	Luis Cardozo (Coordinador de Proyecto / Desarrollador) Sabrina Farías(Analista) Antonio Ramírez (Desarrollador) Raquel Amarilla (Tester)
Analista Responsable – MITIC	Fernando Mancía Klaus Pistilli

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC
Recibido: 11/12/2023
15:15

GRUPO HORUS
GRUPO HORUS S.A.

Análisis de Esfuerzo	
Esfuerzo Estimado:	263 horas/Hombre

Nombre del Producto

Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria

Objetivo

Modificaciones, adaptaciones y desarrollo de funcionalidades a la aplicación móvil (Portal Paraguay), para la generación y validación de los documentos de portación obligatoria en formato digital.

2. Software y Documentación

Release de Software
Ubicación en el repositorio: **App Móvil** https://gitlab.mitic.gov.py/senatics/portal-py-app/tree/2023-ot9 **Backend:** https://gitlab.mitic.gov.py/senatics/documentos-core/tree/2023-OT9v2

Documentación Funcional y Técnica	
Lista de Casos de Prueba	MITIC - OT9 - Cuaderno de Pruebas.docx
Manual de Despliegue	MITIC - OT9 - Manual Despliegue Apple.docx
Documento de arquitectura	MITIC – OT9 – Documento de arquitectura.docx
Manual de Usuario	MITIC - OT9 -Manual de Usuario
Nota de versión	MITIC - OT9 - Nota de Versión.docx

3. Cronograma y Actividades Realizadas

Actividades	nov-23																			dic-23						
	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7
Envío de la OT																									
Acuse de Recepción de la OT																									
Relevamiento y estimacion de la OT																									
Análisis y Diseño de Solución																									
Planificación																									
Generación de Prototipos																									
Modificación de la aplicación Backend "documentos-core"																									
Adaptaciones al backend de la aplicacion para la generación de los documentos digitales																									
Desarrollo de Api REST para generación de codigo QR de cada tipo de documento																									
Desarrollo Api REST para validación de código QR generado																									
Modificaciones a las entidades y colecciones para el concepto de "documentos_digitales																									
Generación de colecciones que contengan el histórico de la trazabilidad de auditoría en Redis así como archivos de logs.																									
Validación de acceso vía Identidad Electrónica																									
Modificación de la Aplicación Móvil Android y IOS																									
Desarrollo de la Sección de documentos digitales * Botón de Generación de código QR para Cédula Policial * Botón de Generación de código QR para Licencia de Conducir * Botón de Generación de código QR para Cédula del Automotor * Botón de Generación de código QR para Validación QR																									
Desarrollo de un código (QR) de validación para los documentos digitales de un único uso																									
Implementación de mecanismos de seguridad a la aplicación para asegurar que los códigos del documento generado sólo puedan ser utilizados una sola vez y sean autodestruidos una [illegible]																									
Actualizar enlaces de redirección a Crear Identidad, Reportes y Sugerencias, Olvide mi contraseña																									
Pruebas funcionales																									
Entrega de Software para verificaciones																									
Elaboración de informe Final																									
Entrega de informe Final																									

GRUPO HORUS

GRUPO HORUS S.A.

4. Pruebas Realizadas

a. Pruebas Funcionales

ID	Categoría	Tipo Test	Resultado	Fecha
1	Descargar la App ParaguayGovPy desde la Play Store.	Funcional	Éxito	04/12/2023
2	Menú Carpeta Ciudadana.	Funcional	Éxito	04/12/2023
3	Iniciar sesión en la aplicación con Identidad Electrónica.	Funcional	Éxito	04/12/2023
4	Consulta de Datos de Cédula Policial	Funcional	Éxito	04/12/2023
5	Consulta de Datos de Cédula del Automotor	Funcional	Éxito	04/12/2023
6	Consulta de Datos de Licencia de Conducir	Funcional	Éxito	04/12/2023
7	Verificación QR	Funcional	Éxito	04/12/2023

Observaciones: Para los siguientes requerimientos no funcionales mencionados en la OT se indican las observaciones relacionadas a cada punto.

- **RNF3: No se deberá permitir la captura de pantalla ni el almacenado de los documentos digitales generados en la aplicación.**
  Obs: Tras una verificación técnica se concluyó que en la versión actual utilizada por la app no es factible implementar este punto, de acuerdo al análisis y pruebas realizadas para implementar el punto mencionado se deberá realizar un upgrade de la versión de la app, este percance fue informado al equipo del MITIC en las reuniones mantenidas.

- **RNFN10: Deberá realizarse un escaneo de vulnerabilidades del tipo "Caja Negra" para las siguientes "URLs base" que tengan un servicio expuesto:**
  - https://www.paraguay.gov.py/docsapi/app/documento
  - https://www.paraguay.gov.py/docsapi/documento
  - https://identidad.paraguay.gov.py/login
- **RNFN11: El escaneo realizado será mediante la utilización de una herramienta no intrusiva**

  Obs: Como respuesta a estos dos requerimientos fue remitido en fecha 21/11/2023 el informe **"MITIC - OT9 - Analisis de Vulnerabilidades"** con el los escaneos de vulnerabilidades tuvo un resultado positivo, con una baja identificación de potenciales vulnerabilidades en virtud de los mecanismos de protección habilitados en el sitio del portal Paraguay. Esta Informe incluye los siguientes puntos:
  a. GAP Análisis
     i. Beneficios de un GAP análisis

ii. Guía de Controles Críticos de Ciberseguridad

b. Análisis de vulnerabilidades

i. Principales Riesgos Identificados

c. Recomendaciones

i. Acciones Implementadas

A su vez se remitió también el documento **"ANEXO B - Reporte Qualys - MITIC - 202311231 - Portal Paraguay"** con las pruebas realizadas.

Nota: para mayores detalles de las demás pruebas, se podrán visualizar en el cuaderno de pruebas que hacen parte de la documentación de la versión. En él, se listan las pruebas y evidencias relacionadas a la presente OT.

5. Conclusiones

Los trabajos se llevaron a cabo de forma satisfactoria. Fueron desarrolladas y probadas las funcionalidades previstas en la Orden de Trabajo en tiempo y forma.

Coordinador – Grupo HORUS SA

GRUPO HORUS

GRUPO HORUS S.A

Contrato Abierto UOC No. 16/2022 MITIC

DOCUMENTACIÓN ADICIONAL

Orden de Trabajo Nro. 9

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria"

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC
Recibido: 11/12/2023
15:15

GRUPO HORUS
GRUPO HORUS S.A.

1. Resumen del Proyecto

Orden de Trabajo Nro.	9
Proyecto: Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria.	
Planificación	
Fecha de Pedido	13/11/2023
Fecha de acuse de recibo del Proveedor	13/11/2023
Aceptación de la OT por parte del Proveedor *(máximo de 5 días hábiles posterior al acuse de recibo)*	14/11/2023
Fecha de entrega al MITIC para inicio de las verificaciones (Código Fuente, Documentación adicional solicitada en la OT, evidencia de control de calidad, Informe final)	07/12/2023
Verificación, ciclo de pruebas y correcciones *(máximo de 40 días hábiles posterior a la entrega al MITIC para verificaciones)*	06/02/2024
Fecha Tope para emisión de Constancia de Recepción Satisfactoria	20/02/2024
Equipo de Proyecto Ejecutor	
Equipo Grupo Horus	Luis Cardozo (Coord. del Proyecto) Sabrina Farías (Analista) Antonio Ramírez(Desarrollador) Mauricio Ramírez(Desarrollador) Raquel Amarilla(Tester)
Analista Responsable – MITIC	Fernando Mancía
Análisis de Esfuerzo	
Esfuerzo Estimado:	263 horas/Hombre
Nombre del Producto Sección "Mis Documentos Digitales" en la Aplicación móvil Portal Paraguay **Objetivo**	

GRUPO HORUS
GRUPO HORUS S.A.

Modificaciones, adaptaciones y desarrollo de funcionalidades a la aplicación móvil (Portal Paraguay), para la generación y validación de los documentos de portación obligatoria en formato digital.

Referencias

- LEY N° 7177 DE VALIDEZ DEL FORMATO DIGITAL DE LOS DOCUMENTOS DE PORTACIÓN OBLIGATORIA.

2. Aceptación y Entregables

Los siguientes entregables están definidos como entregables y formarán parte del criterio de aceptación:

Entregable	Descripción
Código fuente del Sistema	Código fuente de la versión de software que contiene el desarrollo necesario para la implementación de la Orden de Trabajo. El mismo se depositará en el repositorio de versiones de MITIC.
Cuaderno de ejecución de pruebas	Cuaderno que contiene un informe y reporte de las pruebas realizadas para aceptación del producto. El mismo contiene los casos de prueba, evidencias de la ejecución de las pruebas y un registro de la cantidad de interacciones realizadas para su aceptación.
Nota de Versión	Documento que contiene datos de las novedades introducidas en el producto entregado como parte del release.
Manual de despliegue	Manual dirigido al administrador que contiene la información que permite administrar la versión de software generada, incluyendo instrucciones de instalación, monitoreo, y verificación del Software.
Manual de usuario	Manual de operador que contiene la información que permite utilizar las funcionalidades del producto generado.

GRUPO HORUS
GRUPO HORUS S.A.

3. Cronograma y actividades realizadas

Actividades	nov-23																		dic-23						
	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7
Envío de la OT																									
Acuse de Recepción de la OT																									
Relevamiento y estimacion de la OT																									
Análisis y Diseño de Solución																									
Planificación																									
Generación de Prototipos																									
Modificación de la aplicación Backend "documentos-core"																									
Adaptaciones al backend de la aplicación para la generación de los documentos digitales																									
Desarrollo de Api REST para generación de código QR de cada tipo de documento																									
Desarrollo Api REST para validación de código QR generado																									
Modificaciones a las entidades y colecciones para el concepto de "documentos_digitales																									
Generación de colecciones que contengan el histórico de la trazabilidad de auditoría en Redis así como archivos de logs																									
Validación de acceso vía Identidad Electrónica																									
Modificación de la Aplicación Móvil Android y iOS																									
Desarrollo de la Sección de documentos digitales * Botón de Generación de código QR para Cédula Policial * Botón de Generación de código QR para Licencia de Conducir * Botón de Generación de código QR para Cédula del Automotor * Botón de Generación de código QR para Validación QR																									
Desarrollo de un código (QR) de validación para los documentos digitales de un único uso																									
Implementación de mecanismos de seguridad a la aplicación para asegurar que los códigos del documento generado sólo puedan ser utilizados una sola vez y sean autodestruidos una vez validados																									
Actualizar enlaces de redirección a Crear Identidad, Reportes y Sugerencias, Olvide mi contraseña.																									
Pruebas funcionales																									
Entrega de Software para verificaciones																									
Elaboración de Informe Final																									
Entrega de Informe Final																									

GRUPO HORUS S.A.

4. Evaluación de Esfuerzo

El análisis de esfuerzo detallado se realizó conforme a la métrica definida por el MITIC para análisis y evaluación de esfuerzo

Tabla de referencia – Estimación de Esfuerzo

		Horas x Etapa				
	Complejidad	Analisis y Diseño	Desarrollo	Testing y Documentación	Asistencia, Configuración e Implementación	Total Horas-Hombre (H/H)
ESTIMACIÓN TIEMPO	CU - Simple (CU-S)	4	2	4	2	12
	CU - Mediana (CU-M)	4	5	8	2	19
	CU - Compleja (CU-C)	7	27	30	2	66
	CU - Muy Compleja (CU-MC)	10	40	50	5	105
	CU - Super Compleja (CU-SC)	21	50	80	5	156
	Modificacion CU-S	0.5	2	3	0.5	6
	Modificacion CU-M	1.5	4	6	0.5	12
	Modificacion CU-C	2.5	14	28	0.5	45
	HH - Costo por hora	192000				
	Margen Ajustes / Corrección Errores %	20				

Complejidad	Total Horas - Hombre(H/H) referencia	Cantidad de CUs	Total Horas/Hombre Estimas por Tipo de CU
CU-Simple (CU-S)	12	5	60
CU-Mediana (CU-M)	19	3	57
CU-Compleja (CU-C)	66	2	132

CU-Muy Compleja (CU-MC)	105	0	0
CU-Super Compleja (CU-SC)	6	0	0
Modificación CU-Simple (MCU-S)	6	0	0
Modificación CU-Mediana (MCU-M)	12	0	0
Modificación CU-Compleja(MCU-C)	45	0	0
Subtotal			249
Margen de Ajustes / Correcciones			14
Subtotal			263

Grupo Horus S.A
Proveedor

GRUPO HORUS
GRUPO HORUS S.A.

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria"

DOCUMENTO DE NOTAS DE VERSION
V1R1A01-ot9

Versión Software:	V1R1A01
Fecha Preparación	04-12-2023
Preparado Por:	GRUPO HORUS
Verificado Por:	Dirección Desarrollo – Dirección General Gobierno Digital

Versión del Documento: 1.0

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC
Recibido: 11/12/2023
15:15

GRUPO HORUS
GRUPO HORUS S.A

Histórico de Cambios del Documento

Versión	Fecha	Descripción	Autor
1.0	04-12-2023	Versión – Documento base preparado en el marco de la Orden de Trabajo Nro. 9	Grupo Horus

GRUPO HORUS
GRUPO HORUS S.A.

TABLA DE CONTENIDO

1 Introducción **4**
1.1 Información de Versión 4
1.2 Evolución de Versión y Dependencias 4
1 Cambios en la Versión **4**
1.1 Novedades **4**
1.2 Lista de Documentos **4**

1 Introducción

Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria

1.1 Información de Versión

Número de Versión	Fecha de Lanzamiento	Versión de Código Fuente	Motivos de Lanzamiento	Estado de la Versión
V1R1A01	04-12-2023	V1R1A01		

1.2 Evolución de Versión y Dependencias

V1R1A01 (Versión Inicial)

1 Cambios en la Versión

1.1 Novedades

#	Descripción	Tipo
1	Consulta de Cédula Policial	[X] Nueva Funcionalidad [ ] Adecuación Funcionalidad
2	Consulta de Licencia de Conducir	[X] Nueva Funcionalidad [ ] Adecuación Funcionalidad
3	Consulta de Cédula del Automotor	[X] Nueva Funcionalidad [ ] Adecuación Funcionalidad
4	Consulta de Verificación QR	[X] Nueva Funcionalidad [ ] Adecuación Funcionalidad

1.2 Lista de Documentos

Documento	Descripción
Documento de Notas de Versión	Nuevo Documento

Contrato Abierto UOC No. 16/2022 MITIC

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria"

Lista de Casos de Prueba

Orden de Trabajo Nro. 9

GRUPO HORUS

GRUPO HORUS S.A.

Versión del Documento: 1.0

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electróni
Viceministerio TIC - MITIC

RECIBIDO: 11/12/23
15:15

1 Contenido

2 Cuaderno de Pruebas 3
2.1 Descripción del Proceso 3
2.2 Casos de Prueba 3
2.3 Casos de Prueba – Evidencia de las Pruebas 4
2.3.1 Descargar la App ParaguayGovPy desde la Play Store. 4
2.3.2 Menú Carpeta Ciudadana. 5
2.3.3 Iniciar sesión en la aplicación ParaguayGovPy con Identidad Electrónica. 6
2.3.4 Consulta de Datos de Cédula Policial. 7
2.3.5 Consulta de Datos de Cédula del Automotor. 7
2.3.6 Consulta de Datos de Licencia de Conducir. 8
2.3.7 Verificación QR. 8

2 Cuaderno de Pruebas

2.1 Descripción del Proceso

Las pruebas fueron realizadas con un usuario de pruebas, siguiendo el listado de casos de pruebas generado durante el análisis de los requerimientos se reprodujeron los mismos registrando los resultados y evidencias de cada caso.

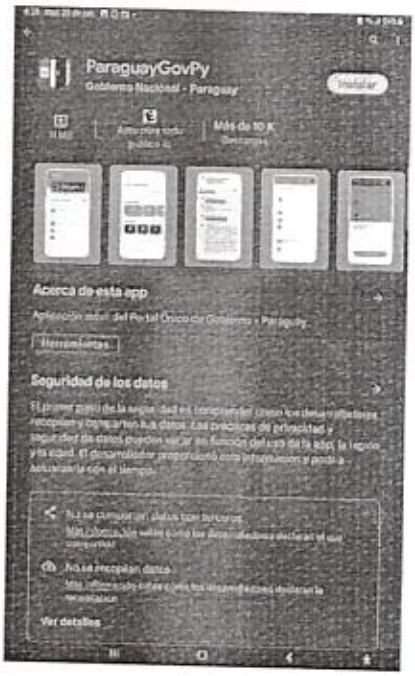
A continuación se detallan los casos probados, los pasos realizados y los resultados obtenidos en cada caso de prueba.

2.2 Casos de Prueba

Descripción de los casos de pruebas					
ID	**Categoría**	**Tipo Test**	**Resultado**	**Fecha**	**Comentarios**
1	Descargar la App ParaguayGovPy desde la Play Store.	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.1**
2	Menú Carpeta Ciudadana.	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.2**
3	Iniciar sesión en la aplicación con Identidad Electrónica.	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.3**
4	Consulta de Datos de Cédula Policial	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.4**
5	Consulta de Datos de Cédula del Automotor	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.5**
6	Consulta de Datos de Licencia de Conducir	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.6**
7	Verificación QR	Funcional	Éxito	04/12/2023	**Evidencia – Casos de prueba 2.3.7**

2.3 Casos de Prueba – Evidencia de las Pruebas

2.3.1 Descargar la App ParaguayGovPy desde la Play Store.



2.3.2 Menú Carpeta Ciudadana.

2.3.3 Iniciar sesión en la aplicación ParaguayGovPy con Identidad Electrónica.

2.3.4 Consulta de Datos de Cédula Policial.

2.3.5 Consulta de Datos de Cédula del Automotor.

2.3.6 Consulta de Datos de Licencia de Conducir.

2.3.7 Verificación QR.

Contrato Abierto UOC No. 16/2022 MITIC

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria."

Manual de Usuarios

Orden de Trabajo Nro. 9

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC
RECIBIDO : 11/12/23
15:15

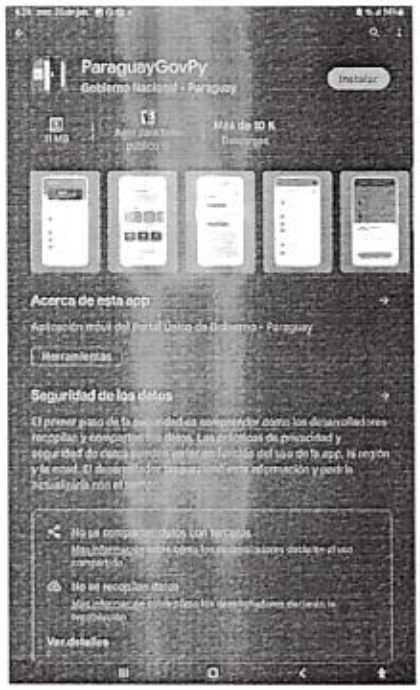
GRUPO HORUS
GRUPO HORUS S.A.

Contenido

Descarga de la App ParaguayGovPy 3
Menú App ParaguayGovPy 3
Iniciar Sesión 4
Sección de Documentos Digitales 4

Descarga de la App ParaguayGovPy

A continuación, veremos la pantalla de la Play Store donde se encuentra la App ParaguayGovPy para la descarga:



Menú App

Empezaremos a recorrer la App ParaguayGovPy, que cuenta con las siguientes secciones:

En la parte superior derecha podremos ver que hay una opción de

que te desplegara las siguientes opciones:

Iniciar Sesión

Para el inicio de sesión deberás ingresar con tus credenciales de Identidad Electrónica, si no cuenta con Identidad Electrónica puede crear la cuenta ingresando los datos solicitado:

Sección de Documentos Digitales

- Cédula Identidad
- Cédula del Automotor
- Licencia de Conducir

- Verificación del documento: permite leer el código QR mediante la habilitación de la cárama y devolver un mensaje de validación: exitosa o no válida

Contrato Abierto UOC No. 16/2022 MITIC

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria"

Manual de Despliegue

Orden de Trabajo Nro. 9

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electróni
Viceministerio TIC - MITIC
RECIBIDO: 11/12/2023 15:15

GRUPO HORUS
GRUPO HORUS S.A.

Asunción – Paraguay

Despliegue en iOS:

Configurar el entorno de desarrollo:

- Tener Flutter instalado en la máquina.
- Descargar desde el sitio web oficial de Flutter.
- Xcode es necesario para compilar y desplegar aplicaciones en iOS.

Configurar el archivo de configuración de iOS:

- Acceder al directorio del proyecto (cd portalpy-app) y abrir el archivo ios/Runner.xcworkspace
- En Xcode, seleccionar el objetivo Runner en el panel de navegación izquierdo.
- Actualizar la información del proyecto, como el nombre de la aplicación, el identificador del paquete, la versión, etc.

Configurar la firma y los certificados:

- En Xcode, ve a los ajustes del proyecto y selecciona tu equipo de desarrollo en la sección "Signing&Capabilities".
- Tener un certificado. Dentro del proyecto acceder al directorio /key.

Ejecutar la aplicación en un dispositivo iOS:

- Conecta tu dispositivo iOS a la Mac.
- En Xcode, selecciona tu dispositivo en la lista de dispositivos de destino.
- Haz clic en el botón de "Play" en la parte superior izquierda de Xcode para compilar y ejecutar la aplicación en tu dispositivo iOS.

Generar un archivo de distribución:

- Distribuir la aplicación a través de la App Store o TestFlight, para ello debemos generar un archivo de distribución.
- En Xcode, ir al menú "Product" y seleccionar "Archive" para crear un archivo de distribución.
- Sigue las instrucciones de Xcode para exportar la aplicación como un archivo. ipa válido.

Publicar en la App Store:

- Si has generado un archivo de distribución, podemos subirlo a App Store Connect para publicar tu aplicación en la App Store.
- Abre App Store Connect en tu navegador web y sigue los pasos para crear una nueva aplicación, completar la información requerida y subir el archivo. ipa.

Despliegue en Android:

Paso 1: Levantar la aplicación

```
flutter run --hot
```

Paso 2: Configurar la versión del código

Actualiza el número de versión de tu aplicación en el archivo pubspec.yaml. Esto es importante para que Google Play Store pueda reconocer las actualizaciones de tu aplicación.

```
version: 1.0.0+1
```

Paso 3: Generar la aplicación firmada

Es importante firmar tu aplicación antes de desplegarla. Puedes hacerlo ejecutando el siguiente comando en el directorio de tu proyecto Flutter:

```
flutterbuildapk --release
```

Este comando generará un archivo APK en la carpeta build/app/outputs/flutter-apk.

Contrato Abierto UOC No. 16/2022 MITIC

"Ajustes a la Aplicación móvil Portal Paraguay para soporte de la validez digital de documentos de portación obligatoria"

Manual de Arquitectura

Orden de Trabajo Nro. 9

Versión Software:	V1R1A01
Fecha Preparación	04-12-2023
Preparado Por:	GRUPO HORUS
Verificado Por:	Dirección Desarrollo – Dirección General Gobierno Digital

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC
Recibido: 11/12/2023
15:15

GRUPO HORUS
GRUPO HORUS S.A.

Histórico de Cambios del Documento

Versión	Fecha	Descripción	Autor
1.0	04-12-2023	Versión Inicial – Documento base preparado en el marco de la Orden de Trabajo Nro. 9	Grupo Horus.

GRUPO HORUS
GRUPO HORUS S.A.

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
Finalidad 4
Universo 4
Definiciones, Acrónimos y Abreviaciones 4
2. REPRESENTACIÓN DE LA ARQUITECTURA 4
3. MODELO CONCEPTUAL 4
4. VISIÓN LÓGICA 5
5. VISIÓN DE IMPLEMENTACIÓN 5
Visión General 5
Capa de Presentación 5
Capa de Negocios 5
Capa de datos 5

GRUPO HORUS
GRUPO HORUS S.A

1. Introducción

Finalidad

El presente documento presenta una visión general que abarca la arquitectura y despliegue del proyecto y está dirigido al personal técnico responsable de realizar la instalación y configuración de la aplicación móvil del Portal Paraguay y el core de documentos digitales; por tanto, se asume que está familiarizado con los conceptos básicos de administración bajo sistema operativo Linux, servidor de aplicación web Wildfly y proxy Nginx. Su intención es capturar y transmitir las decisiones significativas del punto de vista de la arquitectura que serán tomadas en relación con el sistema.

Universo

Este documento de Arquitectura de Software se aplica al proyecto de la aplicación móvil del Portal Paraguay.

Definiciones, Acrónimos y Abreviaciones

JWT: es un estándar RFC 7519 para transmitir información con la identidad y claims de un usuario de forma segura entre un cliente/servidor

Nginx: es un servidor web que también puede ser usado como proxy inverso, balanceador de carga y proxy para protocolos de correo.

2. Representación de la Arquitectura

Este documento presenta la arquitectura como una serie de visiones: modelo conceptual, visión lógica, visión por capas y visión de implementación.

3. Modelo Conceptual

Este modelo muestra las relaciones más importantes con respecto a los componentes principales, la interacción entre los mismos, describiendo el funcionamiento del sistema desde el punto de vista del negocio.

4. Visión Lógica

Esta sección describe las partes significativas del punto de vista de la arquitectura del modelo de diseño, como su división en subsistemas y paquetes. Además de esto, para cada paquete significativo, mostrara su división en clases y utilitarios de clases y las conexiones para obtener datos de cédula policial, licencia de conducir, registro único del automotor a través del módulo de Documentos Digitales.

5. Visión de Implementación

Esta sección del documento describe la estructura general del modelo de implementación, la división del software en capas y subsistemas en el modelo de implementación y todos los componentes significativos del punto de vista de la arquitectura.

Visión General

El Sistema estará dividido en 3 capas, siendo estas la capa 1 o capa de presentación (aplicación móvil), la capa 2 o capa de negocios (backend) y la capa 3 o capa de datos (dataend – mongodb – sistema intercambio de información).

Capa de Presentación

La capa de presentación del sistema constituye todos aquellos componentes del sistema que hacen posible la comunicación entre el usuario y el sistema.

Capa de Negocios

La capa de negocios está organizada en diferentes paquetes.

Capa de datos

La capa de base de datos está conformada por un gestor de base de datos encargada de recibir solicitudes de almacenamiento de los datos o recibir solicitudes de recuperación desde la capa de negocios.

GRUPO HORUS
GRUPO HORUS S.A

ANEXO

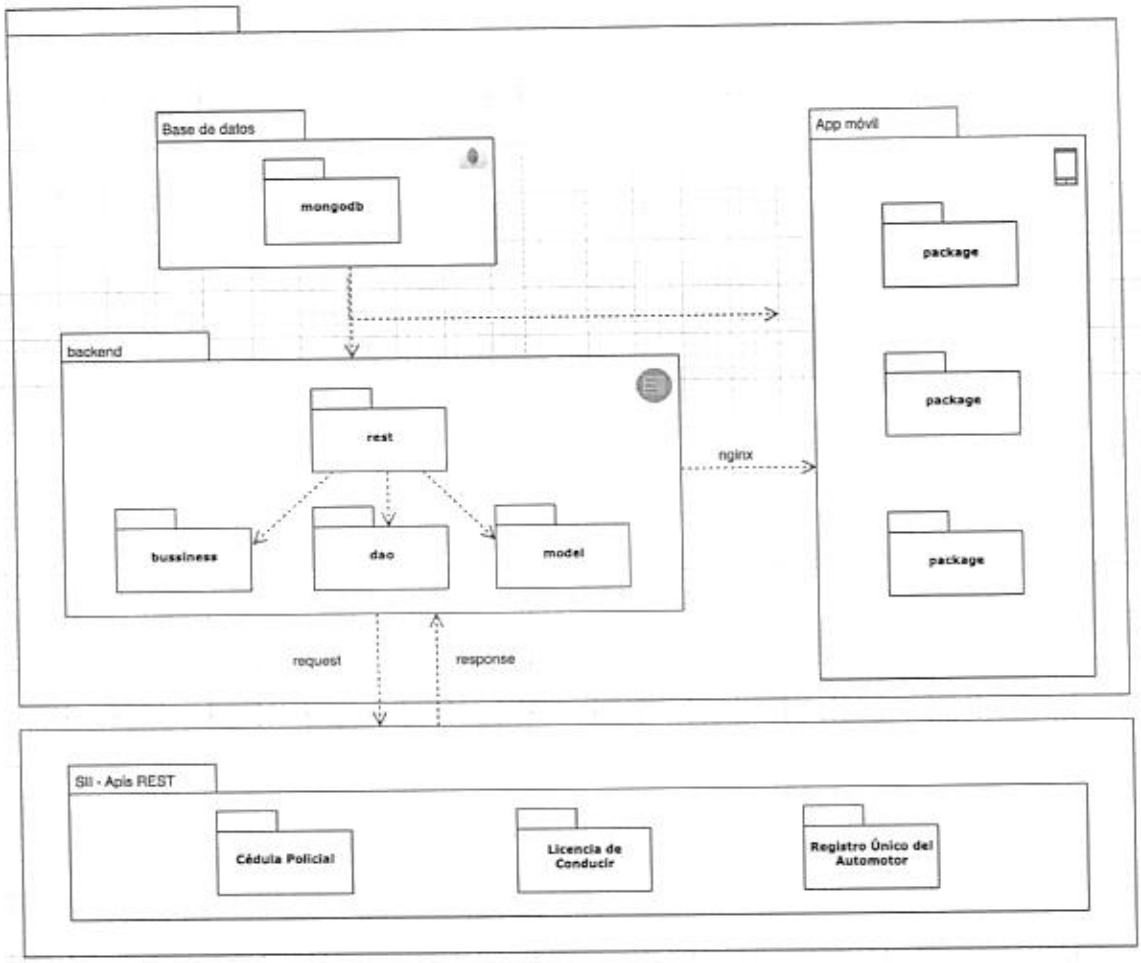


Imagen 1. Diagrama General de paquetes

MINISTERIO DE
TECNOLOGÍAS DE
LA INFORMACIÓN Y
COMUNICACIÓN
PARAGUAY

Ministerio de Tecnologías de la Información y Comunicación (MITIC)

Software Factory MITIC -Orden de Trabajo No. 9

Aplicación Móvil Portal Paraguay – Documentos Digitales

Informe de Análisis de Vulnerabilidades

ELABORADO POR:

GRUPO HORUS

21 de noviembre 2023

Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC
Recibido: 11/12/2023
15:15

DOCUMENTO CONFIDENCIAL

GRUPO HORUS
GRUPO HORUS S.A.

Elaborado Por:	Equipo Grupo Horus SA	
Aprobado Por	(MITIC)	

Histórico de Versiones

Fecha	Versión	Modificación	Realizado por
21-11-23	1.0	Versión Enviada para Aprobación MITIC	Equipo Grupo Horus

Tabla de contenido

Alcance y Metodología de trabajo 2

Resumen de las actividades realizadas 4

Resultados obtenidos 5

Principales riesgos identificados 6

Recomendaciones 7

Anexos 8

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A

1. Alcance y Metodología de trabajo

La realización de un Test de seguridad implica seguir una metodología estructurada para identificar y abordar las posibles vulnerabilidades en un sistema. A continuación, se describe una metodología general de trabajo en un test de seguridad.

1.1. Definición del Alcance:

Se define como alcance del análisis de vulnerabilidades al sitio del Portal Paraguay e Identidad Electrónica, con énfasis en lo que respecta a la aplicación móvil del Portal Paraguay – módulo de documentos digitales.

Se se tiene como alcance inicial las siguientes URLs:

https://www.paraguay.gov.py/docsapi/app/documento/
https://www.paraguay.gov.py/docsapi/documento/
https://identidad.paraguay.gov.py/login

Las actividades fueron realizadas con las siguientes consideraciones:

- Utilización de una herramienta no intrusiva. Para tal efecto, se utilizó la herramienta QUALYS – WAS (https://www.qualys.com/apps/web-app-scanning/)
- No se realizaron simulaciones o exploración de mecanismos que lleven a denegación de servicios.

1.2. Metodología – Etapas

Se realizaron las siguientes actividades y etapas:

Recolección de Información (Reconocimiento):

- Se realizó un análisis de información para recopilar detalles sobre la infraestructura del objetivo.
- Se identificaron posibles puntos de entrada, subdominios, rangos de direcciones IP y tecnologías utilizadas.

Ejecución de Pruebas (Escaneo y Penetración):

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A

- Se realizaron pruebas de escaneo para identificar posibles vulnerabilidades y exposiciones.
- Se ejecutaron pruebas de penetración para explotar y validar las vulnerabilidades identificadas.
- Se Realizaron pruebas manuales para descubrir vulnerabilidades que las herramientas automatizadas puedan pasar por alto.

Análisis de Resultados:

- Por medio del presente informe, se hace una presentación y evaluación de los resultados de las pruebas, clasificando las vulnerabilidades por gravedad.
- Se definió una priorización de las vulnerabilidades en función de su impacto y probabilidad de explotación.
- Se Identificaron posibles vectores de ataque y caminos de compromiso.

Elaboración del Informe:

- Presenación del presente informe, en el cual se proporcionan las recomendaciones detalladas para abordar y remediar cada vulnerabilidad.
- Presentación del informe al cliente, incluyendo hallazgos, análisis de riesgos y acciones recomendadas.

Seguimiento y Retroalimentación:

- Se recomiendan realizar sesiones de retroalimentación para discutir los resultados y proporcionar aclaraciones si es necesario.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

2. Resumen de las Actividades Realizadas

A continuación, se provee un resumen da las principales actividades realizadas:

- Inicio de las Actividades de Preparación: 20/11/2023 18:00
- Inicio del Escaneo lanzado en la Herramienta: 20/11/2023 21:00
- Fin del Escaneo lanzado en la Herramienta: 21/11/2023 4:00
- Análisis de Resultados e Identificación de Falsos Positivos: 21/11/2023 8:00 AM a 12:00AM
- Elaboración del Informe: 21/11/2023 12:00 a 21/11/2023 a 13:00hs

Durante la ejecución de las actividades, se observaron las siguientes situaciones:

- Al momento de la preparación para ejecución de la herramienta, se identificaron medidas de protección anti-DDOS e IPS en el sitio a ser escaneado.
- En función de estas medidas de protección, se procedió a configurar la herramienta para realizar una ejecución de manera menos invasiva y con medidas que enmascaraban el tráfico de escaneo como un tráfico normal. Por tal motivo, el periodo de escaneo tuvo una duración superior a 8 horas.
- Si bien no se identificaron vulnerabilidades directamente asociadas a los *endpoints* solicitados, la herramienta (mediante el proceso de crawling) identificó potenciales vulnerabilidades en el sitio que requieren de atención y están expuestas en las secciones siguientes.
- Como medida complementar, se procedió a realizar un análisis del estado de configuración de frontal WEB, específicamente en lo que respecta a la configuración del certificado SSL utilizado para protocolo HTTPS.
- Inspección del Ambiente: se procedió a verificar con el equipo de desarrollo el stack tecnológico actualmente utilizado. Se menciona cuanto sigue:
    - Versión de Java: 8
    - Versión del Servidor de Aplicaciones: Wildfly 10.1. Final
    - Obras Libs/Frameworks: Redis 3.5.4

  Es importante observar que, al momento de la realización de los escaneos, no fue posible identificar las versiones del stack ya que el servicio se encuentra detrás de un WAF y balanceo de carga, lo cual agrega de manera correcta un nivel adicional de seguridad.

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

3. Resultados Obtenidos

3.1. Análisis Vulnerabilidades

Se han realizado consultas y análisis para identificación de brechas de seguridad de la información sobre el dominio **paraguay.gov.py y identidad.paraguay.gov.py** y endpoints definidos consultas no intrusivas con el fin de identificar vulnerabilidades ya conocidas. La modalidad utilizada para la realización de las pruebas fue del tipo *caja negra*.

Aplicación	Level 5	Level 4	Level 3	Level 2	Level 1	Informativos
https://www.paraguay.gov.py/	2		10	1	2	46
https://identidad.paraguay.gov.py			4		1	22

Nivel de Severidad	Escala CVSS	Cantidad de Vulnerabilidades Identificadas
Alta	7.0 – 10	2
Media	4.0 – 6.9	14
Baja	0 - 3.9	4

En base al resultado y en función del tiempo, se procedió a realizar el análisis para los niveles de Severidad ALTA y descarte de potenciales falsos posiivos.

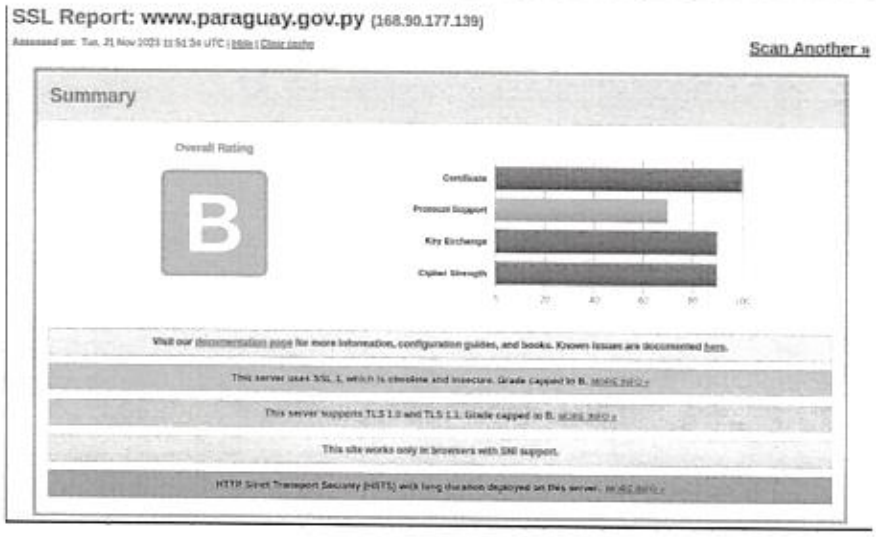
3.2. Análisis SSL

Adicionalmente, se realizó un análisis del uso de SSL en el portal y se obtiene lo siguiente:

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.



Como principal punto, se observa que la configuración actual permite la utilización de protocolos SSL (TLS 1.0, TLS 1.1 y SSL 3) antiguos que poseen vulnerabilidades conocidas.

4. Principales Riesgos Identificados:

Para catalogar las vulnerabilidades se ha utilizado catálogos de vulnerabilidades como CVE (Common Vulnerabilities Enumeration) y CWE (Common Weakness Enumeration) para tener un análisis más acabado de la situación ya que CVE trata los síntomas mientras que el CWE trata una causa. Si el CWE clasifica los tipos de vulnerabilidades de software, el CVE es simplemente una lista de problemas conocidos actualmente con respecto a sistemas y productos específicos.

El presente cuadro refleja las vulnerabilidades encontradas con su correspondiente descripción, tipo y severidad de vulnerabilidades encontradas. Consulte el ANEXO para mayores detalles de las vulnerabilidades aquí listadas.

Tipo	Descripción de la Vulnerabilidad	CVE/s-CWE/s	Severidad Identificada
Cross-Site Scripting	Es un tipo de vulnerabilidad de seguridad en aplicaciones web que ocurre cuando los datos proporcionados por un usuario, generalmente a través de parámetros de URL o formularios web, se incluyen en el código HTML de una página y se ejecutan de	CWE-79	**Level 5**

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS
GRUPO HORUS S.A.

	manera no segura en el navegador del usuario.		
Information Disclosure	El ataque de Clickjacking es una técnica maliciosa en la que un atacante superpone de manera invisible contenido engañoso sobre un sitio web legítimo con el fin de engañar a los usuarios para que hagan clic en elementos que no son lo que parecen.	CWE-451	Level 3

5. Recomendaciones

Recomendación 1 – Implementación CSP.

Considerando las dos principales vulnerabilidades encontradas, se recomienda la configuración en los servidores WEB par la implementación de un Content Security Policy (CSP) de manera efectiva. Para la implementación de CSP, se debe tener un entendimiento claro de los recursos que los servicios las páginas requieren para su correcto funcionamiento ya que una política muy restrictiva puede causar impacto en el servicio.

Recomendación 2 – Mejoras en la configuración SSL.

Se recomienda deshabilitar las compatibilidades a versiones de SSL antiguas.

Recomendación 3 – Análisis Detallado del Resultado del Escaneo

Conforme puede observarse, la herramienta de análisis de vulnerabilidades detectó 20 potenciales vulnerabilidades que potencialmente puedan representar un riesgo o amenaza al servicio. En virtud del alcance del presente servicio, no se ha procedido a realizar un análisis exhaustivo para confirmar/evaluar que la amenaza sea real y el equipo se ha limitado a realizar el análisis con base a las vulnerabilidades identificadas con mayor prioridad.

Recomendación 4 – Actualización del Stack Tecnológico

Si bien no se ha podido identificar de manera correcta el stack tecnológico que el servicio utiliza, un potencial usuario malicioso que posea información privilegiada podría explorar vulnerabilidades de librerías y el software utilizado en virtud de que las versiones utilizadas para los principales componentes son antiguas y poseen vulnerabilidades conocidas. Algunos ejemplos:

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

- Vulnerabilidades del Wildfly 10.1.Final (versión actual es 30.0)
- Vulnerabilidades del Java 8
- Vulnerabilidad del LOG4J (siendo utilizado indirectamente)
- Vulnerabilidades del REDIS

Recomendación 5 – Análisis de Vulnerabilidades – Red Interna

A partir del análisis de vulnerabilidad fue realizado a partir de un sitio externo, se ha podido observar que los mecanismos de protección y prevención han podido mitigar la exposición de potenciales vulnerabilidades de los servicios internos. No obstante, se recomendaría la realización de un análisis de vulnerabilidades a partir de la red interna, ya que un potencial vector de ataque puede iniciarse a partir de la red interna.

ANEXOS

ANEXO A - Detalle de los Riesgos Identificados que requieren atención

1.1. Cross-Site Scripting

Las vulnerabilidades XSS ocurren cuando la aplicación web reproduce datos suministrados por el usuario en una respuesta HTML enviada al navegador web. Por ejemplo, una aplicación web podría incluir el nombre del usuario como parte de un mensaje de bienvenida o mostrar una dirección residencial al confirmar un destino de envío. Si los datos suministrados por el usuario contienen caracteres interpretados como parte de un elemento HTML en lugar de texto literal, entonces un atacante puede modificar el HTML que recibe el navegador web del usuario.

El payload de XSS se reproduce en el documento HTML devuelto por la solicitud. Un payload de XSS puede consistir en HTML, JavaScript u otro contenido que será renderizado por el navegador. Para explotar esta vulnerabilidad, un usuario malintencionado necesitaría engañar a la víctima para que visite la URL con el payload de XSS.

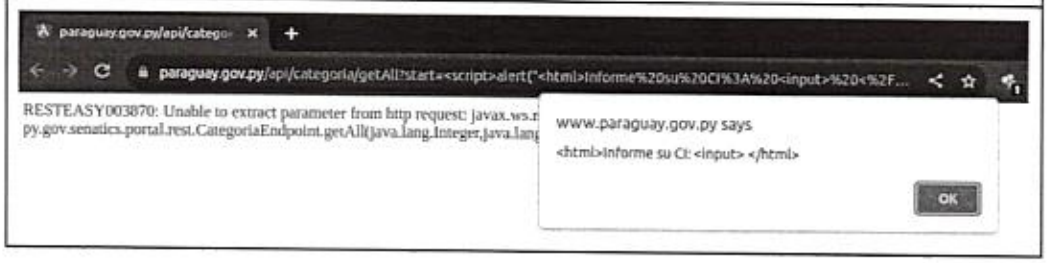
Información de Detección	
https://www.paraguay.gov.py/api/categoria/getAll?start=%3Cscript%3Ealert(%22%3Chtml%3EInforme%20su%20CI%3A%20%3Cinput%3E%20%3C%2Fhtml%3E%22)%3C/script%3E	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

Parámetro:	Se ha detectado al explotar el parámetro "start".
Parámetro:	Se ha detectado al explotar el parámetro "pageSize".



1.1. Information Disclosure

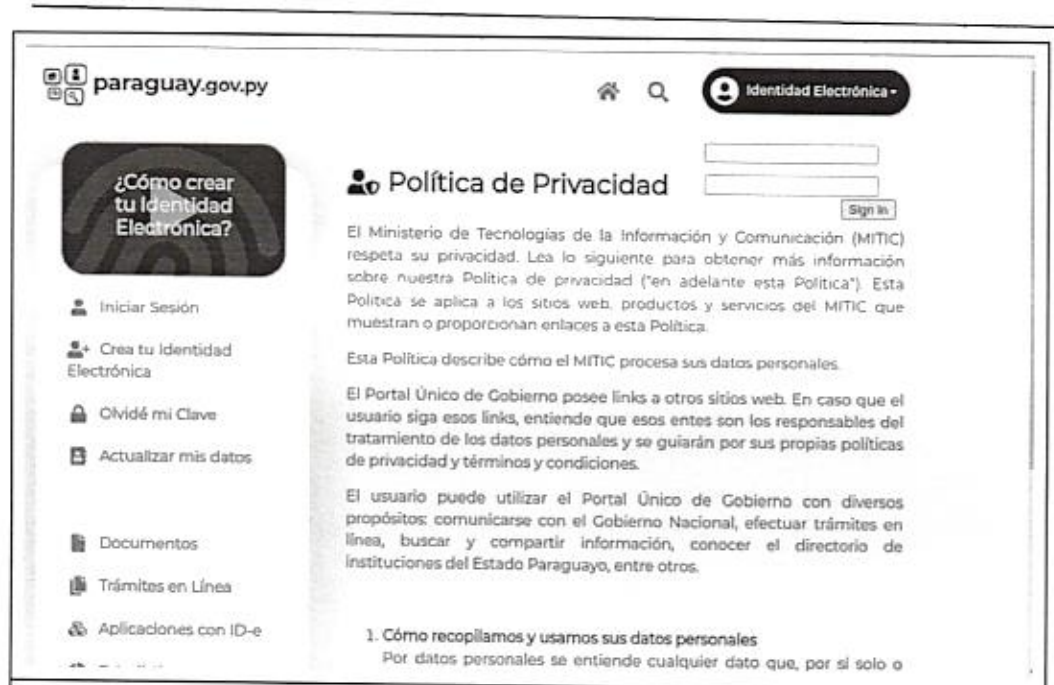
El ataque de Clickjacking es una táctica maliciosa donde un atacante superpone de manera oculta contenido engañoso sobre un sitio web legítimo, llevando a los usuarios a interactuar con elementos que no son visibles para ellos. Esta superposición se logra mediante iframes u otras técnicas de posicionamiento en el código HTML.

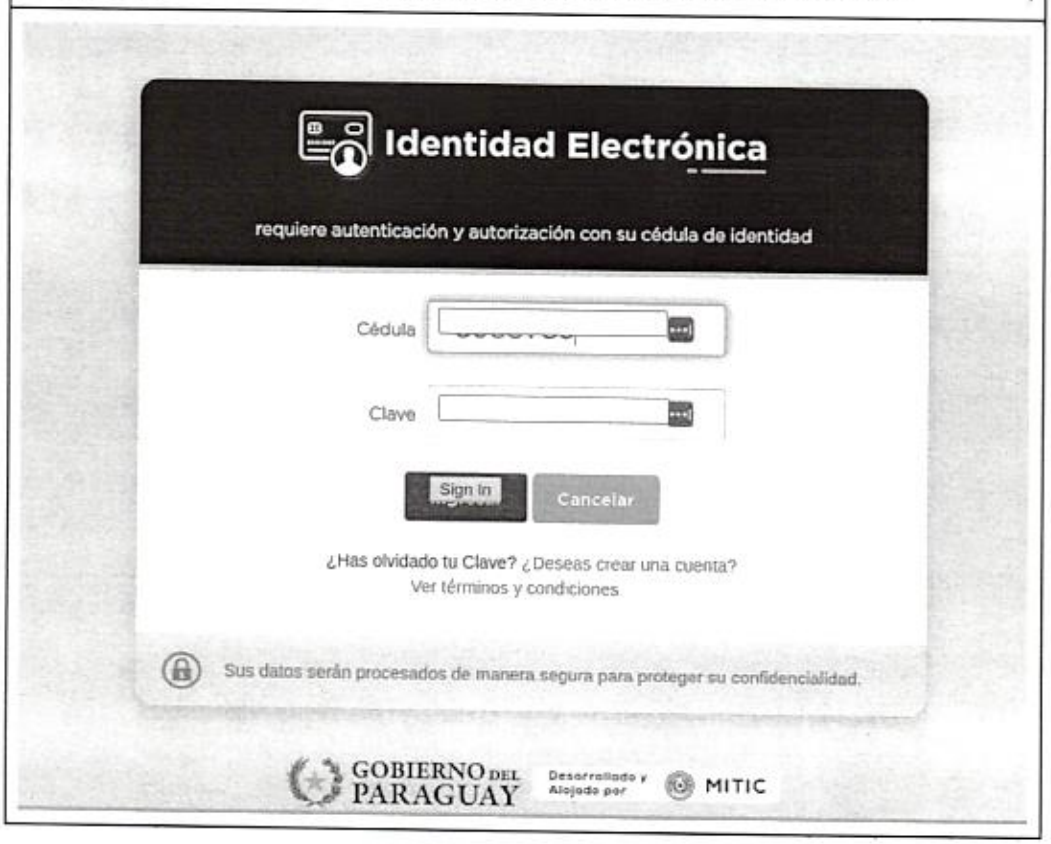
Información de Detección	
https://www.paraguay.gov.py/identidad-electronica/privacidad https://www.paraguay.gov.py/gobierno-electronico https://www.paraguay.gov.py/assets/assets/img/icons/114x114.png https://www.paraguay.gov.py/estadisticas-portal https://www.paraguay.gov.py/planes-nacionales https://www.paraguay.gov.py/assets/assets/img/icons/default.png https://www.paraguay.gov.py/estado/poder-legislativo%20 https://www.paraguay.gov.py/ https://www.paraguay.gov.py/solicitud-cambio-datos https://www.paraguay.gov.py/assets/assets/img/icons/72x72.png https://identidad.paraguay.gov.py/. https://identidad.paraguay.gov.py/login https://identidad.paraguay.gov.py/favicon.ico https://identidad.paraguay.gov.py/	

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.





Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.

GRUPO HORUS

GRUPO HORUS S.A.

ANEXO B- Reporte de la Herramienta Qualys - Vulnerabilidades

Reporte enviado a los siguientes correos:

- desarrollo@mitic.gov.py
- implementacion@mitic.gov.py
- kpistilli@mitic.gov.py

Este documento es CONFIDENCIAL Y SENSIBLE, está destinado de manera única y exclusiva para distribución en el Ministerio de Tecnologías de la Información y Comunicación (MITIC). Su contenido no puede ser copiado, publicado, divulgado o utilizados por terceros en cualquier forma no autorizada expresamente, el uso de este documento implica la aceptación de estos términos.