ISBN 978–987–633–574–4

Gestión de presencialidad en la virtualidad para la Universidad Nacional de Río Negro

Lugani, Carlos Fabián

{clugani} @unrn.edu.ar

Universidad Nacional de Río Negro, Sede Atlántica
Laboratorio de Informática Aplicada

Resumen. Existe una nueva forma de tomar clases, trabajar, o simplemente estar presentes, en donde las personas se conectan mediante las tecnologías de las comunicaciones por videoconferencia, videollamada o algún tipo de conexión a sistemas o aplicaciones. Ante esta realidad se observan varias necesidades: la de comprobar la identidad de las personas que comienzan la conexión debido a que la organización desea dar al acceso sólo a las que deben hacerlo, la de comprobar si la conexión con esa persona se ha visto interrumpida, o se ha desconectado definitiva o momentáneamente; y además si existe la atención de la persona ante el sistema, videoconferencia o la conexión establecida. Esto será dado por un proceso de difícil resolución y existen grados de comprobación asociados a la dificultad de comprobación que irían desde simples pruebas y amplia confianza hasta sistemas más complejos que establezcan un grado de aseguramiento de la presencialidad que se podrán resguardar y ser auditados.

En este primer trabajo se define la problemática anterior y el desarrollo de un esquema sobre el cual se desarrollarán aplicaciones que se puedan utilizar en la Universidad Nacional de Río Negro para las necesidades de las plataformas existentes o futuras para ser utilizadas en forma efectiva por la organización.

Palabras clave: ausentismo, presencialidad, identificación.

1 Introducción

El presente trabajo se define como un esquema en donde se presentará la problemática y posibles cursos de acción o escenarios para desarrollar soluciones y definiciones que sirvan para establecer marcos de trabajo.

La presencialidad como acción de las personas de estar físicamente en un lugar ha sido modificada como resultado de la pandemia Covid y ha modificado en varias formas la forma de trabajar, presenciar clases, participar de reuniones y múltiples actividades. Esta presencialidad también se podría entender como el “estar en línea” o “estar disponible” a tiempo completo, pero se establece que los mecanismos o controles que se diseñen tengan asociados como requerimientos los tiempos estipulados de conexión necesaria o requeridos que se hayan previamente pautado. Siendo importante

CACIC 2021 UNSa

el establecimiento de límites en la definición de las conexiones o disponibilidad del tiempo de las personas.

Actualmente los docentes se enfrentan a un nuevo paradigma que es la enseñanza sin presencialidad [(1)] y se ofrecen herramientas, recomendaciones, ideas que puedan serles útiles y en general formas de pensar o repensar la enseñanza para que sus aulas virtuales o cualquier tipo de estrategia sean enriquecidas. Aun así, existe la necesidad genuina de los docentes de requerir clases en donde los alumnos se conecten y tomen clases en forma remota necesitando de herramientas para comprobar que son los alumnos que tienen que estar conectados y de alguna forma que los mismos cumplen con ciertas pautas de presencialidad en esa virtualidad. Lamentablemente, los docentes no tienen las herramientas para verificar identidades o para comprobar la atención de los alumnos. En este sentido consiste el aporte que se pretende alcanzar con el presente trabajo.

Asimismo, las organizaciones también desean verificar identidades del personal tanto docente como no docente, que realizan tareas en sistemas, en reuniones, atención a personas u otras actividades por las cuales las personas se conectan a computadoras con acceso a Internet y a diversas aplicaciones y por las cuales cumplen con tareas que le han sido encomendadas. Por lo tanto, también las organizaciones desearían tener herramientas de control para poder hacer un seguimiento del presentismo, horarios de disponibilidad de personal, efectividad de atención y tiempos de respuesta.

Por otro lado, se destaca la evolución de herramientas de conectividad [(2)], la mejora en los sistemas de videoconferencia, existencia de pizarras compartidas, así como nuevas situaciones mixtas en donde un conjunto de personas están en forma presencial y otro conjunto están en forma virtual y participando síncronamente gracias a los medios de interacción que estos sistemas aportan y que son propios de la virtualidad. Así, un espacio virtual ha recibido varias denominaciones y se prefiere el nombre de Ambientes Virtuales de Enseñanza -Aprendizaje (AVEA) para el espacio virtual donde los miembros de una comunidad educativa interaccionan con la finalidad de desarrollar un proceso formativo, mediante la aplicación de las nuevas tecnologías de la información y la comunicación [(3)].

Por supuesto que lo anterior implica que las personas que se conecten y sean controladas acepten las condiciones que se plantean, si bien se prevén dificultades en cuanto a la disponibilidad o falta de disponibilidad de la tecnología necesaria para cumplir con los requerimientos de control como cámaras, micrófonos, conexiones estables a Internet y requerimientos de hardware más específicos, es indudable que las personas deberán contar con los medios físicos que aseguren la conexión y controles que se definan.

Se destaca que al realizar este trabajo se han buscado referencias académicas para las bases de su realización y se han encontrado, pero no se han encontrado para las secciones de desarrollo, se considera que el mercado o los productos de alguna forma pueden ofrecer variantes de comprobaciones de que los usuarios están conectados, pero no se ha establecido un esquema como el presentado en este trabajo en forma académica con lo cual no existen muchas referencias que hayan ayudado a definir este marco de trabajo.

CACIC 2021 UNSa

2. Comprobación de identidades

La identidad personal es un conjunto de rasgos característicos de un individuo, por los cuales se puede decir que esa persona es realmente quien dice ser. Como primer paso se debe definir la identidad de la persona que está conectada al sistema que se desea controlar. Existen numerosos métodos para identificar a las personas, podemos diferenciar a los biométricos que dependen del cuerpo de una persona como reconocimiento facial, reconocimiento de voz, venas de los dedos, geometría de la mano, cadencia de movimientos del cuerpo, etc. Por el otro lado, se puede identificar a una persona a través de contraseñas o preguntas que sólo la persona puede conocer. También existen dispositivos que una persona puede poseer como tokens de seguridad (también conocidos como token de autenticación o token criptográfico, son dispositivos portátiles de alta tecnología que generan una clave de forma aleatoria e irreemplazable, y que están asociados a un sistema de firma digital) o certificados digitales que están instalados en computadoras o celulares y que entregan un número o código que sirve para autenticar a la persona que posee ese dispositivo de hardware o teléfono celular.

En resumen, existen tres grandes conjuntos de formas de comprobar la identidad de una persona, (a) por algo que la persona conoce y recuerda como una contraseña, (b) por algo que la persona posee como un token o certificado digital, o (c) por algo que la persona es, como su huella dactilar o su rostro.

En primera instancia se puede definir que de acuerdo al nivel de control que se quiera establecer o el nivel de confianza en que el control será efectivo, será la necesidad de utilizar un mecanismo mas avanzado de autenticación y por lo tanto para sistemas que deban comprobar y registrar en forma segura la identidad de una persona, se necesiten mas niveles de autenticación o la combinación de dos tipos.

Por lo tanto, cualquiera sea la metodología, es conveniente establecer una asociación del tipo: nivel de autenticación requerido, nivel de información, activos de información a los que se accede o a valores (en caso de información contable), a categorías de información confidencial o procedimientos por ejemplos en casos de un proceso jurídico o legal. Es de especial cuidado y se deben analizar otras implicancias en el caso de por ejemplo exámenes en una Universidad que se tomen a través de Internet, ya que la autenticación de la persona y la asociación de un examen realizado por ella constituye un documento con implicancias legales.

También se debe tener en cuenta actos de votación que se pueden dar y otros actos en donde se requiere que una persona sea verificada de alguna forma porque será parte de una decisión que quedará documentada la coordinación.

Se desarrolla una tabla (*Tabla 1 – Actividad relacionada con nivel de autenticación para la Universidad Nacional de Río Negro*) para presentar casos posibles, sin que estos quieran determinar todos los casos posibles que son necesarios en una organización. Al desarrollar los mismos se tiene en cuenta los requerimientos que se observan en la Universidad Nacional de Río Negro, ya que este esquema se considera para su evaluación y uso en esta institución.

CACIC 2021 UNSa

Actividad relacionada con:	Actividad	Posible nivel de autenticación requerido
Docencia	Presentismo en actividad programada ON LINE (Docente)	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital
Docencia	Presentismo en actividad programada ON LINE (Alumno)	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital
Docencia	Presentismo en examen parcial o presentación de trabajo práctico ON LINE (Docente y Alumno)	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital
Docencia	Presentismo en examen final ON LINE (Docente y Alumno)	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital Nivel 3: Reconocimiento facial
No docencia	Presentismo en puesto de trabajo ON LINE	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital
No docencia	Coordinación de trabajo en puesto de trabajo ON LINE	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital Nivel 3: Reconocimiento facial
Investigación	Evaluación de proyectos, integrantes de proyectos, becas.	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital Nivel 3: Reconocimiento facial
Comunidad de la UNRN	Participación en reuniones informativas	Nivel 1: Usuario y Contraseña
Comunidad de la UNRN	Participación en consejo sin voto	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital
Comunidad de la UNRN	Participación en consejo con voto	Nivel 1: Usuario y Contraseña Nivel 2: Certificado digital Nivel 3: Reconocimiento facial

Tabla 1. Actividad relacionada con nivel de autenticación para la Universidad Nacional de Río Negro

La definición de identificación de personas ante el sistema que se vea involucrado siempre debería ser programada y diseñada previamente. Lo que se plantea en este trabajo es el diseño de un grado de requerimientos, nivel de autenticación o la suma de varios métodos de autenticación. Se debe siempre tener en cuenta el valor de la información y las implicancias legales de las acciones que las personas pueden realizar en la virtualidad, asimismo se deben revisar los procesos administrativos asociados que se encuentren involucrados en busca de responsabilidades definidas, actividades requeridas que no pueden faltar o no ser realizadas, controles que deben realizar las personas y dejar registros de su presencia y ejecución, y en general la revisión de las tareas de las personas para identificar aquellas actividades que deben ser analizadas para su realización en la virtualidad y sobre las cuales se puede efectivamente comprobar que han sido realizadas por esas personas.

Este esquema propuesto se lo puede calificar como modelo de identidad de personas, cada componente de comprobación de identidad equivale a un porcentaje que se va sumando para dar un total de comprobación de identidad. Así se puede decir que un numero de 100, sería la comprobación completa de la identidad de una persona a través de diferentes métodos. De acuerdo a la necesidad o requerimiento de un proceso o aplicación se establece que sea un porcentaje determinado de comprobación de identidad, lo cual es algo lógico de realizar ya que a mayor responsabilidad o implicancias de la participación de una persona, se le requerirá mayores comprobaciones de su identidad.

3. Comprobación de presencialidad

Se define la comprobación de presencialidad a un registro que depende de la característica del sistema a que se está conectado la persona, pero que permite siempre dejar un rastro que la persona estaba participando y atento a lo que sucedía en la actividad.

Por ejemplo, si existe una reunión en donde una persona está disertando ON LINE sobre un tema en particular (presentando un gráfico sobre el almidón de maíz y la variación de otras materias primas en la producción de alimentos:) y aparece una ventana en la pantalla de los participantes en donde debe seleccionar una opción de tres presentadas (En este momento se está hablando sobre Almidón de Maíz / Aditivos / Arroz) teniendo 10 segundos para presionar una de las tres opciones y luego desapareciendo la ventana. Este registro de cada participante es suficiente muestra que estaba prestando atención y por sobre todo que estaba en ese momento y que pudo interactuar con el sistema.

Pueden definirse múltiples o diversas comprobaciones de presencialidad y el objetivo es definir estrategias de comprobación de que la persona se encuentre presencialmente delante de la computadora.

Se definirán múltiples comprobaciones de presencialidad que se pueden enumerar como:

1. Comprobación de tipo Opción a completar con pregunta con vencimiento y desaparición de la pregunta (descripto como ejemplo anteriormente).

CACIC 2021 UNSa

2. ¿Comprobación de tipo “Esta Ud. ahí?” mediante chat en que se registra el tiempo de pregunta y el tiempo de respuesta de la persona.
3. Comprobación por foto (para lo cual la cámara debe estar habilitada). En este tipo de comprobación se deben realizar múltiples fotos de la persona que se encuentra delante de la computadora y se puede relacionar con la identificación biométrica (reconocimiento facial).
4. Comprobación de aplicaciones. Se debe analizar la aplicación en uso en la computadora, las aplicaciones abiertas y aplicación en foco durante la conexión, teniendo que ser el resultado un porcentaje mayor de la aplicación que se requiera en la conexión.
5. Encuesta o cuestionario de contestación rápida. Preparada con antelación y a disposición por un tiempo determinado dentro de la actividad comprueba que la persona esta activa y responde en un tiempo también determinado a la misma.
6. Comprobación a través de votación. La persona que diserta solicita que los participantes realicen una votación o selecciones en particular una opción, con un sistema que registra a través del tiempo las selecciones de las personas y las relaciona con las personas conectadas. Entregando un listado de las conexiones efectivas realizadas o los participantes que efectivamente realizaron la premisa tal como fue solicitada.

Además, se establece una relación entre la comprobación de la presencialidad con la comprobación de identidades en que también debe ser definida para cada sistema o aplicación. Al principio de la comunicación se establece que la identidad es la primera acción que se realiza y luego pasa a comprobarse que la persona se encuentra disponible y presente en la comunicación, pero pueden requerirse más comprobaciones de identidad luego de cierto tiempo. Se establece que luego de dos horas de conectado se requerirá de una comprobación de identidad que asimismo servirá de comprobación de presencialidad. Si cualquier situación hace que la comprobación no sea exitosa, se registrará el hecho y se finaliza la conexión.

4. Sistema de auditoria

Se considera que la comprobación de identidad primero y luego las sucesivas comprobaciones de presencialidad dejarán como resultado una cantidad de registros que serán la comprobación de las acciones que las personas realicen en los sistemas o conexiones.

Esta cantidad de registros requieren un sistema de gestión que tenga algunas características como las de:

- Identificación de personas que forman parte del sistema de autenticación con resguardo especial de claves, firmas digitales y datos biométricos
- Acceso a la información sobre actividades y necesidades de identificación en particular
- Participación de personas en actividades en forma general o particular
- Registros de votación

CACIC 2021 UNSa

- Controles efectivos registrados en los sistemas

El almacenamiento de la información de la identidad de las personas, y sus actividades en los sistemas, conexiones contendrá información confidencial y sensible. Se debe resguardar este tipo de información ya que existe una legislación específica en la República Argentina (Ley 25.326 – Protección de Datos Personales) [(4)].

5. Conclusiones

Luego de haber establecido ciertos parámetros y definiciones, se ha realizado una aproximación a un esquema de administración de la autenticación de personas y controles de su presencialidad en actividades virtuales. Si bien el origen de este trabajo es la necesidad de una organización en mejorar los procesos con que se cuentan y tener registros que se puedan comprobar a través de sistemas informáticos; este esquema se puede extender en forma normal a otro tipo de organizaciones que actualmente se encuentran en situaciones similares. También este esquema se puede extender al concepto de Ciudades Inteligentes, mediante estas herramientas, las ciudades pueden contar con realizar transformaciones digitales o incorporar tecnología utilizando el componente de identificación del ciudadano, realizar reuniones informativas con comprobación de personas, o comprobar la participación de los ciudadanos en plebiscitos. Asimismo, se puede aplicar el funcionamiento de este esquema para ampliar los alcances de actividades como las de Fábricas Inteligentes (Smart Factories) o Viviendas Inteligentes (Smart Homes) ya que los componentes que se desarrollan pueden servir tanto para comprobar la identidad de personas como la presencialidad.

Se menciona también que inmediatamente a la definición de este esquema se debe comenzar a desarrollar aplicaciones asociadas las cuales al funcionar en entornos reales será beneficioso para el mejoramiento del presente esquema pudiendo ampliar sus alcances y comprobando su funcionamiento.

Finalmente, se destaca que este esquema es un proceso de apoyo a la virtualización que se está llevando a cabo en todos los ámbitos, siendo valioso el aporte para asegurar que la misma se apoye sobre trabajos formales que establezcan definiciones y sobre experiencia en la formulación de estrategias que se apliquen para solucionar la problemática detectada.

6. Referencias

1. Mazza, D. (2020). Lo que la pandemia nos deja: una oportunidad para pensarnos como docentes. Citep. Centro de Innovación en Tecnología y Pedagogía. [Sitio web] http://citep.rec.uba.ar/covid-19-ens-sin-pres/

2. Medina Uribe, Jury Carla ; Calla Colana, Godofredo Jorge ; Romero Sánchez, Phill Arnold (2019) Las teorías de aprendizaje y su evolución adecuada a la necesidad de la conectividad Revista de la Facultad de Derecho y Ciencia Política de la Universidad Alas Peruanas, ISSN-e 2313-1861, ISSN 1991-1734, págs. 377-388

CACIC 2021 UNSa

3. Mario E. Díaz Durán, Mariela Svetlichich. Nuevas Herramientas Tecnológicas en la Educación Superior PROYECCIONES - Nº 11 - Año XI (2016) pp. 93 – 149 [Sitio web] https://revistas.unlp.edu.ar/proyecciones/article/download/6485/5565/
4. Ley 25.326 Protección de Datos Personales Sancionada: Octubre 4 de 2000 y Normas complementarias Disposición 7 / 2010 Dirección Nacional de Protección de Datos Personales/ Decreto Reglamentario 1558 / 2001 [Sitio web] https://www.argentina.gob.ar/aaip/datospersonales

CACIC 2021 UNSa