RESOLUCION C.S. Nº 004-23

SAN SALVADOR DE JUJUY, 12 de abril de 2023

VISTO el Expediente C- 128/2023, mediante el cual Rectorado de esta Universidad solicita autorización para la Implementación del "SISTEMA ÚNICO DOCUMENTAL (SUDOCU), EN EL ÁMBITO DE LA UNIVERSIDAD NACIONAL DE JUJUY"; y

CONSIDERANDO:

Que por RESOLUCIÓN C.S. N° 239/18 de fecha 29 de agosto de 2018 el Consejo Superior de esta Universidad resolvió en su *Artículo 1°: Autorizar la utilización de Expedientes Electrónicos, Documentos Electrónicos, Firmas Electrónicas y Digitales, Archivos Electrónicos y Digitales en todos los Procesos y Procedimientos en el ámbito de la Universidad Nacional de Jujuy*, así como la *notificación por medios electrónicos*, estableciendo la obligatoriedad de constituir domicilio electrónico en toda tramitación que se origine en el ámbito de la Universidad. Artículo 2º: Establecer que la utilización de cualquiera de aquellos medios tendrá idéntica eficacia jurídica y valor probatorio que sus equivalentes en soporte papel o físico. Artículo 3°: Disponer que por Rectorado se deberán iniciar las gestiones tendientes a la designación de la Universidad Nacional de Jujuy como Autoridad de Registro de la Autoridad Certificante de la Oficina Nacional de Tecnologías de la Información, conforme lo expresado más arriba.

Que por RESOLUCION C.S. N° 058/21 de fecha 17 de marzo de 2021 el Consejo Superior de esta Universidad resolvió en su Artículo 1°*: Aprobar las PAUTAS REGLAMENTARIAS referidas al uso de recursos telemáticos para la realización de las Sesiones Ordinarias y Extraordinarias del Consejo Superior de la Universidad Nacional de Jujuy.*

Que la Universidad Nacional de Jujuy (UNJu) ha incrementado notablemente en los últimos años el volumen de gestiones administrativas, como consecuencia del despliegue de sus funciones principales y el crecimiento de sus equipos y unidades de gestión (debido a la incorporación de nuevas carreras en la UNJu en sedes y sus extensiones áulicas).

Que la UNJu incorporó a lo largo de su historia diferentes módulos y sistema de gestión que han permitido la generación digital de documentación específica de manera más ágil y ordenada, cuyo resguardo final se realiza en archivos y expedientes físicos en soporte físicos (papel).

Que resulta necesaria la implementación de una plataforma informática centralizada que permita la generación de documentos, expedientes electrónicos, contenedores digitales y firma electrónica y digital, facilitando la gestión documental, el acceso a la información y se reduzca los plazos en las tramitaciones y permita su seguimiento en línea.

Que la ley Nº 25.506 reconoce el empleo del documento electrónico, de la firma electrónica y la firma digital y su eficacia jurídica en las condiciones que establece la mencionada ley, promoviendo a su vez su uso masivo a fin de propender a la progresiva despapelización.

Que en el Plenario de Rectores/as del mes de septiembre de 2018 se le encomendó al SIU construir una solución de gestión documental electrónica para el sistema universitario, partiendo de alguna de las soluciones ya existentes en las universidades.

//

Que para avanzar en la tarea encomendada, el SIU conformó un Comité Técnico de Evaluación que debía definir la herramienta que serviría de punto de partida para desarrollar el nuevo Sistema, y un Comité Funcional para definir el alcance y los requisitos funcionales y no funcionales que deberá cubrir el Sistema de Expedientes Digital para el Sistema Universitario.

Que en octubre de 2018 el Comité Técnico de Evaluación, conformado por SEIS (6) Universidades de distintas características Universidad Nacional del Centro de la Provincia de

Buenos Aires (UNICEN), Universidad Nacional de La Plata (UNLP), Universidad Nacional de Quilmes (UNQ), Universidad Nacional del Sur (UNS), Universidad Nacional Santiago del Estero (UNSE), Universidad Nacional Villa María (UNVM), inició el análisis de los proyectos disponibles presentados por las diferentes Instituciones, a fin de concluir, desde el punto de vista de la tecnología, cuál de ellos se tomaría como punto de partida.

Que de SEIS (6) Instituciones que habían presentado sus desarrollos, TRES (3) ofrecieron su producto en las condiciones establecidas como requisitos y se consideraron como soluciones adaptables al uso en otras Instituciones del Sistema Universitario: Universidad Nacional de General Sarmiento (UNGS) con el sistema SUDOCU, Universidad Nacional del Litoral (UNL) con el sistema SGTDU y Universidad Nacional de Rosario (UNR) con el sistema WEMES.

Que el Comité Técnico de Evaluación sugirió la adopción del proyecto SUDOCU de la UNGS, como punto de partida para la nueva solución de la gestión documental electrónica del Sistema Universitario, considerando su arquitectura adaptable y escalable a las distintas necesidades institucionales, como así también su capacidad de asegurar la interoperabilidad con los módulos SIU y otros sistemas internos o externos de las universidades.

Que desde noviembre 2018 se encuentra activo el Comité de Desarrollo del SIU, integrado por distintas Universidades incluida la UNGS, cuyo objetivo es relevar las características principales del proyecto y delinear requerimientos funcionales básicos con los que debía contar la primera versión del sistema SUDOCU.

Que a su vez la Coordinación de SIU y la Dirección General de Informática de la UNJu han realizado avances significativos en la implementación de la versión actualizada: 1.1.9. del Sistema SUDOCU.

Que desde octubre de 2021 la Coordinación de SIU, la Dirección General de Informática, la Secretaría de Asuntos Académicos, la Secretaría de Administración, la Secretaría de Legal y Técnica y la Unidad de Auditoría Interna de la UNJu se encuentran trabajando en conjunto en la planificación de la implementación del sistema SUDOCU en la UNJu.

Que se considera concluida la etapa de desarrollo inicial y testeo del sistema SUDOCU, en el cual se han realizado diferentes pruebas informáticas y de usabilidad, se ha minimizado la posibilidad de aparición de errores críticos y se han planteado diferentes instancias de capacitación inicial para los equipos de gestión de todas las Unidades Académicas, Sedes, Extensiones Áulicas, Institutos de Investigación de la UNJu y Rectorado.

Que a fs. 11/12 de autos la Secretaría Legal y Técnica informa que:"… *habiendo tomado la debida intervención los Organismos Técnicos competentes de nuestra Universidad en materia de implementación de Sistemas de Información y Gestión Digital de Documentos y Expedientes, no existiría obstáculo legal alguno para continuar con los*

trámites de rigor para su aprobación y advirtiendo de que se trataría de una disposición general que se aplicará eventualmente en todas las Unidades Académicas, Escuela Superiores y demás órganos de la Universidad, entiendo que la propuesta debe ser remitida para tratamiento y aprobación del Consejo Superior, conforme lo prevé el Art.16 inc 26) y 35) del Estatuto Universitario …" DICTAMEN S.L.y T. N° 26/2.023 de fecha 23.02.2023.

Que a fs. 13/22 de autos la Comisión de Interpretación y Reglamento del Consejo Superior aconseja: Aprobar el proyecto de Resolución que se adjunta. DICTAMEN C. I. y R. Nº 005/2023.

Que en la Sesión Ordinaria realizada en el día de la fecha, este Cuerpo Colegiado trata y aprueba el dictamen antes mencionado en general y particular por unanimidad de los miembros presentes.

Por ello y en ejercicio de las atribuciones conferidas que le son propias,

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD NACIONAL DE JUJUY
RESUELVE

ARTICULO 1°: Apruébase la **IMPLEMENTACIÓN DEL SISTEMA ÚNICO DOCUMENTAL (SUDOCU)** como plataforma centralizada de Gestión Digital de Documentos y Expedientes para la Universidad Nacional de Jujuy (UNJu.), cuyas especificaciones técnicas forman parte integrante como **ANEXO I** de la presente Resolución.

ARTICULO 2°: La Dirección General de Informática de Rectorado de la UNJu. y la Coordinación del SIU de esta Universidad, tendrán a su cargo la administración del **SISTEMA ÚNICO DOCUMENTAL (SUDOCU)**, cuyas competencias se detallan en el **ANEXO II** de la presente Resolución.

ARTICULO 3°: Recomiéndase a las Autoridades de cada Unidad Académica, Escuela de Minas Dr. Horacio CARRILLO, Escuelas Superiores e Institutos de Investigación de la UNJu., designe UN (1) Responsable para coordinar toma de decisiones en la implementación de SUDOCU.

ARTICULO 4°: Regístrese. Publíquese. Comuníquese a todas las Dependencias de la UNJu.,por medio electrónico. Cumplido, ARCHÍVESE.

Tcb

ANEXO I

Informe sobre Arquitectura y Seguridad del sistema SUDOCU.

El sistema SUDOCU (Sistema Único Documental) es un sistema de gestión integral de documentación y trámites orientado a la administración pública. El mismo esta implementado y mantenido ininterrumpidamente desde el año 2021 por la Coordinación de SIU y la Dirección General de Informática de la Universidad Nacional de Jujuy.

Excede a este informe presentar un análisis detallado de la funcionalidad del sistema ya que esa información está disponible y se mantiene actualizada en el sitio oficial de SUDOCU (https://sudocu.dev). En el presente informe se describirán los elementos de infraestructura y las condiciones de seguridad en el despliegue llevado adelante en el entorno de producción de la Universidad Nacional de Jujuy, ya que dadas las características que el sistema hereda de las tecnologías con las que es construido, y dada también su arquitectura de sistema distribuido orientado a microservicios permite múltiples estrategias de despliegue.

Arquitectura

SUDOCU es una solución distribuida que se despliega desde contenedores de docker, los cuales pueden ser administrados a través de alguna solución de orquestación, como Docker Swarm o Kubernetes. El sistema contiene múltiples servicios que conforman el stack SUDOCU y que son servidos en un cluster Docker Swarm. Dichos servicios son:

- API-Server: Backend de administración orientado a microservicios
- SUDOCU-Gestion: Frontend de gestión de documentos y trámites
- SUDOCU-MPD: Frontend de publicación y digesto
- SUDOCU-MPC: Frontend de configuración
- SUDOCU-Inicio: Frontend de acceso al sistema
- Redis: Base de datos NOSQL para el manejo de sesiones y cache.
- Browserless: Servicio de generación de PDF

Además se incluyen dentro del mismo cluster, algunas aplicaciones de administración y monitoreo cuyo acceso está restringido solo dentro de la red interna de la UNJu.
Dichas aplicaciones son:

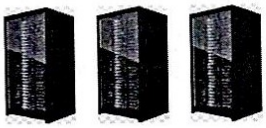
- Prometheus
- Portainer.io
- Grafana

Además de estos servicios que se instalan con el stack de SUDOCU, también es necesario tener dos servidores dedicados, uno con un motor de base de datos Postgresql y otro con un servidor de Nuxeo para la persistencia de los documentos digitales generados por SUDOCU.

Además, en el caso del despliegue en la UNJU, el sistema fue desplegado de manera integrada con SIU-Arai usuarios y SIU-Arai documentos ambos en su versión 2, por lo que fue necesario anexar un servidor más para servir dichas aplicaciones del SIU.

De esta manera, la estructura total del despliegue en producción consta de un cluster docker swarm de tres nodos donde se sirve el stack de SUDOCU, un servidor para postgres, uno para Nuxeo y uno para SIU-Arai. De esta manera en total la solución se encuentra desplegada sobre seis servidores virtuales, todos creados sobre servidores físicos administrados con VMWare.

A) Cluster Docker Swarm con SUDOCU (backend + frontend) + herramientas de monitoreo



3 VMs con:
4 CPU
8 GB RAM
200 GB HDD

B) Servidor Postgres con base de SUDOCU, Arai usuarios y Arai documentos

1 VMs con:
4 CPU
4 GB RAM
250 GB HDD

C) Nuxeo

1 VMs con:
4 CPU
4 GB RAM
2 TB HDD

D) Servidor con Arai usuarios y Arai documentos:

1 VMs con:
4 CPU
8 GB RAM
120 GB HDD

Tecnologías utilizadas:

Para la administración y virtualización de las distintas máquinas virtuales que componen el despliegue se utiliza VMWare. Cada VM además tiene como sistema operativo base Debian 10. Para el cluster, cada nodo también posee Debian 10 como sistema base con Docker Swarm 1.24. Los contenedores contienen Linux Alpine como sistema Base, y están desarrollados integramente con NodeJS +
Angular.

Backups:

Tolerancia (MTD) 4 horas:

- Servicio DNS
- Sistema SUDOCU (API-Server, Frontends y servicios de generación d documentos)

Tolerancia (MTD) 6 horas:

- Servicios SS0 (Nuxeo, BD)

Tolerancia de pérdida de datos (todos los sistemas): 24 hs

Seguridad en frontend y backend:

TLS/ SSL implementado con express en todos los servidores involucrados: El transporte de datos se realiza bajo el protocolo TLS (https) con certificados válidos provistos por la empresa Macroseguridad. Este protocolo permite y garantiza el intercambio de datos en un entorno securizado y privado entre dos entes, el usuario y el servidor, mediante el protocolo https a través de la encriptación en el transporte de la información.

Protección de cabeceras: en el desarrollo del backend se utiliza helmet, una dependencia que protege a las solicitudes de distintos tipos de ataques que se pueden hacer mediante la inclusión de cabeceras http. Helmet es realmente una colección de nueve funciones de middleware más paquetes que establecen cabeceras HTTP relacionadas con la seguridad:

- csp establece la cabecera Content-Security-Policy para evitar ataques de scripts entre sitios y otras inyecciones entre sitios.
- hidePowerBy elimina la cabecera X-Powered-By.
- hpkp añade cabeceras Public Key Pinning para evitar ataques de intermediarios con certificados falsos.
- hsts establece la cabecera Strict-Transport-Security que fuerza conexiones seguras (HTTP sobre SSL/TLS) con el servidor.
- ieNoOpen establece X-Download-Options para IE8+.
- noCache establece cabeceras Cache-Control y Pragma para inhabilitar el almacenamiento en memoria cache del lado de cliente.
- noSnift establece X-Content-Type-Options para evitar que los navegadores rastreen mediante MIME una respuesta del tipo de contenido declarado.
- frameguard establece la cabecera X-Frame-Options para proporcionar protección contra el clickjacking.
- xssFilter establece X-XSS-Protection para habilitar el filtro de scripts entre sitios (XSS) en los navegadores web más recientes.

Autenticación y acceso a las apis: Todos los endpoints de las apis se encuentran por defecto restringidos y solo se puede acceder previo login válido en Arai-Usuarios que autentica a través del protocolo SAML pero en el caso de la UNGS en particular delegando la autenticación en las APIs de Firebase. Se exceptúan de este modelo aquellos endpoints que por necesidades particulares necesiten ser accedidos públicamente. El sistema de autentificación genera sesiones en una base de datos redis, y a través de estas se valida cada petición al servidor de APIs. Cuando un usuario se loguea en SIU-Arai se genera una cookie en el browser la cual contiene el ID único de sesión generado en Redis, que además caducará cada hora. Para poder hacer una petición a una API, la misma debe hacerse desde un browser con un aplicación que se ejecute bajo un dominio habilitado, que tenga generada la cookie con el id de sesión y que esta sesión sea válida en la base Redis.

Seguridad de Usuarios y Claves y segmentación de accesos a las bases: Todos los datos de configuración de las aplicaciones y las apis, como urls, IPs, usuarios y claves, se encuentran fuera de los contenedores donde se alojan las aplicaciones web. Además del esquema de seguridad formado por el acceso a las apis comentado en el punto anterior, también se aplica un esquema de restricción a los distintos usuarios de bases de datos. Por ejemplo, se utiliza un usuario de solo lectura para el acceso a las apis públicas y un usuario con permisos sobre la tabla de preinscripciones para hacer los inserts.

/////

Express Limiter: Esta dependencia nos permite prevenir ataques de denegación de servicio para servidores web montados sobre Express. La misma limita la cantidad de peticiones posibles durante determinado lapso de tiempo sobre una misma IP, de esta manera se detecta y bloquea actividad maliciosa.

Minificación y ofuscación de código: El frontend utiliza todos los beneficios en seguridad que brinda el uso de AngularJS como framework pero también utilizamos Gulp para minificar, unificar, empaquetar y ofuscar el código del frontend. De esta manera se mejora la carga y se dificulta la tarea de lectura del código y el acceso a la lógica por parte de los visitantes.

ANEXO II

Informe sobre firma electrónica del sistema SUDOCU.

Autorización básica en SUDOCU y SIU-Arai

El modelo de autorización básica de SUDOCU y SIU-Arai documentos se encuentra resguardado por las medidas de seguridad integradas en todo el sistema. Estas medidas son múltiples y se encuentran tanto del lado del cliente como del servidor y en todos los servicios intervinientes en el proceso.

Proceso

Cuando un usuario autoriza un documento, realiza una petición de autorización a SUDOCU que a su vez genera una solicitud de autorización a SIU-Arai con el documento generado. SIU-Arai almacena este documento en nuxeo y en su propia base, y crea la solicitud de autorización. Con la solicitud de autorización creada, informa a SUDOCU mediante una notificación que la solicitud fue creada. Cuando SUDOCU recibe esta notificación valida la sesión del usuario y envía la confirmación de autorización a SIU-Arai. Una vez que SIU-Arai recibe el evento de confirmación de autorización procesa el mismo, y una vez terminado informa a SUDOCU a través de una notificación que el proceso fue terminado y en esta instancia el documento se da por autorizado en SUDOCU.

Arquitectura

Todo el proceso de autorización puede dividirse en dos estructuras claramente diferenciadas. La primera, la comunicación entre el cliente (browser) y el servidor de SUDOCU, y en segundo lugar la comunicación entre el servidor de SUDOCU y el servicio de SIU-Arai documentos.

En todos los pasos del circuito de autorización las comunicaciones viajan sobre TLS/SSL (https), por lo que toda comunicación viaja encriptada entre dos puntos y esto protege la comunicación y los datos.

Del lado de la comunicación entre cliente y servidor, el usuario accede a la aplicación a través de un usuario y contraseña que se gestiona a través del servicio ACTIVA UNJU, el cual delega el resguardo de los datos de usuario y la validación de la autenticación en el servicio de Firebase de Google. Este servicio utiliza el protocolo OAUTH2 para validar la autenticación del usuario y los datos viajan en todos los casos bajo TLS.

Del lado de las comunicaciones entre el servidor de SUDOCU y el de SIU-Arai el transporte de datos también se hace siempre sobre TLS y la conexión entre ambos servicios se realiza a través de autenticación básica, con datos de conexión que se encuentran resguardados en archivos de config que se encuentran fuera del código fuente de la aplicación y que se administra a través de secretos.

Medidas de seguridad

Las medidas de seguridad que se encuentran implementadas en la conexión cliente-servidor y servidor-servidor son ampliamente recomendadas por las buenas prácticas en el desarrollo de aplicaciones distribuidas y la arquitectura orientada a microservicios:

TLs: esta tecnología cifra los datos antes de enviarlos desde el cliente al servidor, lo que evita algunos de los ataques de pirateo más comunes.

Versiones: se mantienen actualizadas las versiones de las librerías y componentes a la última versión disponible.

Helmet: ayuda a proteger la aplicación de algunas vulnerabilidades web conocidas mediante el establecimiento correcto de cabeceras HTTP. Helmet es realmente una colección de nueve funciones de middleware más paquetes que establecen cabeceras HTTP relacionadas con la seguridad:

- csp establece la cabecera Content-Security-Policy para evitar ataques de scripts entre sitios y otras inyecciones entre sitios.
- hidePoweredBy elimina la cabecera X-Powered-By.
- hsts establece la cabecera Strict-Transport-Security que fuerza conexiones seguras (HTTP sobre SSL/TLS) con el servidor.
- ieNoOpen establece X-Download-Options para IE8+.
- noCache establece cabeceras Cache-Control y Pragma para inhabilitar el almacenamiento en memoria caché del lado de cliente.
- noSniff establece X-Content-Type-Options para evitar que los navegadores rastreen mediante MIME una respuesta del tipo de contenido declarado.
- frameguard establece la cabecera X-Frame-Options para proporcionar protección contra el clickjacking.
- xssFilter establece X-XSS-Protection para habilitar el filtro de scripts entre sitios (XSS) en los navegadores web más recientes.

La Dirección General de Informática y la Coordinación del SIU tendrán a su cargo la administración del Sistema Único Documental (SUDOCU), y en consecuencia les compete:

a) Administrar la manera de integrar el sistema.
b) Habilitar administradores locales en las distintas unidades de gestión.
c) Aprobar la nómina de documentos y contenedores digitales disponibles en el sistema.
d) Asignar usuarios y permisos.
e) Definir el funcionamiento, los usuarios y el ingreso de datos al sistema, en función de procedimientos establecidos.
f) Capacitar y prestar asistencias a los administradores de las unidades de gestión.

Tcb