TRABAJO FINAL INTEGRADOR

Marco de trabajo estructurado para la seguridad de la información en servidores Web basado en estándares internacionales

EMISI

Especialización en Ingeniería en Sistemas de Información

Universidad Tecnológica Nacional

Facultad Regional Santa Fe

Autor: Ing. Simón A. Cifre

Director: Dr. Jorge M. Roa.

Año 2018

Resumen

Las áreas de seguridad de la información de las organizaciones realizan actividades en pos de la protección de sus activos de información, las cuales en muchos casos no disponen de una estructura de procesos asociada, impidiendo de cierta forma tomar las mejores decisiones posibles en beneficio de los objetivos del área como la reducción de vulnerabilidades y la prevención de ataques informáticos.

La seguridad debe establecerse mediante normas de funcionamiento y uso, para garantizar la protección y disponibilidad de la información, de la infraestructura computacional y de los recursos informáticos.

Garantizar un nivel de seguridad total es imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

El objetivo del presente TFI es definir un marco de trabajo estructurado que permita hacer uso eficiente de técnicas, herramientas y estándares de seguridad de la información para servidores Web a fin de lograr confidencialidad, integridad y disponibilidad de datos y servicios. El propósito es proponer buenas prácticas que colaboren con la implementación de un sistema de gestión de seguridad de la información organizacional, adaptado al Estándar O-ISM3, certificable con el Estándar internacional ISO/IEC 27001 y aplicable a todo tipo de organizaciones.

La metodología utilizada para el desarrollo del trabajo es prescriptiva, que permite seguir una serie de pasos detallando el proceso operacional de la gestión de parches, así como la documentación técnica, las posibles métricas asociadas, la relación existente entre estándares y el ciclo de vida asociado a la gestión de

vulnerabilidades de servidores; logrando de esta forma, establecer como modelo un marco estructurado para la seguridad de la información en servidores Web basado en estándares internacionales.

Contenido

Resumen **2**

Contenido **3**

1. Introducción **5**

2. Contexto **8**

2.1. Seguridad Informática 8

2.2. Ataque Informático 9

2.3. Estándares 10

3. Estándar ISO/IEC 27000 **12**

3.1. Clasificación 13

3.2. Certificación 14

3.3. Herramientas de Software 16

3.4. Gestión de vulnerabilidades 17

3.5. Beneficios 20

3.6. Limitaciones 21

4. Estándar O-ISM3 **22**

4.1. Modelo O-ISM3 22

4.2. Clasificación 24

4.3. Procesos de Gestión Operacional 25

4.4. OSP-5 Actualizaciones de Seguridad 26

4.5. Documentación 28

4.6. Especificación de Métricas 28

4.7. Beneficios 30

4.8. Limitaciones 30

5. Marco de trabajo para la seguridad de la información en Servidores Web **31**

5.1. Gestión de roles de Usuarios 32

5.2. Gestión de vulnerabilidades 32

5.3. Gestión de documentación 35
5.4. Monitoreo de seguridad de información en servidores Web 39
5.5. Beneficios 40

6. Conclusiones **41**

7. Trabajos Futuros **43**

8. Referencias bibliográficas **44**

Anexo I - Definiciones **47**

Anexo II - Documentación **49**

II.1. Documento de procesador de texto 49
II.2. Documento de hoja de cálculo 50

1. Introducción

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos [1].

Las organizaciones se apoyan cada día más en las tecnologías para sus negocios y desarrollan gran parte de su actividad conectadas a Internet o haciendo uso de servicios que utilizan Internet como medio de comunicación. La mayoría de ellas, independientemente de su tamaño, disponen de un sitio Web para divulgar por Internet su negocio, su identidad, su imagen, sus productos o servicios, entre otros [2]. A su vez, Internet presenta un número enorme de usuarios que frecuentemente utilizan el navegador para buscar información, hacer transacciones o pagos online, compras, leer los periódicos, acceder a una red social o revisar una cuenta de correo electrónico. De este modo, los servidores Web son el principal blanco de ataque que presentan los Sistemas de Información de una organización, por lo que es imprescindible contar con un conjunto de técnicas y herramientas de seguridad dedicadas exclusivamente a la seguridad de la información de los servidores Web, como así también métodos y estrategias para gestionar y controlar los activos y sus servicios [3].

La era digital ha impuesto nuevos retos a las organizaciones incluyendo la seguridad de su información e infraestructura. Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Las amenazas avanzan de forma exponencial y si no se establecen marcos estructurados para gestionar la seguridad se hace más difícil que las organizaciones

las combatan efectivamente [4]. En un futuro no tan lejano, mejores prácticas como el Estándar ISO/IEC 27000 seguramente se convertirán en un estándar obligatorio para todas las organizaciones [3].

La serie de certificaciones ISO/IEC 27000 abarcan un amplio abanico respecto a la seguridad de la información. Dentro de esta serie, la dos más importantes y conocidas son ISO/IEC 27001 e ISO/IEC 27002. La norma ISO/IEC 27001 establece la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) como forma de salvaguardar la red de información que contiene la organización. ISO/IEC 27002 es un Estándar para la seguridad de la información que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener un sistema de gestión de la seguridad de la información [5].

La seguridad de la información se define en el Estándar ISO/IEC 27000 como un sistema automatizado de información a fin de lograr los objetivos aplicables de preservación de la confidencialidad, integridad y disponibilidad [6]. Los objetivos de ISO/IEC 27000 son: (1) Preservación de la Confidencialidad para asegurar que sólo quienes estén autorizados pueden acceder a la información; (2) Integridad, para asegurar que la información y sus métodos de proceso son exactos y completos; (3) Disponibilidad, para asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran y de manera oportuna.

El inconveniente que presenta este Estándar es que no ofrece un guía de estricto seguimiento para la protección de activos, sino que otorga en su lugar un "marco de actuación" que orienta a la organización sobre la forma de actuar ante una amenaza. Esto puede suponer cierta dificultad para las organizaciones porque se ofrece solo un modo de pensar que sienta las bases sobre la manera de gestionar los riesgos y los activos, y no presentan una lista de cumplimiento obligado [6].

Por otro lado, encontramos el modelo O-ISM3 que es un Estándar de madurez de seguridad de la información orientado a procesos, adaptable a cualquier tipo de

organización y compatible con la implantación de ISO/IEC 27001 [7]. Este Estándar permite que las organizaciones puedan focalizarse sobre la adecuada administración de políticas, procesos, métricas y controles de seguridad para mitigar los riesgos sobre sus activos de información. A diferencia de ISO/IEC 27001, presenta un enfoque por niveles donde en el nivel operacional, se especifican procesos técnicos particulares que indican aplicaciones de estricto cumplimiento para la implementación.

De este modo, el objetivo del presente TFI es definir un marco de trabajo estructurado que permita hacer uso eficiente de técnicas, herramientas y estándares de seguridad de la información para servidores Web a fin de lograr confidencialidad, integridad y disponibilidad de datos y servicios dentro de un ambiente seguro. El propósito es proponer buenas prácticas que colaboren con la implementación de un sistema de gestión de seguridad de la información organizacional, adaptado al Estándar O-ISM3, certificable con el Estándar internacional ISO/IEC 27001 y aplicable a todo tipo de organizaciones.

A continuación, se detalla la estructura del presente informe. La Sección 2 detalla el estado actual de la seguridad informática, los ataques informáticos existentes y la importancia de aplicar y/o certificar estándares en las organizaciones. La Sección 2 presenta la clasificación de la norma, su certificación, beneficios y limitaciones que lo caracterizan. La Sección 3 muestra el modelo de madurez O-ISM3 con su segregación en cuanto a procesos operacionales y particularmente, el proceso de actualizaciones de seguridad, además de sus beneficios y limitantes. La Sección 4 detalla el marco de seguridad con sus características propuesto en el presente informe de TFI. A continuación, la Sección 5 concluye sobre la propuesta del modelo con sus beneficios. Finalmente, la Sección 6, presenta un detalle de los trabajos futuros.

2. Contexto

2.1. Seguridad Informática

La Seguridad Informática es un estado de cualquier tipo de información que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo [8]. La seguridad informática se obtiene a partir de la Seguridad de la Información, que tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada [8].

Para la mayoría de los expertos, el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe presentar tres características principales: Integridad, Confidencialidad y Disponibilidad [8]. La normativa NIST (National Institute of Standards and Technology), incorpora además de estos tres conceptos, otros dos como características principales: Autenticidad, y Auditoria y Registros.

La seguridad de la información se logra mediante la implementación de un apropiado sistema de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software, principalmente [9]. Estos controles necesitan ser establecidos para asegurar que los objetivos específicos de seguridad se cumplan. Para analizar la seguridad de un sistema se debe pensar en la forma en que el mismo pudiera sufrir determinada pérdida o daño, para lo cual es necesario identificar las debilidades del sistema [8].

El objetivo principal de la seguridad de la información es proteger los activos de información que están asociados directamente con los elementos que integran un sistema informático, haciendo frente a los distintos tipos de ataques informáticos que personas malintencionadas realizan.

2.2. Ataque Informático

Un ataque informático es un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red. Los ataques en grupo normalmente son hechos por bandas llamados "piratas informáticos" que suelen atacar para causar daño, por malas intenciones, por espionaje, para ganar dinero, entre otras. Los mayores ataques suelen pasar en corporaciones [10].

Un ataque informático consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización [10].

Existen numerosos casos a nivel mundial de importantes y prestigiosas organizaciones que fueron víctimas de ataques informáticos, filtrados mediante vulnerabilidades en los sistemas operativos o software instalado en los activos (equipos y/o servidores). Los ataques más comunes permiten la ejecución de código remoto sobre el equipo infectado, robo de datos, denegación de servicios, eliminación o modificación de ficheros y cifrado de archivos.

En los últimos años, se destacaron ataques de malware llamado Ransomware. Los ataques Ransomware normalmente infectan un ordenador cuándo un usuario abre un email Phishing, utilizando técnicas de ingeniería social para convencer a estos usuarios de descargar archivos o abrir enlaces Web [11]. En ambos casos, el virus se descarga y ejecuta localmente en el equipo. Una vez instalado, cifra todos los archivos y el disco del equipo en un formato ilegible, y además tiene la capacidad para extenderse a través de redes locales y anfitriones remotos que no hayan recibido la actualización de seguridad, y de esta manera infecta directamente cualquier sistema

expuesto. Posteriormente, intenta obtener un pago de rescate a cambio de desbloquear el acceso a su computadora, servidor o archivo [12].

Existen numerosas técnicas de seguridad de la información recomendadas como medidas preventivas frente a los ataques informáticos. Entre ellas, se destaca la actualización de los sistemas operativos y software de los equipos informáticos de forma regular, dentro de un esquema controlado y regulado que permita la correcta gestión de los servidores y activos de la organización. Los cibercriminales explotan las vulnerabilidades del software para comprometer los sistemas, por los que expertos en seguridad deben utilizar herramientas de evaluación de vulnerabilidades y de gestión de parches, para mantener los sistemas actualizados. Además, se debe seguir un procedimiento estandarizado, con documentación pertinente que permita optimizar los procedimientos operativos y que generen un resultado de valor para los niveles tácticos y gerenciales de la organización.

2.3. Estándares

Los estándares son documentos técnico-legales que contienen especificaciones técnicas de aplicación voluntaria, aprobados por un organismo nacional, regional o internacional de normalización reconocido. Son elaborados por consenso de las partes interesadas: fabricantes, administraciones, usuarios y consumidores, centros de investigación y laboratorios, asociaciones, agentes sociales, entre otros, basados en los resultados de la experiencia y el desarrollo tecnológico [13].

Los estándares permiten implantar de forma clara y precisa métodos y formas de trabajo concretos, que siguen un procedimiento definido. Con esto, las organizaciones que lo implementen pueden obtener ventajas competitivas ya que mejora la eficiencia y aumenta el potencial organizacional, previene errores humanos y puede derivar en ahorros económicos [13].

Los estándares de seguridad de la información, en particular, aportan los siguientes beneficios: uso de mejores prácticas en materia de seguridad, contribución a la madurez de los procesos organizacionales, conjunción de distintos enfoques con un objetivo común, desarrollo y aplicación de experiencia acumulada, y creación de un marco de trabajo [13].

Existen estándares certificables por una organización. Para esto, la organización debe demostrar que cumple con todos los requisitos impuestos por la entidad certificadora.

Certificar un estándar puede significarle a la organización un reconocimiento en cuanto a su forma de trabajo, como así también, la posibilidad de mejorar su imagen frente a los propios empleados y clientes dado que le transmite confianza, generando una diferenciación frente a sus competidores y mayores oportunidades de negocio.

3. Estándar ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña [5].

Esta es una serie compuesta por distintas normas que tienen por objetivo proporcionar a cualquier organización un conjunto de buenas prácticas para la gestión de la seguridad de su información, y se indica ésta cómo puede implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001 como forma de salvaguardar la red de información que contiene [5].

ISO/IEC 27000 es de carácter internacional, aplicable a todo tipo de organizaciones y entidades, y en un mundo que cada vez posee mayor cantidad de amenazas a nivel informático, se está convirtiendo en imprescindible para la seguridad de las organizaciones [6].

El beneficio general y más importante de implementar ISO/IEC 27000 de forma consciente y planeada, es apoyar los objetivos estratégicos del negocio organizando el mismo a través de la gestión efectiva de la seguridad de la información, ya que se definen procesos, responsables y actividades a seguir dentro de la organización, lo cual implica que cada quién sepa lo que debe hacer en cada situación [14].

ISO e IEC han continuado, y continúan aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie [5].

3.1. Clasificación

La serie ISO/IEC 27000 se clasifica de acuerdo a las distintas características que se consideran en la implementación de un sistema de gestión de seguridad de la información, como se observa en la Figura 1. Las normas de la serie que son interés, en este informe de TFI son las siguientes:

- ISO/IEC 27000: Norma que proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de la importancia sobre la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI [5].
- ISO/IEC 27001: Norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Es la única norma de la serie que es posible certificar. Actualmente, la última edición de este Estándar es de 2013 y se encuentra en inglés y en francés [5]. En Argentina, el instituto IRAM avalado por ISO e IEC, publicó su traducción al español en 2014.
- ISO/IEC 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. La última edición disponible es de 2013 y presenta un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés [5].

Figura 1 - Serie ISO/IEC 27000

3.2. Certificación

La única norma certificable dentro del Estándar es la ISO/IEC 27001. El hecho de certificar la ISO/IEC 27001 le otorga a la organización una mejora de su imagen ante los propios empleados y clientes dado que les transmite confianza sobre la protección de los datos depositados en la misma. Además, generan confianza frente a sus clientes, ya que les hacen ver a los mismos, que cuentan con las políticas requeridas para proteger su información frente a las amenazas actuales [6].

Hay sectores de actividades, en los que a la hora de elegir socios se tiene en cuenta la posesión o no de la certificación ISO/IEC 27001, por lo que contar con tal certificado le da la reputación de ser un socio seguro y protegido. Algunas organizaciones afirman, que la certificación ISO/IEC 27001 le ha permitido aumentar

sus beneficios, así como reducir de forma notable sus gastos operativos consecuencia de introducir procesos de revisión en su gestión [6].

Cuando se establece un SGSI en una organización no es obligatorio certificarlo, sin embargo, es recomendable.

En primer lugar, es fundamental elegir bien la empresa certificadora, que debe estar reconocida internacionalmente. Una vez elegida, esta enviará un auditor a la organización con el que mantendrá una relación de varios años. Es de gran ayuda que los auditores estén familiarizados con la industria de la organización, ya que podrán detectar mejor cualquier brecha de seguridad y ofrecerle consejos más detallados y apropiados [15].

El proceso de certificación consta de tres etapas [15]:

- Revisión de la documentación.
- Auditoría de la información. El auditor verificará la aplicación del SGSI.
- Obtención del certificado.

Conseguir la certificación puede tardar, dependiendo del tamaño de la organización, entre tres meses y un año. Una vez conseguido, tendrá una validez de tres años. La entidad certificadora podría retirarle la certificación si detecta algún incumplimiento de la norma durante esos 3 años, por ello se debe seguir revisando el SGSI constantemente. No existe un criterio único para implementar esta norma internacional, pero sí una serie de directrices que de seguirlas llevarán a conseguir un buen resultado [15]. Si bien el Estándar presenta un conjunto numeroso de controles, no es obligatoria la implementación de todos ellos sino de algunos de manera individual. En este caso, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados [5].

3.3. Herramientas de Software

Existen múltiples fabricantes de software enfocados en la seguridad de la información que ofrecen herramientas informáticas para optimizar los procedimientos asociados a los reportes resultantes de los procesos que aplican ISO/IEC 27001. Estos colaboran con el cumplimiento y la certificación del Estándar, a partir de la documentación formal que generan tanto para los niveles operativos, tácticos y estratégicos de la organización.

Todas las herramientas de software disponibles actualmente con las funcionalidades recomendadas son comerciales, y se obtienen a costos muy elevados. Por otro lado, existen algunas herramientas de uso libre, pero con grandes limitaciones en cuanto a los reportes y diversas dificultades en su implementación e integración.

Se pueden destacar las siguientes herramientas de software, ya que colaboraron en el proceso de certificación en numerosas organizaciones:

- ISO 27001 ISMS Documentation Toolkit es una herramienta desarrollada por IT Governance y se caracteriza por presentar un conjunto de herramientas que le permite a la organización ahorrar costos y tiempo de trabajo. Además, colabora en acelerar la implementación de la certificación ISO 27001. Una de las tareas más complicadas para lograr la certificación ISO 27001 es recopilar toda la información solicitada por el auditor. En las grandes organizaciones, pueden requerirse hasta 1.000 documentos [15].
- Software ISO de ISOTools Excellence es una herramienta para la Seguridad de la Información constituida por diferentes aplicaciones que se ocupan de que la información que maneja a diario la organización esté protegida y mantenga sus principales propiedades. Además, agiliza la administración y control del Sistema de Gestión de la Seguridad de la Información aumentando su eficacia. Cuenta con una serie de

aplicaciones específicas para esta temática tales como evaluación de riesgos de seguridad de la información o aplicaciones de autodiagnóstico que dan la posibilidad de automatizar la implantación y mantenimiento de la norma ISO-27001 de forma eficaz en cualquier tipo de organización, independientemente de su sector o tamaño [6].

La utilización de estas herramientas no forma parte obligada del cumplimiento o certificación del Estándar, pero pueden colaborar en la automatización de reportes y tareas, ya que se adaptan completamente a los estándares internacionales como ISO/IEC 27001 y el modelo O-ISM3.

3.4. Gestión de vulnerabilidades

Las intrusiones y los ataques informáticos provienen principalmente a partir de las vulnerabilidades que presentan los servidores en sus versiones de sistema operativo, software instalado, service pack de aplicaciones, entre otros. Manteniendo los objetivos de confidencialidad, integridad y disponibilidad de la información y los sistemas dentro de la organización, es necesario identificar, analizar y prevenir las amenazas gestionando y controlando la implementación de los parches y actualizaciones correspondientes.

La norma ISO/IEC 27002 define un conjunto de buenas prácticas para aplicar en este ambiente y se identifican dentro del dominio “12. Seguridad en la Operativa” y el objetivo de control “12.6 Gestión de la vulnerabilidad técnica”.

El propósito que presenta el dominio “12. Seguridad en la Operativa” es el siguiente [5]:

- Controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento, y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización, a partir del control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

Dentro del dominio planteado, el objetivo de control “12.6 Gestión de la vulnerabilidad técnica” presenta los siguientes propósitos [5]:

- Minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

- Verificar que los cambios sean gestionados por personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso.
- Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.
- Aplicar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de backups y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y envolver a usuarios finales en pruebas de aceptación del nuevo estado.
- Evitar quedarse atrás en la rutina de actualización de versiones que sus sistemas queden fuera de soporte por el fabricante.
- Probar y aplicar los parches críticos, o tomar otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente.

Este objetivo de control presenta dos controles específicos:

12.6.1. Control de las vulnerabilidades técnicas: Se debe obtener, de manera oportuna, información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas para tratar los riesgos asociados.

12.6.2. Restricciones a la instalación de software: Se deben establecer e implementar reglas que gobiernen la instalación de software por parte de los usuarios.

3.5. Beneficios

A continuación, se ofrece un listado de beneficios que una organización tendrá de cara a su equipo y clientes al implantar sistemas de seguridad de la información y certificar ISO/IEC 27001 [6]:

- Ventaja competitiva: Los mercados cada día son más competitivos y las organizaciones que establecen un SGSI y aquellas que por su foco o decisión estratégica obtienen la certificación ISO/IEC 27001, sin duda tienen una ventaja sobre las que no la han implementado, ya que pueden demostrar que se rigen bajo estrictos estándares internacionales y que todos sus procesos funcionan de acuerdo a las mejores prácticas. Esto genera diferenciación frente a los competidores.
- Oportunidad de negocio: Otorga a la organización una mejora de su imagen ante los propios empleados y clientes dado que les transmite confianza sobre la protección de los datos depositados en la misma, ya que con esto demuestran que cuentan con las políticas requeridas para proteger su información frente a las amenazas actuales.
- Confianza y credibilidad: Toda certificación en este caso la ISO/IEC 27001 genera confianza y credibilidad, pues genera el voto, promesa o demostración a clientes y proveedores acerca del correcto aseguramiento y tratamiento de su información durante toda la cadena de suministro, y en general la organización materializa su promesa de valor al tomar en serio la seguridad de la información empleando buenas prácticas aprobadas a nivel internacional [14].

- Futuro propicio: Eventualmente, como pasó con la norma ISO 9001, ISO/IEC 27001 llegará a un punto en el que todas las organizaciones deberán tenerla y se convertirá en un requisito global, no únicamente para poder competir sino para permanecer [14].
- Cumplimiento: La norma ISO/IEC 27001 proporciona la metodología necesaria para un caminar adecuado y más sencillo, en busca del cumplimiento [14].
- Marco legal: Ofrece conocimientos para abordar requisitos legales y evitar posibles sanciones.
- Disminución de costos imprevistos: Sean o no de gran tamaño, los incidentes de seguridad implican costos y desgaste operativo para las organizaciones. Tener implementados controles apoyados en la norma ayuda en gran medida a prevenirlos y/o tratarlos de manera proactiva evitando que se repitan las causas que los originaron, de esta forma se logra disminuir los costos asociados [14].
- Cultura organizacional: Permite crear una cultura organizacional de concientizar a todos los usuarios ante las amenazas informáticas, y hacer una utilización eficiente de los activos de TI contra estas amenazas.
- Reducción de intrusiones y ataques informáticos: Más concretamente, la ISO/IEC 27001 ayuda a las organizaciones a protegerse frente a problemas tales como delincuencia cibernética, robo de datos internos, pérdida de datos por malversación, uso indebido de la información, violación de datos personales, así como ataques virales [6].

3.6. Limitaciones

ISO/IEC 27001 no ofrece un guía de estricto seguimiento para la protección de activos, sino que otorga en su lugar un marco de actuación que orienta a la organización sobre la forma de actuar ante una amenaza [6]. Esto puede suponer

cierta dificultad para las organizaciones porque se ofrece solo un modo de pensar que sienta las bases sobre la manera de gestionar los riesgos y los activos, y no presentan una lista de cumplimiento obligado. Por tal motivo, surgen distintos métodos y estándares específicos que si presentan una guía de estricto seguimiento que permiten definir las acciones a seguir para el cumplimiento de cada control, como es el caso del Estándar O-ISM3.

4. Estándar O-ISM3

La gestión de la seguridad de la información en las organizaciones debe estar focalizada sobre la adecuada administración de políticas, procesos, métricas y controles de seguridad que permitan mitigar riesgos sobre sus activos de información, de una forma rentable. Por este motivo se exige a las áreas de seguridad actuales, pasar de una visión netamente operativa a una visión más estratégica y gerencial, es decir, se debe tener una adecuada gestión de riesgos que permita identificar y estimar niveles de exposición, controles de seguridad para proteger sus activos, y gestión de seguridad que incluyen auditoría y cumplimiento normativo.

El Estándar O-ISM3 se basa en los procesos comunes de seguridad de la información que deberían estar implementados y gestionados. Además, se caracteriza por proporcionar un enfoque por niveles (genérico, estratégico, táctico y operacional), donde en cada nivel se implementan diferentes procesos de seguridad, los cuales pueden ir interrelacionados con procesos de otros niveles [7].

4.1. Modelo O-ISM3

El modelo de seguridad de O-ISM3 es adaptable a cualquier tipo de organización, debido a que su metodología se fundamenta en traducir los objetivos del negocio a nivel de seguridad, en especificaciones técnicas de seguridad. Conocer las metas corporativas es el primer paso para garantizar la gestión de la seguridad, y sus relaciones se observan en la Figura 2 [16]:

- Objetivos de negocio: Independiente del objeto de negocio de cada organización, estas se encargan de fijar metas u objetivos, el logro de cada uno de ellos dependerá de muchos factores que pueden ser críticos o no, uno de estos factores tiene que ver con la seguridad de la información, que puede ser originada por una cultura interna o impuesta por entidades externas.

- Objetivos de Seguridad: O-ISM3 propone un análisis de dependencia para dar cumplimiento a los objetivos de negocio de la entidad, el objetivo de este análisis es una lista de objetivos de seguridad como base para el diseño, implementación y monitoreo del SGSI. En otras palabras, es poder definir como la seguridad de la información contribuye a la obtención de los objetivos de negocio. O-ISM3 define cinco categorías de objetivos de seguridad:
    - Prioridad: Disponibilidad para el negocio, por ejemplo, copias de seguridad e identificación de puntos únicos de falla, canales de comunicación e interfaces.
    - Durabilidad: Integridad de la información, incluyen políticas de mantenimiento planificado y destrucción de la información.
    - Calidad de la información: Los objetivos también se refieren a la integridad de la información, técnica de control de calidad que incluyen precisión (o exactitud), relevancia, integridad y consistencia de los repositorios.
    - Control de acceso: Requiere la identificación y gestión de los usuarios autorizados.
    - Seguridad Técnica: Generalmente es la infraestructura del Centro de datos. Por ejemplo, tecnologías como firewalls, antivirus, parches de seguridad, actualizaciones. El incumplimiento de estos objetivos pone en situación de riesgo a los demás objetivos de seguridad y del negocio.
- Metas de Seguridad: Se definen normalmente en términos de frecuencia de ocurrencia y el umbral de costo de implementación del Estándar, teniendo como base el impacto en el negocio, es aquí la importancia de hacer un análisis de dependencia adecuado para soportar la inversión en seguridad.

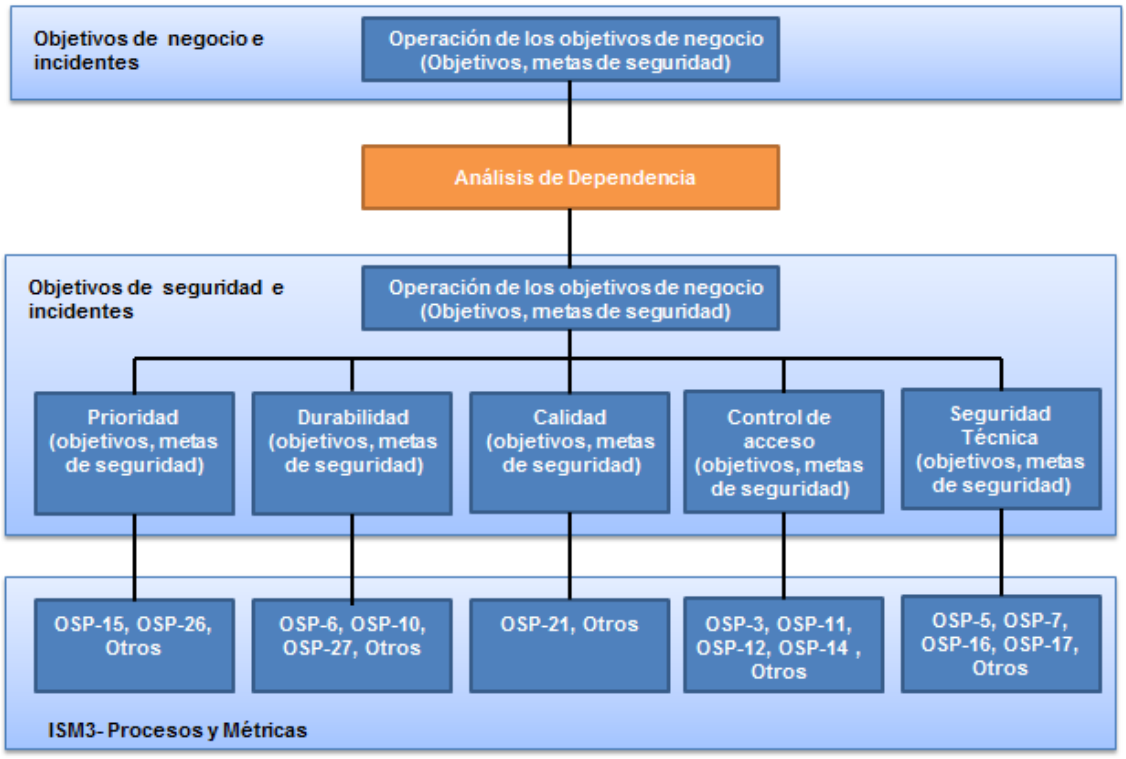

Figura 2 - Modelo O-ISM3

4.2. Clasificación

El O-ISM3 se clasifica en cuatro niveles de procesos para la administración de la seguridad de la información [17]:

- Procesos Genéricos (GP): suministra la infraestructura para la implementación, evaluación y mejora de los procesos de gestión de la seguridad de la información.
- Procesos Estratégicos (SSP) – Direcciona y provee: Define los objetivos generales, la coordinación y la provisión de recursos.
- Procesos Tácticos (TSP) – Implementa y Optimiza: Establece el diseño e implementación del SGSI, objetivos específicos, y la gestión de los recursos.

- Procesos Operacionales (OSP) – Ejecuta y Reporta: Establece el cumplimento de los objetivos definidos, por medio de procesos técnicos.

A continuación, teniendo en cuenta que el objetivo principal del proyecto es definir un marco estructurado para la seguridad de la información en servidores Web, nos enfocamos específicamente en los procesos operacionales del modelo O-ISM3, debido a que hacen hincapié en la gestión de vulnerabilidades y protección de los activos de la organización, como es el caso de los servidores Web.

4.3. Procesos de Gestión Operacional

La gestión operacional reporta al Gerente de TI y al Gerente de Seguridad de la información. El proceso se divide en 28 componentes específicos [7]:

- OSP-1 Reporte de la Gestión Operacional de seguridad.
- OSP-2 Adquisición en Seguridad.
- OSP-3 Gestión de inventario de activos de información.
- OSP-4 Seguridad en la Gestión de Cambios.
- OSP-5 Actualizaciones de Seguridad.
- OSP-6 Depuración y/o Destrucción de Activos de Información.
- OSP-7 Aseguramiento de Activos.
- OSP-8 Seguridad en el ciclo de vida de desarrollo de Software.
- OSP-9 Medidas de Seguridad de control de Cambios.
- OSP-10 Gestión de Backup.
- OSP-11 Control de Acceso.
- OSP-12 Registro de Usuarios.
- OSP-14 Protección de ambientes físicos.
- OSP-15 Gestión de continuidad de operaciones.
- OSP-16 Gestión de Trafico de Redes.
- OSP-17 Gestión de protección contra código malicioso.

- OSP-19 Auditoría Técnica Interna.
- OSP-20 Emulación de Incidentes.
- OSP-21 Calidad de Información y evaluación de Cumplimiento.
- OSP-22 Monitoreo de Alertas.
- OSP-23 Detección y Análisis de eventos internos.
- OSP-24 Gestión de incidentes.
- OSP-25 Informática forense.
- OSP-26 Gestión de infraestructura critica de seguridad.
- OSP-27 Gestión de archivo.
- OSP-28 Detección y Análisis de eventos externos.

Si bien los procesos operacionales se relacionan todos directa o indirectamente entre sí, en este proyecto nos enfocamos específicamente en el proceso de gestión operacional OSP-05 Actualizaciones de Seguridad, ya que es el proceso operacional de mayor importancia para reducir o mitigar amenazas asociadas a ataques o incidentes de seguridad.

4.4. OSP-5 Actualizaciones de Seguridad

Proceso operacional que describe la actualización de servicios tendientes a prevenir incidentes relacionados con vulnerabilidades conocidas y mejorando de este modo la confiabilidad de los sistemas actualizados [7].

Proceso	**OSP-5 Actualizaciones de Seguridad**
Descripción	Este proceso controla la actualización de los sistemas y aplicativos, a fin de prevenir incidentes y/o la explotación de vulnerabilidades.

Valor	La actualización de parches de seguridad evita incidentes derivados de la explotación de las debilidades conocidas de los sistemas y aplicativos.
Documentación	Procedimiento de gestión de parches.
Entrada	OSP-3 Inventario de activos
Salida	● Reporte de nivel de actualización de los sistemas y aplicaciones. ● TSP-4 Reporte de métricas.
Descripción de Métricas	● Cantidad de parches de seguridad que se implementaron para hacer frente a las vulnerabilidades identificadas. ● Número de parches de seguridad pendientes de implementación, por criticidad y tipo de tecnología. ● Nivel general de actualización de la red.
Responsabilidades	Supervisor: TSP-14 Dueño del proceso. Dueño del proceso: Gerente de Operaciones de TI.
Procesos Relacionados	OSP-4 Gestión de Cambios. OSP-9 Medidas de seguridad de control de cambios.
Mapeo a otros Frameworks o Normativa	
ISO/IEC 27002	12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Control de vulnerabilidades técnicas. 12.6.2 Restricciones a la instalación del software.
COBIT 5	Dominio DSS: Entregar, dar servicio y soporte. DSS01 – Gestionar las operaciones.

ITIL	Fase Operación del Servicio. Función Gestión de Operaciones de TI.

4.5. Documentación

Los documentos asociados a todos los procesos operacionales, tanto de políticas, procedimientos y prácticas, como así también planillas de completado periódico, deben presentar la misma estructura de documentación.

Es importante que la información esté ordenada del mismo modo en todos los documentos, utilizando los mismos estilos y formatos, de manera que los usuarios tengan mayor facilidad y rapidez en su utilización. A su vez, se debe definir una nomenclatura específica para el nombre de los documentos. En cada documento se debe detallar: autores, fecha de generación, fecha de modificaciones, propósito del documento, interesados, glosario de acrónimos y definiciones.

Los documentos se deben almacenar en un repositorio común, con un control de accesos específico en cuanto a los permisos de lectura o modificación, dependiente de los intereses de los usuarios. El repositorio debe contener carpetas por cada proceso operacional, y dentro de ellas, dividir lo que es: documentación general, administración y operaciones.

Se debe asegurar que la información esté disponible y apta para su uso, cuándo y dónde sea necesario; y que esté adecuadamente protegida contra la pérdida de confidencialidad, el uso inapropiado o la pérdida de integridad. Además, se debe controlar su distribución, acceso, recuperación y uso; el almacenamiento y preservación; el control de cambios; y la conservación y disposición final.

4.6. Especificación de Métricas

Las métricas permiten a las áreas de seguridad de la información formular indicadores de desempeño sobre los productos, procesos o servicios que ofrecen, facilitando la toma de decisiones, ya que de ellas se obtiene la recopilación y análisis de datos importantes. Dichas decisiones sirven como soporte para la asignación de recursos, capacitaciones, mejoras de procesos, etc. Existen diferentes estándares que proponen métricas de seguridad, algunos de ellos son: ISO/IEC 27004, NIST11 800-55, CISWG12, entre otros [17].

Tipos de métricas

Las buenas prácticas del Estándar proponen tres tipos de métricas de seguridad, que permiten establecer un programa de seguridad de la información lo suficientemente maduro en relación con el rendimiento de los procesos definidos para el área. Los tres tipos de métricas que se describen a continuación:

Métricas de implementación**:** Se utilizan para demostrar el progreso en la implementación de programas de seguridad de la información, controles de seguridad específicos, políticas y procedimientos asociados. Su progreso se mide a través de porcentaje o cantidad de implementación llevada a cabo. Ejemplo: porcentaje de servidores de la organización a los que se les ha aplicado una configuración estándar.

Métricas de eficacia y eficiencia: Este tipo de métricas están diseñadas para monitorear si los controles de seguridad están funcionando de acuerdo con la planificación realizada y si se están obteniendo los resultados esperados. Estos controles se enfocan en las pruebas realizadas y en los resultados que espera cubrir la organización en temas asociados a la seguridad de la información. Ejemplo: Cantidad de parches de seguridad que han cubierto las vulnerabilidades encontradas.

Métricas de impacto en el negocio: Son utilizadas para articular el impacto de la seguridad de la información sobre la misión de organización. Dependiendo de la misión que tenga la organización este tipo de métricas pueden ser utilizadas para cuantificar el ahorro de costos en relación con eventos de seguridad, así como el grado de confianza que la organización proyecta hacia sus clientes y proveedores. Ejemplo: Porcentaje de asignación del presupuesto de TI asociado a la seguridad de la información.

4.7. Beneficios

A continuación, se ofrece un listado de beneficios que proporciona implantar el Estándar O-ISM3 en una organización [7]:

- Un enfoque por niveles (genérico, estratégico, táctico y operacional), donde en cada nivel se implementan diferentes procesos de seguridad, los cuales pueden ir interrelacionados con otros procesos de otros niveles.
- Sirve como herramienta para la creación de SGSI alineados con la misión de la organización y el cumplimiento de las necesidades.
- Se aplica a cualquier organización independientemente de su tamaño, el contexto y los recursos.
- Permite a las organizaciones priorizar y optimizar su inversión en seguridad de la información.
- Permite la mejora continua del SGSI estableciendo metas de seguridad y midiendo el desempeño mediante la aplicación de métricas.
- Se adapta al Estándar internacional ISO/IEC 27001 para su certificación. Además, tiene cumplimiento con otros estándares como Cobit e ITIL, y a normas regulatorias como la 4609 del Banco Central de la República Argentina.

- Sirve como soporte a Auditorías.
- Permite mejorar la gobernabilidad de la organización a nivel tecnológico.

4.8. Limitaciones

Si bien el Estándar O-ISM3 ofrece una guía de estricto seguimiento para su implementación, no define las tareas operativas puntuales que se deben desarrollar, como así también, no especifica los documentos a generar, los roles de usuarios en cuanto a permiso de acceso, y las métricas a evaluar.

5. Marco de trabajo para la seguridad de la información en Servidores Web

El Estándar ISO/IEC 27001 es una normativa certificable de carácter internacional, pero en sus requerimientos plantea solo un marco de actuación y no define una guía de estricto seguimiento para la protección de servidores Web. A su vez, el modelo de seguridad que plantea el Estándar O-ISM3 propone procesos de seguridad de acuerdo a niveles pero no tiene suficiente nivel de detalle en cuanto a la ejecución de tareas operativas, documentación a generar, roles de usuarios a asignar y métricas a evaluar. Para solucionar estos aspectos, en este Trabajo Final Integrador se propone un marco de trabajo estructurado para la seguridad de la información en servidores Web, el cual ofrece una solución con el suficiente nivel de detalle para que pueda ser directamente implementado en una organización. Este marco, se define bajo los requisitos y cumplimientos del Estándar ISO/IEC 27000 para la certificación de ISO/IEC 27001, y está basado en las buenas prácticas que se especifican en el modelo de seguridad propuesto por el Estándar O-ISM3, con lo cual hereda los beneficios de ambos estándares.

El marco de trabajo propuesto en la presente TFI se compone de módulos para:

- Gestión de roles de usuarios con privilegios específicos, para la ejecución de tareas y acceso a documentación.
- Gestión de vulnerabilidades en una organización, mediante la implementación de un ciclo de vida o procedimiento paso a paso con las tareas que deben realizar los operadores.
- Gestión de documentación, en el cual se propone una estructura para el almacenamiento de documentación, tanto a nivel de repositorio como de estructura de los documentos en sí mismo.

- Monitoreo de seguridad de información, el cual se basa en métrica para medir el desempeño de las operaciones realizadas.

5.1. Gestión de roles de Usuarios

ISO/IEC 27000 destaca la importancia y necesidad de establecer roles de usuarios dentro de la organización, debido a que permite definir privilegios en cuanto a permisos de acceso a directorios y ejecución de tareas. De acuerdo con este requerimiento y basado en la limitante con respecto a que no están definidos claramente, como parte del presente TFI se definen los siguientes roles de usuarios para el marco de trabajo de seguridad de la información propuesto:

- Responsable: Usuario que define políticas, procedimientos y métricas del marco de trabajo a implementar.
- Operador: Usuario que realiza las tareas operativas sobre las herramientas de seguridad específicas en función del cumplimiento del marco de trabajo.
- Supervisor: Usuario que audita el cumplimiento de políticas y procedimientos establecidos, como así también, la consecución de las métricas definidas.
- Interesados: Usuario que por su tarea en la organización, requiere observar los resultados obtenidos del proceso.

Cada uno de los roles de usuarios tienen asociados un conjunto de tareas que los usuarios pueden ejecutar en base a sus permisos y responsabilidades dentro del marco de trabajo.

5.2. Gestión de vulnerabilidades

Como parte de este TFI, se propone un ciclo de vida en la gestión de parches y actualizaciones para servidores, basado en los fundamentos del proceso operacional "OSP-05 Actualizaciones de Seguridad" que propone el Estándar O-ISM3 (referirse a Sección 4.4). Este ciclo de vida tiene la capacidad de controlar las actualizaciones de los sistemas y aplicativos, a fin de prevenir incidentes y/o la explotación de vulnerabilidades, y cumple con los objetivos de control especificados en el punto "12.6 Gestión de la vulnerabilidad técnica", requeridos por el Estándar ISO/IEC 27002 (referirse a Sección 3.4).

Este ciclo de vida de gestión de vulnerabilidades engloba todas las tareas operativas que se deben desarrollar para el cumplimiento del objetivo asociado a detectar y mitigar las vulnerabilidades en los servidores Web. Las tareas deben ser dirigidas por un usuario con el rol "Responsable", ejecutadas por uno o múltiples usuarios con rol "Operador" y auditadas por un usuario con rol "Supervisor".

El ciclo de vida propuesto consta de 6 fases, como se observa en la Figura 3.

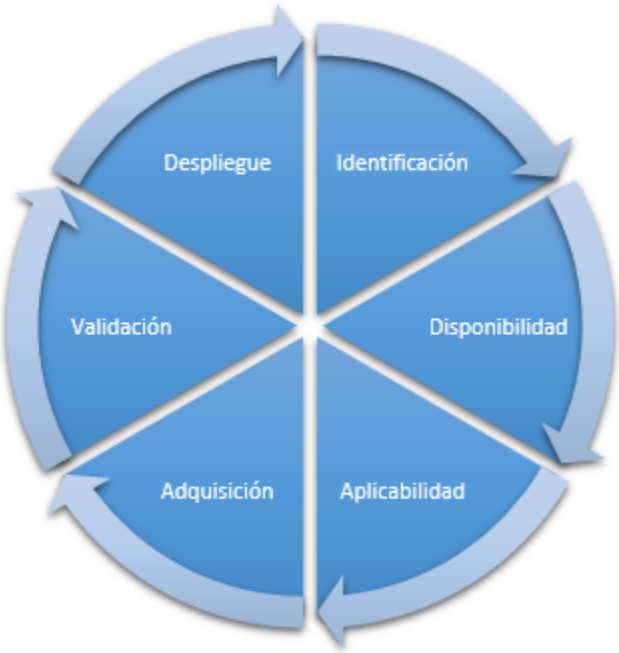

Figura 3 - Ciclo de vida de la gestión de parches.

A continuación, se describen cada una de las fases de este ciclo de vida:

- Identificación: En esta fase se identifican los activos y su software base instalado, así como el nivel de parches. Es una tarea compleja pero que mejora la seguridad y las actividades de los operadores. Disponer de esta base permite llevar a cabo cambios en el sistema sin riesgos y volver a un estado previo conocido y funcional en el caso de producirse algún problema a la hora de instalar una actualización [18]. El primer paso es contar con un inventario de activos actualizados y completos, donde se detallen todos los servidores Web con cada uno de las aplicaciones y software instalados.
- Disponibilidad: En esta fase se verifica la existencia y disponibilidad de parches para la mitigación de vulnerabilidades. En función del inventario de servidores Web y el software identificado, se ha de revisar el listado de parches detectados e identificar cuál de ellos afecta a cada activo. En la realización de esta fase, los operadores deben trabajar con herramientas de análisis de vulnerabilidades específicas que permitan detectar posibles parches de seguridad para que solucionen las vulnerabilidades del sistema inventariado.
- Aplicabilidad: En esta fase se valida la posibilidad real de aplicar los parches detectados y disponibles. Los parches publicados no siempre son válidos para todos los dispositivos, por lo que se ha de verificar si la actualización en concreto es apta para los activos de nuestro proceso [18]. Esto depende de la versión del sistema operativo en el servidor Web, como así también la versión de las aplicaciones de software instaladas en el mismo.
- Adquisición: En esta fase se adquieren los parches para la mitigación de las vulnerabilidades detectadas. Obtener los parches de actualización de una fuente fidedigna, comprobando la veracidad de los mismos. Para

esto, se deben reconocer los sitios o fuentes oficiales de descarga de cada uno de los parches o actualizaciones, dependiendo su fabricante.

- Validación: Durante la fase de validación se asegura que la actualización no impacta en la gestión de vulnerabilidades de forma adversa, afectando por incompatibilidad con otro componente de software o introduciendo errores. Para llevarla a cabo se han de utilizar servidores Web de pruebas y seguir la fase de despliegue. Puede ocurrir que la instalación de un parche o actualización de un sistema, genere incompatibilidades con ciertas funcionalidades importantes del servidor Web, por lo que las pruebas previas son importantes para minimizar posibles fallas.
- Despliegue: La última fase del ciclo de vida se centra en distribuir las actualizaciones mediante un gestor centralizado que garantice su instalación en todos los activos requeridos. Para el cumplimiento de esta fase, los operadores pueden apoyarse en herramientas de software que permiten la distribución segura y remota de parches para servidores Web.

El ciclo de vida planteado se ejecuta sobre los servidores Web existentes, que son detectados en la primera fase del mismo. Estos servidores Web se caracterizan por estar en entorno "productivo" ya que brindan servicios Web, por lo que son identificados desde el momento de su creación y configuración. El ciclo de vida se ejecuta de forma continua hasta el momento que, por algún motivo en particular, el servidor Web es quitado del área "productiva" y deja de brindar servicios Web.

5.3. Gestión de documentación

Teniendo en cuenta uno de los propósitos del dominio "12 Seguridad en la Operativa" que impone el Estándar ISO/IEC 27002 (referirse a Sección 3.4) asociado a definir y controlar una estructura de documentos actualizados, y a partir de la propuesta del Estándar O-ISM3 (referirse a Sección 4.5) que especifica requerimientos de documentación y repositorios de almacenamiento, se propone

como parte del presente TFI un repositorio de documentación común compartido entre los usuarios interesados, donde se almacenarán los documentos necesarios para el registro de la operación del marco de trabajo.

La propuesta de gestión de documentación se basa en las limitaciones de los mencionados estándares, quienes si bien expresan la importancia de la utilización de los mismos, no detallan su estructura de almacenamiento, el formato y tipo de documentos, y los permisos de acceso a cada uno.

El repositorio propuesto presenta un conjunto de directorios específicos, donde en cada uno se almacenarán documentos puntuales con formato estandarizado. La estructura del mismo se propone del siguiente modo:

- Procesos de Gestión Organizacional
    - OSP-05 – Actualizaciones de Seguridad
        - 05.01 Documentación
        - 05.02 Administración
        - 05.03 Operación
            - 05.03.01 Reportes
            - 05.03.02 Registros

De cada directorio especificado, se detalla el contenido de los documentos que se deberán alojar:

- 05.01 Documentación: Bibliografía de las herramientas de software utilizadas en la gestión de vulnerabilidades y soluciones de seguridad implementadas para el proceso operacional.
- 05.02 Administración: Políticas y Procedimientos definidos.
- 05.03 Operación: Contiene reportes y registros de las tareas realizadas por los usuarios con rol Operador.
- 05.03.01 Reportes: Reportes generados por las herramientas y soluciones de software de seguridad utilizadas.

- 05.03.02 Registros: Planillas con registros de las operaciones realizadas.

Se propone la definición de permisos de acceso a los usuarios en cuanto a lectura o escritura de los documentos almacenados en el repositorio, dependiendo de los roles de usuarios, del siguiente modo:

- Responsable: Lectura y escritura sobre los directorios "05.01 Documentación", "05.02 Administración" y "05.03 Operación".
- Operador: Lectura sobre los directorios "05.01 Documentación" y "05.02 Administración", y permiso de lectura y escritura sobre el directorio "05.03 Operación".
- Supervisor: Lectura sobre los directorios "05.01 Documentación", "05.02 Administración" y "05.03 Operación".
- Interesados: Lectura sobre el directorio "05.03 Operación".

A continuación, se detalla la nomenclatura de nombres de los archivos almacenados en el directorio:

- Reportes: <Nombre-Activo>_AAAA_MM_DD [Herramienta].pdf
- Registros: <Nombre-Proceso>_Bitácora_AAAA.xls
- <Nombre-Proceso>_Estadísticas_AAAA.xls

Los caracteres en mayúsculas están asociados a una fecha:

- AAAA: Año en curso. Ejemplo 2018.
- MM: Mes en particular. Ejemplo 07.
- DD: Día en particular. Ejemplo 31.

Es importante que los documentos de políticas y procedimientos, como así también todas las planillas de completado periódico, presenten la misma estructura de documentación. Es decir, que la información esté ordenada del mismo modo permite que los usuarios se sientan identificados con la bibliografía y encuentren de manera

más rápida la información. Esto incluye utilizar el mismo formato, color y tipografía para todos los documentos, donde se identifiquen: título, subtítulos y cuerpo de texto.

Se propone la realización de dos tipos de documentos, dependiendo el propósito de cada uno en cuanto a la información a almacenar. Los documentos que definen políticas, procedimientos y detalles de herramientas de seguridad utilizadas, deberán tener el formato denominado "Documento de procesador de texto". Los documentos que permiten almacenar información de manera periódica en cuanto a las tareas realizadas, deberán tener el formato denominado "Documento de hoja de cálculo".

Los documentos de procesador de texto deben contener los campos indicados a continuación. Un ejemplo del mismo se encuentra en “Anexo II – Documentación”, sección "II.1 Documento de procesador de texto":

- Encabezado: Indica nombre del documento y tipo de documento (ejemplo: Documento de procedimiento, Documento de política interna, Documento técnico, entre otros).
- Pié de página: Autor del documento y numeración de hoja.
- Título principal: En la parte central superior de la primera hoja.
- Subtítulos principales:
    - Historia de revisiones. Se registran fecha y autores de cambios.
    - Índice. Contenido del documento indicando número de hoja.
    - Definiciones y glosario.
    - Propósito del documento.
    - Desarrollo. Sección en la que se desarrolla el documento, dependiendo su propósito, donde se detallarán los procedimientos, políticas internas, entre otros.

Los documentos de hoja de cálculo deben contener los campos indicados a continuación. Un ejemplo del mismo se encuentra en “Anexo II – Documentación”, sección "II.2 Documento de hoja de cálculo":

- Pestaña 1: Debe llamarse con el nombre "Carátula" y contener la siguiente información:
    - Encabezado: Indica nombre del documento y tipo de documento (ejemplo: Documento de operación, Documento de control de cambios, entre otros).
    - Historial de revisiones: Se registran fecha y autores de cambios.
    - Índice. Contenido del documento indicando número de hoja.
    - Definiciones y glosario.
    - Propósito del documento.
- Pestañas siguientes: El nombre de las mismas depende del propósito del documento (ejemplo: Listado, Relevamiento, Parches, entre otros) y debe contener la siguiente información:
    - ID: Identificador único de cada tarea realizada por un usuario con rol Operador. Aumenta de manera secuencial.
    - Fecha. Fecha de ejecución de la tarea.
    - Descripción. Detalle de la tarea ejecutada.
    - Autor. Usuario que ejecutó la tarea.

5.4. Monitoreo de seguridad de información en servidores Web

De acuerdo a lo solicitado por el Estándar O-ISM3 se requieren definir un conjunto de métricas que permitan medir el desempeño de las operaciones realizadas (referirse a Sección 4.6). En el presente TFI y como parte del marco de trabajo estructurado, se propone llevar a cabo el Monitoreo de la seguridad de la información en servidores Web que será ejecutado por el rol de usuario "Supervisor". Es el encargado de revisar los procedimientos definidos, políticas establecidas, correcta

conformación de la documentación y cumplimiento de las tareas de los demás usuarios. Además, en base a su revisión, se deben calcular y completar métricas de desempeño.

El Estándar O-ISM3, de acuerdo a lo analizado en la Sección 4.6, establece la formulación de tres tipos de métricas:

- IM: Métricas de implementación.
- EF: Métricas de eficacia y eficiencia.
- NE: Métricas de impacto en el negocio.

Este Estándar no provee ninguna métrica específica. Como parte de este TFI, se proponen las siguientes métricas que dan cumplimiento a los requerimientos del Estándar O-ISM3 y permiten que el usuario con rol "Supervisor" tenga mayor facilidad para la evaluación y toma de decisión:

- Métricas IM:
    - Número de parches de seguridad pendientes de implementación, por criticidad y tipo de tecnología.
    - Cantidad de parches de seguridad que se implementaron con respecto a las vulnerabilidades identificadas.
- Métricas EF:
    - Cantidad de intentos ataques detectados por servidores Web.
    - Cantidad de ataques efectivos en relación a la cantidad de intentos de ataques detectados.
- Métricas NE:
    - Tiempo promedio de no operatividad de los servidores Web.

Cabe aclarar que las métricas propuestas representan un marco de referencia. Cada organización que implementa el marco de trabajo propuesto puede agregar nuevas métricas para monitorear la seguridad de sus servidores de acuerdo a los requerimientos de negocio o técnicos de la misma.

5.5. Beneficios

El marco de trabajo estructurado para la seguridad de la información en servidores Web propuesto permite identificar y mitigar vulnerabilidades, definir controles de acceso con privilegios a usuarios, especificar la documentación requerida, establecer controles y monitorear el desempeño de los procesos a partir de métricas.

Además, tiene la capacidad de adaptarse a cualquier organización independientemente de su tamaño, el contexto y los recursos, ya que es independiente de la tecnología que lo utilice.

Para los usuarios que ejecutan las tareas dentro del marco de trabajo propuesto, estos tienen completamente definidos sus roles, permisos, accesos y actividades a realizar, lo que facilita sus labores y permite que estén enfocados en las mismas.

Por otro lado, al estar basado en los principios del modelo de seguridad propuesto por el Estándar O-ISM3, colabora con la elaboración de un SGSI para la organización. Además, el marco de trabajo es consistente para la certificación del Estándar ISO/IEC 27001, y hereda los beneficios de estos estándares analizados ya que es compatible con otros estándares internacionales como ITIL y Cobit, y las normas regulatorias del Banco Central de la República Argentina.

6. Conclusiones

Los servidores Web publican información valiosa para cualquier tipo de organización por lo que deben ser protegidos contra ataques y amenazas, que cada día son más sofisticadas y que intentan vulnerar controles débiles o mal implementados, para así poder tener acceso a los datos restringidos o confidenciales. Algunas organizaciones pueden contar con las mejores herramientas tecnológicas a nivel de software y hardware, pero muchas de ellas dejan a un lado la gestión de la seguridad de la información. Si no se cuenta con un proceso definido dentro de un marco estructurado, será muy difícil que un modelo de gestión de la seguridad cumpla con el objetivo definido y por ende, que los activos estén protegidos de manera segura.

Implementar un marco estructurado de seguridad de la información sirve de base para gestionar la seguridad, ayuda a las organizaciones a identificar los procesos claves que están ejecutando y que a su vez soportan activos críticos, o en un mayor nivel, objetivos o metas de negocio. De esta forma, es posible establecer controles, medir el desempeño del proceso y mejorar continuamente el mismo.

O-ISM3 establece elementos fundamentales que tiene como fin la implementación de un modelo de seguridad, ya que establece todo el circuito de una manera detallada relacionando aspecto como: descripción del proceso, definición de métricas y documentación, relación con otros procesos, metodologías o herramientas utilizadas, y su adaptabilidad a ISO/IEC 27001, entre otros aspectos relevantes.

El modelo de seguridad propuesto se adapta completamente a los estándares internacionales más importantes como ISO/IEC 27001, Cobit 5 e ITIL. En particular, ISO/IEC 27001 que es la norma de seguridad de uso generalizado para todas las organizaciones a nivel mundial. Al estar implementado mediante el Estándar O-ISM3, se tienen definidos todos los procesos operativos a realizar y se obtiene un modelo que otorga una mejora de la imagen empresarial ante los propios empleados y clientes dado que les transmite confianza sobre la protección de los datos depositados en la misma, generando una diferenciación frente a sus competidores y mayores

oportunidades de negocio. Además, permite que los operadores puedan realizar sus tareas de manera más ágil, organizada y optimizada, reduciendo los costos, tiempos y amenazas posibles.

El modelo es independiente de la tecnología que se utilice y de los recursos humanos que lo apliquen, por lo que se puede utilizar con todas las herramientas operativas de seguridad, y es capaz de adaptarse completamente a cualquier organización independientemente de su tamaño, el contexto y los recursos. Además, contribuye oportunamente para la creación de un SGSI alineado con la misión de la organización, el cumplimiento de sus necesidades, y la priorización y optimización de las inversiones en seguridad de la información, midiendo el desempeño mediante la aplicación de métricas.

Con este modelo, el área de Seguridad puede brindar elementos suficientes para que las áreas operativas puedan abordar puntos frágiles y administrar tanto estratégica como operativamente, con el fin de disminuir vulnerabilidades y amenazas que puedan generar impacto sobre los activos de información, principalmente los servidores Web. Además, para que el área operativa tenga una serie de tareas funcionales, administradas y gestionadas de una manera eficiente, y para que las áreas estratégicas tengan información relevante y suficiente que le permita la toma de decisiones.

Como desventaja del marco de trabajo propuesto, se considera la dificultad de aceptación para su implementación en algunas organizaciones, debido a que puede conllevar a un cambio de paradigmas en el pensamiento de los usuarios en cuanto a la manera de trabajar y de organizar sus tareas. Además, teniendo en cuenta la completa adaptación que debe hacer una organización sobre el marco de trabajo, puede incurrir en largos períodos de tiempo hasta su implantación completa. Por último, se considera que puede resultar tedioso para algunos usuarios generar los documentos recomendados.

7. Trabajos Futuros

Con la finalización del actual TFI, se vislumbran nuevos proyectos e investigaciones futuras, entre los que se pueden destacar:

- Completar los requerimientos de ISO/IEC 27001 con todos los procesos operacionales de O-ISM3 asociados a "OSP-5 Actualizaciones de Seguridad", lo que incluye: Gestión de inventario de activos de información (OSP-3), Gestión de cambios (OSP-4) y Medidas de seguridad de control de cambios (OSP-9).
- Agregar el marco de trabajo estructurado para la seguridad de la información en servidores Web los niveles estratégicos y tácticos que propone O-ISM3.
- Desarrollar un proceso para la seguridad de la información en servidores Web, identificando flujos de control y de datos, y las tareas ejecutadas por herramientas de seguridad, que pueda ser integrado al marco estructurado propuesto.
- Estudiar y analizar aspectos culturales y organizacionales considerando un enfoque socio-técnico que procure entender la complejidad de las situaciones reales y lidiar con problemas de las condiciones laborales en las organizaciones, para gestionar de manera adecuada una implementación exitosa del marco de trabajo propuesto.

8. Referencias bibliográficas

1. ALVARO ROLDAN (2015). Seguridad en servidores Web: La importancia de tener un sistema seguro. IV Congreso Internacional de Ciberseguridad Industrial.

2. HENRY PAUL FINO, SALVADOR ALEJANDRO MIRANDA MARTELL. (2011). Seguridad en el servidor. Publicado en Biblioteca digital de Bogotá.

3. ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN, COMISIÓN ELECTROTÉCNICA INTERNACIONAL (2011). ISO/IEC 27000.

4. JULIO ARDITA (2018). Transformación del área de Ciberseguridad. Congreso y Feria Iberoamericana de Seguridad de la Información - Segurinfo 2018.

5. ISO 27000 – EL PORTAL DE ISO EN ESPAÑOL (2013). ISO 27000. Disponible en: http://www.iso27000.es/iso27000.html. Fecha de consulta: 26/12/2017.

6. ISO TOOLS EXCELLENCE (2016). ¿Por qué las organizaciones necesitan certificar la ISO 27001? Publicado por Excellence Chile.

7. THE OPEN GROUP (2011). Open Information Security Management Maturity Model (O-ISM3). Van Haren Publishing.

8. AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (2013). Seguridad de la Información. Publicado por La Revista Calidad AEC.

9. ANDRES MENDOZA (2018). Como lograr la Transformación Digital cumpliendo con ISO 27001. Congreso y Feria Iberoamericana de Seguridad de la Información - Segurinfo 2018.

10. KEVIN MITNICK Y WILLIAM SIMÓN (2007). El arte de la Intrusión. Alfaomega 1° Edición.

11. DAMIAN MAURO (2018). Threats Revolution: Massive Attacks & Trends. Congreso y Feria Iberoamericana de Seguridad de la Información - Segurinfo 2018.

12. CARLOS AGRELO (2018). Interceptando las nuevas amenazas. Protección contra Ransomware y Exploits. Congreso y Feria Iberoamericana de Seguridad de la Información - Segurinfo 2018.

13. MAX DE GORBITZ (2018). Evolución en modelos y marcos de gestión de la seguridad de la información y la ciberseguridad. Congreso y Feria Iberoamericana de Seguridad de la Información - Segurinfo 2018.

14. LESLY GRANJALES (2015). Vale la pena certificarse ISO 27001. Publicado por B-SECURE.

15. HANNA GUIJARRO (2017). La importancia de certificar la norma ISO 27001 en su empresa. Publicado por IT Governance European.

16. JORGE AGUIRRE, ALFONSO MUÑOZ (2010). O-ISM3 Information Security Management Maturity Model. VIII Jornada Internacional de Seguridad Informática.

17. THE OPEN GROUP (2016). O-ISM3 Security Body of Knowledge. Van Haren Publishing.

18. INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Gestión de parches. Fecha de consulta: 17/03/2018.

19. PMG-SSI (2014). ISO 27001: ¿Cómo gestionar las vulnerabilidades técnicas? Publicado por Excellence Chile.

20. ISO 27000 – EL PORTAL DE ISO EN ESPAÑOL (2013). SGSI. Disponible en: http://www.iso27000.es/sgsi.html. Fecha de consulta: 24/02/2018.

21. C. PARDO, F. PINO, F. GARCIA, M. PIATTINI, M. BALDASSARRE (2009). A process for Driving the Harmonization of Models. Publicado en 11th International Conference on Product Focused Software Development and Process Improvement - Limerick, Irlanda.

22. JOSE MANUEL POVEDA (2011). Los activos de seguridad de la información. Sección 7. Publicado en UNI - RUACS.

23. INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Parches. Fecha de consulta: 24/02/2018.

24. INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA. Amenaza vs Vulnerabilidad. Fecha de consulta: 24/02/2018.

25. CRISTINA LEDESMA (2016). Métricas de seguridad de la información. Seminario de Seguridad de la Información - UNIT.

26. M. MACHADO, F. HOURNEAUX JUNIOR, F. SOBRAL (2017). Sustainability in information technology: An analysis of the aspects considered in the model Cobit. Publicado en JISTEM J.Inf.Syst. Technol. Manag.

27. J. CALVO, L. LEMA, M. ARCILLA, J. RUBIO (2015). How small and medium enterprises can begin their implementation of ITIL?. Publicado en Revista F.I.U.A.

28. BANCO CENTRAL DE LA REPÚBLICA ARGENTINA (2006). Comunicación "A" 4609. Publicada en Circular de Banco Central.

Anexo I - Definiciones

SGSI: Sistema de Gestión de Seguridad de la información. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información [20].

O-ISM3: Information Security Management Maturity Model. Es un Estándar de madurez de seguridad de la información orientado a procesos y compatible con la implantación de ISO/IEC 27001, Cobit, ITIL e ISO 9001 [7].

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados [21].

TI: Tecnología de la información. Es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras organizaciones. Engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones [22].

Activo de información: Elemento que contiene o manipula información: equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, software de sistema, ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, utilidades generales y personas. Estos últimos que son los que en última instancia generan, transmiten y destruyen información, es decir, dentro de una organización se han de considerar todos los tipos de activos de información [22].

Parche: Un parche es una pieza de software diseñado para actualizar un programa de computadora o sus datos de apoyo, para corregir o mejorar la misma. Esto incluye la fijación de las vulnerabilidades de seguridad y otros aspectos. Con

este tipo de parches, generalmente llamados correcciones de errores, permite mejorar la facilidad de uso o el rendimiento [23].

Vulnerabilidad: Errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario. Estos permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo [24].

Métrica: Herramientas para facilitar la toma de decisiones, mejorar el desempeño y la contabilidad a través de la colección, análisis y reporte de datos de desempeño relevantes. El propósito de medir el desempeño es monitorear el estado de las actividades medidas y facilitar la mejora de éstas aplicando acciones correctivas basadas en medidas observadas [25].

COBIT: Control Objectives for Information and related Technology. Es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI). Presenta una serie de recursos que se utilizan como modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, objetivos de control, mapas de auditoría, herramientas para su implementación y una guía de técnicas de gestión [26].

ITIL: Information Technology Infrastructure Library. Es un marco de trabajo de buenas prácticas aplicables a la Gestión de Servicios de TI y definidas para ayudar a las organizaciones proveedoras de servicios de TI a conseguir una mayor calidad y eficiencia en la entrega y gestión de sus servicios [27].

Norma 4609 de Banco Central: Norma nacional sobre requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras, emitido por el Banco Central de la República Argentina [28].

Anexo II - Documentación

II.1. Documento de procesador de texto

Nombre del Documento Documento de Procedimiento

Nombre del Documento

Historial de Revisiones

Fecha	Versión	Descripción	Autor
DD/MM/AA	1.0	Generación de documento	Nombre y Apellido

Índice

HISTORIAL DE REVISIONES 49
INDICE **¡ERROR! MARCADOR NO DEFINIDO.**
DEFINICIONES Y GLOSARIO 49
PROPÓSITO DEL DOCUMENTO 49
DESARROLLO 49

Definiciones y Glosario

DD: Día
MM: Mes.
AA: Año.

Propósito del documento

Descripción del propósito del documento.

Desarrollo

Descripción del desarrollo del documento.

Autor: Nombre y Apellido	Página 1 de 1

II.2. Documento de hoja de cálculo

Pestaña "Carátula":

Nombre del Documento Documento de Operación				
Nombre del Documento				
Historial de Revisiones				
Fecha	**Versión**	**Descripción**	**Autor**	
DD/MM/AA	1.0	Generación de documento	Nombre y Apellido	
Índice				
Carátula	1			
Pestaña 1	2			
Pestaña 2	3			
Definiciones y Glosario				
DD	Día			
MM	Mes			
AA	Año			
Propósito del documento				
Descripción del propósito del documento.				

Pestaña "Pestaña 1":

ID	Fecha	Descripción	Autor
1	DD/MM/AA	Detalle operación 1.	Nombre y Apellido
2	DD/MM/AA	Detalle operación 2.	Nombre y Apellido
3	DD/MM/AA	Detalle operación 3.	Nombre y Apellido