Proveedor: Grupo Horus S.A.

Orden de Trabajo (OT)

Resumen	
Nro. de Orden	14
Horas	167 Horas
Total de días hábiles	93 días hábiles
Detalle	
Fecha de pedido de la OT	05/01/2021
Fecha de acuse de recibo de la OT por parte del proveedor	05/01/2021
Fecha tope para presentación del Plan de Trabajo (Máximo de 3 días hábiles posterior a la recepción de la OT)	08/01/2021
Fecha de entrega al MITIC para inicio de las verificaciones	05/03/2021
Fecha tope para emisión de Constancia de recepción satisfactoria (Máximo de 50 días hábiles)	20/05/2021

Nombre del Producto
Mejoras en la Aplicación Móvil del Portal Único de Gobierno y Módulo de Controles Críticos.

Objetivo
Implementar nuevos métodos de autenticación en la aplicación móvil del Portal Único de Gobierno y mejorías en el módulo de controles críticos.

Referencias

- Decreto 8709/2018
- Portal Paraguay: https://www.paraguay.gov.py/
- Documentos disponibles: https://www.paraguay.gov.py/documentos
- Mi carpeta ciudadana: https://www.paraguay.gov.py/carpeta-ciudadana

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

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

GRUPO HORUS
GRUPO HORUS S.A.
ALEJANDRO DE FILIPPIS

1. Visión General

1.1. Descripción del Alcance.

El presente documento abarca la descripción acerca de los requisitos funcionales y no funcionales que deberán ser considerados en el proceso de desarrollo de los siguientes componentes:

- Autenticación Biométrica local en la Aplicación móvil del portal Paraguay: Adecuación de la aplicación móvil del portal Paraguay para incorporar mecanismos de identificación biométrica disponibles en el móvil del usuario. Específicamente la autenticación vía autenticación biométrica local (ya sea mediante reconocimiento facial o dactilar). Se deberán prever las adecuaciones en el flujo de autenticación, configuración e interfaz gráfica de la aplicación móvil.
- Mejorías en el Módulo de Controles Críticos del Portal Paraguay: Implementación de mejoras en el módulo de controles críticos a nivel funcional y de usabilidad de este.

1.2. Requisitos Funcionales

A continuación, se listan los requisitos funcionales.

A- Mecanismo de Autenticación en la Aplicación del Portal Paraguay	RF1. Habilitar el desbloqueo de la App mediante Autenticación Biométrica – Primer Acceso. RFA2. Acceso a la App mediante autenticación biométrica – Posterior al Primer Acceso. RFA3. Ajustes en la pantalla de login para incorporar nueva opción de autenticación. RFA4. Ajustes en el menú de configuraciones del usuario para incorporar opción de autenticación biométrica. RFA5. Adecuaciones en el Backend de Portal Paraguay (portal-py-backend-core) para envío de parámetros relacionados a sesión.

B- Mejorías en el Módulo de Controles Críticos	Implementación de mejoras en el módulo de controles críticos.

2. Requerimientos Funcionales - Mecanismo de Autenticación en la Aplicación del Portal Paraguay.

RFA1. Habilitar el desbloqueo de la App mediante Autenticación Biométrica – Primer Acceso:

Se deberá integrar a la APP una librería (definido en **RNF.1**) que permita la Autenticación Biométrica al usuario. A continuación, se describe un paso a paso del flujo de ingreso a la aplicación portal Paraguay:

- Primer Acceso a la App:

Paso 1: El usuario, una vez que tenga instalada la APP y autorizado los permisos de uso iniciará la APP.

Paso 2: El usuario ingresa a la APP con su usuario y password correspondiente a su identidad electrónica.

- Se deberá guardar una información local en la APP para identificar que este es el primer ingreso.
  - Nota: la información que será guardada localmente será un TOKEN.
- En este paso se generará su TOKEN de sesión y se obtendrá el valor de tiempo de EXPIRACIÓN LOCAL

Paso 3: Al identificar que se trata del primer ingreso e identificado que la APP posee los permisos necesarios, se mostrará un pop-up al usuario preguntando si el mismo desea habilitar la autenticación mediante "Autenticación Biométrica" en la APP.

Paso 4: El usuario escoge la opción de habilitar la autenticación biométrica. Se registra localmente:

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

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

1- La información de que posee autenticación biométrica habilitada.
2- Actualizar la información del primer acceso.
3- Token de Acceso generado, vinculado a la autenticación biométrica.
4- Se registra un tiempo de EXPIRACIÓN LOCAL definido en la fecha y hora actual incrementada en T1 (**RNF2**).

Paso 5: El flujo continúa conforme a la versión actual de la APP.

RFA2. Acceso a la APP mediante Autenticación Biométrica – Posterior al Primer Acceso:

Paso 1: el usuario inicia o activa la App en su móvil. Nota: esta situación se deberá aplicar tanto en el caso de que la aplicación este en background, suspendida como en el caso de que la aplicación se esté iniciando.

Paso 2: en este momento, se procede a la siguiente lógica de decisión en la app:

1. Verificación de existencia de un TOKEN asociado a la Autenticación Biométrica.
2. Verificación si el TOKEN no se encuentra expirado para el tiempo de EXPIRACIÓN GENERAL.
3. Verificación si el TOKEN no se encuentra expirado para el tiempo de EXPIRACIÓN LOCAL.
4. Se verifica el tiempo que el usuario tenía abierto por última vez la APP. Dependiendo de la configuración definida por el usuario, la APP deberá solicitar la autenticación biométrica o no.

Paso 3: en este momento, se procede a la siguiente lógica de decisión en la App:

1. En el caso de que el tiempo de EXPIRACIÓN GENERAL y EXPIRACIÓN LOCAL no esté expirado:
   a. La APP exhibirá una pantalla de bloqueo en el cual le solicitará su autenticación vía Autenticación Biométrica.
   b. En caso de autenticación con éxito, la APP incrementará el tiempo de sesión de EXPIRACIÓN LOCAL en T1 tiempo (**RNF2**) y avanza al **Paso 4.**

2. En caso de que el tiempo de EXPIRACIÓN GENERAL o EXPIRACIÓN LOCAL esté expirado:
    a. La APP exhibirá una pantalla de bloqueo en el cual le solicitará su identificación vía Identidad Electrónica.
    b. En caso de autenticación con éxito:
        i. No se volverá a preguntar si desea habilitar autenticación biométrica.
        ii. Se define el tiempo de EXPIRACIÓN LOCAL a partir de la fecha y hora actual incrementado de T1 (**RNF2**)
        iii. Se avanza al **Paso 4**.

Paso 4: el flujo continuo conforme a la APP actual.

RFA3. Ajustes en la pantalla de login para incorporar nueva opción de autenticación

Se deberá crear nueva pantalla o ajustar la pantalla existente para incorporar la opción de autenticar vía Autenticación Biométrica. La mecánica de funcionamiento de esta pantalla deberá ser:

1. Al momento de iniciar/activar la APP se exhibirá esta pantalla.
2. En el caso de autenticación vía reconocimiento facial, la pantalla se deberá desactivar automáticamente.
3. En el caso de autenticación vía huella dactilar, falla de autenticación se deberá mantener exhibida esta pantalla.
4. En el caso de X reintentos fallidos, se deberá exhibir un botón/enlace que lleve a la pantalla de login original de tal forma que el usuario pueda autenticarse vía su identidad electrónica.

RFA4. Ajustes en el menú de configuraciones del usuario para incorporar opción de Autenticación Biométrica:

Se deberá habilitar una opción en la sección de informaciones personales del usuario en el cual el mismo tenga las siguientes opciones:

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

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

- Habilitar/Deshabilitar autenticación biométrica
- Volver a pedir autenticación biométrica en el primer acceso.
- Opción de "No pedir autenticación si el reingreso ocurrió en menos de X minutos".

RFA5. Adecuaciones en el Backend del Portal Paraguay para envío de parámetros relacionados a sesión:

Se deberán realizar los ajustes en el módulo de Identidad Electrónica para que al momento de que un usuario se autentique, los siguientes parámetros deberán ser enviados:

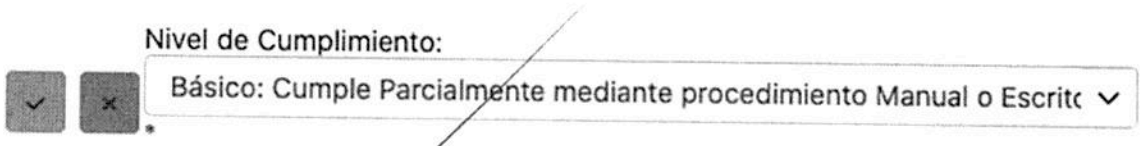
- Tiempo de Sesión Global.
- Tiempo de Sesión Local.
- Cantidad límite de intentos (autenticación biométrica).

La APP deberá estar preparada para obtener esta información al momento de autenticarse y utilizar como parámetros a ser utilizado.

3. Requerimientos Funcionales - Mecanismo de Autenticación en la Aplicación del Portal Paraguay.

RFB1. Campo observación en Nivel de Cumplimiento:

- Se debe poder editar Observación, e indicar textualmente que es opcional.



ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

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

RFB2. Adecuaciones en el tiempo de sesión

El tiempo de cierre de sesión es muy corto - por la naturaleza de las evaluaciones, debería ser al menos 1 hora. Además, el cierre de sesión se debe dar únicamente cuando hay INACTIVIDAD durante ese tiempo - actualmente se cierra, aunque haya actividad.

RFB3. Filtro de OEEs en la generación de reportes

En el filtro no aparecen todas instituciones que están siendo evaluadas... (ejemplo fuerzas militares), por ende, no se genera el reporte con la información completa, desde el super admin. Se agregó un control de OEE del usuario al loguearse y solo permite loguearse cuando está activa

RFB5. Alta Usuario con rol de Administrador

Agregar validación en el alta de usuarios para que Alta de nuevos usuarios, el rol de administrador de ciberseguridad solo debe pueda ser asignado a usuarios del MITIC

RFB6. Agregar tabla de referencia al nivel de cumplimiento

Al momento de editar una evaluación, el número del nivel de cumplimiento no es intuitivo, poner una tabla de referencia o escribir un texto

Subcontrol 1-Utilizar una herramienta de descubrimiento activo

Descripción: Utilice una herramienta de descubrimiento activo para identificar equipos conectados a la red de la organización y actualizar el inventario de activos hardware.

Tipo Activo: Equipos-Función Seguridad: Identificar

Nivel de Cumplimiento: 2
Observación:
Editar

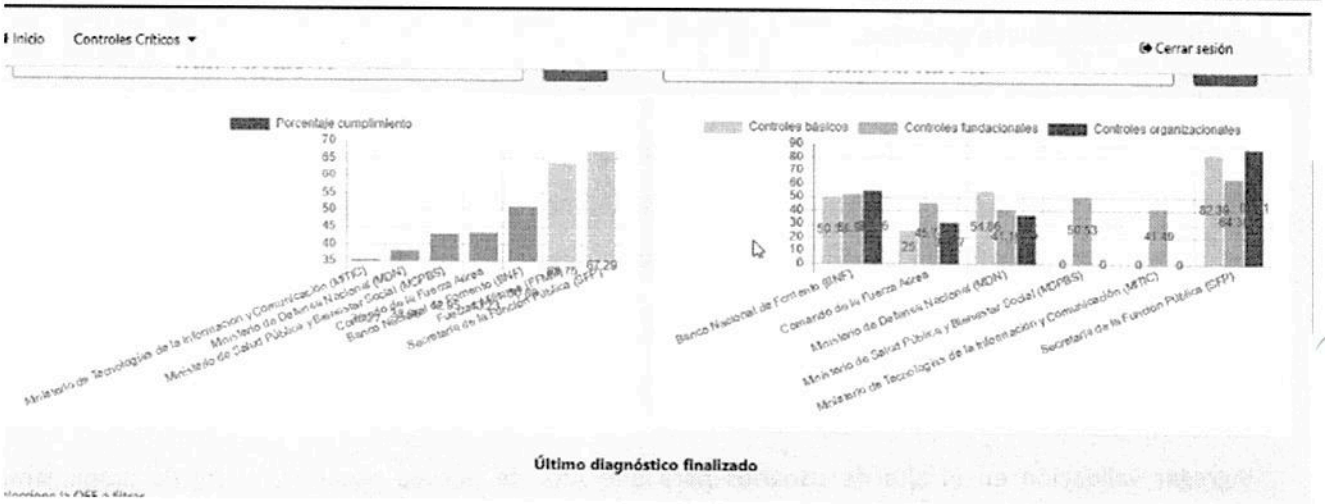
RFB7. Ajustes visuales en el reporte de Controles Críticos

- Mejorar la visualización en el caso de que existan más instituciones, usar todo el espacio de la pantalla para cada gráfico, bajar uno de ellos
- Agregar etiqueta en el primer gráfico
- Ajustar el gráfico para que inicie en 0

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

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.



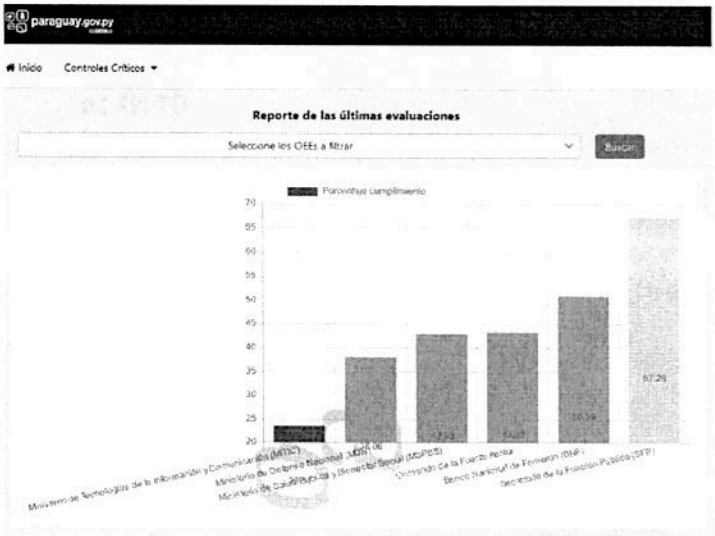
RFB8. Reportes Globales - Reporte de las últimas evaluaciones

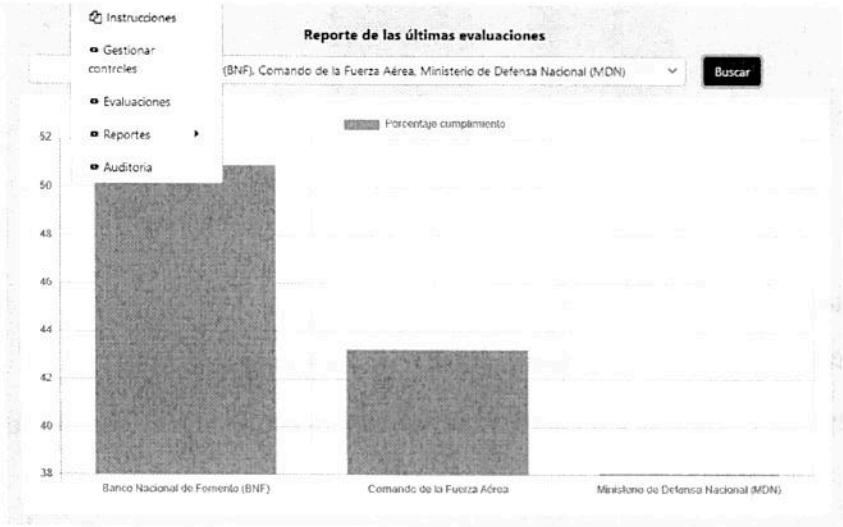
- Ajustar la descripción del color de referencia.
- Ajustar la disposición de los porcentajes de cumplimiento para que se visualización en vertical y centrado.
- Ajustar el filtro seleccionado para que aparezca en cualquier tipo de selección el porcentaje de cumplimiento.
- Ajustar el inicio del gráfico de tal forma a que inicie en 0.

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

ALEJANDRO DE FILIPPIS
GRUPO HORUS

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

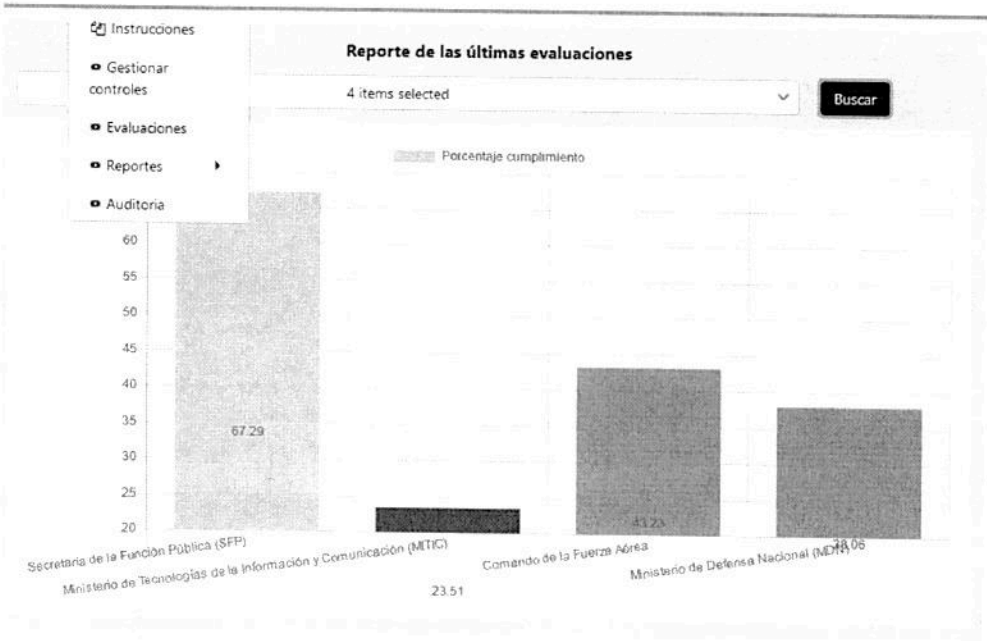




Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

Viceministerio de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

ALEJANDRO DE [illegible]
GRUPO HORUS
GRUPO HORUS S.A.



RFB9 Reporte de las evaluaciones por tipo de control

2.1 Los porcentajes de cumplimiento no se leen correctamente. Ajustar de forma vertical

1.2 Dependiendo del filtro seleccionado, en algunas ocasiones no se muestra el porcentaje de cumplimiento. Se debe mostrar el porcentaje de cumplimiento.

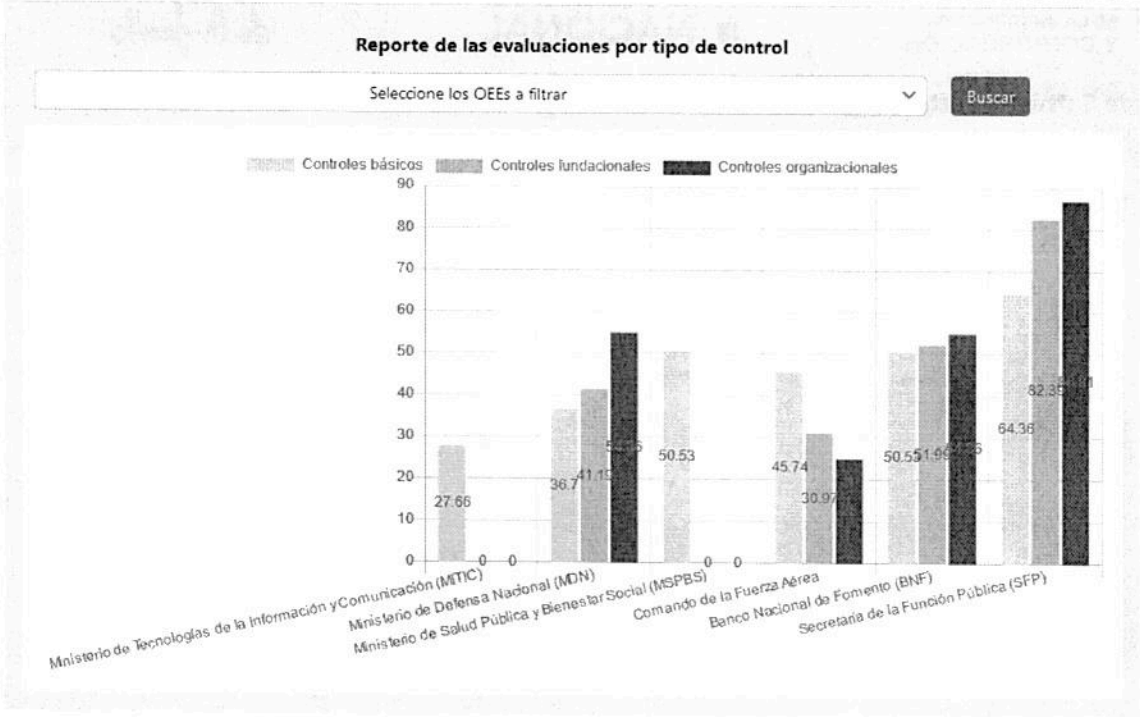
1.3 Hacer con que el gráfico inicie en 0.

1.4 Mostrar los porcentajes de cumplimiento centrados y en vertical.

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

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

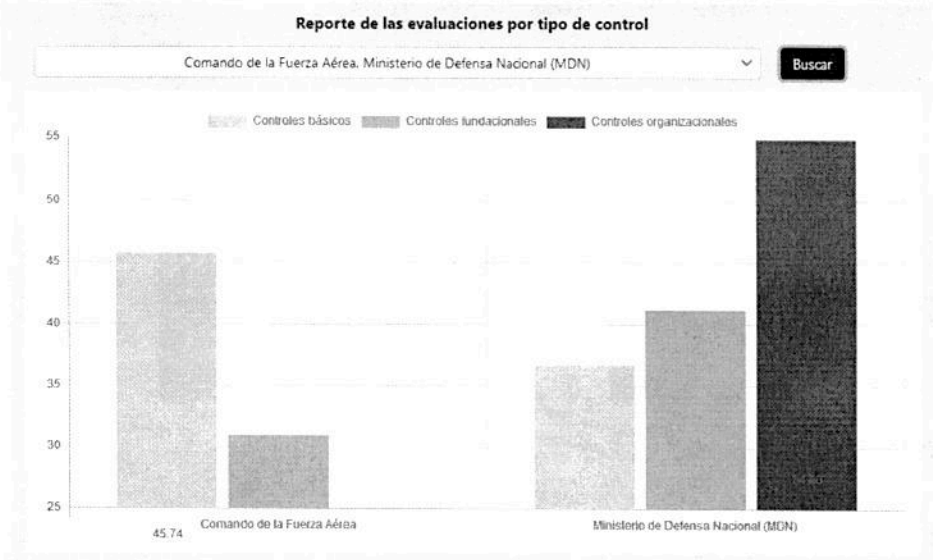
Viceministerio de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

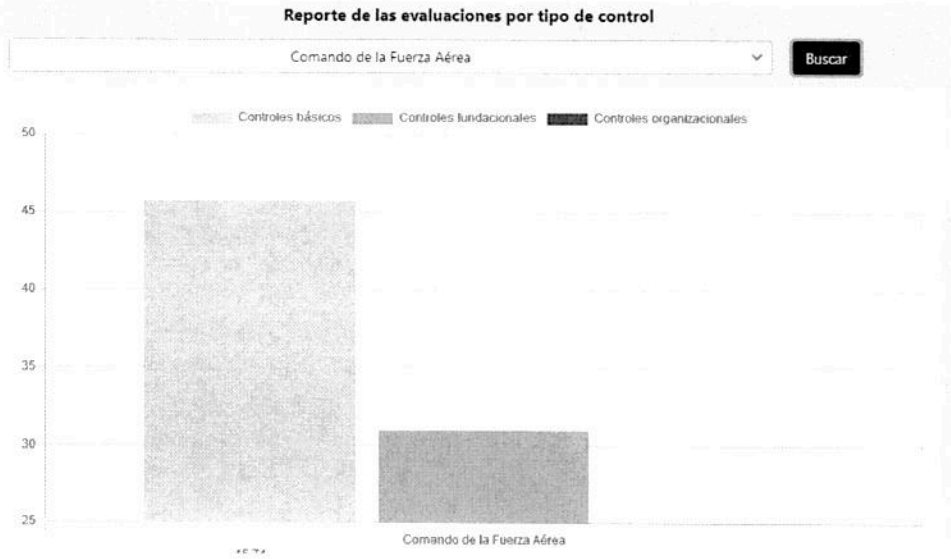


Ing. Klaus Pistilli
Dir. Gral. de Gobierno Electrónico
Viceministerio TIC - MITIC

Miguel M...
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.





4. Requerimientos No Funcionales

RNF 1. Librería de Autenticación Local: se deberá utilizar la librería flutter Local Auth para la implementación requerida (local_auth | Flutter Package (pub.dev))

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

ALEJANDRO DE PEDRIS
GRUPO HORUS
GRUPO HORUS S.A.

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

RNF 2. Manejo de valores de tiempo de Sesión: los valores de tiempo de sesión deberán ser configurables. Los parámetros/variables que se obtendrán a partir de obtención del servidor entonces serian:

- Tiempo expiración del TOKEN (ya está definido).
- Tiempo expiración Local (nuevo parámetro).
- Cantidad Reintentos (nuevo parámetro).

RNF 3. Cualquier librería adicional deberá ser documentada y comunicada al equipo técnico del MITIC.

RNF 4. Para todos los casos, los servicios REST deben devolver únicamente aquellos datos a utilizarse.

RNF 5. Deberán utilizarse los proyectos (repositorio y ramas) de código fuente entregados por el equipo técnico del MITIC, modificando y entregando los productos y documentaciones en dichos repositorios.

RNF 6. Las adecuaciones relacionadas a sesión, a ser desarrolladas, se deberá realizar en el proyecto portal-py-backend-core.

RNF 7. Renovación de cuenta de desarrollador en la AppStore.

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

Dirección General de Gobierno Electrónico
Administrador de contrato

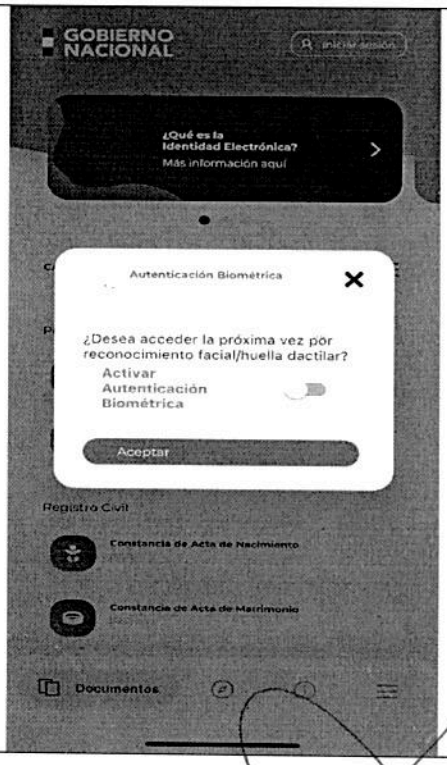
Grupo Horus S.A
Proveedor

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

4. ANEXOS

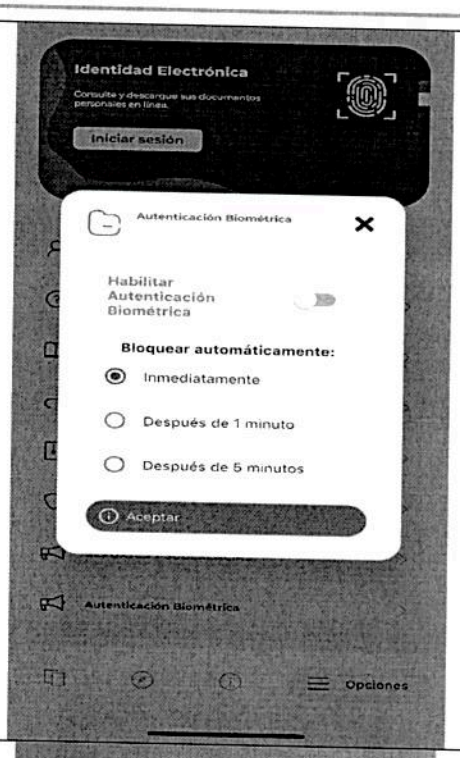
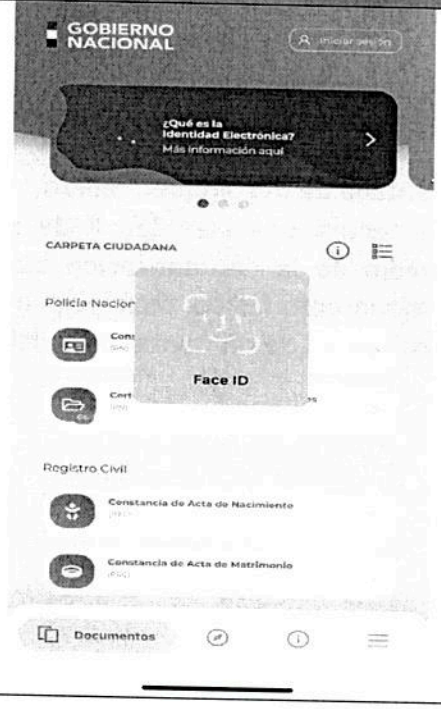
4.1 Prototipo de Pantallas – Ajuste en la Aplicación Móvil del Portal Paraguay

Pantalla	Descripción
	Solicitud de permisos para la autenticación biométrica. Al ingresar a la aplicación, solicitará permiso para la autenticación biométrica. Para este caso, de acuerdo con el soporte del teléfono, estará disponible la autenticación por medio de reconocimiento facial o huella dactilar. Acceso a la Pantalla: Login (1ra. vez) Habilitar permiso.
	**Pantalla de activación biométrica (reconocimiento facial/huella dactilar)** Una vez autorizado los permisos de uso para la autenticación biométrica, y accedido por primera vez a través de su identidad electrónica, solicitará la confirmación para el desbloqueo por medio del reconocimiento facial o huella dactilar, esto dependiendo de la compatibilidad del teléfono. **Acceso**: Login (1ra vez) habilitar permiso y al activar la APP.

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

ALEJANDRO DE FILIPPIS
GRUPO HORUS

Miguel Martín
Viceministro de Tecnologías de la Información y Comunicación - MITIC

	**Pantalla de menú de configuración** En la sección de informaciones personales del usuario, se tendrá la posibilidad de conceder el permiso de "Autenticación biométrica". La opción de "Bloquear automáticamente", solo estará disponible para Android. Para el caso de iOS, esta pantalla no será presentada y la opción estará disponible en directamente en la configuración de permisos del teléfono. Acceso: Opciones de Autenticación biométrica.
	**Pantalla de desbloqueo** El usuario inicia o activa la aplicación, y en caso de que el usuario haya concedido los permisos para la autenticación biométrica, solicitará la opción de desbloqueo.

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

Miguel Martín
Viceministerio de Tecnología
Ministerio de Tecnología de la Información y Comunicación - MITIC

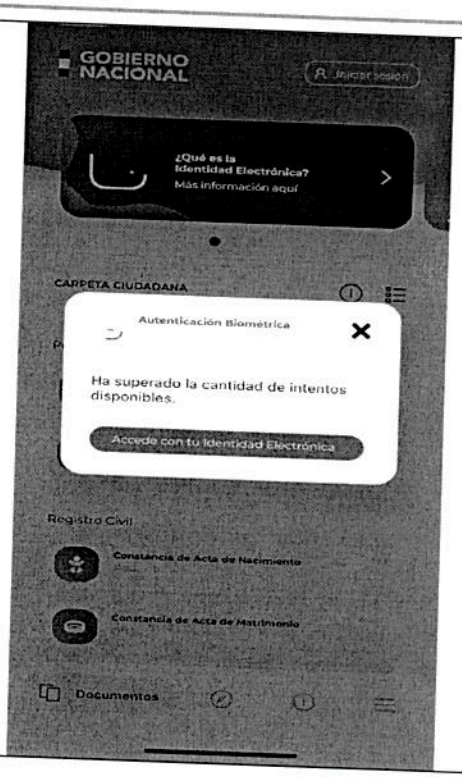
ARMANDO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

	Autenticación biométrica realizada con éxito Una vez solicitado el desbloqueo, y autenticado correctamente, accederá automáticamente a la sección de carpeta ciudadana con la posibilidad de gestionar los servicios disponibles.
	Pantalla de desbloqueo fallido. Se tendrá una cantidad X de reintentos por medio de la "Autenticación biométrica". Por cada intento fallido, mostrará un pop-up con la posibilidad de reintentar o cancelar.

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

ALEJANDRO DE FILIPPIS
GRUPO HORUS
GRUPO HORUS S.A.

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la Información y Comunicación - MITIC

	**Intento de desbloqueo superado** En caso de superar la cantidad máxima de intentos fallidos, aparecerá un pop-up para acceder por medio de su Identidad Electrónica.

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

Miguel Martín
Viceministro de Tecnologías
Ministerio de Tecnología de la
Información y Comunicación - MITIC

GRUPO HORUS S.A.