GOBIERNO DIGITAL

Autenticación Electrónica

GOBIERNO DE COLOMBIA

MINTIC

GOBIERNO DIGITAL

Definición

La Autenticación Electrónica es un servicio que permite validar la identidad de los usuarios por medios digitales.
Así, los ciudadanos en Colombia tendremos un único par de credenciales electrónicas para interactuar con todas las entidades públicas por medios digitales. Con estas credenciales podremos acceder a las plataformas del estado para realizar trámites y adicionalmente nos servirá para podrá firmar documentos electrónicamente e incluso interactuar con el sector privado.

Funcionalidades

- Provee nivel de garantía de Autenticación Electrónica adecuado para cada trámite y servicio.
- Provee el servicio de firmado electrónico de documentos o transacciones.
- Aceptar, actualizar y revocar las autorizaciones de autenticación y envío de atributos a las entidades públicas
- Consultar el estado y la vigencia de las credenciales de acceso, solicitar la renovación o la revocación de sus credenciales.
- Administrar la información personalizada que le permite al Ciudadano estar seguro de que está ingresando al sistema del operador.

BENEFICIOS

- Asegurar a los Ciudadanos el derecho de acceso a la administración pública por medios electrónicos en condiciones de calidad.
- Ofrecer un servicio a las entidades públicas y privadas que permita validar la identidad de los usuarios por medios digitales, mitigando los riesgos de suplantación de identidad, asegurando un nivel de seguridad apropiado para cada servicio o trámite a realizar por medios electrónicos.
- Garantizar la validez jurídica de las transacciones adelantadas por medios digitales, garantizando la autenticidad e integridad de las transacciones.
- Proveer los mecanismos necesarios para que los usuarios puedan firmar mensajes de datos y así garantizar la validez jurídica de sus actuaciones con el Estado.
- Mitigar los riesgos de seguridad a los que se ven expuestos los trámites y servicios en línea.

Relación entre actores

- Ciudadanos
- Empresas
- Organizaciones

Hace uso del servicio de Autenticación Electrónica cuando requira adelantar tramites y procedimientos administrativos por medios digitales

AGENCIA NACIONAL DIGITAL

Agencia NACIONAL DIGITAL

Coordina la prestación de los Servicios Ciudadanos Digitales

Dos factores de Autenticación Electrónica

Operador Autenticación Electrónica-i

Opera y ofrece el servicio de Autenticación Electrónica

Dos factores de Autenticación Electrónica

Operador Autenticación Electrónica-j

Opera y ofrece el servicio de Autenticación Electrónica

AFIS Registraduría Nacional del Estado Civil

Operador Autenticación Biométrica

Opera y ofrece el servicio de Autenticación Biométrica

Hace uso del servicio de Autenticación Electrónica cuando require firmar electrónicamente mensajes de datos

ENTIDAD

Hace uso del servicio de Autenticación Electrónica para validar que los usuarios que realizan transacciones realmente sean quienes afirman ser

Procesos en la Autenticación Electrónica

Ciudadano

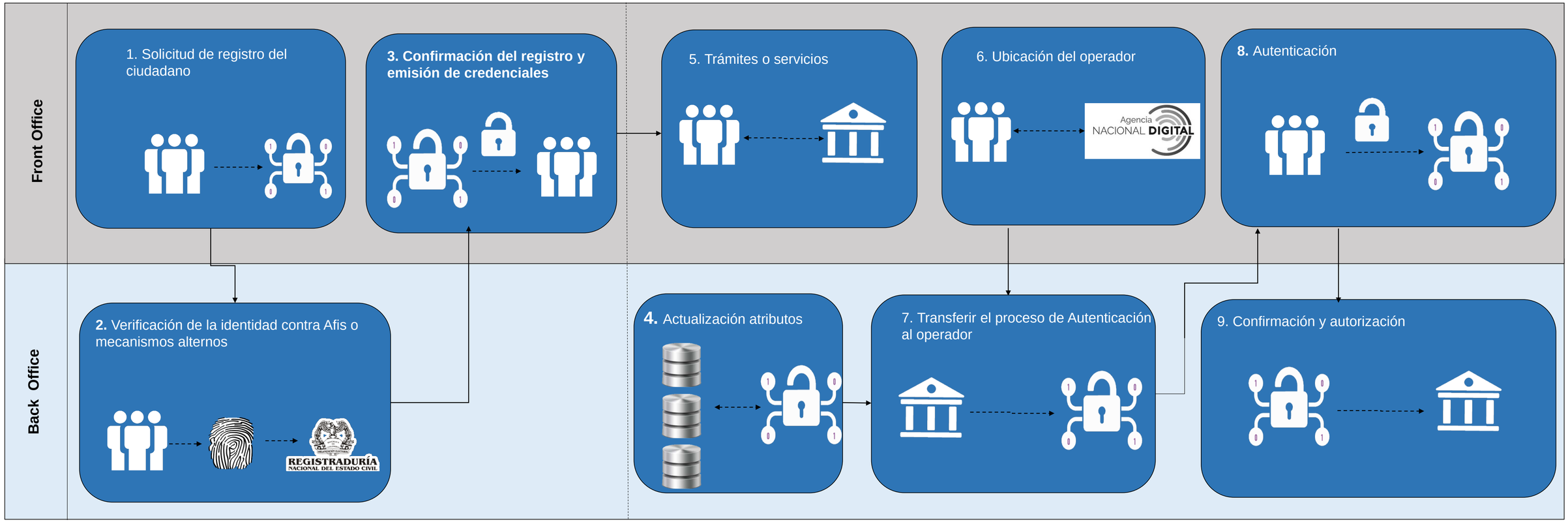
RNEC

Articulador

Operador de AE

Entidades Publicas

Credenciales de autenticación



REGISTRO

OPERACIÓN DEL TRÁMITE Y AE

Características actores

USUARIO

Beneficiarios de los Servicios Ciudadanos Digitales quienes podrán acceder a trámites y servicios con las entidades públicas haciendo uso de sus credenciales de Autenticación Electrónica.

ENTIDADES

Encargados de incorporar a sus sistemas de información los servicios de Autenticación Electrónica y Carpeta Ciudadana, e Interoperar con otras entidades y empresas (publicar y consumir servicios de información

AGENCIA NACIONAL DIGITAL

Persona jurídica definida por el Ministerio de TIC encargada de adelantar las interacciones con los distintos actores involucrados en la prestación de los servicios ciudadanos digitales para lograr una prestación coordinada y adecuada de tales servicios

OPERADORES

Personas jurídicas, públicas o privadas, que proveen los Servicios Ciudadanos Digitales de Autenticación Electrónica, Carpeta Ciudadana e Interoperabilidad como Servicio, y reciben una contraprestación económica de empresas y entidades públicas.

VIGILANCIA Y CONTROL

La vigilancia y control de las actividades involucradas en la prestación de los servicios ciudadanos digitales se realizará por cada uno de los organismos del Estado que en el marco de sus competencias tengan que conocer de una o varias de las actividades involucradas en la prestación de tales servicios. Min TIC, la Superintendencia de Industria y Comercio, la Registraduría Nacional del Estado Civil, el Archivo General de la Nación y el Ministerio Público.

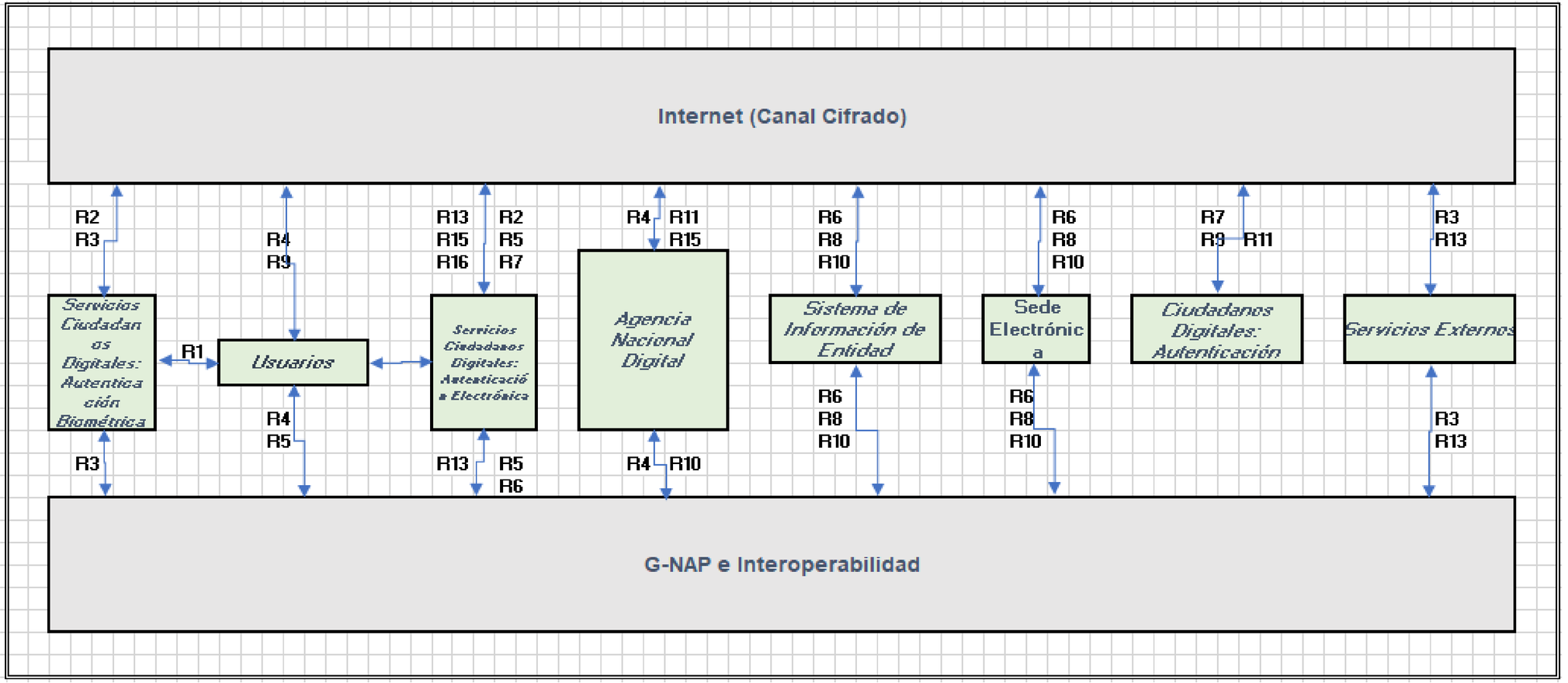
SERVICIOS EXTERNOS

Interacción entre los operadores de Autenticación Electrónica y los servicios que pueden proveen atributos del ciudadano, tales como el Registro Único Empresarial y Social (RUES), Sistema de Información y Gestión del Empleo Público (SIGEP), Archivo Nacional de Identificación (ANI) provisto por la RNEC entre otros
SIGEP
RUES
AFIS-RNEC
ANI-RNEC

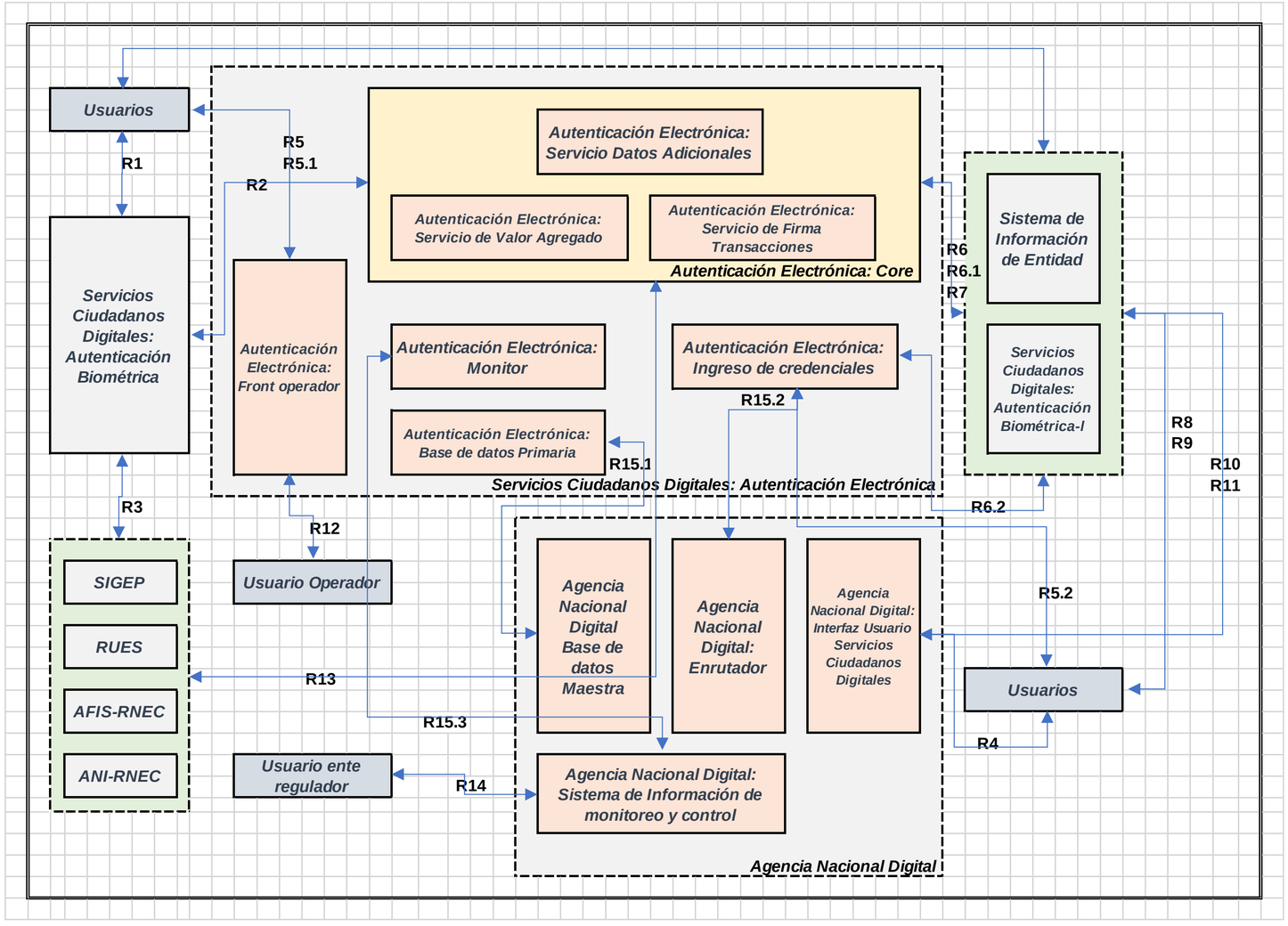
SEDE ELECTRÓNICA

La sede electrónica es una dirección electrónica que permite identificar la entidad y la información o servicios que provee en la web, a través de la cual se puede acceder de forma segura y realizar con todas las garantías legales, los procedimientos, servicios y trámites electrónicos que requieran autenticación de sus usuarios.

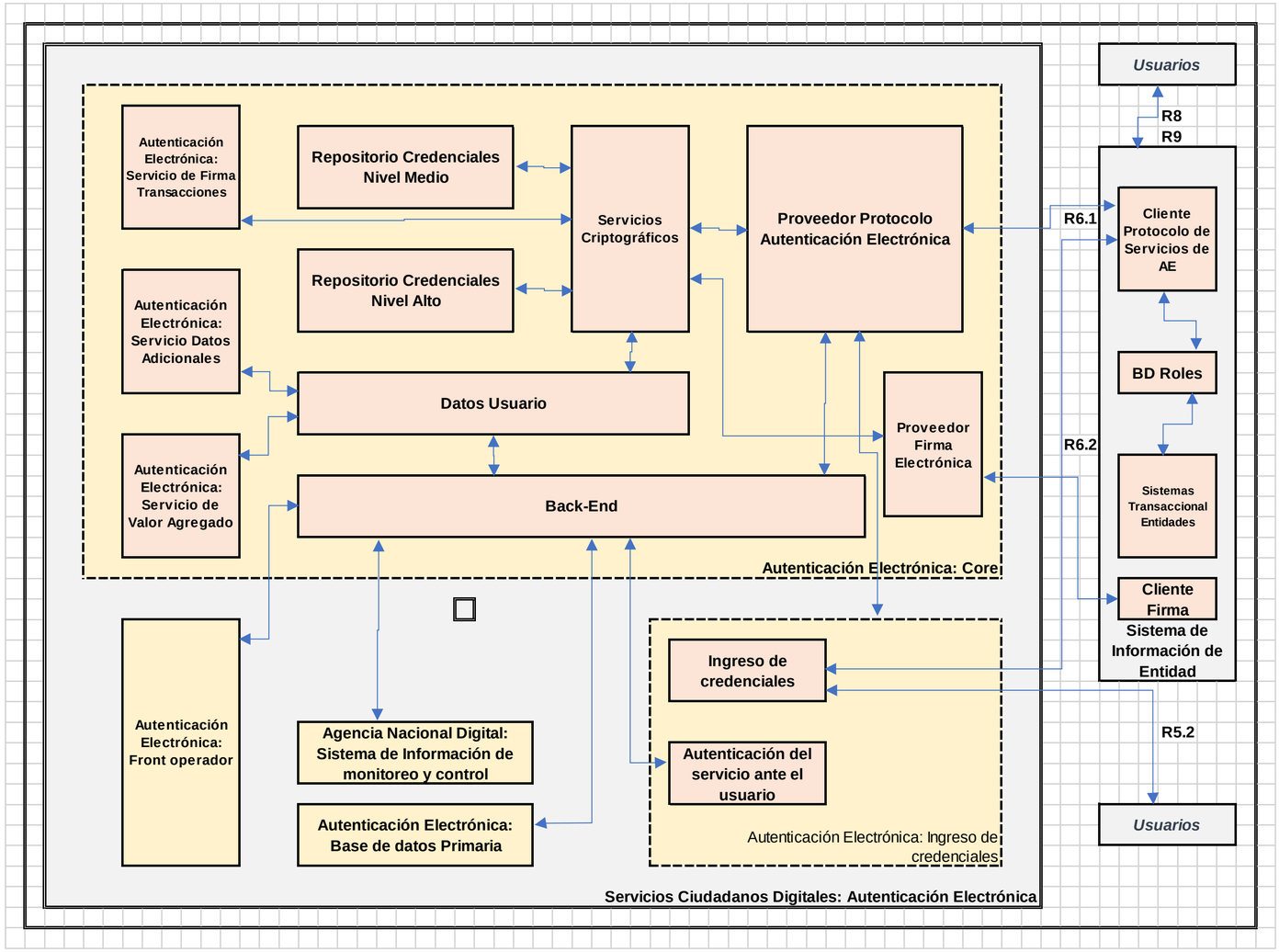
ARQUITECTURA DE COMPONENTES NIVEL 0



ARQUITECTURA DE COMPONENTES NIVEL 3



ARQUITECTURA DE COMPONENTES NIVEL 4



CREDENCIALES DE AUTENTICACIÓN ELECTRÓNICA

El Nivel de Garantía Medio ofrece confianza en la identidad declarada o aseverada por parte del operador de Autenticación Electrónica y es equivalente al nivel de Garantía 2 (NdG2) establecido en las recomendaciones de la ITU X.1254, ISO 29115. Se exigen mínimo un factor de autenticación y pueden emplearse los siguientes tipos de credenciales:
o Contraseña-Secreto memorizado
o Dispositivo de contraseña única de un solo factor (OTP)
o Dispositivo OTP Multi Factor
o Software Criptográfico de Un Solo Factor
o Dispositivo criptográfico de un solo factor
o Software Criptográfico Multi Factor
o Dispositivo criptográfico Multi Factor
o Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 de la ONAC.
El Nivel de Garantía Muy Alto tiene un nivel muy alto de confianza en la exactitud de la identidad presentada y se emplea para el acceso a datos muy restringidos y es equivalente al nivel de Garantía 4 (NdG4) establecido en las recomendaciones de la ITU X.1254, ISO 29115. Se exigen mínimo dos factores de autenticación y pueden emplearse los siguientes tipos de credenciales:
o Dispositivo criptográfico Multi Factor
o Dispositivo criptográfico de un solo factor utilizado junto con Contraseña-Secreto memorizado
o Dispositivo OTP multi-factor utilizado junto con un Dispositivo Criptográfico de Un Factor
o Dispositivo OTP multi-factor (sólo hardware) utilizado junto con un software criptográfico de factor único
o Dispositivo OTP de factor único (sólo hardware) utilizado junto con un Software Criptográfico Multi-Factor
o Dispositivo OTP de factor único (sólo hardware) utilizado junto con un software criptográfico de un solo factor y una Contraseña-Secreto memorizados.
o Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 V 01 de la ONAC utilizado junto con Contraseña-Secreto memorizado

MODELO NO FUNCIONAL

ATRIBUTOS	CARACTERISTICA	DESCRIPCION-META
FUNCIONAMIENTO	• Precio • Capacidad del Sistema • Rendimiento • Soporte • Aseguramiento de la información • Capacidad del sistema • Mantenimiento • Conformidad	• Gratuitos para los usuarios • Número Máximo de usuarios concurrentes 1000 • Tiempo máximo de respuesta <1 seg • Personal especializado y documentación técnica • Copias cifradas y protegidas • Garantizar ancho de banda suficiente proporcional al número de usuarios • Disponer de sistema de mantenimiento para nuevas versiones paquetes y servicios.
ESCALIBILIDAD	• Crecimiento del sistema • Rendimiento al escalar	• Deberá proveer los medios para adicionar capacidad de procesamiento y almacenamiento sin tener que migrar a un nuevo ambiente • Deberá mantener: el rendimiento especificado, tiempo máximo de búsqueda especificado, procesos de eliminación especificada.
MONITOREO	• Auditoria • Registro de errores • Alertas • Monitoreo del uso de recursos • Reportes comparados	• Esta capacidad de observación incluye la capacidad de mantener en el tiempo lo observado, almacenando los registros de toda la operación, con el fin de poder ejecutar procesos de auditoría, seguimiento, diagnóstico y mejora del sistema. Debe ser capaz de utilizar la información recolectada para generar indicadores de tipo estratégico, táctico y operativo, incluyendo diversos reportes y análisis estadístico. En particular debe mantener trazas de los errores, del uso inadecuado del sistema y de toda situación considerada anormal.
USABILIDAD	• Capacitación a usuarios • Interacción con usuarios • Uniformidad de la interacción • Ayuda en línea al usuario • Configuración en la interacción • Accesibilidad	• Interfaces limpias, consistencia, capacidad de respuesta, mensajes de error, procesamiento automático y otras formas de minimizar el número de decisiones que los usuarios deben tomar, personalización y localización, facilidades de ayuda, documentación de usuario, preguntas frecuentes, videos y tutoriales en línea, etc. • Programas de capacitación y formación
DISPONIBILIDAD	• Horarios de indisponibilidad • Traslado de responsabilidad • Monitoreo de la disponibilidad • Calculo de la Disponibilidad • Penalidad por indisponibilidad	• Qué sucede cuando una falla ocurre, • Que tan frecuentes pueden ser las fallas. • Cuánto tiempo puede estar el sistema fuera de operación debido a una falla. • Cómo pueden ser prevenidas las fallas, (e) cómo se deben informar las fallas y a quiénes. • Cómo se debe recuperar el sistema después de una falla. • A través de qué indicadores se deben medir los niveles de servicio. El nivel de disponibilidad que el sistema puede proporcionar debe estar claramente establecido por el operador. • La disponibilidad del sistema deberá estar constantemente monitoreada para observar si las metas del servicio están siendo alcanzadas o si han sido sobrepasadas
CONFIABILIDAD	• Integridad • Inmutabilidad de la Información • Recuperación ante fallas • Sustitución de medios del almacenamiento • Garantizar Preservación	• Confiabilidad requerido se seguirán las recomendaciones de la ITU e ISO dispuestas en sus documentos ITU X.1254 e ISO/IEC 29115:2013. • El sistema debe tener herramientas y mecanismos que permitan garantizar que la información no sea alterada. • Si el sistema se cae o no responde, se deben identificar las fallas y automáticamente iniciar la recuperación o redireccionar a sistemas de respaldo o sistemas alternos. • Debe permitir el seguimiento y la sustitución de medios de almacenamiento para protegerse contra la degradación de los medios de comunicación. • Los medios de almacenamiento del sistema deben ser utilizados y almacenados en ambientes que son compatibles con la vida útil deseada/ esperada, y que estén dentro de la tolerancia de la especificación del fabricante de medios de comunicación.

GOBIERNO DIGITAL

Servicios Ciudadanos Digitales

GOBIERNO DE COLOMBIA

MINTIC

GOBIERNO DIGITAL