



Tipo de artículo: Artículos originales
Temática: Desarrollo de aplicaciones informáticas
Recibido: 12/10/2022 | Aceptado: 03/12/2022 | Publicado: 30/03/2023

Identificadores persistentes:
ARK: ark:/42411/s11/a80
PURL: 42411/s11/a80

Implementación de controles de acceso para un sistema web de gestión de prácticas profesionales

Implementation of access controls for a professional practice management system

Galvez Mori Edisson Alejandro ¹[0000-0003-3280-7661]*, Torres Correa Robert Emmanuel ²[0000-0002-7729-9026], Valdivia Valderrama Jorge ³[0000-0003-3280-7661], Mendoza de los Santos Alberto Carlos ⁴[0000-0002-0469-915X]

¹ Universidad Nacional de Trujillo. egalvez@unitru.edu.pe

² Universidad Nacional de Trujillo. rtorresc@unitru.edu.pe

³ Universidad Nacional de Trujillo. jvaldiviav@unitru.edu.pe

⁴ Universidad Nacional de Trujillo. amendozad@unitru.edu.pe

* Autor para correspondencia: rtorresc@unitru.edu.pe

Resumen

El presente artículo presenta un sistema de información web que facilitará la gestión de las prácticas profesionales en la Universidad Nacional de Trujillo. Para ello, se aplicó una metodología ágil SCRUM debido a que es adaptable a los constantes cambios en el proceso de desarrollo del software y los controles de acceso que proporciona la normativa ISO 27001:2013 con el objetivo de garantizar la integridad, autenticidad y disponibilidad de los activos de información que posee el sistema. Los resultados obtenidos apoyan la implementación de la autenticación de doble factor y la firma digital como controles esenciales para la gestión de la información de acuerdo con la confiabilidad calculada. Se concluye que los controles de acceso proporcionan seguridad en la información manejada en el sistema de acuerdo a las pruebas de confianza.

Palabras clave: Sistema web de información, prácticas profesionales, ISO/IEC-27001, SCRUM, control de acceso

Abstract

This article presents a web information system that will facilitate the management of professional practices at the National University of Trujillo. For this, an agile SCRUM methodology was applied because it is adaptable to the constant changes in the software development process and the access controls provided by the ISO 27001:2013 standard with the aim of guaranteeing the integrity, authenticity and availability of data. the information assets that the system possesses. The results obtained support the implementation of two-factor authentication and digital signature

as essential controls for information management according to the calculated reliability. It is concluded that the access controls provide security in the information handled in the system according to the trust tests.

Keywords: *Web information system, professional practices, ISO/IEC-27001, SCRUM, access control.*

Introducción

Las prácticas preprofesionales corresponden a la primera aproximación al mercado laboral y a la vida profesional que tienen los estudiantes de la Facultad de Ingeniería, cuyo propósito es, según la Ley 28518: Ley sobre modalidades formativas laborales, permitir a la persona en formación durante su condición de estudiante aplicar sus conocimientos teóricos y prácticos mediante el desempeño de tareas programadas de capacitación y formación profesional en una situación real de trabajo [4]. En la Universidad Nacional de Trujillo se requiere de un sistema que realice la gestión de las prácticas profesionales de las distintas facultades. Además, se necesita que el sistema actúe como una vía de comunicación entre los estudiantes y las empresas que requieran de la fuerza laboral de los estudiantes a través de las convocatorias de prácticas preprofesionales. Esto porque la universidad, como institución responsable de administrar la educación superior a la sociedad emergente del conocimiento, está obligada a reinventarse para evolucionar al ritmo de los tiempos [2]. En lo que respecta a la seguridad de la información se aprecia una vital importancia en los procesos que comprenden la cadena de valor de los negocios y empresas, y es por esto que los riesgos en los SI están cada vez más presentes, afectando a la integridad y protección de los mismos, resultando en un impacto negativo [1]. Algunas investigaciones sugieren que, además de las implementaciones de SGSI a los sistemas de información siguiendo el estándar ISO-27001, se debe considerar una mejora continua de los servicios ofrecidos, es decir, dar el respectivo seguimiento para garantizar de esa forma una comunicación eficaz que contribuyan a los objetivos de seguridad planeados [2, 3].

Por lo tanto, este artículo busca elaborar un prototipo con los respectivos controles de acceso de un sistema de gestión de prácticas profesionales, específicamente autenticaciones desde doble factor y firma digital para los certificados necesarios en los procesos de evaluación. Esto permitirá la integridad, confidencialidad y disponibilidad, además de ayudar en la agilidad de todos los procesos implicados. También se busca analizar la

confiabilidad de dichos controles de acceso para analizar la factibilidad de su respectiva implementación. Esta investigación se justifica en la necesidad de implementar el sistema mencionado, puesto que no existe uno actualmente y para las demandas actuales, son necesarias de implementar para evitar las vulneraciones de la información que se puedan dar en los sistemas ya existentes.

Métodos y Metodología computacional

Descripción del proyecto

La función principal del sistema de prácticas profesionales es optimizar el proceso de gestión de prácticas profesionales para las diferentes escuelas profesionales de la universidad. Facilitando el registro, seguimiento y evaluación de las prácticas profesionales realizadas por los estudiantes. Además de reducir tiempo en realizar los trámites, disminuir los costos de impresión de documentos, ahorrar espacio y almacenar documentos en la base datos sin riesgo a que se dañen [13]. En la Figura 1 se visualiza el diagrama general del sistema que representa la forma en que interactúan los usuarios con el sistema.

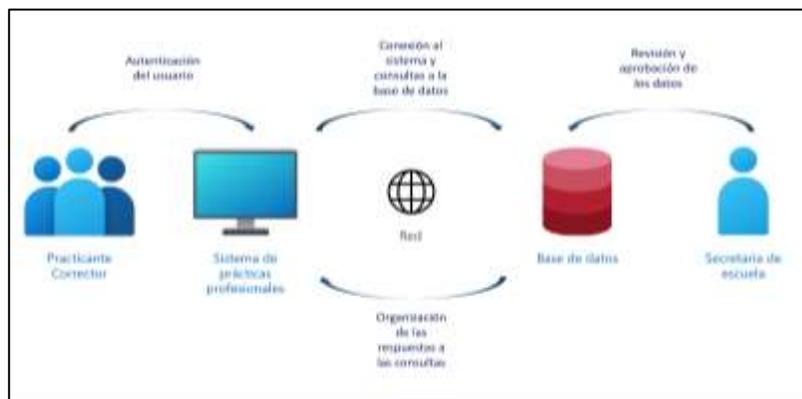


Figura 1. Diagrama general del sistema.

Modelo del proyecto

En la Figura 2 se presenta el modelo planteado para el sistema de prácticas profesionales. Dicho modelo se basa en 3 módulos: gestión de usuarios, relacionado a la administración de cuentas de los usuarios y sus roles; gestión de

actividades, relacionado al control de las tareas que deben cumplir los usuarios en el sistema como la entrega de los documentos en determinados plazos de tiempo; y la gestión de documentos, relacionado a la verificación y almacenamiento de la documentación generada por las actividades.



Figura 2. Modelo planteado para el sistema.

Diseño de base de datos

Para el diseño de la base de datos, las tablas se organizaron en dos categorías: tablas de cuentas de usuarios y tablas de prácticas preprofesionales. En la Figura 1, se muestra el diseño lógico de la base de datos con los campos y relaciones.

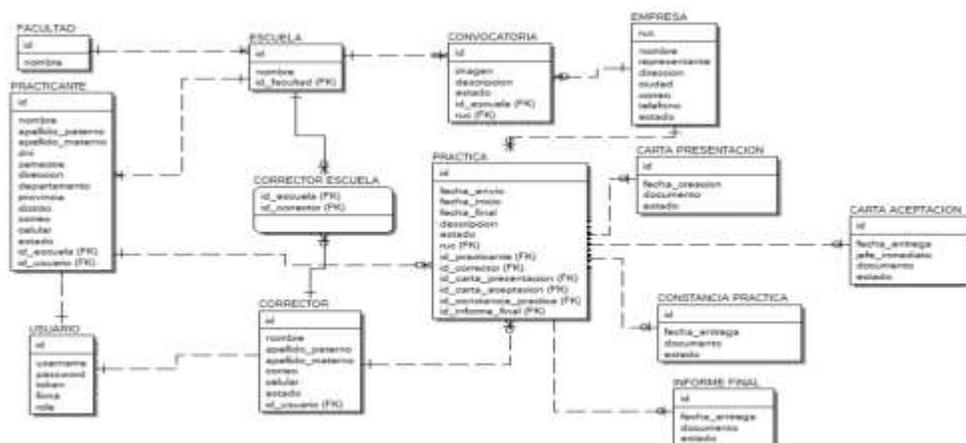


Figura 3. Diseño lógico de base de datos para el sistema.

Arquitectura de solución

El software a utilizar para el desarrollo de la aplicación web será gratuito y de código abierto con el fin de disminuir costos. El presente proyecto se realizó bajo el framework de aplicaciones web Django escrito en el lenguaje de programación Python y con el uso del motor de base de datos MySQL. Se empleó la metodología de desarrollo de software SCRUM y se realizaron 6 Sprint.

Desarrollo Sprint 1 - Funcionalidades base

El propósito del Sprint 1 es comenzar con las funcionalidades básicas de la aplicación que son importantes para el primer caudal dentro de lo planificado. Se revisan temas como la seguridad de la cuenta del usuario y la actualización de datos. En el sistema existen dos tipos de usuarios: el practicante (el estudiante) y el corrector (el docente). En la figura 4, se muestra la interfaz de inicio de la aplicación web donde se ingresan las credenciales del usuario. En la figura 5, se muestra la vista de los datos de la cuenta del usuario con la posibilidad de actualizar algunos datos.



Figura 4. Diseño de interfaz entregado en Sprint 1 en interfaz de inicio de sesión.



Figura 5. Diseño de interfaz entregado en Sprint 1 en interfaz de datos de cuenta de usuario.

Desarrollo Sprint 2 - Funcionalidades base 2

Con Sprint 2 se pretende implementar funcionalidades que complementen el proceso de preinscripción a la práctica preprofesional. En la figura 6, se muestra la interfaz de inscripción donde se mostrará la lista detallada de las inscripciones hechas por el practicante. En la figura 7, se muestra el formulario para el registro de una carta de presentación donde se ingresarán datos de la organización donde el practicante ofrecerá sus servicios, una vez registrado hay un tiempo límite de 7 días para que el practicante registre la carta de aceptación por parte de la empresa, en caso contrario la carta de presentación es anulada. En la figura 8, se muestra el formulario para el registro de la carta de aceptación por parte de la empresa, detallando la fecha de inicio y fin de la práctica, así como los datos del jefe encargado de monitorear las actividades del practicante.



Figura 6. Diseño de interfaz entregado en Sprint 2 en interfaz de inscripción para el practicante.



Figura 10. Diseño de interfaz entregado en Sprint 3 en interfaz de entregas de constancia de prácticas e informe final.

Desarrollo Sprint 4 - Funcionalidades base 4

Con Sprint 4 se pretende implementar funcionalidades que complementen el proceso de publicación de convocatorias de prácticas preprofesionales. En la figura 11, se muestra la interfaz de convocatorias donde se visualizará los anuncios por parte de las empresas solicitando practicantes.



Figura 11. Diseño de interfaz entregado en Sprint 4 en interfaz de convocatoria.

Desarrollo Sprint 5 – Autenticación de doble factor (2AF)

Con Sprint 5 se plantea implementar autenticación de doble factor que proporcione seguridad al proceso de inicio de sesión al sistema. Después que el usuario ingrese sus credenciales, el sistema emitirá un correo electrónico con un

código aleatorio al buzón del usuario, el usuario deberá introducir el código al sistema para completar la autenticación en un tiempo determinado, en caso contrario el sistema volverá a pedir credenciales al usuario. En la figura 12 se muestra el formulario de ingreso del código de verificación enviado previamente por el correo electrónico del usuario. En la figura 13 se muestra un ejemplo del correo que contiene el código que envía el sistema a los usuarios.

The image shows a web form titled "Ingresar código de verificación". Below the title, there is a small instruction: "Se ha enviado un código a su correo electrónico (*****@univru.edu.pe). Ingrese el código en el siguiente campo para completar la autenticación." Below this, there is a large hash symbol "#". Underneath the hash symbol is a text input field labeled "Código de verificación". At the bottom right of the form, there is a blue button labeled "Ingresar código".

Figura 12. Diseño de interfaz entregado en Sprint 5 en interfaz de ingreso de código de verificación por 2AF.



Figura 13: Formato entregado en Sprint 5 en formato de correo electrónico generado por el sistema que contiene el código de verificación de autenticidad.

Desarrollo Sprint 6 – Firma digital

Con Sprint 6 se plantea implementar firma digital para que asocie la identidad del usuario a cada uno de los documentos, además de asegurar la integridad de los documentos generados o registrados. Para ello se registrará las firmas de los usuarios, en la Figura 14 se muestra el formulario de registro, y se guardará en la base de datos, también se añadirán campos donde se realizará la firma en los formularios que impliquen entrega de documentos. El sistema pedirá previamente la contraseña del usuario para realizar la firma, tal como se muestra en la Figura 15, y comprobará que la firma sea similar a la firma registrada en la cuenta del usuario, en caso contrario se anulará el formulario.



Figura 14. Diseño de interfaz entregado en Sprint 6 en interfaz de registro de firma digital a la cuenta.



Figura 15. Diseño de interfaz entregado en Sprint 6 en interfaz de formulario de entrega de documentos implementando firma digital.

Fundamentación teórica

Prácticas profesionales

Corresponden a la primera aproximación al mercado laboral y a la vida profesional que tienen los estudiantes universitarios, cuyo propósito es, según la Ley 28518: Ley sobre modalidades formativas laborales, permitir aplicar sus conocimientos teóricos y prácticos mediante el desempeño de tareas programadas de capacitación y formación profesional en una situación real de trabajo [4].

Sistema de información

Conjunto de elementos organizados y relacionados que permite, según las políticas de la organización donde opera, almacenar, analizar y utilizar datos a favor para las actividades que se realizan dentro de la empresa. Esto ayuda a la toma de decisiones dentro de la organización con el fin de mejorar sus procesos y satisfacer las necesidades de los clientes. Actualmente, son alojadas en servidores web para obtener alcance a grandes masas de usuarios mediante internet [5].

Control de acceso

El control de acceso es el proceso de decidir si el usuario tiene permiso para ejecutar algo o no. También llamado autorización, se refiere a la gestión del acceso a los recursos protegidos y al proceso de determinar si un usuario está autorizado a acceder a un recurso particular [7].

Metodología de desarrollo de software SCRUM

Metodología no ágil y flexible para el desarrollo de software, cuyo principal objetivo es maximizar el retorno de la inversión para la organización. Se basa en construir primero la funcionalidad de mayor valor para los usuarios y en los principios de inspección continua, adaptación, autogestión e innovación [6].

Sistema de gestión de seguridad de información

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr sus objetivos. Consta de políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información [7].

Norma ISO 27001:2013

La ISO 27001:2013 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal [12]. Es esencial para resguardar los activos de información de los empleados y clientes, y la reputación de la organización.

Resultados y discusión

En este trabajo de investigación se trata de explicar la implementación de los controles de acceso definidos por la normativa ISO 27001:2013. Aquellos controles mencionados son los pilares de la seguridad de los sistemas de información, garantizando que solo los usuarios autorizados accedan a la información además de saber si realmente son quien dicen ser [8].

Un ejemplo clásico es el uso de contraseñas para realizar la autenticación de usuario, sin embargo, con el crecimiento de los casos de ataques cibernéticos y de la necesidad de preservar la integridad de la información se ha optado por usar la autenticación de doble factor con el fin de proteger el sistema de información.

La autenticación de doble factor (2AF) consiste en una capa adicional de seguridad para las cuentas de usuario con la finalidad de garantizar que el usuario sea el único quien pueda acceder con su cuenta al sistema, aunque alguien más conozca su contraseña [9]. Es decir, se añade un paso adicional para iniciar sesión en el sistema que puede ser por una llave de seguridad física, por una aplicación (como Google Authenticator o Microsoft Authenticator) o por un código de verificación de un solo uso [14]. En el sistema de prácticas profesionales se aplica 2AF por código de verificación, implementado en Sprint 5, que se envía al correo electrónico registrado en la cuenta del usuario a autenticar, tal como se presenta en la Figura 16.



Figura 16: Pasos de la autenticación de doble factor por código de verificación.

Además de la autenticación de doble factor, al tratarse de un sistema que se centra básicamente en la gestión de los documentos generados por el proceso de prácticas profesionales plantea la necesidad de poder adjuntar la identidad del autor con el documento que genera con el fin de proteger la integridad de la documentación [10]. Para cubrir aquella

necesidad se implementa la firma digital, lo cual nos permite demostrar que el autor del documento existe, que no puede negar que envió el documento y que el documento no ha sido modificado desde el envío. En la Figura 17 se muestran los pasos para realizar una firma digital en el sistema.



Figura 17: Pasos de la firma digital.

Estas dos herramientas disponibles en el sistema están basadas en las medidas de control de accesos que la norma ISO 27001:2013 detalla, con el objetivo de controlar y monitorizar los accesos a los medios de información según las políticas definidas por la organización [11]. Y, para comprobar el funcionamiento de las herramientas mencionadas, se ha realizado pruebas para verificar cuántas veces puede ejecutarse sin presentar errores, el procedimiento se muestra a continuación. Primero se define la Ecuación 1 para evaluar el programa.

$$\text{Confiabilidad} = 100\% * \frac{\text{N}^\circ \text{ de casos fallidos}}{\text{N}^\circ \text{ de casos totales}} \quad (1)$$

También se determinó una escala, la cual se muestra:

- 0% -10%, **Seguro**
- 11% -20%, **Regular**
- 21% - 100%, **Inseguro**

Se realizaron 200 casos de uso para cada apartado. Los casos fallidos son aquellas situaciones donde se ejecuta el programa y se lanzan errores de codificación o el programa no responde como debería. Con la fórmula de confiabilidad (Ecuación 1) se obtienen los siguientes resultados:

Evaluación de efectividad: Autenticación de dos factores

$$\text{Confiabilidad} = 100\% * \frac{19}{200} = 9,5\%$$

Evaluación de efectividad: Autenticación de dos factores

$$\text{Confiabilidad} = 100\% * \frac{32}{200} = 16\%$$

Conclusiones

Concluimos que los controles de acceso proporcionan seguridad en la información manejada en el sistema de acuerdo a las pruebas de confianza. De esta manera, es posible afirmar que los controles de acceso en los sistemas académicos representan un activo importante en los planes de seguridad de los sistemas académicos, y de acuerdo a ISO 27001, son importantes en la elaboración a futuro de un Sistema de Gestión de Seguridad de la Información (SGSI). También se concluye que la implementación hipotética de dicho servicio junto a los controles de acceso para el proceso de gestión de prácticas profesionales ayudaría enormemente a la agilización de los procesos, además de la seguridad de los datos que son utilizados dentro del sistema. Se recomienda realizar la mejora continua de estos controles de acceso para el beneficio de los sistemas de información implementados a futuro en la Universidad Nacional de Trujillo.

Referencias

- [1] Dronov, V.Y. and Dronova, G.A. Principles of Information Security Management System - Journal of Physics: Conference Series. Disponible: <https://iopscience.iop.org/article/10.1088/1742-6596/2182/1/012092> (Accedido: November 25, 2022).
- [2] Molina, D. 2002, Material de Apoyo Instruccional. Curso Orientación Educativa. Barinas: Unellez.

- [3] Tatiara, R., Fajar, A.N., Siregar, B. & Gunawan, W. 2018, "Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001", Journal of Physics: Conference Series. (Accedido: November 26, 2022).
- [4] Congreso de la República. Ley No 28518. Ley sobre Modalidades Formativas Laborales. (2018, 12 diciembre). SITEAL. https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/pe_6114.pdf
- [5] RODRIGUEZ PEROJO, Keilyn & RONDA LEON, Rodrigo. (2006). El web como sistema de información. ACIMED [online]. 2006, vol.14, n.1. ISSN 1024-9435.
- [6] Xavier Albaladejo. Qué es SCRUM. (2021, 20 septiembre). Proyectos Ágiles. <https://proyectosagiles.org/que-es-scrum/>
- [7] Sistema de gestión de seguridad de la información. (2022, 25 diciembre). Orientación - Presidencia del Consejo de Ministros - Gobierno del Perú. <https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion>
- [8] ISOTools Chile. (2017, 14 diciembre). Cómo la autenticación de dos factores permite cumplir con los controles de acceso ISO 27001. <https://www.isotools.cl/como-la-autenticacion-de-dos-factores-permite-cumplir-con-los-controles-de-acceso-iso-27001/>
- [9] Apple. (2022, 11 noviembre). Autenticación de doble factor para el ID de Apple. Apple Support. <https://support.apple.com/es-es/HT204915>
- [10] Soto, L. (2022, 22 noviembre). ¿Qué es una firma digital? <https://blog.signaturit.com/es/que-es-una-firma-digital>
- [11] Norma ISO 27001. (2013). ISO 27002 punto por punto A9 Control de acceso - Caso Práctico. (s. f.-b). ISO 27001. <https://normaiso27001.es/a9-control-de-acceso/>
- [12] What is ISO 27001 and How To Get an ISO 27001 Certification. (s. f.). NQA Certification Body. <https://www.nqa.com/es-pe/certification/standards/iso-27001>
- [13] Margarita Labastida Roldán, José Luis Ruiz Islas & Fernando Saldaña Ramírez. (2019). SSGPP: Sistema de Semi-Automatización y Gestión de Prácticas profesionales. Iztatl Computación, 15, 48. <https://ingenieria.uatx.mx/docs/RevistaIztatlComputacionNo15.pdf>
- [14] Nica Latto. (2020). ¿Qué es la autenticación de doble factor (2FA)? ¿Por qué la necesita? Blog AVG Signal. <https://www.avg.com/es/signal/what-is-two-factor-authentication>
- [15] Junta de Andalucía. (2012). Control de Acceso y Autenticación. Marco de Desarrollo de la Junta de Andalucía. <https://www.juntadeandalucia.es/servicios/madeja/contenido/subsistemas/desarrollo/control-acceso-y-autenticacion>

Roles de Autoría

Robert Emmanuel Torres Correa: Conceptualización, Análisis formal, Investigación, Metodología, Software, Validación, Redacción - borrador original. **Edison Alejandro Galvez Mori:** Conceptualización, Análisis formal, Investigación, Metodología, Software, Validación, Redacción - borrador original. **Jorge Valdivia Valderrama:** Conceptualización, Análisis formal, Investigación, Metodología, Software, Validación, Redacción - borrador original. **Alberto Carlos Mendoza de los Santos:** Análisis formal, Investigación, Software, Supervisión, Validación, Redacción - borrador original.