Instructivo de Integración de Sistemas de Información al Single Sign On

Proceso:

Gestión de Servicios de Información y Soporte Tecnológico

Versión 1

11/06/2024

TABLA DE CONTENIDO

1. OBJETIVO

Definir los lineamientos para la integración de nuevos sistemas de información al single sign on del Ministerio de Ambiente y Desarrollo Sostenible con el fin de unificar el método de autenticación y centralizar los usuarios internos y externos de la entidad.

2. POLÍTICAS DE OPERACIÓN

- Para realizar las integraciones requeridas se debe dar cumplimiento a la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y a la política de tratamiento y protección de datos personales del Ministerio.
- Toda solicitud para integración de sistemas de información o aplicaciones al SSO del Ministerio debe ser emitida por el Líder técnico o Líder funcional de dicha solución tecnológica a través de GEMA.

3. TÉRMINOS Y/O CONCEPTOS

Autenticación: Es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador.

Endpoint: es una dirección de una API, o bien un backend que se encarga de dar respuesta a una petición.

GEMA (Gestión y mesa de asistencia): Es el sistema de gestión de solicitudes de servicios hacia la Oficina de Tecnologías de la Información y la Comunicación del Ministerio, fue implementado haciendo uso del software Aranda.

Inicio de sesión unificado (single sign-on, SSO): Es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación; permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos.

4. REQUISITOS PARA LA SOLICITUD DE INTEGRACIÓN AL SSO.

A continuación, se describen los pasos para realizar la solicitud de integración al single signo on de un sistema de información o aplicación del Ministerio u Autoridad ambiental:

Paso 1: Crear caso en GEMA a través de los siguientes pasos:

a. Autenticarse en GEMA

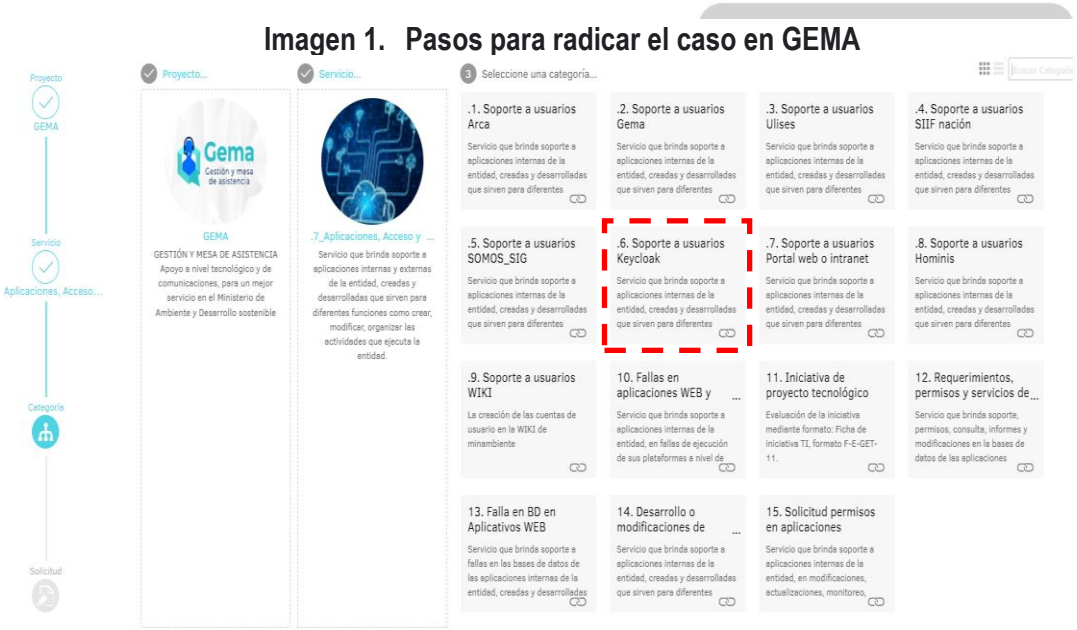
b. Hacer clic en la opción “Registrar caso”

c. Seleccionar el proyecto “GEMA”

d. Seleccionar el servicio “Aplicaciones, accesos y desarrollo web”

e. Seleccionar la categoría “Soporte a usuarios Keycloak”

Imagen 1. Pasos para radicar el caso en GEMA



Fuente: GEMA, agosto de 2023

Paso 2: Diligenciar caso en GEMA: a continuación, se describen las variables que deben ser registradas en el caso en GEMA:

- **Client ID (ID del Cliente):** Es el identificador único de la aplicación, y en general deberá corresponder con el repositorio en Gitlab donde se encuentra versionado el código fuente. Se debe digitar sin espacios y en minúscula.

  Ejemplo: cardinal-admin

- **Name (Nombre):** Corresponde al nombre completo legible del API o sistema de información; puede ser el mismo Client ID con espacios.

  Ejemplo: Cardinal Administrador

- **Description (Descripción):** Realizar una breve descripción del sistema información a integrar y sus funcionalidades.

  Ejemplo: Este sistema de información permitirá la gestión y administración de los planes de acción de las Corporaciones Autónomas Regionales, así como el seguimiento a su ejecución financiera y operativa.

- **Acces Type (Tipo de cliente)**: Definir el tipo de acceso al API o sistema de información, si es público o confidencial.

  Si estamos hablando de un componente de interfaz de usuario o de elementos presentes en los servidores en función de la interfaz de usuario, como proyectos de Angular o componentes web que operan en el lado del cliente, debemos categorizarlos como **públicos**. Sin embargo, en el caso de aplicaciones como gestores de información en Django, PHP o APIs que proveen servicios y se ejecutan en los servidores de la entidad, es necesario categorizarlos como **confidenciales**.

  Ejemplo: Confidencial

- **URL:** Definir la URL donde se expondrá el servicio en los diferentes ambientes. En ambiente de desarrollo (dev) se permitirá el uso de URLs locales y de desarrollo.

  Ejemplo:
  Ambiente de desarrollo: https://dev-cardinal-admin.minambiente.gov.co/
  Ambiente de pruebas: https://qa-cardinal-admin.minambiente.gov.co/
  Ambiente de producción: https://cardinal-admin.minambiente.gov.co/

- **Valid Redirect URIs (URI de redirección válida)**: Establecer cuáles son las URI que permitirán la redirección; es decir, las URL que usaran el servicio de autenticación.

  Ejemplo:
  Ambiente de desarrollo: https://dev-cardinal-admin.minambiente.gov.co/*
  Ambiente de pruebas: https://qa-cardinal-admin.minambiente.gov.co/*

Ambiente de producción: https://cardinal-admin.minambiente.gov.co/*

- **Web Origins (Ruta de origen):** Se debe establecer cuáles son las rutas de origen que se aceptaran en el servicio de autenticación en cada uno de los ambientes.

  Ejemplo:
  Ambiente de desarrollo: https://dev-cardinal-admin.minambiente.gov.co/+
  Ambiente de pruebas: https://qa-cardinal-admin.minambiente.gov.co/+
  Ambiente de producción: https://cardinal-admin.minambiente.gov.co/+

- **Roles:** Se deberán listar los roles que usa la aplicación o sistema de información con su nombre o identificador técnico y una descripción.

  Ejemplo:

ROL	DESCRIPCIÓN
711_SOL_ASIG_ACT	Responsable de seleccionar y asignar actividades en el trámite Sustracción de áreas de reserva forestal del orden nacional en la etapa de solicitud
711_SOL_VER_INFO	Responsable de verificar la información de la solicitud en el trámite Sustracción de áreas de reserva forestal del orden nacional en la etapa de solicitud
711_SOL_SOL_INFO	Responsable de generar oficio solicitando soporte a la solicitud en el trámite Sustracción de áreas de reserva forestal del orden nacional en la etapa de solicitud
711_SOL_EVA_JURID	Responsable de realizar la evaluación jurídica del recurso de reposición en el trámite Sustracción de áreas de reserva forestal del orden nacional en la etapa de solicitud

5. DATOS DE RESPUESTA PARA LA INTEGRACIÓN CON EL SSO

Una vez creado el cliente en el single sign on, el usuario solicitante recibirá una respuesta en GEMA y a través de correo electrónico con la siguiente información:

- **El protocolo de openid conect por ambiente:** Corresponde a la dirección URL del cliente en Keycloak.

  Ejemplo:
  Ambiente de desarrollo: https://dev-login.minambiente.gov.co/realms/ambiente/.well-known/openid-configuration
  Ambiente de pruebas: https://qa-login.minambiente.gov.co/realms/ambiente/.well-known/openid-configuration

Ambiente de producción: https:// login.minambiente.gov.co/realms/ambiente/.well-known/openid-configuration

- **Endpoints:** Corresponde a la URL que dará respuesta a la petición.

  Ejemplo:
  Ambiente de desarrollo: https://dev-login.minambiente.gov.co/realms/ambiente/.well-known/openid-configuration
  Ambiente de pruebas: https://qa-login.minambiente.gov.co/realms/ambiente/.well-known/openid-configuration
  Ambiente de producción: https://login.minambiente.gov.co/realms/ambiente/.well-known/openid-configuration

- **REALM:** Corresponde al reinado donde estará alojado el cliente; el cual debe ser siempre "ambiente".

- **Client-id:** ID referenciado en las URLs y tokens

  Ejemplo: cardinal-admin

- **Client secret:** Corresponde al cliente secreto, aplica únicamente para solicitudes de tipo de acceso Confidencial

  Ejemplo: Client id and secret

- **Secret password:** Contraseña del cliente en el servidor

  Ejemplo: 8MMCeaCgWb1M9INT03INJOhtgceVqYHq