Reseña – ISO/IEC 24760-3:2016

Tecnología de la Información - Técnicas de seguridad - Marco para la gestión de identidades - Parte 3: Aplicación

"Seguridad y Privacidad TI - Marco para la gestión de identidades - Parte 3: Aplicación", *Organización Internacional de Normalización*, Comité Técnico ISO/IEC JTC 1, Subcomité SC 27, agosto 2016, https://www.iso.org/standard/57915.html.

Reseñador: Espen Bago

Resumen

El documento que reseñamos aquí es la tercera y última parte del estándar ISO/IEC 24760, que se enfoca en la "aplicación" cuyo objetivo se describe en el resumen del mismo como "*una guía para la gestión de información de identidad y para garantizar que un sistema de gestión de identidad esté en conformidad con ISO/IEC 24760-1 e ISO/IEC 24760-2*". Las partes 1 y 2 abarcan la "*terminología y conceptos*" y la "*arquitectura de referencia y requisitos*". ISO/IEC 24760-3 se encuentra en su primera versión, con fecha de agosto de 2016.

Reseña

Cabe destacar que esta reseña fue escrita en base a la parte 3 exclusivamente y sin conocimiento detallado de las partes anteriores. Dado que en la parte 3 se encuentran referencias a las otras partes, este documento no debe ser usado separadamente. Sin embargo, ya que cada parte tiene su licencia única y se vende por separado, reseñarla separademente de las demás puede darnos una pista sobre su valor individual.

ISO/IEC 24760-3 define su propio objetivo como *especificar conceptos relevantes, estructuras operativas y aplicaciones que habiliten la garantía y el control requeridos para el uso tanto de la información de identidad como de los sistemas de gestión de la identidad*. Se infiere que el documento provee buenas prácticas para la gestión de la identidad a su audiencia objetivo que son aquellos que estén comenzando una iniciativa de identidad o que necesiten tener un mejor control de una iniciativa de este tipo que ya esté en marcha.

Dicha intención de proveer prácticas para lograr los objetivos centrales y típicos en lo que refiere a la identidad es meritoria ya que es algo que muchos profesionales buscan. Sin embargo, el documento falla en cumplir sus promesas por varios motivos, siendo los más importantes la falta de consistencia en la estructura y en el contenido de cada sección.

El núcleo de ISO/IEC 24760-3 son las 12 páginas sobre la reducción de riesgos de la identidad, los identificadores y la información de identidad, las auditorías, los objetivos del control y los controles, siendo esta última parte (los objetivos del control y los controles) la principal. Estas secciones enlistan recomendaciones necesarias (aplicaciones) para las diferentes partes del trabajo a la hora de implementar y mantener sistemas de gestión de identidad. Al extraer dichas recomendaciones, nos encontramos con mucha información útil que puede servir a modo de una lista de verificación de recomendaciones y sugerencias.

El desafío está en encontrar y extraer la información útil por lo confuso de la disposición de las subsecciones que son difíciles de seguir, especialmente porque estas subsecciones no son consistentes en cuanto al nivel o detalle de la información provista. Por lo tanto, es innecesariamente complicado comprender las aplicaciones en su totalidad como encontrar aquellas que son relevantes para determinada situación. Además, cuando es encontrada, dicha información tiende a ser demasiado simple o superficial. Por ejemplo, la sección sobre auditar un sistema de gestión de identidad dice básicamente que se deben llevar a cabo auditorías y que su objetivo debe ser validar que el sistema funcione en concordancia con sus requisitos y políticas.

En una futura revisión de este estándar sería bueno simplificar la estructura de sus secciones poniendo el énfasis en esclarecer qué se está tratando de decir. Dado que por su naturaleza la mayoría de la información es de alto nivel, sería beneficioso trabajar un formato cercano a una lista de verificación.

Tal y como está ahora, este estándar es accesible en su mayoría para gran parte de los profesionales experimentados ya que están capacitados para explorar el documento. No obstante, estos profesionales son también quienes menos necesitan la información ya que normalmente y por su propia experiencia, ya conocen la mayoría de las aplicaciones. A la mayoría de los profesionales que recién empiezan en este ámbito, se les hará cuesta arriba utilizar la versión actual (08-2016) ISO/IEC 24760-3 con los fines propuestos.

No hay figuras en el cuerpo principal del documental lo cual parece razonable ya que las aplicaciones descritas no permiten ser visualizadas fácilmente.

Aparte del núcleo del documento mencionado anteriormente, la mitad del ISO/IEC 24760-3 se recoge en dos anexos los cuales no son reseñados aquí ya que no hay referencia a ellos en el texto principal y no están directamente relacionados con lo mencionado en el texto que los precede. En pocas palabras: estos anexos que suman 16 de las 38 páginas totales están desconectados del resto, dando la impresión de que fueron incluidos únicamente para alcanzar cierta cantidad de páginas.

Dicho esto, los dos artículos en los anexos están bien escritos y abarcan áreas de interés. De haber sido relevantes para el objetivo propuesto por el estándar, estos anexos serían suficientes para recomendar la totalidad del documento.

Los anexos incluyen figuras descriptivas y diagramas, proveen aplicaciones para la gestión de sistemas federados de identidades (Anexo A) y aportan un análisis de qué son las credenciales basadas en atributos y cómo pueden utilizarse para la autenticación. Cualquier persona que necesite información específica sobre la instalación de sistemas federados o que esté trabajando con credenciales basadas en atributos, considerará que vale la pena leer detenidamente este documento.