AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información (SDRSI) para su integración a Sistemas de Gestión de Calidad

Autores
Riva, Fabiana María; Maenza, Rosa Rita; Pereira, Nicolás; Font, Gabriela; Martin, Vilma;
Fabbri, Lucía; Dolan, Guillermo; Butti, Julián; Bidart, Franco
Departamento de Ingeniería en Sistemas de Información
Facultad Regional Rosario - Universidad Tecnológica Nacional
E. Zeballos 1341, 2000 Rosario, Argentina
fabiana_riva@hotmail.com

Resumen

El presente artículo tiene el propósito de dar a conocer el origen, avances y perspectivas del proyecto: ***Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información (SDRSI) para su integración a Sistemas de Gestión de Calidad****.*

El proyecto está vinculado a las empresas pertenecientes a la Industria del Software y Servicios Informáticos (SSI) que al presente han optado por implementar Normas de Calidad con el objetivo de acreditar la calidad de sus productos y procesos.

A los variados factores que explican esta adopción, se suman requerimientos de control emanados de normativas a nivel nacional e internacional que obligan a estas organizaciones a asegurar uno de sus activos más importantes: ***la información****. En este sentido la Norma ISO 27001, que orienta a la implementación de Sistemas de Gestión de Seguridad de la información, puede apoyar en el cumplimiento de este objetivo.*

Tomando en consideración la posibilidad dada por los Sistemas Integrados de Gestión de Calidad (SIGC) que suman a las Normas de Gestión de Calidad (ISO 9001), las de Gestión Ambiental (ISO 14001) y las de Gestión de Seguridad y Salud en el trabajo (ISO 45001); la estructura de alto nivel de las normas ISO que permite una terminología común entre las normas; y el enfoque basado en riesgos de la Norma ISO 9001:2015, este proyecto se planteó el objetivo de avanzar, a partir del mencionado enfoque, en la integración de la Norma ISO 27001 a los SIGC.

Palabras clave: *Sistemas Integrados de Gestión de Calidad - Seguridad de la Información - Riesgos*

1. Introducción

Las empresas pertenecientes a la Industria del Software y Servicios Informáticos(SSI) han experimentado un crecimiento sostenido en Argentina en los últimos 20 años. Estudios en relación a este crecimiento [1], [2], [3], [4], [5], dan cuenta que las mismas han optado por implementar Sistemas de Gestión de Calidad (SGC), y certificar Normas de Calidad Internacionales, inicialmente las relacionadas con el desarrollo de Software como la Norma CMMi del Software Engineering Institute(SEI), y posteriormente la Norma ISO 9001 para la calidad de sus procesos. Entre los factores que explican esta adopción se encuentran demandas específicas de sus clientes [6] y el apoyo recibido por el sector a partir de políticas impulsadas a nivel nacional, provincial y municipal [7], [8], [9], [10].

El uso intensivo de Tecnologías de la Información y Comunicaciones(TIC), y los requerimientos de control emanados de normativas a nivel nacional [11], [12] e internacional [13], hacen que estas organizaciones deban cumplir con un nuevo objetivo, asegurar uno de sus activos más importantes: **la información**. Avanzar con la implementación de Sistemas de Gestión de Seguridad de la Información bajo los lineamientos de la norma ISO 27001, puede ayudar a cumplir con este objetivo [14] y es lo que fundamenta la presentación del Proyecto: *Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información (SDRSI), para su integración a Sistemas de Gestión de Calidad.*

La implementación de un SGC basados en Normas, como conjunto de recomendaciones o buenas prácticas, le permite a las organizaciones un marco de referencia para el establecimiento de políticas, objetivos y toma de decisiones oportunas para la mejora de sus procesos. Los SGC contri-

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

buyen a que los procesos de negocio sean repetibles, medibles y auditables, y así proceder a su mejora. El beneficio de los SGC será, además, la mitigación de impactos negativos generados por la materialización de potenciales riesgos como demoras en los procesos, una utilización excesiva de recursos, errores en los productos que se obtienen o servicios que se brindan, que podrían redundar en una disminución en la calidad, efectividad y eficacia con las que opera la organización. Gran cantidad de información interrelacionada configura la base de un SGC que proviene del análisis de los procesos de negocio; productos y servicios como resultado de los procesos; clientes y otros involucrados; recursos humanos, de infraestructura, materiales y de capital; estructura organizativa; entre otros [15]. Un SGC estará en constante cambio, no sólo en cuanto a la información que lo sustenta, cuyos cambios se originarán en función de aquellos que operen sobre cualquiera de los elementos que lo constituyen, sino también por mejoras incorporadas a las Normas y requerimientos de la Industria que obligan a las organizaciones a adaptarse al contexto. La Norma ISO 14001, de Gestión Ambiental, y la Norma ISO 45001 para la Gestión de la Seguridad y Salud en el Trabajo, se han incorporado a los sistemas de Gestión de Calidad, basados inicialmente en las Normas ISO 9001 de Calidad, dando lugar a los denominados Sistemas Integrados de Gestión de Calidad o Sistemas HSEQ, por sus siglas en inglés Health (salud), Safety (seguridad), Environment (Medio Ambiente), Quality (calidad). Hablaremos a partir de aquí de los Sistemas Integrados de Gestión de Calidad (SIGC) aceptando el hecho que las mencionadas normas no son las únicas que deben integrarse para lograr la necesaria mejora en la calidad de una organización, y que la integración de Normas estará en relación de las necesidades de cada industria en particular. Ahora bien, uno de los conceptos que introduce la Norma ISO 9001:2015 es el enfoque basado en riesgos [15], [16], [17] que, para la implementación de un SIGC, induce a definir indicadores para los procesos, valores esperados, metodología de medición y seguimiento, y formas de actuar sobre estos procesos en caso de que los indicadores no cumplan sus valores esperados. Este enfoque basado en riesgos es también una de las alternativas para el tratamiento de los problemas de integridad, confidencialidad y disponibilidad que pueden darse en cuanto a Seguridad de la Información. La propuesta será que el Modelo del SDRSI sirva para la mejora del SIGC incorporando al mismo el diagnóstico de los riesgos de Seguridad de la Información, como paso previo para la integración de la Norma ISO 27001 al SIGC. Serán facilitadores de esta integración no solo la estructura de alto nivel desarrollada por ISO(International Organization for Standardization) [15] y los procesos específicos que la norma ISO 27001 propone, sino la nueva versión de su guía de buenas prácticas ISO 27002 de febrero de 2022, que orienta a que cada organización pueda desarrollar atributos propios posibilitando la integración de la norma con otros marcos de gobierno y de gestión [18]. El planteo de la metodología de modelado del SDRSI estará basada en la vasta propuesta de metodologías existentes centradas en el análisis de riesgos evaluadas por nuestro equipo [19], [20] y que serán objeto de revisión en el proyecto. El insumo fundamental para el SDRSI será la documentación de los procesos organizacionales críticos ya que sus propiedades [21]; Fiabilidad (Reliability), Seguridad Externa (Safety), Seguridad Interna (Security), Desempeño (Performance), Integridad (Integrality) y Disponibilidad (Availability), están directamente relacionadas con los conceptos de Seguridad de la Información. En este sentido será de gran utilidad la metodología de modelización de procesos trabajada anteriormente por nuestro equipo [22]. El modelo del SDRSI deberá contar con la posibilidad de identificación de los activos involucrados en los procesos críticos, clasificación de los mismos y de los riesgos inherentes tanto a los activos como a los procesos, análisis de su severidad, especificación completa, e identificación de alertas que podrán estar basadas en indicadores claves de riesgos (KRI, por sus siglas en inglés Key Risk Indicator), que proporcionen una señal temprana de exposición al riesgo identificado. La implementación del SDRSI estará en relación a las herramientas disponibles. Para ello serán necesarios un relevamiento a las empresas del sector SSI que hayan realizado proyectos de este tipo, como así también de las características de gestores de contenido disponibles en el mercado. Finalmente, será necesario validar que el modelo SDRSI propuesto sirva como disparador de las restantes actividades de la Gestión de Riesgos, alternativas de tratamiento, activación de planes de contingencia, recuperación y continuidad de negocio, y controles de auditoría de los mismos, cuya especificación deberá pasar a ser parte de la documentación de los procesos en el SIGC, completando así la integración del Sistema de Gestión de Seguridad de la Información al SIGC.

2. Implementación de Normas de Calidad en las empresas de la Industria del Software y Servicios Informáticos

A partir del año 2002 las empresas relacionadas a la industria del software y servicios informáticos(SSI) experimentan un crecimiento sostenido en Argentina. Algunos de los factores que explican este desempeño son: una mayor competitividad por la devaluación de principios de 2002, el aumento de la externalización en el desarrollo de software a nivel global, características culturales y contextuales favorables a la inserción externa, como dominio del idioma inglés, husos horarios y disponibilidad de recursos humanos calificados [6]. Entre las políticas públicas que apoyaron este crecimiento se pueden mencionar: la Ley 25.856 del año 2003 [7] que establece que la actividad de produc-

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

ción de Software debe considerarse como una actividad productiva de transformación asimilable a una actividad industrial a los efectos de la percepción de beneficios impositivos, crediticios y de cualquier otro tipo, y la Ley 25.922 [7] de Promoción de la Industria del Software, junto con su Decreto Reglamentario 1593/2004. El régimen de promoción establecía importantes beneficios impositivos y fiscales para quienes acreditaran gastos en investigación, desarrollo y/o procesos de certificación de calidad y/o exportaciones de software. Además obligaba, a partir del tercer año de su vigencia, a cumplir con alguna norma de calidad reconocida aplicable a los productos de software. La Ley 25.922 estableció, además, la creación del Fondo Fiduciario de Promoción de la Industria del Software (FONSOFT), designando como autoridad de aplicación a la Secretaría de Ciencia, Tecnología e Innovación Productiva, a través de la Agencia Nacional de Promoción Científica y Tecnológica. Entre los objetivos se mencionan Programas para la mejora en la calidad de los procesos de creación, diseño, desarrollo y producción de software. La participación de Polos y Clusters de empresas relacionadas al sector de desarrollo de software y servicios informáticos (SSI), en discusiones en distintos niveles y en Foros de Competitividad Nacionales, fue muy importante para el reconocimiento del sector como industria y la promulgación de las mencionadas Leyes. Adquiere relevancia para nuestro proyecto la participación del Polo Tecnológico Rosario, creado en el año 2000 como iniciativa del gobierno municipal y provincial, Universidad Nacional de Rosario, Universidad Tecnológica Nacional, Universidad Austral, Fundación Libertad y algunas empresas, cuyo primer proyecto asociativo, en el año 2005, fue la conformación del primer grupo de empresas de software, para la certificación de normas de calidad CMMI. En la actualidad, el Polo Tecnológico sigue acompañando a empresas del sector para avanzar con certificaciones de la Norma ISO 9001, como lo cita en su página institucional [5]. La Ley 25.922 fue renovada mediante la Ley 26.692 en el año 2011 [8]. Esta ley mejora beneficios impositivos, refuerza las exigencias en cuanto a acreditar dos de las condiciones que establecía la Ley anterior: Acreditación de gastos en actividades de investigación y desarrollo de software, acreditación de una norma de calidad reconocida aplicable a los productos o procesos de software, o el desarrollo de actividades tendientes a la obtención de la misma, y realización de exportaciones de software. A los tres años de su inscripción en el registro, los beneficiarios deberían contar con la certificación de calidad estipulada. En el año 2019, la sanción de la Ley 27.506 [9] de Promoción de la Economía del Conocimiento, mejora el alcance del régimen establecido en la Ley 25.922, extendiéndose la promoción a actividades económicas que impliquen el uso del conocimiento y la digitalización de la información apoyado en los avances de la ciencia y de las tecnologías, a la obtención de bienes, prestación de servicios y/o mejoras de procesos, con los alcances y limitaciones establecidos en la citada ley y las normas reglamentarias que en su consecuencia se dicten. En particular y en relación al sector SSI, la promoción alcanza a los Servicios Informáticos no incluidos en el régimen anterior. Vuelve a mencionarse como requisito para los inscriptos en el régimen, la acreditación de la realización de mejoras continuas en la calidad de servicios, productos y/o procesos, o mediante una norma de calidad reconocida aplicable a sus servicios, productos y/o procesos. La crisis sanitaria generada por COVID-19, iniciada en marzo de 2020, retrasó la entrada en vigencia de la nueva normativa, que vuelve a modificarse por Ley 27.570 del 2021 [10]. Todas estas normativas han impulsado a la incorporación de Sistemas de Gestión de Calidad en las empresas de la Industria SSI.

3. Certificación de Normas ISO

En referencia a la certificación de Normas, la ISO (International Organization for Standardization) realiza una encuesta anual de certificaciones de sus estándares. La encuesta es respondida por los organismos de certificación que han sido acreditados por miembros del Foro Internacional de Acreditación. La Tabla 1 muestra los resultados de la última encuesta disponible publicada en septiembre de 2021 con datos al 31/12/2020 [23].

Como se puede observar las Normas ISO 9001, ISO 14001 e ISO 45001, ocupan los primeros puestos. Esto es así porque se han incorporado a los Sistemas de Gestión de Calidad (ISO 9001), la Normas de Gestión Ambiental (ISO 14001) y las Normas para la Gestión de la Seguridad y Salud en el Trabajo (ISO 45001), dando lugar a los denominados Sistemas Integrados de Gestión de Calidad (SIGC).
La versión de la Norma ISO 9001:2015, vigente en la actualidad, fue puesta en revisión producto de un estudio de opinión lanzado por ISO, que indicó que se debían reforzar algunos de los conceptos de gestión que podían ser abordados desde la perspectiva de la gestión de la calidad, entre ellos: el liderazgo imprescindible de la alta dirección, la consideración del contexto como factor estratégico; el pensamiento basado en el riesgo, como un elemento dinamizador del enfoque a procesos; y la gestión del cambio, como valor diferenciador de la organización en un entorno cada vez más exigente. La Norma incorporó entonces una estructura de alto nivel de forma tal de mantener una estructura común en todas las normas de sistemas de gestión desarrolladas [19], lo que facilita la implementación de los SIGC. Particularmente interesa al Proyecto el enfoque basado en riesgos[19],[20],[21] que introduce la Norma ISO 9001:2015, cuyas directrices, mencionadas anteriormente, están en relación a los principios básicos que plantea ISO 31001:2018 de Gestión de Riesgos. Las Normas ISO 27001 de Gestión

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

Tabla 1. The Iso Survey Of Management System Standard Certifications – 2020

Norma	Total valid certificates	Total number of sites
ISO 9001	916.842	1.299.837
ISO 14001	348.473	568.798
ISO 45001	190.481	251.191
ISO/IEC 27001	44.499	84.181
ISO 22000	33.741	39.894
ISO 13485	25.656	34.954
ISO 50001	19.731	45.092
ISO 20000-1	7.846	9.927
ISO 22301	2.205	4.662
ISO 37001	2.065	5.946
ISO 39001	972	2.341
ISO 28000	520	968

de Seguridad de la Información ocupan el cuarto lugar en el resumen de la encuesta de la Tabla 1, si bien con un número bastante distante a los referidos a las normas anteriores, pero con un crecimiento sostenido en los últimos años (24,7 % si se lo compara con las certificaciones del año 2019) [23].

La Familia de Normas ISO 27000 [18], donde la última versión certificable es la ISO 27001:2013 (con correcciones al 2015), propone un marco para el Sistema de Gestión de la Seguridad de la Información (SGSI), que permite coordinar la definición de políticas, objetivos y alcance de la seguridad de la información en la organización, el análisis, valorización y tratamiento de los riesgos sobre los activos involucrados, los controles a realizar y su monitorización para luego efectuar las mejoras correspondientes. Uno de los factores asociados al crecimiento de su certificación en los últimos años, es que esta norma facilita la implementación de los controles establecidos en la Regulación General de Protección de Datos Europea (GDPR, por sus siglas en inglés: General Data Protection Regulation) [14]. La GDPR [13] tiene su correlato en Argentina en la Ley 25.326 de Protección de Datos personales(LPDP) [11], cuyos principios han permitido el reconocimiento por parte de la Unión Europea(UE) como un país con un nivel de protección adecuada para el tratamiento de los datos. Basado en el artículo 45 de la GDPR, la UE sólo reconoce hasta el momento 14 países no pertenecientes a la misma con el mencionado nivel, siendo Argentina, Uruguay y Canadá, hasta el momento, los únicos países de América reconocidos. Para ello la LPDP debe someterse a revisiones periódicas y acompañar a los constantes cambios que las tecnologías, las personas y los intereses gubernamentales requieran. A partir de esto, se abrirán espacios de debate con organismos públicos, organizaciones de la sociedad civil, universidades y el sector privado, para iniciar el proceso de su modificación [24].

4. Integración de los Sistemas de Gestión de Seguridad de la Información a los Sistemas de Gestión de Calidad

La implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las empresas de la Industria del Software y Servicios Informáticos es vital, visto que tanto el desarrollo de software como la prestación de servicios de tecnologías de información, son actividades directamente relacionadas al manejo de datos y esto les genera obligaciones de cumplimiento de las citadas reglamentaciones LPDP y GDPR. En este sentido y considerando que aquellas empresas que han optado por la implementación de Sistemas de Gestión de Calidad(SGC) o Sistemas Integrados de Gestión de Calidad(SIGC) han desarrollado la documentación de sus procesos en el marco de la Norma ISO 9001, solo resta alinear dicha documentación a los procesos planteados por la Norma ISO 27001.

Como se mencionó anteriormente, el enfoque basado en riesgos [16], [15], [17] que introduce la Norma ISO 9001:2015 está en relación al enfoque que plantea la ISO 31000:2018 específica de Gestión de Riesgos y no dista del enfoque que plantea la ISO 27001 en cuanto a las alternativas para el tratamiento de los problemas que pueden darse en torno a la Seguridad de la Información. El siguiente paso para la implementación de un SGSI, una vez definidas las políticas de seguridad de la información por parte de la organización, será la Identificación de Riesgos para luego proceder a las restantes actividades que configuran su gestión. Del análisis bibliográfico realizado al momento [20], [19], se pueden diferenciar dos líneas metodológicas para la identificación de riesgos, ambas comparten la característica de utilizar taxonomías, por un lado las orientadas a la identificación de las fuentes de riesgos en función de la actividad desarrollada, y por el otro las que desarrollan un inventario de activos a partir de los cuales establecer

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

la identificación. Entre las primeras, se puede mencionar la Taxonomía de riesgos operacionales del Software Engineering Institute [25], que organiza las fuentes de riesgos en cuatro clases: Acciones (o inacción) de las personas: realizadas tanto deliberada como accidentalmente, Fallas de los sistemas y tecnología: fallas del hardware, software y sistemas de información, Fallas de los procesos internos: problemas en los procesos internos del negocio que impactan en la habilidad para implementar, gestionar y sostener a la seguridad, y Eventos externos: cuestiones fuera del control de la organización. También puede incluirse en esta línea la Guía de Buenas Prácticas ISO 27002:2022. Cabe destacar la reestructuración y actualización de los controles de esta nueva versión que agrupa los mismos en: Personas, Organización, Tecnológicos y Físicos; y asocia atributos a cada control. Entre estos atributos se pueden mencionar tipos de control: preventivos, detectivos y correctivos; requisitos de la información: Confidencialidad, Integridad y Disponibilidad; Conceptos de Ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar. Estos conceptos de Ciberseguridad propuestos por NIST (National Institute of Standards and Technology) en conjunto con la incorporación de controles como cobertura de seguridad para computación en la nube, eliminación de información, enmascaramiento de datos, prevención de fuga de datos, inteligencia de las amenazas y cuestiones relacionadas a la producción de software como Codificación segura, están alineados con el estado actual del arte de la seguridad informática específicamente. La segunda línea metodológica para la identificación de riesgos es la basada en el inventario de activos, entre las cuales se pueden mencionar MAGERIT V3 y OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) donde la forma de analizar los activos para determinar los riesgos puede visualizarse en los gráficos 1[1] y 2[2] respectivamente.

Para cualquiera de las dos alternativas de identificación de riesgos, y siguiendo el lineamiento de la ISO 27001, se tendrá como producto un inventario de activos. Un activo, en el contexto de la seguridad de la información, es cualquier cosa que tenga valor para la organización. Las clasificaciones de los activos varían en las propuestas analizadas [19], [20], aunque la mayoría distingue: Hardware, Software, Información, Infraestructura, Recursos Humanos y Servicios. Habiendo identificado los activos será necesario identificar las amenazas que pueden actuar sobre dichos activos, y las vulnerabilidades que pueden ser aprovechadas por las mismas, generando un daño sobre el activo y por consiguiente afectando al proceso. Basadas en la identificación de activos, las taxonomías hacen mención a amenazas (MAGERIT), perfiles de amenaza (OCTAVE) o comunidades de amenazas (FAIR- Factor Analysis Information Risk). Todos ellos intentan establecer subconjuntos de la población total de amenazas que comparten características claves y proponen metodologías para la identificación y clasificación de las mismas. Identificado el riesgo inherente al activo dentro del proceso se debe proceder al cálculo de su severidad. La severidad del riesgo estará dada por el valor de reposición del activo dañado y la probabilidad de ocurrencia del riesgo. Entre las propuestas para esta actividad, FAIR [26], [27], [28], es la más completa y su desagregado se muestra en el Gráfico 3.

El valor de los activos de información variará de una organización a otra, no sólo en relación al tamaño de la misma sino al rol que desempeñen estos activos en los procesos para la entrega de un servicio o desarrollo de un producto en particular. Las taxonomías deberán ser revisadas con el objetivo de analizar si están en relación a la evaluación de riesgos que plantean las tecnologías en constante cambio y el nivel de conocimiento de los atacantes [29].

La posibilidad de la integración del conjunto de actividades mencionadas referidas a la Gestión de los Riesgos en el marco del SGSI a los SIGC, según nuestra propuesta, estará dada por la posibilidad de modelizar un sistema de diagnóstico de riesgos de seguridad de la información basado en la documentación existente en el SIGC. Esta documentación deberá permitir, a partir de la identificación de procesos de gestión o estratégicos, procesos críticos [21] que hacen a la operatoria de la organización y procesos que dan soporte a los mismos, la elaboración del inventario de activos como punto de partida para el diagnóstico de riesgos. En particular, nos interesa la posibilidad de que esa documentación se encuentre desarrollada con alguna notación gráfica como BPMN (Business Process Model Notation) o Diagramas SIPOC (por sus siglas en inglés Suppliers, Inputs, Process, Output, Customers), también llamados diagramas de tortuga por su semejanza al animal. En nuestra experiencia [22], las herramientas gráficas para el mapeo de procesos son de gran ayuda para analizar las interrelaciones entre los mismos.

[1]Fuente: https://administracionelectronica.gob.es/ctt/magerit

[2]Fuente: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

Gráfico 1. MAGERIT

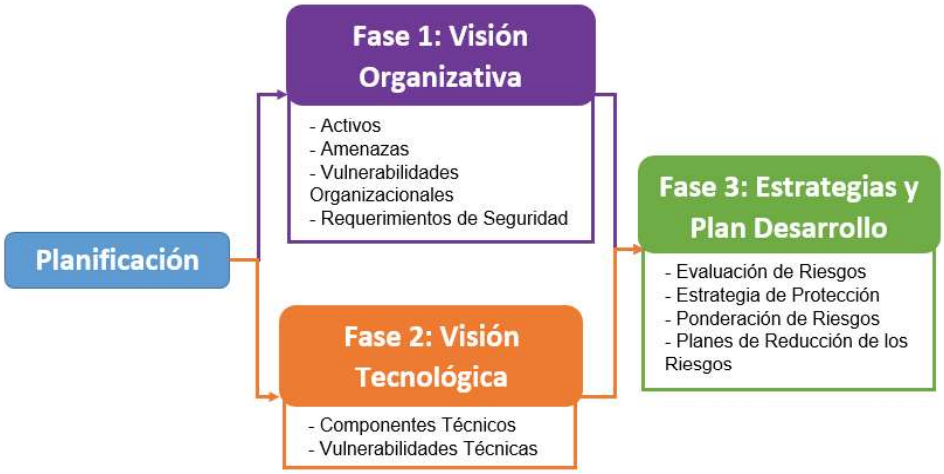

Gráfico 2. OCTAVE

5. De la Presentación del Proyecto

La presentación del Proyecto: **Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información (SDRSI) para su integración a Sistemas de Gestión de Calidad**, como se ha mencionado a lo largo de este trabajo, tiene sus antecedentes en temáticas abordadas por el equipo en los Proyectos de Universidad: Observatorio Regional de Desarrollo de la Ingeniería en Sistemas de Información e Informática (IISI.d.Ro) [1], Modelización de un Observatorio de Desarrollo Productivo. Industria de Software y Servicios Informáticos en el Área Rosario [22] y Desarrollo de un Modelo de Gestión por Procesos enfocado en cadenas de valor en instituciones universitarias públicas. Caso FR Rosario-UTN [22], como así también en el proyecto de Facultad: Seguridad de la Información [20] que se utilizó como base para el desarrollo de una la unidad temática: Seguridad y Auditoría que se dicta actualmente en la asignatura Administración de Recursos integradora del 4to. nivel de la carrera de Ingeniería en Sistemas de Información de la UTN Facultad Regional Rosario [19]. La selección de cuestiones de interés en relación a la Industria del software y Servicios Informáticos(SSI) radica en la pertenencia de los integrantes del Proyecto a la carrera de Ingeniería en Sistemas de Información de la Facultad Regional Rosario, entre los que contamos con académicos y graduados con experiencia tanto en investigación como en la profesión específica.

Para el desarrollo del Modelo del Observatorio [2], 23 empresas del Sector de la Industria SSI de la ciudad de Rosario fueron encuestadas. Una de las temáticas abordadas, y definidas por el Proyecto Integrador, se enfocó en aspectos relacionados con el cambio y la innovación en la orga-

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

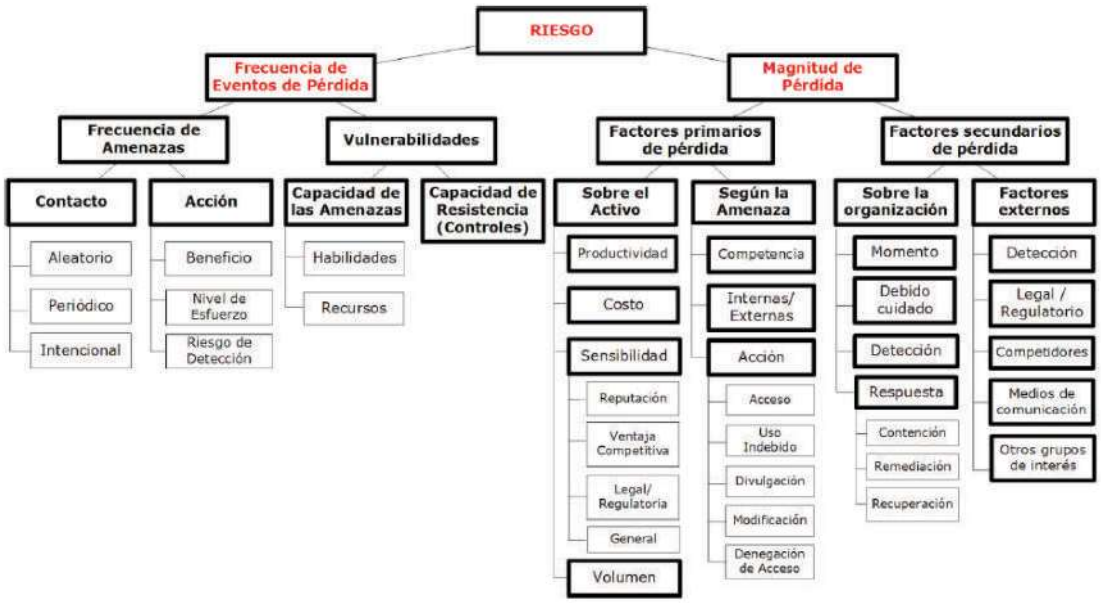

Gráfico 3. Taxonomía FAIR (Factor Analysis for Information Risk)

nización, donde se incluyó la consulta sobre Certificación de Normas. Del análisis de la encuesta pudimos observar que un 74 % de las empresas había certificado alguna norma de calidad y que esto estaba en relación a los requisitos impuestos para ser consideradas empresas incluidas en la Ley de Promoción de la Industria del Software [7]. Sobre este aspecto se tienen los resultados que se exponen en el Gráfico 4. Además, al ser consultadas las empresas por este tema, muchas de ellas expusieron que, habiendo certificado Normas CMMi, decidieron la Certificación de Normas ISO 9001, visto que las anteriores exigían un esfuerzo que no se traducía en una mejora de la visibilidad de sus productos. Se observa además en el gráfico una incipiente referencia a la Norma ISO 27001. Teniendo en cuenta la preocupación por la implementación de Sistemas de Gestión de Seguridad de la Información planteada por los referentes de la Industria SSI, en un relevamiento preliminar realizado, y considerando que las empresas continuaron con la implementación y, en algunos casos, certificación de la Norma ISO 9001 [5], nos planteamos el objetivo de analizar qué podíamos aportar en referencia a la temática. A partir de allí avanzamos en la identificación de las actuales políticas públicas referidas a la Industria SSI, en el análisis de las certificaciones a nivel mundial publicadas por ISO y de las características que llevaron a la definición de una estructura de alto nivel para facilitar la implementación y certificación de los Sistemas Integrados de Gestión de Calidad (SIGC). Observando el crecimiento en la certificación de la Norma ISO 27001 y considerando la relación de éste con los requerimientos impuestos por la Regulación General de Protección de Datos (GDPR: General Data Protection Regulation) [13] que afectan en nuestro caso a empresas que deciden exportar, y que dichos requerimientos pueden asimilarse a la normativa definida por nuestra Ley 25326 de Protección de Datos Personales [11] encontramos fundamento a la preocupación planteada. Continuamos entonces con el análisis específico de la Norma 27001 advirtiendo la publicación de la nueva versión de su Guía de Buenas Prácticas: ISO 27002:2022, cuya estructura y controles están alineados con el estado actual del arte de la seguridad informática específicamente. Considerando que esta modificación de la guía llevará a la necesidad de desarrollar una nueva versión de la Norma ISO 27001, y que ésta estará guiada por estructura de alto nivel definida por ISO y por uno de los conceptos que refuerza: el enfoque basado en riesgos, encontramos en este enfoque una alternativa para la integración de la norma a los Sistemas Integrados de Gestión de Calidad. A partir de esto, fueron importantes las revisiones bibliográficas en relación a los conceptos de Seguridad de la Información realizadas anteriormente [19], [20], para avanzar, no solo con el análisis del estado del arte de la temática, que continúa en revisión, sino con las características que se deberán contemplar para el desarrollo del modelo y las expectativas a futuro de su implementación.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

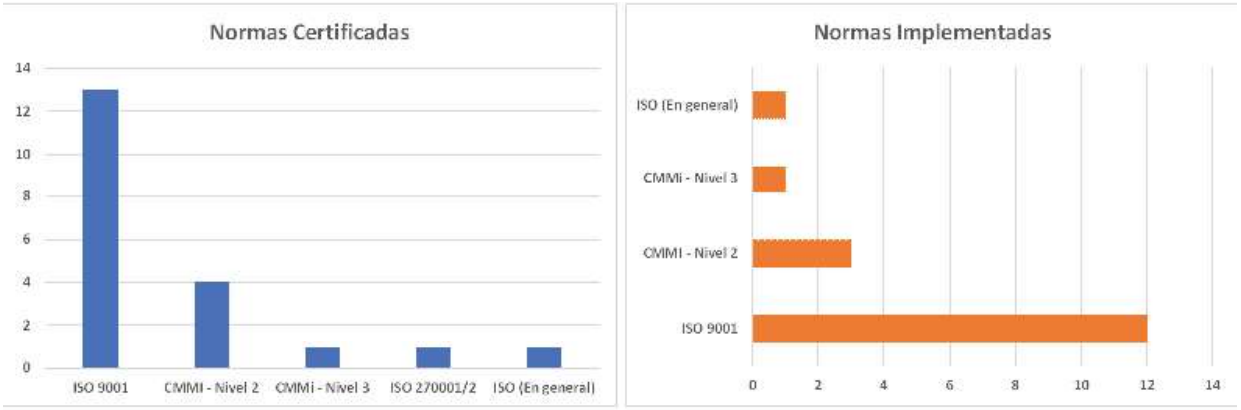

Gráfico 4. Aspectos Relacionados con el cambio y la innovación - Certificación de Normas

6. Trabajo a futuro y Conclusiones

Avanzar, a partir de la idea fundacional del Proyecto, nos lleva por un lado al necesario relevamiento detallado de la modalidad que han optado las empresas del Sector SSI para la implementación de sus SGC o SIGC ya que como se mencionó, la documentación de los procesos es esencial como insumo para el desarrollo del modelo del SDRSI. Por otro lado, la identificación y caracterización de los Gestores de Contenido para el resguardo de la documentación, la existencia de guías, metodologías, técnicas y herramientas que hayan sido utilizadas para implementar, mantener, auditar y mejorar los SGC o SIGC permitirán analizar la posibilidad de validación del modelo en su operación. Además, una vez identificada la viabilidad de obtención de los insumos, la definición de los requerimientos de información del SDRSI, sus interrelaciones y salidas deberán estar en relación a la posibilidad de cumplir con uno de los controles de la ISO 27002:2022 que creemos es el que guía la necesario ciclo de mejora que deberá tener el modelo: *inteligencia de las amenazas*. Este control o concepto clave de la ciberseguridad conlleva a examinar los datos en su contexto para permitir una correcta toma de decisiones. Para finalizar y como integrantes de la comunidad educativa de la carrera de Ingeniería en Sistemas de Información, creemos muy importante el abanico de posibilidades que abre el Proyecto. Desde la posibilidad dada por la transferencia de los conocimientos que se podrán adquirir, la de formación de Recursos Humanos en I+D&i fomentando la participación de docentes, graduados y alumnos, tanto como integrantes iniciales del proyecto, como los que se vayan incorporando a partir de las acciones del mismo fortaleciendo la función de investigación del Departamento de Ingeniería en Sistemas de Información hasta el aporte para el desarrollo de material de estudios de la asignatura Seguridad de la Información, prevista para el nuevo Plan de la carrera de Ingeniería en Sistemas de Información, próximo a implementarse en la Universidad Tecnológica Nacional

Referencias

[1] "Proyecto: Observatorio regional de desarrollo de la ingeniería de sistemas de información e informática (IISI.d.r.O)." Código: TOTUNAV0004307 Vigencia: Del 1/4/2016 al 31/03/2019. Universidad Tecnológica Nacional – Facultad Regional Rosario.

[2] "Proyecto: Modelización de un observatorio de desarrollo productivo. industria de software y servicios informáticos en el Área Rosario." Código: UTN1923. Vigencia: 1/1/2013 al 31/12/2015. Universidad Tecnológica Nacional – Facultad Regional Rosario.

[3] F. M. Riva, E. Amar, V. Martín, E. Porta, C. Galmarini, y M. Puyo, "Modelización de un observatorio de desarrollo productivo. industria del software y servicios informáticos en el Área de rosario. informe técnico 1: Relevamiento a empresas del sector ssi.," *Presentación Avance del Proyecto - IV Jornada del Programa de Tecnología de las Organizaciones*, 2014.

[4] F. M. Riva, E. Amar, V. Martín, y E. Porta, *El Sector Industrial y Empresario de la Industria del Software y Servicios Informáticos (SSI) en el área de Rosario*, vol. 7, pp. 91–94. Secretaría de Ciencia, Tecnología y Posgrado de la UTN-FRA, 2015.

[5] "Polo tecnológico rosario. historia y actualidad." `https://polotecnologico.net/`. Última fecha de acceso: 05/10/2022.

[6] F. Barletta, M. Pereira, G. Yoguel, y V. Robert, "Argentina: dinámica reciente del sector de software y servicios informáticos," *Revista Cepal*, 2013.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

[7] "Estrategia de agenda digital de la republica argentina: Ley 25856." https://www.argentina.gob.ar/normativa/nacional/ley-25856-91606/normas-modifican/. Última fecha de acceso: 05/10/2022.

[8] "Registro de apoderados del regimen de promocion de la industria del software - creacion: Ley 26692." https://www.argentina.gob.ar/normativa/nacional/ley-26692-185701/normas-modifican/. Última fecha de acceso: 05/10/2022.

[9] "Regimen de promocion de la economia del conocimiento: Ley 27506." https://www.argentina.gob.ar/normativa/nacional/ley-27506-324101/normas-modifican/. Última fecha de acceso: 05/10/2022.

[10] "Regimen de promocion de la economia del conocimiento: Ley 27570 - modifica ley 27506." https://www.argentina.gob.ar/normativa/nacional/ley-27570-343520/normas-modifican/. Última fecha de acceso: 05/10/2022.

[11] "Ley de protección de datos personales (habeas data): Ley 25326." https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/normas-modifican/. Última fecha de acceso: 05/10/2022.

[12] G. Allonca, J. CRUZ, y E. Ruiz Martínez, "Cloud computing: la regulación de la transferencia internacional de datos personales y la prestación de servicios por parte de terceros," dossier habeas data, Sistema Argentino de Información Juridica. Ministerio de Justicia y Derechos Humanos. Argentina, 2020. pp. 214-221.

[13] "General data protection regulation." https://gdprinfo.eu/, 2016. Última fecha de acceso: 05/10/2022.

[14] I. M. Lopes, T. Guarda, y P. Oliveira, "How ISO 27001 can help achieve GDPR compliance.," vol. 14, pp. 1–6, Iberian Conference on Information Systems and Technologies (CISTI), IEEE, June 2019.

[15] J. M. P. Álvarez y N. C. Morales, "Guía práctica para la integración de sistemas de gestión. iso 9001, iso 14001 e iso 45001," 2018. AENOR - Asociación Española de Normalización y Certificación.

[16] J. A. G. Martínez, "Guía para la aplicación de une-en iso 9001: 2015," 2015. AENOR - Asociación Española de Normalización y Certificación.

[17] I. Akkiyat y N. Souissi, "Modelling risk management process according to iso standard," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, pp. 5830–5835, 2019.

[18] "Documentación publicada hasta el momento por iso directamente relacionada con los requisitos de la norma iso/iec 27001. guías de referencia útiles para la implantación, mantenimiento, auditoría y certificación de los sistemas de gestión de la seguridad de la información(2022)." https:////www.iso27000.es/iso27000.html. Última fecha de acceso: 05/10/2022.

[19] F. M. Riva, "Revisión Bibliográfica realizada para el desarrollo de la Unidad 2: Seguridad y Auditoría. Cátedra: Administración de Recursos - Ingeniería en Sistemas de Información - UTN-FRRO." https://frro.cvg.utn.edu.ar/course/view.php?id=25#section-2/. Última fecha de acceso: 05/10/2022.

[20] "Proyecto: Seguridad de la Información en el ámbito de la UTN-Facultad Regional Rosario." Vigencia: 1/1/2012 al 31/12/2012. Universidad Tecnológica Nacional – Facultad Regional Rosario.

[21] H. Mijares, D. Marizé, M. Mendoza, y E. Luis, "Conceptual model for the specification of the quality properties of the critical business process," vol. 8, pp. 1–6, Iberian Conference on Information Systems and Technologies (CISTI), IEEE, June 2013.

[22] "Proyecto: Desarrollo de un modelo de gestión por procesos enfocado en cadenas de valor en instituciones universitarias públicas. caso fr rosario-utn." Código: UTN1893 - Vigencia: 1/1/2013 al 31/12/2015. Universidad Tecnológica Nacional – Facultad Regional Rosario.

[23] "The iso survey of management system standard certifications – 2020." https:////www.iso.org/the-iso-survey.html. Última fecha de acceso: 05/10/2022.

[24] "Nuevo proyecto de ley de protección de datos personales." https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales. Última fecha de acceso: 05/10/2022.

[25] J. J. Cebula, M. E. Popeck, y L. R. Young, "A taxonomy of operational cyber security risks version 2," tech. rep., 2014.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

[26] G. Wangen, C. Hallstensen, y E. Snekkenes, "A framework for estimating information security risk assessment method completeness," *International Journal of Information Security*, vol. 17, no. 6, pp. 681–699, 2018.

[27] J. Jones, "An introduction to factor analysis of information risk (fair)," *Norwich Journal of Information Assurance*, vol. 2, no. 1, p. 67, 2006.

[28] J. Freund y J. Jones, *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann, 2014.

[29] A. Shameli-Sendi, R. Aghababaei-Barzegar, y M. Cheriet, "Taxonomy of information security risk assessment (isra)," *Computers & security*, vol. 57, pp. 14–30, 2016.