Consejo Asesor Técnico del Sistema Estadístico Nacional (CASEN) 2023 - 2025
ACTA SEGUNDA SESIÓN ORDINARIA - AYUDA DE MEMORIA

Ciudad: Bogotá D.C
Lugar: Sesión virtual
Tema: Socialización procedimiento de ingreso seguro por Single Sing On (SSO)

Hora: 02:00 p. m. a 4:00 p. m.
Fecha: 08/07/2025
Dependencia responsable: OSIS -DIRPEN

Participantes

Miembros de la Sala Especializada para la Modernización Tecnológica de la Producción Estadística del CASEN

Mario Linares Vásquez, experto asesor
Nicolás Cardozo Álvarez, experto asesor
León Darío Parra, experto asesor

Departamento Administrativo Nacional de Estadística (DANE)

Luis Martín Barrera pino, jefe oficina de sistemas - OSIS
Diego Antonio Campos Cáceres, Asesor OSIS
Carmen Aldana, designada OSIS
Juan Manuel Rivera, designado OSIS
José Jhefferson Mora, designado OSIS
Monica Patricia Pinzon Suarez, designada OSIS
Jose Humberto Rincon Pineda, designado OSIS
Andrea Catherine Neira Bustamante, designada OSIS

Julieth Alejandra Solano Villa, directora técnica Dirección de Regulación, Estandarización y Normalización - DIRPEN y secretaria técnica CASEN

Ruth Constanza Triana Acuña, coordinadora (E) GIT planificación y articulación estadística
Mauricio Valencia, contratista GIT planificación y articulación estadística
Carlos Eduardo Castro Zarate, responsable (E) Sala Especializada para la Modernización Tecnológica de la Producción Estadística

Orden del día

Tiempo	Actividad	Responsable
2:00 p.m. a 2:05 p. m	Instalación, verificación del quorum y registro fotográfico.	Carlos Castro, responsable (E) de la sala.
2:05 p. m. a 2:10 p. m.	Apertura de la reunión	Julieth Solano Villa directora técnica DIRPEN y secretaria técnica del CASEN
2:10 p. m. a 2:15 p. m.	Síntesis reunión anterior	Carlos Castro, responsable (E) de la sala.
2:15 p. m. a 3:00 p. m.	Presentación procedimiento de ingreso seguro por Single Sign On (SSO)	Carmen Aldana, Juan Manuel Rivera y José Mora Modera: Carlos Castro
3:00 p. m. a 3:50 p. m.	Realimentación por parte de los miembros de la sala	Miembros de la Sala Modera: Carlos Castro
3:50 p. m a 3:55 p. m.	Compromisos	Carlos Castro, responsable (E) de la sala
3:55 p. m a 4:00 p. m.	Conclusiones y cierre	Julieth Solano Villa directora técnica DIRPEN y secretaria técnica del CASEN

Desarrollo

Objetivo

Presentar y socializar el procedimiento de ingreso seguro a los sistemas de información mediante el esquema Single Sign-On (SSO) para fortalecer los procesos de seguridad de la información dentro del DANE. Se buscó también recoger observaciones y recomendaciones para robustecer este protocolo.

1. Apertura

La directora técnica de DIRPEN y secretaria técnica del CASEN Julieth Solano realizó la apertura de la reunión, destacando el propósito principal de este espacio el cual fue

presentar la iniciativa de SSO como parte del fortalecimiento de la seguridad en los sistemas de información y recibir retroalimentación del equipo.

2. Síntesis de la reunión anterior

Carlos Eduardo Castro del GIT de planificación y articulación estadística, desarrollo la síntesis, destacando que en el espacio previo se presentó las mejoras a la guía de interoperabilidad y realimentación por los expertos. Además de incluir la estructuración del evento para la difusión de la guía. Se destacó el cumplimiento de los compromisos pactados para esa sesión.

3. Presentación Técnica del Procedimiento de ingreso seguro Single Sing On – SSO

Presentación Técnica del Procedimiento SSO

Carmen Aldana explicó la agenda de presentación y el alcance del procedimiento, el cual aplica especialmente para nuevos desarrollos en la Oficina de Sistemas, para grupos específicos como Apoyo Informático a Operaciones Censales y Sistemas de Información.

Se describió la arquitectura técnica basada en microservicios, el uso de la herramienta Keycloak para sincronización con directorio activo y gestión de roles y permisos.

Se expusieron definiciones técnicas alineadas con la norma ISO 27000, enfatizando conceptos como confidencialidad, disponibilidad, integridad, desarrollador y administrador de encuestas.

Juan Manuel Rivera detalló el flujo operativo técnico del SSO, desde la pantalla de login personalizada, pasando por la validación con directorio activo o base de datos local, emisión de tokens JWT, inyección para consumo de servicios REST, hasta la gestión de auditorías.

4. Procedimiento Documentado

Carmen presentó el procedimiento documentado con un total de 11 actividades que incluye desde la validación de solicitudes en la mesa de servicios, desarrollo de componentes, creación y configuración de roles en el SSO, pruebas de integración, administración y validación en ambientes internos y de usuario final, hasta monitoreo y verificación del estado de la integración.

Se hizo énfasis en que el control de accesos se basa en el principio de mínimo privilegio y que la gestión de usuarios finales (como, por ejemplo, los de encuestas) es autónoma, no cubierta por este procedimiento.

Se incluyeron controles de auditoría automáticos y actividades a demanda para registro de sesiones, intentos fallidos y detección de accesos por IP.

5. Realimentación por miembros de la sala

Se discutieron varias inquietudes relevantes asociadas a las siguientes temáticas por parte de los expertos de la sala:

La práctica real del proceso de login y la utilización de autenticación multifactor.

La cobertura del procedimiento: si aplica solamente para sistemas de encuestas o para todos los nuevos sistemas de información desarrollados.

Claridad en la denominación de "administrador de encuestas" y si debería ser más general como "administrador del sistema".

Posible cambio en el nombre del procedimiento para reflejar que es la habilitación de ingreso seguro mediante SSO, más que el ingreso seguro per se.

Procedimientos para actualizaciones de la herramienta Keycloak en caso de detección de vulnerabilidades o parches.

Ambigüedad sobre registros automáticos vs. a demanda en controles de auditoría y la necesidad de reforzar gobernanza para que ciertos registros sean obligatorios.

Solicitud de mayor claridad en documentos, como el qué debe actualizarse en la mesa de servicios en las pruebas de integración.

El equipo de la oficina de sistemas resolvió las inquietudes generadas por cada experto y se destaca:

La implementación se centra en nuevos desarrollos dentro de los grupos de trabajo específicos y no para sistemas legados, aunque estos últimos podrían integrarse gradualmente.

El procedimiento está enfocado en la habilitación e implementación técnica del ingreso seguro y requiere la gobernanza y políticas claras desde la OTIC para estandarizar los procesos.

Se señaló que la arquitectura es modular y flexible para atender necesidades específicas del negocio, lo que justifica algunas diferencias en aplicación.

Se reconoció que la autenticación multifactor y controles más amplios de seguridad (hardening a nivel de hardware, redes, etc.) forman parte de otro nivel de controles gestionados por otras áreas.

La necesidad de mejorar la redacción y aclarar ciertos puntos documentales para evitar malentendidos fue reconocida.

A Continuación, se detalla las preguntas y respuestas desarrolladas en la sesión entre los expertos asesores y el equipo de la OSIS la cual fue moderada por Carlos Castro:

Pregunta de Nicolás Cardozo sobre el proceso de login y la integración con métodos de autenticación adicional (como autenticación multifactor):

Nicolás preguntó cómo se lleva a cabo el proceso de login en la práctica, si es solo usuario y contraseña, y si la arquitectura contempla la integración con métodos adicionales como autenticación multifactor.

Respuesta de José: explicó que el proceso depende del negocio, utilizando principalmente correo electrónico y contraseña institucional o autenticación mediante directorio activo. Además, manejan estándares para recolección de datos fuera del directorio activo con usuarios propios. Indicó que usan protocolos como OAuth y OpenID Connect que permiten integrar diversos frontends, incluso móviles.

Pregunta de Nicolás sobre la combinación de permisos y accesos para evitar excesos:

Nicolás consultó si se ha revisado cómo evitar que un usuario tenga acceso a recursos que no debería, por la combinación de roles y permisos.

Respuesta de José: explicó que los privilegios se conceden bajo el principio del mínimo privilegio, usando "reinos" particulares para asegurar que los roles y permisos sean otorgados solo según la necesidad y procesos definidos. Además, aclaró que en caso de comportamiento compartido de usuarios, también se controla el acceso según roles y permisos establecidos.

Intervención de Carmen: añadió que la administración de usuarios y roles depende de matrices definidas por el negocio según requerimientos y que estas son configuradas en el SSO.

Consulta e intervención del profesor Mario sobre la aplicabilidad del procedimiento (si es solo para encuestas o para cualquier sistema):

Mario preguntó si el procedimiento aplica solo para sistemas de recolección de datos o para cualquier nuevo sistema de información desarrollado en la Oficina de Sistemas.

Respuesta inicial de Carmen: que aplica para nuevos sistemas desarrollados por dos grupos específicos (SIPA y AIOC), que manejan sistemas de producción estadística y apoyo informático a operaciones censales.

José aclaró: que el procedimiento está pensado para nuevos sistemas desde una fecha específica, pero con posibilidad de que sistemas heredados también se vinculen progresivamente. Aclaró que, aunque inicialmente está asociado a encuestas, está abierto para cualquier sistema que requiera acceso seguro.

Mario puntualizó: que sería conveniente aclarar en el objetivo que aplica solo para nuevos sistemas y que en el procedimiento aparece el término "administrador de la encuesta", lo que puede generar confusión, sugiriendo cambiarlo por "administrador del sistema" o similar.

Carmen explicó: que el término "administrador de encuesta" se usa porque muchos sistemas son de encuestas, pero es válido ampliar o aclarar el término para otros sistemas.

Carlos coincidió: y sugirió ajustar el documento para evitar confusiones.

Inquietud del profesor León sobre el alcance global del procedimiento y su relación con otros controles de seguridad:

León señaló que el procedimiento aborda solo acceso a usuarios mediante SSO, pero el ingreso seguro incluye también otros aspectos del hardening a nivel de hardware, red, sistema operativo, certificados SSL/TLS, y autenticación multifactor. Preguntó cómo se integran esas otras piezas.

Respuesta de Jose y Andrea: señalaron que este procedimiento está enfocado en la capa de software y autenticación centralizada, mientras que el resto de controles de infraestructura los gestiona otra área (plataforma). Aclararon que el procedimiento fortalece específicamente la gestión y acceso seguro a sistemas de información, pero que existen otros procedimientos para controles más amplios.

Andrea añadió: que es una capa más en la defensa en profundidad, fortaleciendo la superficie de ataque mediante un control unificado y monitoreo centralizado.

Comentarios y sugerencias del profesor Mario sobre el nombre y objetivo del procedimiento:

Mario opinó que el nombre y el objetivo actual pueden inducir a error, ya que el procedimiento no explica cómo el usuario ingresa de forma segura, sino cómo se implementa la autenticación basada en SSO para sistemas nuevos. Sugirió que el nombre sea más específico: "Procedimiento para habilitar/implementar ingreso seguro mediante

Single Sign On". Asimismo, propuso aclarar que contribuye a los controles preventivos, pero no los abarca todos.

Carmen y Diego coincidieron: en la necesidad de aclarar y ajustar semánticamente para evitar malinterpretaciones en auditorías. Diego añadió que se debe hacer un análisis para mejorar la estructura y claridad del procedimiento.

Consulta de Mario sobre actualizaciones del Keycloak (SSO) en caso de vulnerabilidades o nuevas versiones:

Mario preguntó si el procedimiento contempla qué hacer cuando hay actualizaciones del Keycloak, vulnerabilidades CVE, o ajustes necesarios.

Respuesta de Mónica de la Oficina de Sistemas: indicó que en esta primera fase no está contemplado, pero reconoció que es una buena oportunidad para incluirlo en futuras versiones.

Discusión sobre los controles de auditoría automáticos y la nota de que su activación es "a demanda o por solicitud":

Mario expresó preocupación porque la redacción actual puede interpretarse como que nadie está obligado a activar los registros automáticos de inicio/cierre de sesión, intentos fallidos, acceso por IP, etc., y sugirió que estos controles deberían ser obligatorios para todos los sistemas autenticados salvo excepciones justificadas.

José: explico que depende de la arquitectura y del negocio, y que algunas excepciones se contemplan, pero coincidieron en que debe incluirse una nota aclaratoria para evidenciar que esos registros son la norma salvo casos puntuales.

Mario sugirió: modificar la nota para que diga que esos controles se activan automáticamente según habilite el negocio o arquitectura, no solo a demanda.

Detalle sobre la actualización del caso en la mesa de servicios:

La inquietud estuvo dirigida a la actividad No. 4, específicamente en el punto de control: "Actualización del caso en la mesa de servicios reportando el resultado de la integración" del procedimiento. Se solicitó aclarar cuál es la evidencia o el resultado que se registra en la mesa de servicios.

La ingeniera Carmen indicó que el resultado a registrar en la mesa de servicios corresponde a la validación del servicio probado, el cual se documenta en el formato de pruebas del programador.

6. Cierre

Ruth Constanza coordinadora (E) del GIT de planificación y articulación estadística cerro indicando los avances en la presentación desarrollada por la OSIS al procedimiento para el ingreso seguro de los sistemas de información mediante Single Sign-On (SSO). Destaca que se recibieron las observaciones de los expertos en los diferentes componentes del procedimiento que serán revisados y evaluados para su implementación acorde con las políticas de la entidad.

Compromisos

Tarea	Envío de acta de la para revisión y aprobación
Responsable	Carlos Castro, responsable de la sala (E)
Fecha entrega	14/07/2025
Tarea	Enviar insumo de la siguiente reunión
Responsable	Derly Lizarazo, responsable de la sala.
Fecha entrega	5 días antes de la siguiente reunión

Próxima reunión:

Responsable de convocar: DIRPEN

Fecha: Ciclos cada dos semanas de acuerdo con el avance de implementación de las recomendaciones – estimado 29-07-2025