Reseña - ISO/IEC 24760-2:2015

Seguridad y Privacidad TI - Marco para la gestión de identidades - Parte 2: Arquitectura de referencia y requisitos

"Seguridad y Privacidad TI - Marco para la gestión de identidades - Parte 2: Arquitectura de referencia y requisitos", *Organización Internacional de Normalización*, Comité Técnico ISO/IEC JTC 1, Subcomité SC 27, junio 2015, https://www.iso.org/standard/57915.html.

Reseñador: George Dobbs

Resumen

El presente texto es un resumen del contenido del ISO/IEC 24760-2:2015, uno de los estándares centrales de IAM, acompañado de una opinión sobre su idoneidad para su uso por los profesionales de identidad.

Reseña

El documento es de naturaleza formal y provee un modelo riguroso de un sistema de gestión de identidades, así como una noción de lo que debería incluirse en el diseño de dicho sistema. Quienes no posean una formación en arquitectura quizás encuentren que el abordaje es demasiado académico, pero si lo que quieren es sumar un grado de rigurosidad a su planificación, continúen leyendo.

Luego de los textos introductorios, el documento ofrece un conjunto de puntos de vista operativos y de contexto para la implementación de un diseño documentado mínimamente aceptable. Luego, el documento desarrolla estos puntos de vista en términos de definiciones, factores de preocupación y modelos.

Una vez abordados los distintos puntos de vista, el documento se enfoca en detalle en las dos visiones más importantes. Respecto al punto de vista de contexto, el texto profundiza en las partes interesadas, los actores, el modelo de contexto, el modelo de caso de uso y el modelo de conformidad y gobernanza. El abordaje sobre las partes interesadas es útil ya que identifica algunas de las mismas que muchas veces son olvidadas como los entes regulatorios o las raramente mencionadas defensorías del consumidor/cliente.

El texto no se limita a enlistar el conjunto de las partes interesadas que se deben tener en cuenta, sino que también identifica sus preocupaciones. El documento diferencia las partes interesadas de los actores, aunque muchas veces coincidan. Allí donde las partes interesadas tienen preocupaciones, los actores tienen responsabilidades y en algunos

casos aportan capacidades, todo lo cual se encuentra enlistado. El lector ávido querrá estudiar a fondo la sección de “actores” ya que es muy precisa y aporta muchos conceptos en pocas palabras.

Posteriormente el documento abarca los casos de uso. El texto ofrece de ejemplo un caso de uso simple y luego describe varios tipos de caso de uso específicos (de empleado, empleador, entidad y dispositivo). Es curioso que el texto no menciona el caso de uso de cliente/ciudadano, pero sí el de empleado. En su lugar, dichos conceptos están incluidos en la sección de casos de uso de entidad. Algunos ejemplos adicionales se encuentran en el Anexo B. Estos ejemplos son útiles. Para un profesional que sea fluido en el Lenguaje unificado de modelado (UML, por sus siglas en inglés), los diagramas y la sección de casos de uso deberían ser claros. Para otros, su comprensión puede resultar más compleja.

La visión de contexto se completa con una breve sección sobre qué debe incluirse en un modelo de conformidad y gobernanza. Dicha sección provee una lista de verificación.

Seguidamente se encuentra la visión operativa. Esta sección enlista las interacciones esperables en el sistema entre los actores y los elementos arquitectónicos. Abarca diez procesos entre ellos el mantenimiento de la información de identidad y el acceso a información de identidad, así como otros menos comunes como el descubrimiento de autoridades de identidad y la publicación de información de identidad (en conformidad con una política determinada). Una vez más, los mismos están presentados de manera muy concisa, pero proveen listas de verificación muy útiles para el profesional. Los componentes operativos están desplegados en un diagrama UML en el Anexo C, donde aparecen nuevos conceptos como “Raíz de Confianza”.

Antes de adentrarse en la sección de requisitos, el texto describe 4 escenarios. Los escenarios se utilizan para determinar las relaciones de confianza que se necesitan. Esta breve sección anima al arquitecto a diseñar en función de la confidencialidad, integridad y confianza necesarias para cada escenario. Se proveen muy pocos detalles sobre esto. Por ejemplo, el escenario de federación está descrito en términos abstractos sin mencionar nociones básicas sobre un proveedor de identidad o terceros confiables. Pero sí anima al arquitecto a tener en consideración qué escenarios son deseables, ayudando a establecer los requisitos.

El texto principal concluye con una lista de requisitos operativos y no operativos. La misma es una fuente excelente para utilizar a la hora de establecer los requisitos de un sistema. Además de los Anexos A - C, el documento ofrece el Anexo D que aborda algunos procesos de negocio seleccionados como la gestión del consentimiento, la administración de credenciales del ciclo de vida, la administración de configuración (en una federación), la gestión de políticas y la administración del ciclo de vida de una entidad.

En términos generales el documento es muy formal y estructurado lo cual permite que se utilicen los conceptos fundacionales de la gestión de identidad. La gestión de acceso es referenciada casi de forma involuntaria: como una forma de controlar el acceso a la información de identidad. La gestión de acceso es abarcada en otro documento ISO/IEC: ISO/IEC 29146, *Tecnología de la información. Técnicas de seguridad. Marco para la gestión de acceso*. Esto puede resultar frustrante para el lector que busca información detallada sobre autorización y autenticación.

El reseñador considera que este documento es valioso para los profesionales de identidad que se encuentran desarrollando un nuevo sistema de identidad o que están evaluando el estado actual de un sistema de identidad con el fin de reducir brechas y limitaciones. Provee un marco estructurado de conceptos que pueden ser utilizados para informar dicho trabajo. Dicho esto, es un texto que requiere que el lector ponga mucho de sí para su lectura. La presentación no cubre la gestión de acceso; se enfoca exclusivamente en la gestión de identidad. Referencia a otro documento ISO/IEC para la gestión de acceso. Si bien hay referencias a otros documentos externos, el reseñador considera que estos últimos pueden omitirse sin afectar la comprensión general. El documento es apropiado para quienes quieren construir o revisar un sistema de identidad robusto y buscan comparar sus propias opiniones con las de otros a fin de asegurarse que se ha llevado a cabo un diseño completo.