UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULACIÓN DE INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

Desarrollo de una guía metodológica de elicitación de requisitos sobre sistemas de información para el manejo de resiliencia enfocada en los activos de personal, información, tecnología e instalaciones del modelo CERT-RMM

TRABAJO DE FIN DE TITULACIÓN

AUTOR: Palacios Alulima, Jackeline Marisol

DIRECTOR: Jaramillo Hurtado, Danilo Rubén, Ing.

LOJA – ECUADOR

2014

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN

Ing.

Danilo Rubén Jaramillo Hurtado

DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN

De mi consideración:

El presente trabajo de fin de titulación: Desarrollo de una guía metodológica de elicitación de requisitos sobre sistemas de información para el manejo de resiliencia enfocada en los activos de personal, información, tecnología e instalaciones del modelo CERT-RMM realizado por Palacios Alulima Jackeline Marisol ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, junio 2014

f) ……..

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

“ Yo Palacios Alulima Jackeline Marisol declaro ser autor (a) del presente trabajo de fin de titulación: Desarrollo de una guía metodológica de elicitación de requisitos sobre sistemas de información para el manejo de resiliencia enfocada en los activos de personal, información, tecnología e instalaciones del modelo CERT-RMM, de la Titulación de Sistemas Informáticos y Computación, siendo Danilo Rubén Jaramillo Hurtado director del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Además certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

f. ……

Autor: Palacios Alulima Jackeline Marisol

Cedula: 1105037772

DEDICATORIA

A Dios y toda mi familia que me han apoyado incondicionalmente, incentivándome a fortalecer la perseverancia y esfuerzo en cumplir mis objetivos, gracias por su compañía, por su aliento, por sus buenos deseos que me han servido de mucho en este arduo camino lleno de múltiples experiencias enriquecedoras en mi vida personal y en un futuro profesional.

AGRADECIMIENTO

Quisiera agradecer a Dios, mi familia, amigos y de manera especial a Danilo Jaramillo por su guía durante el desarrollo de este trabajo, por su paciencia, esfuerzo y sobre todo por el apoyo incondicional que me ha brindado transmitiéndome sus conocimientos a través de tutorías que fueron fundamentales para encaminar y profundizar en estas áreas de conocimiento.

A las personas que directa o indirectamente me han ayudado a que salga adelante este trabajo de Fin de Carrera.

ÍNDICE DE CONTENIDOS

CARÁTULA …… i
APROBACIÓN DEL DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN ii
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS iii
DEDICATORIA iv
AGRADECIMIENTO v
ÍNDICE DE CONTENIDOS vi
RESUMEN …… 1
ABSTRACT …… 2
ACRÓNIMOS …… 3
INTRODUCCIÓN 6
CAPITULO I: ESTADO DEL ARTE 8
1.1. Requisitos 9
1.1.1. Requisitos funcionales. 9
1.1.2. Requisitos no funcionales. 10
1.1.3. Requisitos de seguridad. 10
1.2. Elicitación de requisitos 11
1.2.1. Proceso de elicitación. 11
1.2.2. Técnicas de elicitación. 13
1.2.3. Análisis comparativo: técnicas de elicitación de requisitos. 15
1.3. Arquitectura y diseño de software 16
1.3.1. Retos del diseño. 17
1.3.2. Análisis comparativo (aspectos claves de diseño arquitectónico). 17
1.4. Resiliencia 18
1.4.1. Estándares de seguridad ISO 27000. 20
1.4.2. CERT Metodología de gestión de resiliencia (CERT-RMM). 21
1.4.3. Software resiliente. 27
CAPITULO II: DESARROLLO DE LA GUÍA METODOLÓGICA EN BASE A LAS ÁREAS DEL MODELO DE RESILIENCIA CERT-RMM. 35
2.1. Propósito de la guía 36
2.2. Herramientas y recursos tecnológicos base para el desarrollo de la guía metodológica 36
2.2.1. Definición de la técnica de elicitación. 36

2.2.2. Estándares de seguridad ISO 27000. 36
2.2.3. Áreas de proceso CERT-RMM. 40
2.2.4. Tipos de software. 46
2.2.5. Análisis comparativo: áreas de la metodología CERT-RMM y estándares ISO 27000 47
2.3. Diseño de la guía 48
2.3.1. Estructura de la plantilla. 48
2.3.2. Desarrollo de plantillas. 50
2.4. Beneficios de la guía 97
2.5. Aplicaciones de la guía 97
CAPITLO III: IMPLEMENTACIÓN DE LA GUÍA A TRAVÉS DE UN SISTEMA DE INFORMACIÓN 98
3.1. Tipo de aplicación 99
3.2. Metodología RUP 99
3.2.1. Gestión del proyecto. 99
3.2.2. Gestión del producto/software. 100
3.3. Herramientas para el desarrollo del SI 102
3.4. Prototipo del SI 102
3.4.1. Interfaz del SI. 102
3.4.2. Funcionalidades. 103
3.4.5. Resultados esperados. 111
3.5. Construcción del SI 111
3.5.1. Control de acceso. 112
3.5.2. Carga de datos. 112
3.5.3. Presentar datos. 112
3.5.4. Calcular datos. 112
3.5.5. Guardar datos. 113
3.6. Pruebas del SI 113
CAPITULO IV: VERIFICACIÓN DE LA APLICABILIDAD DE LA GUÍA METODOLÓGICA ……. 114
4.1. Parte I: Estadística descriptiva para la totalidad de sistemas encuestados 115
4.2. Parte II: Estudio comparativo del proceso de elicitación de requerimientos entre tipos de software 134
4.2.1. Parte II - 1: Tipos de software y técnicas utilizadas para el proceso de elicitación de requerimientos. 134

4.2.2. Parte II - 2: Requisitos de resiliencia de software en sistemas resilientes y sistemas no resilientes. 135
CONCLUSIONES 137
RECOMENDACIONES 139
BIBLIOGRAFÍA 140
ANEXOS 144
A. CERT-RMM 144
B. WBS 180
C. Cronograma 181
D. Documento de visión 182
E. Especificación de requisitos de software 195
F. Diagrama de casos de uso 204
G. Especificación de casos de uso 205
H. Diagrama de clases 231
I. Diagrama de secuencia 232
J. Diagrama de actividades 238
K. Manual de usuario 269

RESUMEN

Se pretende enfatizar la importancia de una elicitación de requisitos de resiliencia eficaz para determinar la resiliencia de los sistemas de información en base a técnicas de elicitación y el modelo CERT-RMM, además de una comparativa entre los tipos de requisitos, técnicas de elicitación, características de resiliencia de software y las áreas del modelo CERT-RMM, que estipulen la relación entre las actividades de resiliencia y la Ingeniería de software.

PALABRAS CLAVES: Elicitación de requisitos, resiliencia, modelo CERT-RMM, requisitos de resiliencia, software resiliente.

ABSTRACT

It is intended emphasize the importance of an effective requirements elicitation of resilience to determine the resilience of information systems based on elicitation techniques and CERT-RMM model, along with a comparison of the types of requirements elicitation techniques, characteristics resilience of software and areas of CERT-RMM model, stipulating the relationship between the activities of resilience and software Engineering.

KEYWORDS: Requirements elicitation, resilience, CERT-RMM model, resilience requirements, software resiliency.

ACRÓNIMOS

ADM. Gestión y Definición de Activos.

AM. Gestión de Acceso.

BSI. Instituto Británico de Estándares.

CERT. Equipo de Respuesta a Emergencias Informáticas.

CISM. Certificado en Gerencia de Seguridad de la Información.

CISSP. Certificado Profesional en Sistemas de Seguridad de la Información.

CISTI. Conferencia Ibérica de Sistemas y Tecnologías de Información.

CMMI. Modelo de Madurez y Capacidad Integrado.

COBIT. Objetivos de Control para la Información y Tecnologías Relacionadas.

COMM. Comunicaciones.

COMP. Cumplimiento.

CP. Cambios de Propagación.

CPU. Unidad Central de Procesamiento.

COSO. Comité de Organizaciones Patrocinadoras de la Comisión Treadway.

CRTL. Gestión del Control.

EC. Control del Entorno.

EF. Enfoque Empresarial.

ERM. Gestión de Riesgos Empresariales.

EXD. Gestión de Dependencias Externas.

FRM. Gestión de Recursos Financieros.

GBRAM. Metodología de Análisis de Requisitos Basado en Objetivos.

HRM. Gestión de Recursos Humanos.

IEC. Comisión Internacional Electrotécnica.

ID. Gestión de Identidades.

IMC. Gestión y Control de Incidentes.

ISO. Organización Internacional de Normalización.

ITIL. Biblioteca de Infraestructura de Tecnologías de Información.

ITU. Unión Internacional de Telecomunicaciones.

JAD. Desarrollo de Aplicaciones en Grupo.

KAOS. Adquisición del Conocimiento en la Especificación Automática.

KIM. Gestión de Información y Conocimiento.

LEL. Léxico Extendido del Lenguaje.

MA. Medición y Análisis.

MON. Monitorización.

MVC. Modelo-Vista-Controlador.

NIST. Instituto Nacional de Estándares y Tecnología.

MySQL. Sistema de Bases de Datos.

OPD. Definición de Proceso Organizacional.

OPF. Enfoque de Proceso Organizacional.

OTA. Formación y Conciencia Organizacional.

PDCA. Planear-Hacer-Chequear-Actuar.

PHP. Procesador de Hipertexto.

PM. Gestión de Personas.

RF. Requisitos Funcionales.

RISK. Gestión de Riesgos.

RNF. Requisitos No Funcionales.

RRD. Definición de Requisitos de Resiliencia.

RSTE. Ingeniería de Soluciones Técnicas Resilientes.

RUP. Proceso Unificado de Rational.

SC. Continuidad del Servicio.

SCSM. Componentes Software del Modelo Estructural.

SI. Sistemas de Información.

SLAs. Acuerdo a Nivel de Servicios.

SG. Meta Específica.

SGSI. Sistema de Gestión de Seguridad de la Información.

SP. Práctica Específica.

SVC. Servicios.

SWEBOK. Cuerpo de la Ingeniería de Software y del Conocimiento.

TI. Tecnología de la Información.

UTPL. Universidad Técnica Particular de Loja.

VAR. Análisis y Resolución de Vulnerabilidades.

WBS. Estructura de Desglose de Trabajo.

INTRODUCCIÓN

Actualmente los estándares de seguridad y metodologías de resiliencia promueven una revolución tecnológica en la ingeniería de software proyectada a conseguir sistemas de calidad, flexibles y sobre todo seguros.

En algunos proyectos de software ya se incluye el concepto de software seguro, el cual según (Ducón & Carrillo, 2013) consiste en aplicar las mejores prácticas de seguridad para el diseño, construcción y pruebas. De hecho, las relaciones que mantiene el software con otros activos y por ende con los servicios asociados, provoca el planteamiento de requisitos de resiliencia enmarcados en el software para conseguir seguridad y continuidad en sus operaciones cuando se materialicen los riesgos, ya que (Ducón & Carrillo, 2013) afirman que "un software seguro no necesariamente es un software resiliente, pero todo software resiliente debe ser un software seguro", en su desarrollo se debería incluir características propias de resiliencia como flexibilidad, confidencialidad, modularidad, escalabilidad, confiabilidad, etc., las cuales influyen directamente en el proceso de recuperación autónoma del software después de alguna interrupción.

Es así, que se desarrollará una guía metodológica para obtener requisitos de resiliencia de sistemas de información (SI), de modo que oriente a las organizaciones a incluir tales requisitos, tomando como base técnicas, modelos y estándares que garanticen seguridad y continuidad en los SI. A continuación se describe cada una de las secciones que compone este trabajo.

En la sección de Estado del Arte se describe los requisitos, el proceso y técnicas de elicitación, se analiza el diseño y arquitectura del sistema, se describe la resiliencia que incluye estándares ISO y la metodología CERT-RMM, y finalmente se mencionan las características claves que determinan la resiliencia del software.

En la sección de Desarrollo de la Guía Metodológica en base a las Áreas del modelo de resiliencia CERT-RMM se toma como base el estudio realizado en la sección de Estado del Arte para definir las herramientas a utilizar, el diseño, los beneficios y la aplicabilidad de la guía.

En la sección de Implementación de la Guía a través de un Sistema de Información se describe el tipo de aplicación a desarrollar, la metodología de desarrollo, las herramientas como lenguaje de programación, servidor de base de datos, etc., se define el prototipo y se codifica el software.

En la sección de Verificación de la aplicabilidad de la Guía Metodológica, una vez ya desarrollada la guía e implementada en el sistema de información desarrollado (propio), finalmente se evalúa en un sistema de información externo y muestra los resultados. Y finalmente se presenta las conclusiones y recomendaciones del trabajo realizado.

La importancia del trabajo de fin de titulación radica en el análisis del software resiliente, como factor primordial para el establecimiento de estrategias que mejoren la seguridad y garanticen el funcionamiento normal de los SI, posterior a un evento de interrupción, lo cual beneficia a la organización, usuarios y a las personas que deseen conocer el estado de resiliencia de sus SI.

Como solución se determinó las características que definen a un software como resiliente, además se diseñó y desarrolló plantillas de elicitación de requisitos de resiliencia en base a técnicas de elicitación de requisitos, características de resiliencia y la metodología CERT-RMM, que fueron implementadas en una aplicación web (que fue desarrollada).

Es grato referirse a los resultados del presente trabajo, pues gracias al esfuerzo realizado todos los objetivos se han cumplido con un alcance mayor al esperado, ya que a más de aplicarse en las organizaciones adyacentes a la Universidad Técnica Particular de Loja (UTPL) se aplicó también en organizaciones externas como Funeraria Jaramillo y Electrictelecom.

Son varios los conocimientos que se adquirió y fortaleció, la mayoría relacionados con resiliencia como la capacidad de tolerar la aparición de cambios imprevistos y recuperarse en un periodo de tiempo conocido, limitado y generalmente aceptable. Cabe mencionar que el conseguir información relacionada con este tema no fue una tarea fácil, pero el ingenio del ser humano es muy hábil, pues se indagó en bibliotecas virtuales, repositorios gratuitos y pagados, artículos científicos, informes, libros, etc. con la aspiración de encontrar todo el material posible y útil para el desarrollo del presente trabajo.

La metodología que se utilizó se basa en el estudio teórico con el cual se recogió toda la información y el estudio descriptivo mediante encuestas para la obtención e interpretación de resultados.

CAPITULO I: ESTADO DEL ARTE

1.1. Requisitos

Para iniciar un proyecto de desarrollo de Sistemas de Información (SI) es necesario conocer lo que se debe realizar, según Zebehacy (citado por Pressman, 2005) menciona que “las ideas son los bloques de construcción de las ideas”. En este caso se podría enfocar a los requisitos como “los bloques de construcción de un sistema” ya que Jacobson, Booch y Rumbaugh (citado por Fernández, Mnendoza, Martínez, Mendoza, & Sumano, 2003) los define como “una condición o restricción que el sistema debe cumplir”.

De hecho, el procesamiento de los requisitos incluye la especificación y validación de los servicios que el sistema debe proporcionar, su gestión se basa en el área de conocimiento de la Ingeniería de Requisitos definida en SWEBOK[1] donde se destaca la importancia de una recolección de requisitos eficaz como apoyo al desarrollo de sistemas de calidad.

Hay varias clases de requisitos, por ejemplo los que especifican de forma muy general la operación del sistema conocidos como requisitos de usuario y los que son más específicos en la definición de servicios y funciones llamados requisitos de sistema.

Los requisitos son necesidades que el cliente busca resolver con la ayuda de algún sistema, estos deben ser válidos y coherentes para que puedan ser representados como: historias, escenarios, reglas, etc., dentro de un documento formal que los respalde, ya que son la base para la definición del alcance del proyecto de software.

Existen varios tipos de requisitos para determinar el comportamiento y limitaciones del sistema, verificar y otorgar protección a sus procesos, los cuales que se detallan a continuación.

1.1.1. Requisitos funcionales.

Estos requisitos refieren a la funcionalidad del sistema, (Sommerville, 2011) los define claramente como “enunciados de servicios que el sistema debe proveer, de cómo debería reaccionar el sistema a entradas particulares y de cómo debería comportarse el sistema en situaciones específicas y en algunos casos explican lo que no debe hacer el sistema”.

[1] SWEBOK: Cuerpo de la Ingeniería de Software y del Conocimiento, se define como una guía al conocimiento presente en el área de la Ingeniería del Software, referencia: (SWEBOK, 2004)

La especificación de requisitos funcionales (RF) se puede considerar como la tarea más fuerte de la Ingeniería del Software, puesto que las interpretaciones que el desarrollador de sistemas asimila muchas de las veces no concuerda con lo que el cliente desea, lo cual tiende a provocar cambios en el sistema que retrasa la entrega y por ende incrementa el costo del proyecto de software. Por tales razones, (Sommerville, 2006) menciona que este documento debe estar completo (la completitud significa que todos los servicios solicitados por el usuario deben estar definidos) y se r consistente (la consistencia significa que los requisitos no deben tener definiciones contradictorias).

1.1.2. Requisitos no funcionales.

A diferencia de los requisitos funcionales, estos definen limitaciones para el sistema apoyándose en atributos de calidad claves como rapidez, tamaño, facilidad de uso, fiabilidad, robustez, portabilidad, aceptabilidad, etc. en cuanto al producto, la organización y externos según lo menciona (Sommerville, 2006), de tal modo se disminuye en un buen porcentaje el nivel generalista con el que la mayoría de los casos se define a los requisitos, que tiende a producir confusión y por consiguiente errores en el sistema.

De hecho, los requisitos no funcionales (RNF) no siempre se refieren al sistema a desarrollar sino que también pueden restringir los procesos que se deberán utilizar para el desarrollo del software. No se debe subestimar estos requisitos, ya que según el énfasis de (Sommerville, 2006) “el incumplimiento de un requisito no funcional puede significar que el sistema entero sea inutilizable”.

1.1.3. Requisitos de seguridad.

Constituyen aquellos requisitos mínimos que debe satisfacer un sistema para que pretenda ser considerado seguro. Según (Sommerville, 2006) y en base al estándar IEC 61508[2] se define dos tipos de requisitos de seguridad; los funcionales dedicados a las funciones de protección del sistema y los requisitos de integridad enfocados en la fiabilidad y disponibilidad en cuanto a la protección de sistema. También (Devanbu & Stubblebine, 2013) los define como una manifestación de una política organizacional de alto nivel en los requisitos detallados de un sistema específico.

Es así que los requisitos de seguridad son considerados parte de los RNF y complementan los RF con aspectos de fiabilidad y disponibilidad para mejorar la protección del SI.

[2] IEC 61508: Estándar internacional para la Gestión de Seguridad.

1.2. Elicitación de requisitos

(Ian & Pete, 1997) definen a la elicitación de requisitos como el proceso de descubrir los requisitos para un sistema a través de la comunicación con los clientes, usuarios del sistema y otras personas que tengan un interés en el desarrollo del SI.

La buena elicitación de requisitos ayuda a los usuarios a comprender lo que necesitan y a los desarrolladores a resolver lo que el cliente desea. Al culminar este proceso se obtiene como resultado requisitos necesarios, concisos, completos, consistentes, alcanzables, verificables, etc. para el desarrollo de un software de calidad.

1.2.1. Proceso de elicitación.

El proceso de la elicitación amerita el trabajo colaborativo entre analistas y clientes para descubrir las necesidades reales del producto y llegar a un mutuo acuerdo en cuanto a la visión y objetivos del proyecto a desarrollar.

(Borland, 2005) afirma que este proceso merece una inversión de tiempo por adelantado y que además debe ser manejado por un analista experto en el negocio, el cual debe cumplir un rol crítico para la administración del proyecto, ya que relaciona las necesidades de los stakeholders, el sistema y los requisitos de software.

1.2.1.1. Identificación de fuentes de información.

La información por naturaleza existe, para conseguirla se cuenta con estrategias de investigación que identifican las fuentes de información adecuadas para su extracción y su posterior transformación en conocimiento (información útil). Dentro de este proceso juega un papel importante el universo de información que marca el contexto de desarrollo del software.

Según (Kotonya & Ian, 1997) las fuentes que más se identifican son:

- Stakeholders: conformados por clientes, usuarios, expertos del dominio además de grupos formales e informales.
- Documentos propios del universo de discurso: constituido por actas de reunión, políticas, formularios, manuales.
- Documentos externos al universo de discurso: formado por manuales de otro software, libros y artículos sobre temas relacionados.
- Software interno/externo: constituye generalmente la parte lógica del proyecto.

En base a las aportaciones de (Antonelli & Oliveros, 2002) se identifican varios enfoques que complementan este estudio como el de (Antón, 1997) donde propone el desarrollo de

requisitos mediante un modelo donde los stakeholders puedan percibirlos y entenderlos con facilidad, reduciendo así la complejidad del problema y propone el método Goal-Based Requirements Analysis Method (GBRAM) el cual se centra en la identificación y abstracción inicial de los objetivos de todas las fuentes disponibles de información independientemente del alcance de los conocimientos base; no está demás mencionar que los requisitos deberán satisfacer los objetivos para los que fueron definidos; (Lamswerde, 2003) lo manifiesta en su especificación Adquisición del Conocimientos en la Especificación Automática (KAOS) la cual se enfoca en la captura de los requisitos de software y está muy relacionado con técnicas de Inteligencia Artificial.

Se habla de la necesidad de comprender los requisitos, pero ¿se está gestionando su fuente? para solventarlo *Mylopoulos, Chung, Liao, Wang y* Yu (citados por Antonelli & Oliveros, 2002) presentan su enfoque estimulando el análisis orientado a objetivos donde se realiza un seguimiento total de los factores que influyen de manera positiva como negativa para llegar a un cumplimiento total y fortalecimiento de las técnicas de análisis de requisitos.

Estos objetivos necesitan algo más para focalizar mejor su interacción así que *Rolland* (citado por Antonelli & Oliveros, 2002) plantea el uso de escenarios con el manejo de pares *Objetivo-Escenario* (G, Sc), para alcanzar niveles mucho más elevados de alternativas, refinamiento y composición.

Es importante recalcar también que el comportamiento de dichos objetivos dentro del sistema no se puede dejar de lado, esta visión la tuvieron (Loucopoulos & Karakostas, 1995) los cuales presentan su enfoque de *Visión Teológica* de los sistemas organizándolos en jerarquías.

Y por último se menciona el enfoque *Middle-Out* definido por (Hadad, Doorn, Kaplan, & Sampaio, 2003) que se basa en los modelos de Léxico Extendido del Lenguaje (LEL) y Escenarios orientado a la extracción máxima del conocimiento desde el momento de su planteamiento.

Técnicas de comunicación.

Gracias a la comunicación es posible recoger y transmitir información entre analistas y clientes durante el proceso de elicitación de requisitos.

Para lograr una comunicación de calidad (Oloriz, 2004) menciona técnicas que manejan niveles fundamentales de Abstracción y Retroalimentación, las cuales se describen a continuación.

- *Nivel de Abstracción:* la comunicación se verá afectada por la existencia de ruido cuando los individuos entran en diálogo al estar ubicados en diferentes niveles de abstracción (cultura).
- *Retroalimentación*: confirma la información recibida por parte del receptor hasta que sea correcta, de modo que el emisor podrá entender y confirmar una respuesta.

1.2.2. Técnicas de elicitación.

Existe un conjunto de técnicas para realizar este proceso de elicitación, donde la intervención del equipo de análisis y desarrollo, clientes y usuarios marca el éxito de sus resultados.

En la elección de la mejor técnica intervienen varios factores como los riegos, influencias ajenas de terceros y organizacionales en el proyecto, los niveles de detalle, en fin, entre las técnicas con las que actualmente se cuenta están las de muestreo, creatividad, observación y soporte. Dentro de las herramientas que más se utilizan, por que ofrecen mayor nivel de detalle, están:

1.2.2.1. *Entrevistas*.

Describe la comunicación directa con los actores que tienen el conocimiento sobre los objetivos del software y la posibilidad de validación inmediata. Dentro de la ingeniería de requisitos las entrevistas son realizadas con el objetivo de conocer características propias de los procesos de negocio y del software a desarrollar.

1.2.2.2. Encuestas/Cuestionarios.

Consta de una lista de preguntas que generalmente se aplica a un gran grupo de participantes, ofrece una serie de opciones finitas que los encuestados pueden responder sin sentir miedo al dar sus respuestas. Existen varias formas de realizar las encuestas entre ellas tenemos las encuestas en línea que según (Sharmila & Umarani, 2011) tienen un gran potencial debido a su fácil acceso y la retroalimentación potencial pero tiene sus límites, ya que se mantiene la duda acerca de quiénes son en realidad los encuestados.

1.2.2.3. JAD (Joint Application Development).

Basada en reuniones entre el cliente y los interesados en el proyecto, mantiene una estrategia de integración en los equipos por cada reunión, de modo que decrementa el

grado de dificultad al realizar la documentación. Si JAD permite fomentar la participación ¿Quiénes pueden participar en JAD? Entre las personas que pueden participar está un facilitador, representante de TI, observador, de manera primordial el *Patrocinador Ejecutivo* generalmente el líder que controla, incentiva, planea estrategias e informa a todos los miembros del estado del proyecto, además comparte soluciones y por último el usuario según lo mencionan (Rumbaugh, Blaha, Premerlani, Eddy, & Lorensen, 1996), ya que si no existiera una necesidad no habría un ¿por qué? para realizar proyectos.

1.2.2.4. Brainstorming.

"Otorga mucha importancia a las opiniones de los miembros del proyecto que cuentan como base en la toma de decisiones, ya que ayuda a entender a estos dos actores claves del proyecto como son el cliente y analista" según lo afirman (Rumbaugh, Blaha, Premerlani, Eddy, & Lorensen, 1996). De hecho no siempre puede ser útil, puesto que la información conseguida con esta técnica no puede ser del todo verídica, lo cual hace parecer un tanto riesgosa su utilización, sin embargo, el manejarse en grupos de trabajo se considera la manera más amplia de conseguir la información que en una entrevista donde intervienen sólo dos personas.

1.2.2.5. Casos de Uso.

Describen los pasos para desarrollar o llevar a cabo un proceso y por lo tanto representa los requisitos más importantes. (Rumbaugh, Blaha, Premerlani, Eddy, & Lorensen, 1996) identifican a los involucrados como: el cliente, usuario, arquitecto, desarrollador y líder del proyecto con los cuales se valida los requisitos, ayuda a determinar el alcance, se modela la interacción, evalúa riesgos, etc.

1.2.2.6. Prototipos.

Permite visualizar el software que se construirá, (Bastani, Fu, & Yen, 2008) manifiestan que los prototipos generalmente son de mayor utilidad cuando existe incertidumbre al recopilar las necesidades poco claras de los clientes ya que se presenta una visión un tanto acertada de cómo será el software.

Debido a que algunas técnicas son limitadas lo más recomendable será combinarlas con técnicas de cuestionarios, observación y documentación para obtener mejores resultados.

1.2.3. Análisis comparativo: técnicas de elicitación de requisitos.

Dentro de la elicitación se cuenta con diversas técnicas, las mismas que han sido mencionadas anteriormente, pero ¿cuál es el nivel de incidencia o importancia dentro de este proceso? Está claro que con dichas técnicas se levanta requisitos, pero cada técnica ¿extrae todos los tipos de requisitos? o ¿se enfoca en extraer un tipo de requisito en especial?

En respuesta a las interrogantes en la tabla 1 se presenta los tipos de requisitos por cada Técnica.

Tabla 1. Contrastación técnicas de recolección, comunicación y requisitos.

Técnicas de Elicitación	**Requisitos Funcionales**			**Requisitos No Funcionales**			**Requisitos de Seguridad**		
	Alto	Medio	Bajo	Alto	Medio	Bajo	Alto	Medio	Bajo
Entrevistas	X					X			X
Encuestas/ Cuestionarios	X				X			X	
JAD	X					X			
Brainstorming		X				X			X
Casos de Uso	X					X			X
Prototipos		X			X			X	
Nivel de Abstracción									
Retroalimentación									

Fuente: El autor.

En base al estudio realizado por (Durán & Bernárdez, 2000) se muestra que en un 75% son los requisitos funcionales aquellos que presentan un alto nivel de percepción por la mayoría de las técnicas de elicitación, ¿por qué sucede esto? Dichos requisitos constituyen la parte inicial en la definición del SI a construir, los mismos que extraen de manera directa las necesidades que los clientes necesitan satisfacer y así los analistas podrán moldearlas en funcionalidades, actores, procesos, etc.

Entonces, si ya se cuenta con la necesidad del cliente, lo que se debe desarrollar e implementar son las estrategias de trabajo que reafirmen los requisitos recogidos, logrando de esta manera procesos eficientes que suplan el porcentaje restante correspondiente a los requisitos no funcionales y de seguridad.

No está demás mencionar que en todas las técnicas para la elicitación de requisitos funcionales, no funcionales y de seguridad debe existir una buena comunicación entre el

analista y cliente, de modo que se culmine el proceso de recolección con un entendimiento mutuo entre estos individuos.

1.3. Arquitectura y diseño de software

El mantener un orden ¿incluye también al software? Pues sí, todo deberá mantener un orden y más aún el software, ya que al cumplir varias funcionalidades estas deben estar separadas en subsistemas más pequeños, cada uno enfocado en componentes tanto de hardware como software.

Entonces, ¿por dónde empezar? Es aquí donde el diseño juega un papel importante ya que según (Rumbaugh, Blaha, Premerlani, Eddy, & Lorensen, 1996) se caracteriza como "la estrategia de alto nivel para resolver problemas y construir soluciones" que se adapten a los requisitos (funcionales y no-funcionales), de tal forma que pueda conservarse hasta culminar el proyecto.

Todo lo que se realice en el diseño representará la arquitectura del sistema, ya que según (Pressman, 2005) el diseño se enfoca en "la estructura de los componentes, sus propiedades e interacciones, que proporcionan una vista general y aseguran que se obtenga lo que desea".

Pero ¿por qué tanta importancia a la arquitectura? La arquitectura juega un papel muy importante puesto que como mencionan (Rumbaugh, Blaha, Premerlani, Eddy, & Lorensen, 1996) para cumplir con los requisitos no puede trabajar sola, sino que necesita de la comunicación permanente entre todos sus componentes para estar informada de cómo trabajan juntos.

De hecho, deben existir varias arquitecturas para un proyecto de software, pero decidir cuál es la que mejor se adapta para el proyecto que está desarrollando es lo que se torna complicado; (Braude, 2003) alude que: "Suele ser difícil satisfacer todas las metas, ya que un diseño que satisface una, puede no satisfacer otra. Por esto se les asignan prioridades". Pues bien, es importante recalcar que el diseño no puede trabajar sólo, (Sommerville, 2011) lo relaciona con "el establecimiento de un marco estructural básico donde identifica los principales componentes de un sistema y la comunicación entre los mismos".

No todos los grandes pensadores y escritores de la Ingeniería de Software consideran importante mencionar la gran intervención de los requisitos no-funcionales en el estilo de la arquitectura, es así, que en este estudio, al igual que (Sommerville, 2011) se resalta los

que más impacto tienen, como lo es: rendimiento enfocado en la localización de operaciones, seguridad que utiliza la estructura en capas, protección que separa sus operaciones en componentes individuales o más pequeños, disponibilidad que incluye componentes redundantes y problemas de mantenibilidad que usa componentes autocontenidos de grano fino que puedan cambiarse con facilidad, todos estos requisitos con un solo objetivo de apoyar la construcción de sistemas de información con una arquitectura robusta.

Se puede concluir en cuanto al diseño, que en un sistema a más de los atributos mencionados, su arquitectura deberá ser consistente y flexible de modo que pueda acoplarse a la mayoría de las necesidades y mejor aún ser capaz de recuperarse ante los posibles incidentes sin dejar de cumplir sus objetivos, estos aspectos son fundamentales en el tratamiento de la *resiliencia* la cual se hablará en mayor detalle en puntos posteriores.

1.3.1. Retos del diseño.

Al diseñar software es inevitable enfrentarse a problemas o dificultades que no necesariamente son del dominio del problema o aplicación que en fin afectan el comportamiento y funcionalidad del sistema. Los principales aspectos son:

- *Concurrencia*, el cual cubre el problema de planificación, sincronización y eficiencia, al descomponer el software en procesos o tareas.
- *Control de Eventos,* organiza y maneja datos de eventos (reactivos o temporales) utilizando callbacks o invocación implícita.
- *Interacción y Presentación,* enfocado en la interacción del usuario y las estrategias de presentación de la información, la más común es el MVC (Modelo-Vista-Controlador).
- *Persistencia de Datos,* maneja datos externos o superiores independientes a las ejecuciones del software.

1.3.2. Análisis comparativo (aspectos claves de diseño arquitectónico).

Para mantener equilibrio dentro del diseño y la arquitectura del sistema se deberán analizar aspectos claves mencionados en la tabla 2, los cuales en caso de sufrir cambios ya sean planeados o inesperados el impacto no debería ser muy notable, de modo que se demuestre la eficacia en su arquitectura, esto en cuanto al mejor de los casos, pero ¿qué pasaría si dichos cambios sobrepasaran el nivel de tolerancia del sistema? Sería inevitable una crisis o inclusive la baja del mismo en el peor de los casos.

El diseño se incluye dentro de la arquitectura general del sistema, afectando también de manera especial a los requisitos no-funcionales, por ello se realiza una comparación de los aspectos claves del diseño con las vistas fundamentales de la Arquitectura (lógica, de proceso, física, desarrollo).

Es así, que en la tabla 2 lo que se puede denotar es la necesidad de colaboración de las clases de diseño como medida de interconexión que dependen además de la complejidad de la interfaz entre módulos.

En si se intenta conseguir el menor nivel posible de acoplamiento utilizando conexiones sencillas de modo que el software sea fácil de entender.

Tabla 2. Comparación aspectos de diseño y vistas de arquitectura de software.

Aspectos de Diseño	**Lógica**	**De proceso**	**Física**	**Desarrollo**
Comunicación	X	X	X	X
Colaboración	X	X		
Reusabilidad			X	X
Prueba individual			X	X
Integración gradual de los componentes			X	X
Flexibilidad				
Tolerancia a cambios				

Fuente: El autor.

Así la reusabilidad podrá minimizar tiempos de diseño y por lo tanto el número de pruebas facilitando la integración de los componentes resultantes en cada vista que conforman la arquitectura del software, denotando así la flexibilidad y tolerancia a cambios que cubre todas las vistas para alcanzar la eficiencia en los procesos y lograr que exista eficacia en el diseño arquitectónico.

1.4. Resiliencia

La falta de estrategias para el tratamiento de inconvenientes que se suscitan en los SI puede implicar el incremento de costos, recursos, tiempo e incluso la baja del sistema. Es así, que hoy en día para mejorar la protección del SI existe lo que se conoce como *resiliencia,* (Starr, Newfrock, & Delurey, 2003) la definen como la capacidad de resistencia ante los riesgos, regresando a un estado original, siempre y cuando el impacto no exceda el límite de tolerancia, y sin dejar de cumplir con sus objetivos misionales.

La resiliencia según se menciona en (Vanthinking, 2013) cubre tres áreas como son:

- *Gestión de Riesgos y Desastres:* Lo que se desea es estar preparados para eventos de alto impacto dentro de la organización, algunas de ellas no aceptan este enfoque ya que les implica gastar recursos así que su nivel de vulnerabilidad crece. Si el evento ocurre ¿Quién sería el culpable? ¿Será acaso el encargado de la toma de decisiones? Un caso típico es culpar a aquellos que ignoraron los factores desencadenantes más pequeños que llevaron a la caída de la última falta según lo menciona (Vanthinking, 2013), pero cabe mencionar que sí podría ser responsabilidad de los encargados de la toma de decisiones al presentar cierto grado de negligencia y de la organización por no tomar atención y no invertir para el tratamiento de eventos supuestamente pequeños.
- *Desarrollo Sostenible:* Holling (citado por Mitchell & Harris, 2012) piensa que "la resiliencia se ha convertido en una fusión de ideas de varias tradiciones disciplinarias, incluyendo la estabilidad del ecosistema" donde se asegura que el desarrollo sostenible se lleva a cabo con amplias visiones de consistencia y mejora en la organización.
- *Ventaja Estratégica:* En algunas ocasiones para la resolución de problemas se cuenta con el conocido *Plan B* (solución adicional), pero ¿qué pasa cuando no se la tiene? Al no tenerla se adquiriere cierta vulnerabilidad y la organización queda propensa a sufrir inconsistencias, entonces ¿por qué no contar con una estrategia que sea sostenible frente a los cambios del entorno? La resiliencia según (Mitchell & Harris, 2012) no es lo contrario de la vulnerabilidad, de como un individuo puede ser predispuesto a un impacto y se puede recuperar en forma oportuna y eficiente, sino que ayuda a facilitar decisiones y acciones para el refortalecimiento de las oportunidades, es así que también este enfoque considera a la resiliencia como próspera sobre la gestión del cambio según las menciones de (Davies, 1993), (Manyena, 2006) y, finalmente (Mitchell & Harris, 2012) que ubica a la resiliencia en el contexto de sistemas dinámicos.

Ser resiliente es más que ser sostenible menciona (Vanthinking, 2013), es cumplir con las condiciones, enfrentar riesgos, regresar los procesos a la normalidad, mejorar y controlar los procesos, y finalmente continuar con sus obligaciones sin que se vea alterado por las interrupciones.

1.4.1. Estándares de seguridad ISO 27000.

Se habla mucho de seguridad y calidad, para los cuales existen estándares establecidos como son las normas ISO. Al tratar el tema de resiliencia también se incluye la seguridad en base a la intervención de los estándares ISO con su serie ISO/IEC 27000, que se enfocan en mantener una gestión competente del Sistema de Gestión de Seguridad de la Información (SGSI). Existen algunos estándares dentro de esta familia, como son:

- ISO 27001: Detalla lo primordial que son los requisitos de SGSI.
- ISO 27002: Describe los objetivos de control en cuanto a la seguridad de la información.
- ISO 27003: Mantiene información concerniente al uso del modelo PDCA (Plan-Do-Check-Act).
- ISO 27004: Determina la eficacia de un SGSI basándose en técnicas y métricas de medida.
- ISO 27005: Enfoca estrategias de gestión de riesgos que atenten contra la seguridad de la organización.
- ISO 27006: Interpreta criterios de auditoría y acreditación.
- ISO 27007: Se enfoca directamente en la auditoria del SGSI.
- ISO 27011: Se apoya en la Unión Internacional de Telecomunicaciones (ITU) para enfocarse específicamente en esta área.
- ISO 27031: Mantiene su mirada en tecnologías de información y comunicación, para el desarrollo de técnicas de continuidad de negocio.
- ISO 27032: Se enfoca en la ciber-seguridad.
- ISO 27033: Se basa en las redes, todo lo que es seguridad, arquitectura, escenarios, acceso remoto, implementación, comunicaciones, etc.
- ISO 2734: Describe la seguridad en cuanto a las aplicaciones.

Estos son los estándares básicos que se toman en consideración en las organizaciones, pero como se hablará en puntos posteriores del modelo CERT-RMM es importante mencionar el estándar ISO-27799, el cual se enfoca en la salud informática garantizando la protección de la información en cuanto a confidencialidad, integridad y disponibilidad.

1.4.1.1. ISO 27001.

Este estándar proporciona un modelo que establece, implementa, opera, monitorea, revisa, mantiene y mejora el SGSI ya que en su contenido se describe puntos importantes

como comprender los requisitos reales de seguridad, establecer políticas y objetivos que protejan la información, facilitar la implementación y operación del control de riesgos que ayudarán en el monitoreo del desempeño y el mejoramiento continuo. Por tales razones la inclusión de este estándar será bastante significativo para la seguridad organizacional.

1.4.1.2. ISO 27005.

Proyecta su estructura en aval de la gestión de riesgos en la seguridad de la información en las organizaciones, inicia con la evaluación de los activos importantes como lo es la información para el soporte de los requisitos del sistema según lo establece en la norma ISO 27001.

1.4.1.3. ISO 27034.

Define conceptos, marcos y procesos para ayudar a las organizaciones a integrar la seguridad dentro de su ciclo de vida de desarrollo de software, con el objetivo de proporcionar el nivel de seguridad deseado y necesario en apoyo del SGSI.

1.4.2. CERT Metodología de gestión de resiliencia (CERT-RMM).

(Peláez, 2012) caracteriza al modelo como una guía que medirá la capacidad actual, el establecimiento de objetivos de mejora, planes y acciones para cerrar las brechas identificadas, basados en un enfoque de mejora de los procesos de seguridad, continuidad del negocio y los aspectos de la gestión de operaciones de Tecnología de la Información (TI) en base a las aportaciones de (Caralli, Allen, & White, 2011). CERT-RMM no busca reemplazar las operaciones y procesos de las organizaciones sino brindar ayuda en el mejoramiento de su recuperación ante los riegos operacionales y de software.

En base a lo que mencionan (Caralli, Allen, & White, 2011) que esta metodología CERT-RMM no cubre las actividades necesarias para establecer y entregar servicios de gerencia, se puede acotar que CERT-RMM aborda algunos procesos interesantes de TI descritos en el punto anterior de resiliencia pero se incluye con otras actividades como contingencia, requisitos de resiliencia, servicio continuo y manejo de controles.

Ahora, para el establecimiento de sistemas de gestión de servicios con alto grado de madurez no lo trata el CERT-RMM sino el Modelo de Madurez y Capacidad Integrado (CMMI). Sin embargo, a medida que la gestión del servicio requiere una fuente considerable de resiliencia, CERT-RMM puede utilizar CMMI-Services (SVC) para ampliar la definición de la prestación de servicios de alta calidad e incluir la resiliencia como un atributo de calidad, según lo mencionan (Caralli, Allen, & White, 2011).

Las demandas y los factores de estrés según (Caralli, Allen, & White, 2011) conspiran para obligar a las organizaciones a repensar la forma de llevar a cabo algunos aspectos de la gestión del riesgo operacional y cómo hacer frente a la resiliencia de los procesos y servicios empresariales de alto valor. Estos riesgos operacionales impactan de manera directa a los elementos base de las organizaciones compuestos por los activos y procesos internos.

La resiliencia operacional aborda elementos claves como lo son las *personas,* constituyendo una parte sumamente necesaria para hacer posible que el servicio funcione y lo haga de forma eficiente; la *información,* permite mantener metas, planear estrategias, desarrollar planes, etc. que al unirlos se transforman en conocimiento; la *tecnología,* que facilita el desarrollo de la organización al poderse acoplar a diferentes fines empresariales y por último las *instalaciones,* concernientes a la estructura física de la organización donde se desarrollan los servicios.

1.4.2.1. Marco de trabajo del CERT-RMM.

Este modelo al igual que los demás, es calificado de acuerdo al nivel de capacidad, esto es en *incompleto, realizado, gestionado y definido,* similares al modelo de madurez CMMI, que sirve de guía a las organizaciones para estructurar y mejorar continuamente sus procesos logrando un alto grado de institucionalización.

En el modelo CERT-RMM intervendrán mayormente aspectos relacionados con la seguridad, la continuidad de los procesos, manejo de riesgos y otros aspectos importantes, pero ¿cómo se relaciona con el CMMI? Dentro del modelo CMMI se habla de capacidad y madurez de las organizaciones, *capacidad* en cuanto a los procesos que estructuran un *área de proceso* los cuales mantienen metas y prácticas que cumplir, y *madurez* en cambio involucra un conjunto de *áreas de proceso* para realizar una mejora continua de modo que se pueda controlar la seguridad en la organización.

Mientras exista mayor madurez en las organizaciones la calidad de sus productos o servicios será más rentable y ya no dependerá de los integrantes y esfuerzos sobrenaturales, sino que se regirá en definiciones, gerenciamiento, mediciones, control y utilización de procesos claros basados en los datos históricos con la opción de tomar expectativas realistas.

Cuando se habla de madurez en las organizaciones, ¿se aplica también la madurez en los procesos? Al contar con niveles de madurez en la organización es porque los

procesos son confiables, entonces ¿se podría decir que se cuenta con procesos maduros? Los procesos presentan niveles de madurez siempre y cuando se verifique y valide su rendimiento, se mantenga documentación de sus definiciones, se cuente con personal apto y capacitado para los procesos y se disponga de elementos cuantificables, a partir de los cuales pueda proponer mejoras.

¿Madurez es igual a mejora continua?

No, son distintos, aunque la mejora continua también va ligada a la calidad según (Deming, 2012) “consiste en desarrollar ciclos de mejora en todos los niveles, donde se ejecutan las funciones y los procesos de la organización”.

Al referirse a modelos de madurez, ya se habla de CMMI y también de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) que es otro modelo, un tanto diferente a CMMI y CERT-RMM por presentar 6 niveles de madurez, pero en su metodología son bastante parecidos.

El modelo CERT-RMM soporta algunas operaciones de TI presentados también en algunos marcos de trabajo que incluyen los estándares, ISO, COBIT, tales como:

- Control y gestión de riesgos que establecen procesos de análisis y detección de eventos particularmente incidentes (Caralli, Allen, & White, 2011).
- Análisis de vulnerabilidades y resolución, estos identifican, analizan y gestionan las vulnerabilidades dentro de la organización (Caralli, Allen, & White, 2011).
- Gestión de controles, encargado de gestionar el sistema de control interno asegurando eficiencia en las operaciones (Caralli, Allen, & White, 2011).
- Requisitos de resilencia, maneja todo lo referente a los requisitos operacionales, los cuales parten del estudio de servicios y activos de la organización.

Para mantener un proceso resiliente debe mantenerse prevenido ante riesgos, entonces para este tipo de casos también existen estándares que apoyen este proceso como el Instituto Nacional de Estándares y Tecnología (NIST) que mantiene la intención de mejorar la seguridad de la información y fortalece los procesos de gestión de riesgos.

La organización debe introducirse en el mercado, dándose a conocer en más espacios que impulsen un mayor crecimiento orientado hacia el reconocimiento internacional. Para suplir esta necesidad existen las conocidas certificaciones, en relación con este estudio está el Comité de Organizaciones Patrocinadoras de la Comisión Treadway - Gestión de

riesgos empresariales (COSO-ERM)[3] que es una organización voluntaria del sector privado cuya misión es mejorar la calidad de la información financiera mediante la ética en los negocios, los controles internos efectivos y el gobierno corporativo según lo menciona (Ambrosone, 2004). Es así que se convierte en una propuesta sumamente interesante que las organizaciones podrían adoptar para enfrentar los riesgos, ya que ninguna empresa se encuentra libre de ellos.

Como otra opción se encuentra en el Instituto Británico de Estándares (BSI[4]) la cual es una organización global que ofrece servicios basados en normas, formación, auditoria y certificación en más de 100 países, dentro de esta línea están los estándares ISO 27000 y 20000.

Pero ahora ¿cómo aseguramos eficiencia en las operaciones? Como solución está la Biblioteca de Infraestructura de Tecnologías de Información (ITIL) que abarca procedimientos idóneos para la administración de servicios en la organización, la cual se mantiene en continuo contacto con CMMI, COBIT, ISO, para conseguir un mayor entendimiento de lo importante que es gestionar bien los servicios de la organización para satisfacer tanto los objetivos del negocio como las expectativas del cliente.

1.4.2.2. Análisis comparativo: áreas del CERT-RMM.

El modelo CERT-RMM se compone de 26 áreas concernientes a gestión de acceso, control, ambiental, tecnológico, identidad, incidentes, riesgos, financiero, de personal, comunicaciones, cumplimientos, vulnerabilidades, etc., las cuales se las agrupa de acuerdo a los activos del CERT-RMM con los que más se relacionan tales como personal, información, tecnología e instalaciones.

Pero, ¿cuántas en realidad pertenecen a cada activo? ¿Los activos se relacionarán también con las áreas generales de la resiliencia? Como respuesta ante estas interrogantes está la figura 1, presentando el número de áreas que abarca cada activo.

Dentro de la metodología intervienen 4 activos fundamentales como son: la información, personas, tecnología e instalaciones caracterizados como fundamentales en apoyo al proceso de resiliencia sea organizacional o con enfoque en el software. Una visión más

[3] COSO-ERM: Metodología creada por la Comisión Treadway el cual nace como una versión gestionada a través del manejo de riesgo.

[4] BSI: Multinacional cuyo fin se basa en la creación de normas para la estandarización de procesos.

clara y amplia de estos activos se presentará en puntos posteriores donde se hable de software resiliente.

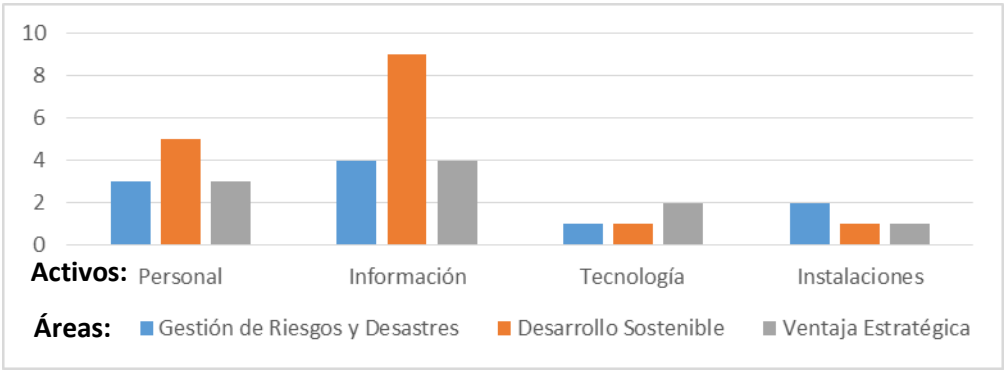


Figura 1. Comparación de activos y áreas de la metodología CERT-RMM.
Fuente: El autor.

Según la figura 1 con la comparación de los activos del CERT-RMM y tomando las áreas de resiliencia (Gestión de Riesgos y Desastres, Desarrollo Sostenible y Ventaja Estratégica) pues el activo que mayor áreas del CERT-RMM agrupa es el activo de Información, puesto que gestiona procesos, estrategias, planes, criterios, reglas, requisitos, cambios, etc. Para el desarrollo, protección y mantenimiento de la resiliencia organizacional, pero eso no es todo, pues se puede observar también que el área de resiliencia que denota incidencia en este activo es el desarrollo sostenible, el cual asegura que se lleve a cabo amplias visiones de consistencia y mejora en la organización.

1.4.2.3. Análisis comparativo: estándares ISO y áreas de la metodología CERT-RMM.

La metodología CERT-RMM gestiona la resiliencia en el software, la cual maneja aspectos claves compartidos con los estándares de seguridad ISO 27000.

Cada uno de los estándares ISO se encuentra relacionado con un área de la metodología CERT-RMM según lo muestra la tabla 3, los mismos que se explican a continuación:

- ISO 27001 al ser la primera serie de estándares ISO 27000 presenta los puntos generales que deben considerarse para gestionar la seguridad de la información, entre los cuales está la comprensión de los requisitos de seguridad que se relaciona con el área de RRD, y ADM al utilizar la información como el activo que se está gestionando; además implementa principios que gobiernan la evaluación de riesgos al igual que en las áreas CRTL y RISK del CERT-RMM y finalmente se evalúa el resultado en base a procesos y acciones que apoyan el mejoramiento continuo de acuerdo al enfoque sea organizacional o de software.

Tabla 3. Áreas CERT-RMM y estándares ISO 27000

Áreas CERT-RMM	ISO 27001	IS0 27005	ISO 27034
ADM ***(Gestión y definición de los activos)***	X	X	X
CRTL ***(Gestión del control)***	X	X	X
EXD ***(Gestión de dependencias externas)***			X
RRD ***(Definición de requisitos de resiliencia)***	X	X	X
RRM ***Gestión de requisitos de resiliencia)***		X	X
RISK ***(Gestión de Riesgos)***	X	X	X
RSTE ***(Ingeniería de soluciones técnicas resilientes)***	X		X
SC ***(Continuidad del Servicio)***	X		X
TM ***(Gestión de tecnología)***			X

Fuente: El autor.

- ISO 27005 identifica los activos de información propensos a sufrir riesgos y define medidas de protección para gestionar las consecuencias si los riesgos se ejecutan, estas actividades son similares a las que se realiza en las áreas de ADM y RISK del CERT-RMM ya que entre sus métodos de control especifican uno conocido como el plan de gestión de riesgos(que también lo realiza el ISO 27005); este estándar define lineamientos para la implementación de requisitos en un SGSI mientras que las áreas RRD y RRM definen requisitos y gestionan su cumplimiento exitoso en el software.
- ISO 27034 se enfoca directamente en el software con la identificación de procesos, personas, datos, tecnología que intervienen en su seguridad (estos aspectos se consideran como activos en el área de ADM), gestiona también requisitos que no se ejecutan de manera aislada sino como parte de los procesos al igual que en RRD y RRM del CERT-RMM. A diferencia de los estándares anteriores aquí se especifica criterios de aceptación de outsourcing como en el área de EXD para la aplicación satisfactoria de la seguridad, con base en el enfoque de gestión de riesgos y controles de seguridad definidos en los estándares ISO 27005 e ISO 27001. Adicionalmente implementa estrategias de supervisión y control para garantizar seguridad al sistema, mientras que en la metodología CERT-RMM son tres las áreas que llegan a mantener

relación con dichas estrategias ya que RSTE define lineamientos que diseña, desarrolla e implementa soluciones en función de las amenazas y el entorno de riesgo al que se enfrentan para proteger a los activos, SC identifica y prioriza los servicios, establece planes de continuidad, y el área de TM que establece y administra la tecnología para facilitar el desarrollo y satisfacción de los requisitos de resiliencia con énfasis en conseguir integridad y disponibilidad en las operaciones del SI.

1.4.3. Software resiliente.

La resiliencia del software consiste en la capacidad de recuperación de los SI frente a los riesgos ya que se adapta a condiciones cambiantes y continúa con el funcionamiento normal de sus operaciones, pero ¿cuándo un SI es resiliente? Lo veremos a continuación.

1.4.3.1. Características del software resiliente.

Para que el software sea considerado como resiliente debe cumplir con determinadas características que proponen ciertos autores.

(Huhn, 2013) como autor y director del proyecto AKKA[5] menciona algunas características, se cita las más importantes:

- Modularidad, el software es segmentado en componentes que actúan de forma independiente, de modo que si uno de ellos falla no afectará al funcionamiento de los demás.
- Acoplamiento mínimo entre componentes, evita la dependencia, puesto que la información que posea un componente con respecto a otro perderá su valor cuando se ejecute la recuperación de errores, ya que se actualiza la información y deja a uno de ellos vulnerable al fracaso de otro.
- Disponibilidad, los métodos se ejecutan en el subproceso que realiza la llamada, una vez que esta se completa su valor resultante estará inmediatamente disponible para recibir los resultados antes de continuar con dicho proceso, de tal modo que todos los efectos secundarios ocurran al retornar el método.
- Acoplamiento flexible, se utiliza un subproceso secundario para que los componentes puedan comunicarse entre sí, de modo que haya cierto tiempo vacante para el procesamiento de los mensajes y pueda ejecutarse de forma independiente en un solo hilo.

[5] AKKA: Software altamente concurrente, distribuido y, orientado a eventos tolerantes en la JVM.

- Redundancia o tolerancia a fallas, cada componente posee un supervisor que se encarga de resolver los errores, puesto que implementa la *supervisión jerárquica* (padre-hijo), donde cada actor padre define una estrategia de control en la que decide si un actor hijo se reanuda, reinicia al estado inicial o se detiene por completo.

(Black & Windley, 1997) en su artículo "Verifying Resilient Software" analizan la resiliencia de un servidor web donde se puede extraer algunas características, tales como:

- Flexibilidad, el tamaño del diseño debe ser pequeño por lo que es factible para examinar a fondo las propiedades de seguridad.
- Control de acceso, como medida de protección que incluye algunos privilegios de operación para limitar la entrada y salida de usuarios e información.
- Confidencialidad, para evitar el acceso en archivos sensibles o especiales como contraseñas o archivos de dispositivos, se establece medidas de restricción a los archivos del sistema.
- Redundancia, se incluye como método de protección (tolerante a fallas y difícil de verificar) para contrarrestar las fallas detectadas en los componentes antes que se conviertan en vulnerabilidades del software.
- Operatividad, los usuarios u operadores del software se encargan de realizar archivos disponibles basándose en varias medidas concretas de protección, para reducir el error humano y disminuir las posibilidades de riesgos y alteraciones severas en el funcionamiento normal del software.

Según Oxford Dictionaries[6], un software para ser resiliente debe cumplir con:

- Elasticidad, puesto que la presencia de cambios y riesgos inesperados por lo general alteran la funcionalidad de los sistemas. Ahora, el software resiliente no evade estas situaciones sino que debe contar con estrategias para enfrentarlas, logrando de esta manera que aún con la presencia de dichas situaciones, el software pueda seguir funcionando normalmente para lograr el cumplimiento de su misión.
- Continuidad, se considera importante que el software enfrente los riesgos en el menor tiempo posible y logre una interrupción mínima en los procesos y funciones del

[6] Oxford Dictionaries: Diccionario publicado por la editorial Oxford University Press, considerado el más erudito y completo diccionario de la lengua inglesa, así como el principal punto de referencia para su estudio etimológico.

sistema, de modo que puedan recuperar su estado normal y no exista desequilibrio en su funcionamiento.

(Hernández, 2013) en su publicación “Software Resilience”, menciona:

- Redundancia-Tolerancia a fallas, el software debe ser capaz de soportar eventos inesperados y seguir con su trabajo, sin dejar tiempos muertos de inactividad.
- Disponibilidad, el software debe estar activo y utilizable durante largos períodos de tiempo, con o sin la existencia de interrupciones.
- Continuidad, el tiempo de recuperación debe ser mínimo para que el rendimiento considere un nivel aceptable de error y pueda acoplarse a ello, dependiendo principalmente del grado de preparación sea a través de la continuidad del negocio o planes de recuperación ante desastres.

(Axelrod, 2009) certificado como CISSP[7] and CISM[8] en su artículo “Investing in Software Resiliency”, menciona:

- Complejidad, las rutinas de resilencia se incorporan mejor en sistemas individuales que presentan una complejidad manejable, en los cuales se disminuye las posibilidades de fallos y se obtiene una respuesta eficaz cuando se presenten.
- Interdependencia e interconexión, se maneja en porcentajes mínimos y para proteger esta situación incluye rutinas de control que preservan la integridad y la continuidad del funcionamiento del sistema.
- Conmutación por error, se utiliza en los sistemas de copia de seguridad, los cuales se ejecutan en paralelo con el sistema principal y cuando detecta un error automáticamente cambia a la copia de seguridad, que puede estar en el mismo sitio o fuera del sitio.

(Ibrahim, Wan Kadir, & Deris, 2008) en su artículo “Comparative Evaluation of Change Propagation Approaches towards Resilient Software Evolution” mencionan:

[7] CISSP (Certified Information Systems Security Professional): Certificación de alto nivel profesional otorgada por la (ISC)2 (International Information Systems Security Certification Consortium, Inc), con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información.

[8] CISM (Certified Information Security Manager): Certificación para administradores de seguridad de la información otorgada por ISACA (Information Systems Audit and Control Association).

- Facilidad de modificación, gestiona la propagación de cambios que se realiza de forma iterativa para cada uno de los componentes y como se trata de un proceso manual, se incluye los CP[9] que muestran las etapas en la gestión de la solicitud de cambio.
- Capacidad de análisis, para identificar las partes que han de ser modificadas con la adición de nuevos requisitos que mejoren el software para ayudar en la productividad y calidad del mismo.
- Adaptabilidad, para realizar el cambio de propagación de programas en varios idiomas utiliza SCSM[10], que consta de aplicaciones de bases de datos distribuidas heterogéneas que se basan en el gráfico de reescritura técnica por Rajlich[11].

(Merkow & Raghavan, 2011) en su libro “Secure and Resilient Software Development” mencionan:

- Disponibilidad, incluye espacios de tiempo para el mantenimiento del software, de modo que pueda tolerar las interrupciones del sistema durante el tiempo que el usuario se encuentra interactuando.
- Eficiencia, enfocado en el nivel de consumo de recursos informáticos, como ciclos de CPU, memoria, espacio en disco, tampones y canales de comunicación, que utiliza dos dimensiones como la capacidad (número máximo de usuarios o transacciones) y la degradación de los servicios para la gestión transacciones en el mismo periodo de tiempo.
- Interoperabilidad, referido a la utilización de las normas internas y herramientas para el desarrollo, de esta manera se aprovecha las herramientas empresariales estandarizadas existentes para implementar características y funciones, que incluyen bibliotecas criptográficas, inicio de sesión único y definiciones comunes de las bases de datos y estructuras de datos para usos internos específicos.
- Manejabilidad, permite mover la aplicación en todo el hardware disponible, según sea necesario o ejecutar el software en una máquina virtual, lo que significa que los desarrolladores no deben vincular la aplicación a un hardware específico o software externo no soportado.
- Acoplamiento flexible, cuando la clase dependiente sólo contiene un puntero a una interfaz, el mismo que puede ser implementado por una o muchas clases concretas.

[9] CP: Cambios de Propagación de procesos en las partes críticas de la gestión de cambios de software.
[10] SCSM: Componentes Software del Modelo Estructural.
[11] V. Rajlich: Autor del artículo "A Model for Change Propagation Based on Graph Rewriting".

- Acoplamiento débil, al agregar nuevas clases sin tener que modificar y recopilar las clases dependientes, lo cual proporciona extensibilidad y capacidad de gestión a los diseños.
- Mantenibilidad, ya que se refiere a la estabilidad y adaptabilidad del software después de realizar modificaciones posteriores a la entrega, para corregir fallos o mejorar el rendimiento.
- Rendimiento, aborda el tema concerniente a la velocidad de procesamiento de una transacción como el tiempo de respuesta y el volumen de transacciones simultáneas donde se especifica que el sistema debe ser capaz de manejar al menos 1.000 transacciones por segundo.
- Escalabilidad, se enfoca en la habilidad de un sistema para crecer en su capacidad de satisfacer la creciente demanda de los servicios que oferta en relación con los RNF.
- Integridad, se refiere a mantener los datos puros y dignos de confianza mediante la protección de los datos del sistema de cambios intencionales o accidentales. Incluye el evitar que los usuarios no autorizados puedan realizar modificaciones en los datos o programas, impedir que los usuarios autorizados realicen modificaciones inadecuadas o no autorizados y por último mantener la coherencia interna y externa de datos y programas.

1.4.3.2. Análisis comparativo: características de resiliencia.

En la tabla 4 se presenta un resumen con los autores de las características mencionadas en el punto anterior que sirven como ayuda para describir a un software como resiliente.

En base a la lista de características presentada en la tabla 4 a continuación se describe su colaboración que distingue al SI de los demás y lo caracteriza como un software resiliente:

Modularidad, consiste en dividir el software en módulos de forma que si uno deja de funcionar no afecte al SI en general.

Independencia, evita la dependencia entre los módulos del SI, y protege el proceso de recuperación ante riesgos.

Disponibilidad, gestiona subprocesos adicionales para resolver las peticiones de llamada y evitar interrupciones o efectos secundarios en el funcionamiento normal del SI.

Flexibilidad, los componentes del SI deben mantener cierta facilidad al momento de acoplarse sin interrumpir en el proceso de comunicación de los procesos del sistema.

Tabla 4. Características de software resiliente frente a sus autores.

CARATERÍSTICAS	AUTORES					
	A1	**A2**	**A3**	**A4**	**A5**	**A6**
Modularidad **(División del software en módulos)**	X					
Independencia **(Acoplamiento mínimo entre componentes)**	X					
Disponibilidad **(Accesible en varios periodos de tiempo)**	X			X		X
Flexibilidad **(Acoplamiento fácil de los componentes)**	X		X			X
Redundancia **(Tolerante a fallas)**		X				
Seguridad **(Protección del software)**		X				
Confidencialidad **(Protección de la información)**		X				X
Operatividad **(Desarrollo correcto de archivos)**						X
Continuidad **(Facilidad de recuperación ante errores)**	X		X	X		X
Complejidad **(Dificultad mínima)**		X			X	
Mantenibilidad **(Funcionamiento normal del software)**			X	X		X
Interdependencia e Interconectividad **(Dependencias de ciertas características de otro sistema)**					X	
Conmutación **(Trabajar sobre copias de seguridad)**						X
Eficiencia **(Manipulación de recursos)**						X
Interoperabilidad **(Uso de herramientas y normas internas)**						X
Manejabilidad **(Administrar la ejecución del software)**		X				X
Rendimiento **(Tiempo de respuesta)**						X
Escalabilidad **(Cubrir la demanda de RNF)**						X
Integridad **(Mantener coherencia entre datos y herramientas)**						X

Fuente: El Autor.

Roland Huuhn(A1), P. E. Black y P. J. Windley(A2), Oxford Dictionaries(A3), Jesús Gil Hernández(A4), Warren Axelrod(A5), Noraini Ibrahim, Wan Kadir, Safaai Deris(A6), Mark Merkow y Lakshmikanth Raghavan(A7).

Redundancia, define estrategias de control que resuelve los errores en los módulos antes que se conviertan en vulnerabilidades para el SI, sin dejar tiempos muertos de inactividad.

Seguridad, incluye el control de acceso que limita y determina los usuarios que pueden ingresar en el SI.

Confidencialidad, restringe el acceso a los archivos e información sensible del SI.

Operatividad, controla el desarrollo correcto de archivos, minimizando errores y posibilidades de riesgos.

Continuidad, consiste en la facilidad del SI para recuperar el estado normal en tiempos imperceptibles después de producirse un error o cambio y evita el desequilibrio en los procesos.

Complejidad, define un nivel de dificultad mínimo en cuanto a la arquitectura del SI facilitando la inclusión de la resiliencia en el desarrollo de sistemas individuales.

Mantenibilidad, adapta el SI a un entorno modificado, ya sea para corregir fallas o mejorar el rendimiento.

Interdependencia e Interconexión, gestiona que la dependencia a otros sistemas se de en porcentajes mínimos.

Conmutación, maneja los sistemas de copia de seguridad como una alternativa de funcionamiento para conservar la ejecución normal del SI.

Eficiencia, consiste en utilización adecuada de recursos informáticos y servicios para la gestión del SI.

Interoperabilidad**,** se introduce en la utilización de normas internas y herramientas para el desarrollo de SI.

Manejabilidad**,** permite ejecutar el SI en todo hardware disponible para su instalación.

Rendimiento**,** corresponde a la velocidad de procesamiento y volumen de las transacciones de al menos 1000 por segundo.

Escalabilidad**,** satisface la creciente demanda de servicios que modifican el SI con relación a los RNF.

Integridad, mantiene la coherencia interna y externa de datos y programas mediante la protección del cifrado de datos.

En las características descritas existen puntos de concordancia y no-concordancia entre los autores, pero cabe mencionar que todos son importantes.

CAPITULO II: DESARROLLO DE LA GUÍA METODOLÓGICA EN BASE A LAS ÁREAS DEL MODELO DE RESILIENCIA CERT-RMM.

2.1. Propósito de la guía

La guía permite evaluar los SI de las organizaciones para conocer el nivel de resiliencia y proponer buenas prácticas que apoyen su mejoramiento en base a características de resiliencia de software, y adicionalmente oriente a las organizaciones a la inclusión de resiliencia en sus SI, en base a técnicas, modelos y estándares que garanticen seguridad y continuidad en su funcionamiento, contribuyendo de esta manera a minimizar los riesgos organizacionales.

Como modelo referencial se basa en la metodología CERT-RMM para la gestión de la resiliencia en activos (información, personal, tecnología, instalaciones) y en la familia de los estándares ISO se toma la serie ISO 27000 para gestionar la seguridad de la información.

2.2. Herramientas y recursos tecnológicos base para el desarrollo de la guía metodológica

2.2.1. Definición de la técnica de elicitación.

En cuanto a la recolección de requisitos se trabajará con la técnica de encuestas/cuestionarios para el proceso de elicitación, puesto que funciona en base a preguntas claves expuestas en un navegador web con la ayuda de alguna herramienta informática, se considera la técnica ideal ya que se podría aplicar con una gran cantidad de clientes organizacionales y la interacción sería directa entre el usuario y el ordenador, además se plantea el uso de plantillas con diseño propio para el proceso de extraer las necesidades del cliente al evaluar su SI.

2.2.2. Estándares de seguridad ISO 27000.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares a partir de los cuales se toma 3 numeraciones relacionadas con los requisitos, riesgos y seguridad tanto de la información como de las aplicaciones. Se describe a continuación cada uno de ellos.

2.2.2.1. ISO 27001.

Proveniente de la familia de los ISO, este estándar se enfoca específicamente en la seguridad de la información de las organizaciones con el objetivo de minimizar el impacto desfavorable que producen los riesgos cuando se ejecutan.

Los riesgos por lo general se los identifica y posteriormente se aplica medidas correctivas, pero en este estándar se propone el uso de dos características adicionales para el

tratamiento de los riesgos como lo es el cuantificar y priorizar, aplicables a cada riesgo de manera que se refuerce la seguridad del sistema o de implementar una cuando no exista alguna de las características mencionadas.

La seguridad al tratar los riesgos no lo hará solamente a nivel de la empresa, sino que se basa en legislaciones (restricciones, objetivos, regulaciones) nacionales e internacionales acordes a la satisfacción y bienestar de los clientes, también al cumplimiento con regulaciones de costos, pues no deben exceder del presupuesto establecido.

Este estándar incluye políticas de seguridad infaltables en la organización donde se regula lineamientos de implementación, acceso, repositorio, exploración y más operaciones fundamentales que ayuden a mantener condiciones favorables, flexibles y en concordancia con los cambios tecnológicos. Es vital resaltar que menciona el planteamiento de políticas concretas y no excesivas, todo bajo documentos formales, de modo que puedan salir del papel e implementarse en la organización.

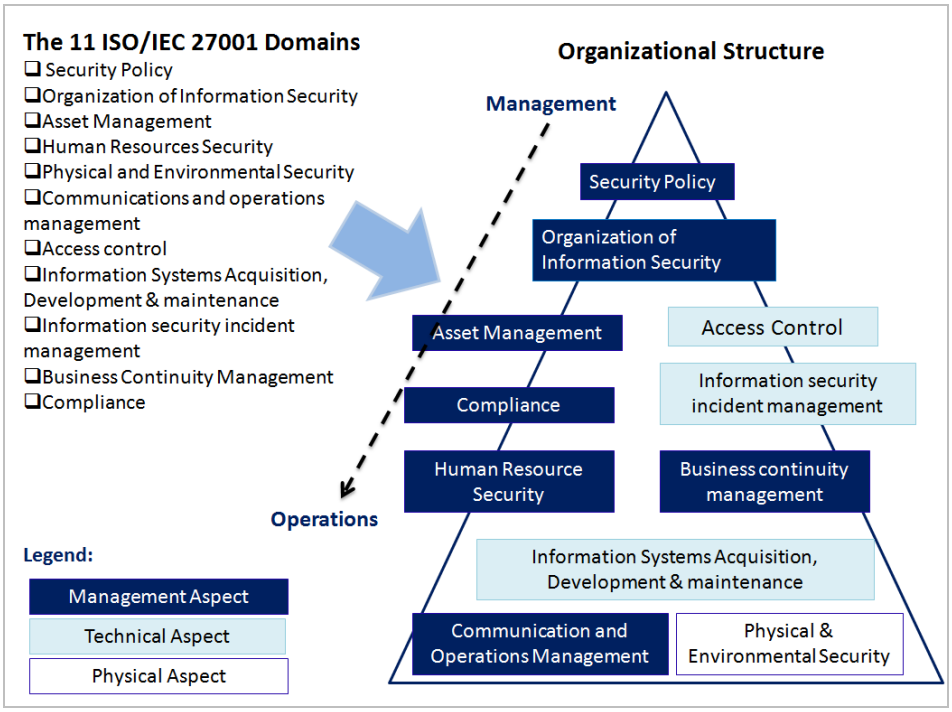


Figura 2. Categorización de dominios ISO 27001.
Fuente: ISO/IEC 27011 (citado por *Cheema, 2014)*.

2.2.2.2. ISO 2005.

Proyecta su estructura en base a la gestión de riesgos en cuanto a la seguridad de la información en las organizaciones, inicia con la evaluación de los activos importantes

como lo es la información para el soporte de los requisitos del sistema según lo establece en la norma ISO 27001.

El estándar sólo proporciona lineamientos para implementar requisitos de seguridad de información que cada organización puede tomar en apoyo a la definición de una metodología que gestione los riesgos en base a sus necesidades, ya que no todas las organizaciones están expuestas a los mismos riesgos.

Quien estará detrás de esta gestión son el personal de nivel superior y los involucrados en gestionar los riesgos para lograr el soporte apropiado. A continuación según la norma ISO 27005 se lista pautas importantes para la gestión de riesgos:

- Identificación de riesgos: no todos los eventos se consideran riesgos puesto que para considerarse como un riesgo no se debe conocer cuándo ocurrirá.
- Evaluación de riesgos: los riesgos pueden ser de alto impacto como tolerables, controlados en determinados periodos de tiempo para estimar su posible efecto en la organización y establecer contramedidas adecuadas que minimicen la probabilidad de sufrir pérdidas.
- Análisis de riesgos: se considera como el punto más importante de este estándar puesto que se basa en toda la información de la organización que incluye requisitos (legales y reglamentarios), procesos estratégicos, misión, valores, estructura, y demás información pertinente que servirán de guía para conocer las posibles partes vulnerables e implementar medidas alternativas de prevención de riesgos.
- Escenarios de riesgos: apoyan el proceso de Evaluación de Riesgos, estos se pueden ejecutar desde dos enfoques, siendo el primero cuando se considera más probable el impacto del riesgo en la organización basado en el *enfoque arriba-abajo* y el segundo cuando ya impactó el riesgo en la organización y se aplica escenarios de riesgo genérico basados en el *enfoque abajo-arriba.*
- Respuesta a los riesgos: para que un riesgo pueda ser tratado deberá estar dentro de los límites del nivel de tolerancia y luego poder aplicarle las estrategias de gestión de riesgos como son: evitarlo (apartar las actividades que generan el riesgo), mitigarlo (implementar medidas de detección y reducción del riesgo), transferirlo (enviar el riesgo a entidades de outsourcing) y aceptarlo (enfrentar el riesgo con medidas de control).

2.2.2.3. ISO 27034.

Define conceptos, marcos y procesos para ayudar a las organizaciones a integrar la seguridad dentro del ciclo de vida de desarrollo del software, con el objetivo de asegurar que las informáticas proporcionen el nivel de seguridad deseado y necesario en apoyo del SGSI.

Esta norma mantiene cierta relación con las demás series del ISO 27000, como se muestra en la figura 3.

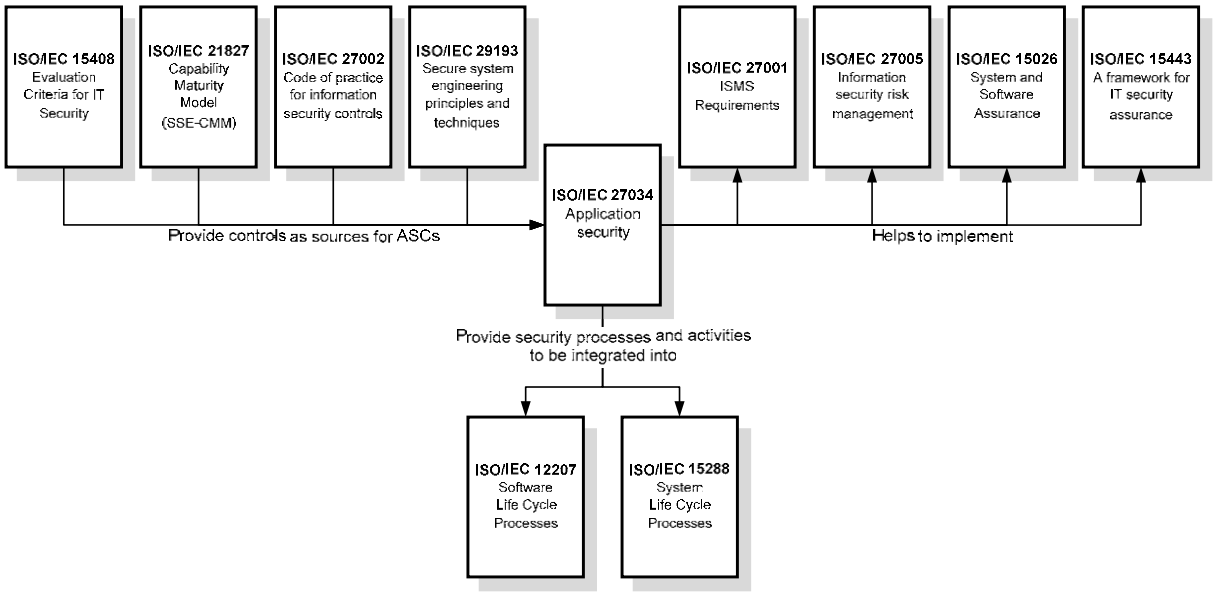


Figura 3. Relación ISO 27034 con otros estándares internacionales.
Fuente: (ISO/IEC, 2011).

Es por ello que a continuación se amerita importante mencionar los lineamientos que presenta (ISO/IEC, 2011) para alcanzar el propósito de la norma ISO/IEC 27034:

a) Proporcionar conceptos, estructuras, componentes y procesos;
b) Proporcionar mecanismos orientados al proceso para el establecimiento de requisitos de seguridad y la selección de los controles de seguridad adecuados.
c) Proporcionar directrices para el establecimiento de los criterios de aceptación para las organizaciones de outsourcing.
d) Brindar mecanismos orientados a los procesos de determinación, la generación y la recogida de las pruebas necesarias para demostrar que sus aplicaciones se puedan utilizar de forma segura en un entorno definido.

e) Apoyar los conceptos generales especificados en la norma ISO/IEC 27001 y asistir en la aplicación satisfactoria de la seguridad de la información basado en un enfoque de gestión de riesgos, y

f) Proporcionar un marco que ayude a poner en práctica los controles de seguridad especificados en la norma ISO/IEC 27002 y otras normas.

2.2.3. Áreas de proceso CERT-RMM.

La metodología CERT-RMM cuenta con 26 áreas de estudio, que se encuentran organizadas en 4 categorías como son Ingeniería, Gestión Empresarial, Operaciones y Gestión de Procesos, las cuales se presentan en la tabla 4.

Tabla 5. Clasificación de las áreas CERT-RMM por categoría.

<table>
<tr><th>GESTIÓN EMPRESARIAL</th><th>GESTIÓN DE PROCESOS</th><th>INGENIERÍA</th><th>OPERACIONES</th></tr>
<tr><td>Comunicaciones (COMM)</td><td>Medición y Análisis (MA)</td><td>Definición y Gestión de Activos (ADM)</td><td>Gestión de Acceso (AM)</td></tr>
<tr><td>Cumplimiento (COMP)</td><td>Monitorización (MON)</td><td>Gestión de Controles (CRTL)</td><td>Control del Entorno (EC)</td></tr>
<tr><td>Enfoque Empresarial (EF)</td><td>Definición de Proceso Organizacional (OPD)</td><td>Desarrollo de Requisitos de Resiliencia (RRD)</td><td>Gestión de Dependencias Externas (EXD)</td></tr>
<tr><td>Gestión de Recursos Financieros (FRM)</td><td rowspan="5">Enfoque de Proceso Organizacional (OPF)</td><td>Gestión de Requisitos de Resiliencia (RRM)</td><td>Gestión de Identidades (ID)</td></tr>
<tr><td>Gestión de Recursos Humanos (HRM)</td><td>Ingeniería de Soluciones Técnicas Resilientes (RTSE)</td><td>Gestión y Control de Incidentes (IMC)</td></tr>
<tr><td>Formación y Conciencia Organizacional (OTA)</td><td rowspan="4">Continuidad del Servicio (SC)</td><td>Gestión de Información y Conocimiento (KIM)</td></tr>
<tr><td rowspan="3">Gestión de Riesgos (RISK)</td><td>Gestión de Personas (PM)</td></tr>
<tr><td>Gestión de la Tecnología (TM)</td></tr>
<tr><td>Análisis y Resolución de Vulnerabilidades (VAR)</td></tr>
</table>

Fuente: (CERT® Resilience Management Model, 2010)

De las categorías mencionadas se trabaja con la de *Ingeniería* y tres áreas externas como son: Gestión de Riesgos de la categoría de Gestión Empresarial y las áreas de Gestión de

Dependencias Externas y de Tecnología en cuanto a la categoría de Operaciones, los cuales son fundamentales en el desarrollo de la guía metodológica. A continuación se describe de manera breve cada uno de ellos, la descripción completa de cada área se encuentra en el Anexo A.

2.2.3.1. Definición y Gestión de Activos (ADM).

Describe la definición, valor, relación con los servicios, establece propietarios, dependencias, perfilación, cambios, entre otros aspectos claves de los activos como centro de la gestión de resiliencia operacional.

Metas	Prácticas
ADM:SG[12]1 Establecer Activos Organizacionales	ADM:SG1.SP[13]1 Inventario de activos
	ADM:SG1.SP2 Establecer un entendimiento común
	ADM:SG1.SP3 Establecer propietarios y vigilantes
ADM:SG2 Establecer relaciones entre Activos y Servicios	ADM:SG2.SP1 Asociar activos con servicios
	ADM:SG2.SP2 Analizar dependencias entre activos y servicios
ADM:SG3 Gestionar Activos	ADM:SG3.SP1 Identificar criterios de cambios
	ADM:SG3.SP2 Mantener cambios a los activos e inventarios

2.2.3.2. Gestión de Control (CTRL).

Determina estrategias para la protección, mantenimiento de los servicios y el cumplimiento de los requisitos mediante el establecimiento de objetivos de control y controles para todos los ámbitos (administrativos, técnicos y físicos).

Metas	Prácticas
CTRL:SG1 Establecer Objetivos de Control de Objetivos	CTRL:SG1.SP1 Definir los objetivos de control
CTRL:SG2 Establecer Controles	CTRL:SG2.SP1 Definir los controles

[12] SG: Meta correspondiente a las áreas de proceso de la metodología CERT-RMM.
[13] SP: Práctica correspondiente a las metas de las áreas de proceso de la metodología CERT-RMM.

CTRL:SG3 Analizar Controles	CTRL:SG3.SP1 Analizar los controles
CTRL:SG4 Evaluar efectividad de los Controles	CTRL:SG4.SP1 Evaluar los controles

2.2.3.3. Gestión de Dependencias Externas (EXD).

Identifica y prioriza los riesgos asociados a las relaciones y dependencias con entidades externas, es en esta área donde toma parte el outsourcing que implica cambios estructurales en la organización.

Metas	Prácticas
EXD:SG1 Identificar y priorizar dependencias externas	EXD:SG1.SP1 Identificar dependencias externas
	EXD:SG1.SP2 Priorizar dependencias externas
EXD:SG2 Gestionar los riesgos debido a dependencias externas	EXD:SG2.SP1 Identificar y evaluar riesgos debido a dependencias externas
	EXD:SG2.SP2 Mitigar riesgos debido a dependencias externas
EXD:SG3 Establecer relaciones formales	EXD:SG3.SP1 Establecer especificaciones empresariales para dependencias externas
	EXD:SG3.SP2 Establecer especificaciones de resiliencia para dependencias externas
	EXD:SG3.SP3 Evaluar y seleccionar entidades externas
	EXD:SG3.SP4 Formalizar relaciones
EXD:SG4 Gestionar desempeño de entidades externas	EXD:SG4.SP1 Monitorear rendimiento de entidades externas
	EXD:SG4.SP2 Corregir rendimiento de entidades externas

2.2.3.4. Gestión de Riesgos (RISK).

Identifica, analiza y prioriza los riesgos que reducen la resiliencia operacional, mantiene estrategias equilibradas tanto en la protección como mantenimiento de los bienes y servicios organizacionales.

Metas	Prácticas
RISK:SG1 Preparación para la Gestión de Riesgos	RISK:SG1.SP1 Determinar las categorías y fuentes de Riesgo
	RISK:SG1.SP2 Establecer una estrategia para la Gestión de Riesgo Operacional

RISK:SG2 Establecer parámetros y enfoque de Riesgos	RISK:SG2.SP1 Definir los parámetros de Riesgo
RISK:SG3 Identificar el Riesgo	RISK:SG3.SP1 Identificar los Niveles de riesgo en los Activos
	RISK:SG3.SP2 Identificar los Niveles de riesgo en los Servicios
RISK:SG4 Analizar el Riesgo	RISK:SG4.SP1 Evaluar Riesgos
	RISK:SG4.SP2 Categorizar y Priorizar Riesgos
	RISK:SG4.SP3 Asignar disposición al Riesgo
RISK:SG5 Mitigar y controlar el Riesgo	RISK:SG5.SP1 Desarrollar planes para la mitigación del riesgo
	RISK:SG5.SP2 Implementar estrategias de Riesgo
RISK:SG6 Usar la información de Riesgo para gestionar la resiliencia	RISK:SG6.SP1 Revisar y ajustar estrategias para proteger los activos y servicios
	RISK:SG6.SP2 Revisar y ajustar estrategias para sostener los servicios

2.2.3.5. Desarrollo de Requisitos de Resiliencia (RRD).

Se encarga de establecer requisitos empresariales y de servicio, que garantizan la viabilidad de los activos y la contribución a los servicios que se asocian.

Metas	Prácticas
RRD:SG1 Identificar requisitos empresariales	RRD:SG1.SP1 Establecer Requisitos de Resiliencia Empresarial
RRD:SG2 Desarrollar requisitos del servicio	RRD:SG2.SP1 Establecer Requisitos de Resiliencia de Activos
	RRD:SG2.SP2 Asignar Requisitos de Resiliencia Empresarial a los Servicios
RRD:SG3 Analizar y validar requisitos	RRD:SG3.SP1 Establecer una definición de la funcionalidad requerida
	RRD:SG3.SP2 Analizar Requisitos de Resiliencia
	RRD:SG3.SP3 Validar Requisitos de Resiliencia

2.2.3.6. Gestión de Requisitos de Resiliencia (RRM).

Busca garantizar que los requisitos del área de RRD permanezcan viables para cada activo asociado con un servicio de alto valor hasta que se retire, o cambie debido a uno o más factores desencadenantes de la organización.

Metas	Prácticas
RRM:SG1 Gestionar Requisitos	RRM:SG1.SP1 Obtener un entendimiento de los Requisitos de Resiliencia
	RRM:SG1.SP2 Obtener un compromiso con los Requisitos de Resiliencia
	RRM:SG1.SP3 Gestionar los cambios en los Requisitos de Resiliencia
	RRM:SG1.SP4 Mantener la trazabilidad de los Requisitos de Resiliencia
	RRM:SG1.SP5 Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos

2.2.3.7. Ingeniería de Soluciones Técnicas Resilientes (RTSE).

Diseña, desarrolla e implementa soluciones para los activos en función de las amenazas y el entorno de riesgo al que se enfrentan, y en el que van a operar.

Metas	Prácticas
RTSE:SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes	RTSE:SG1.SP1 Identificar las directrices generales
	RTSE:SG1.SP2 Identificar las directrices de Requisitos
	RTSE:SG1.SP3 Identificar las directrices de Arquitectura y Diseño
	RTSE:SG1.SP4 Identificar las directrices de Implementación
	RTSE:SG1.SP5 Identificar las directrices de Montaje e Integración
RTSE:SG2 Desarrollar planes para el desarrollo de soluciones técnicas resilientes	RTSE:SG2.SP1 Seleccionar y ajustar directrices
	RTSE:SG2.SP2 Integrar las directrices seleccionadas con un proceso definido de desarrollo de software y sistemas
RTSE:SG3 Ejecutar el Plan	RTSE:SG3.SP1 Monitorear la ejecución del plan de desarrollo
	RTSE:SG3.SP2 Entregar soluciones técnicas resilientes en producción

2.2.3.8. Continuidad del Servicio (SC).

Identifica y prioriza los servicios, se establece planes de continuidad, de operaciones y estándares. Además se encarga de resolver conflictos en los planes, mide la efectividad de los mismos en la organización y establece criterios de cambios.

Metas	Prácticas
SC:SG1 Preparar para la continuidad del servicio	SC:SG1.SP1 Planear la continuidad del servicio
	SC:SG1.SP2 Establecer estándares y directrices para la continuidad del servicio
SC:SG2 Identificar y priorizar servicios de alto valor	SC:SG2.SP1 Identificar los servicios de alto valor para la organización
	SC:SG2.SP2 Identificar dependencias e interdependencias internas y externas
	SC:SG2.SP3 Identificar los registros y bases de datos
SC:SG3 Desarrollar planes de continuidad del servicio	SC:SG3.SP1 Identificar los planes a ser desarrollados
	SC:SG3.SP2 Desarrollar y documentar los planes de continuidad del servicio
	SC:SG3.SP3 Asignar personal a los planes de continuidad del servicio
	SC:SG3.SP4 Almacenar y asegurar los planes de continuidad del servicio
	SC:SG3.SP5 Desarrollar el plan de formación para la continuidad del servicio
SC:SG4 Validar planes de continuidad del servicio	SC:SG4.SP1 Validar los planes con requisitos y estándares
	SC:SG4.SP2 Identificar y resolver los conflictos del plan
SC:SG5 Ejercer planes de continuidad del servicio	SC:SG5.SP1 Desarrollar programas y normas de pruebas
	SC:SG5.SP2 Desarrollar y documentar planes de prueba
	SC:SG5.SP3 Ejercer planes
	SC:SG5.SP4 Evaluar los resultados de las pruebas sobre el plan
SC:SG6 Ejecutar planes de continuidad del servicio	SC:SG6.SP1 Ejecutar planes
	SC:SG6.SP2 Medir la Efectividad del plan en operación
SC:SG7 Mantener planes de continuidad del servicio	SC:SG7.SP1 Establecer criterios de cambio
	SC:SG7.SP2 Mantener los cambios a los planes

2.2.3.9. Gestión de Tecnología (TM).

Establece y administra los activos de tecnología de la organización para facilitar el desarrollo y satisfacción de los requisitos de resiliencia operacional que apoyan los servicios organizacionales para mantener su integridad y disponibilidad.

Metas	Prácticas
TM:SG1 Establecer y priorizar activos de tecnología	TM:SG1.SP1 Priorizar los activos de tecnología
	TM:SG1.SP2 Establecer los activos tecnológicos enfocados en la Resiliencia
TM:SG2 Proteger los activos tecnológicos	TM:SG2.SP1 Asignar Requisitos de Resiliencia a los Activos de Tecnología
	TM:SG2.SP2 Establecer e Implementar Controles
TM:SG3 Gestionar riesgo de los activos de tecnología	TM:SG3.SP1 Identificar y evaluar los riesgos de activos de tecnología
	TM:SG3.SP2 Mitigar los Riesgos Tecnológicos
TM:SG4 Gestionar la integridad de los activos de tecnología	TM:SG4.SP1 Controlar el acceso a los activos de tecnología
	TM:SG4.SP2 Ejecutar la gestión de la configuración
	TM:SG4.SP3 Ejecutar la gestión y control del cambio
	TM:SG4.SP4 Ejecutar la gestión de la entrega
TM:SG5 Gestionar la disponibilidad de los activos de tecnología	TM:SG5.SP1 Ejecutar la planeación para el sostenimiento de activos de tecnología
	TM:SG5.SP2 Gestionar el mantenimiento de los activos de tecnología
	TM:SG5.SP3 Gestionar la capacidad de la tecnología
	TM:SG5.SP4 Gestionar la interoperabilidad de la tecnología

2.2.4. Tipos de software.

Con la finalidad de obtener información más estructurada se da lugar a la creación de sistemas de información donde interactúan datos, personas, actividades, recursos materiales (informáticos o de comunicación) en función de los objetivos organizacionales.

¿Cuándo un sistema de información es efectivo? Un SI es efectivo cuando brinda a los usuarios información exacta, oportuna y relevante.

De entre la variabilidad de tipos de software existentes para este estudio se toma aquellos que se orientan en la automatización de procesos operativos, soporte a la toma de decisiones y logro de ventajas competitivas, de los cuales tenemos:

- ***Sistemas Transaccionales*.-** Automatizan la ejecución de procesos financieros (ingresos, egresos, pólizas, cobros, pagos, etc.) lo cual ahorra la mano de obra del personal de la organización.
- ***Sistemas de Soporte a la Toma de Decisiones*.-** Apoyan el procesamiento de información para la toma de decisiones por parte de la gerencia intermedia.
- ***Sistemas Estratégicos*.-** Se basan en la tecnología de información que suelen desarrollarse "in house[14]", el cual se inicia con un proceso o función en particular a partir del cual se van agregando nuevas funciones o procesos con el fin de lograr innovación en los productos y procesos dentro de la organización.

Sin embargo, aunque estos sistemas de información presenten enfoques diferentes mantienen una similitud al requerir un proceso específico que incluya características resilientes para lograr seguridad y continuidad en sus operaciones.

2.2.5. Análisis comparativo: áreas de la metodología CERT-RMM y estándares ISO 27000.

Para obtener buenos resultados se requiere herramientas claves que apoyen el objetivo del presente proyecto de fin de carrera.

Se inicia con el estudio de la metodología CERT-RMM del cual se toma 9 áreas enfocadas en el ámbito de la Ingeniería (activos, procesos y servicios) guiados por requisitos. Luego de la familia de estándares ISO 27000 se toma las versiones con relación a los requisitos de SGI, objetivos de control, gestión de riesgos y seguridad del software, y finalmente se menciona los tipos de sistemas claves para evaluar la resiliencia.

Luego de identificar las áreas de proceso de la metodología del CERT-RMM y los estándares ISO 27000, se los relaciona de acuerdo a tres tipos de software comunes en un ambiente organizacional como se muestra en la tabla 6.

[14] In house: Se denomina al software construido dentro de la organización.

Tabla 6. Comparación de tipos de software, áreas de la metodología CERT-RMM y las normas ISO 27000.

Tipos de Software	**Áreas de Proceso CERT-RMM**									Estándares ISO 27000		
	ADM	**CTRL**	**EXD**	**RISK**	**RRD**	**RRM**	**RSTE**	**SC**	**TM**	27001	27005	27034
S1	X	X		X	X	X	X	X	X	X	X	X
S2	X	X	X	X	X	X		X	X			X
S3	X	X		X	X	X	X	X	X	X	X	X

Fuente: El autor.

Sistemas transaccionales (S1), sistemas de soporte a la toma de decisiones (S2), sistemas estratégicos (S3).

Se puede observar que el tipo de software que destaca mayor tendencia a ser resiliente son los sistemas estratégicos, pero resulta que existe un área del CERT-RMM que no mantiene relación con este software ¿a qué se debe? Es el área de Gestión de Dependencias Externas (EXD) que se encarga de la gestión de outsourcing y los posibles riesgos que este proceso implica, por tales razones los sistemas estratégicos no forman parte de esta área, puesto que al ser desarrollados *in house*, la organización mayormente no cree conveniente incluir a entidades externas para alcanzar la resiliencia operacional.

2.3. Diseño de la guía

En cuanto al proceso de elicitación, se diseña una plantilla básica donde se adapta la Técnica de requisitos elegida y se solicita puntos claves de la metodología de resiliencia CERT-RMM que mantengan relación con dicha técnica.

2.3.1. Estructura de la plantilla.

La plantilla se estructura en 8 secciones concretas, la cual se muestra a continuación (Ver figura 4).

Código	*<<código de la pregunta>>*
Pregunta	*<planteamiento de la pregunta>*
Característica	*<característica de resiliencia del software>*
Técnicas	*<<técnicas de elicitación>>*
Áreas	• *<nombre del área del CERT-RMM >:<nombre de la meta del área>* …
Respuesta	*<estado>* | *<opciones de respuestas>*
Observación	*Conocer… <Describir lo que se desea conseguir con la pregunta planteada>*
MEDICIONES	
Área relacionada	• *<nombre del área CERT-RMM relacionada>* *< nombre de la meta del área relacionada>* *< nombre de la prácticas de la meta>* - *<medición>* - *<medición>* … …

Figura 4. Plantilla de elicitación de requisitos de resiliencia.
Fuente: El autor.

El significado de las secciones de la plantilla es el siguiente:

1. **Código:** se introduce un identificador único, el cual sirve para ordenar, diferenciar y evitar plantillas duplicadas.
2. **Pregunta**: este campo debe contener preguntas específicas basadas en las características claves del software resiliente y algunas áreas del CERT-RMM. Por ejemplo tomando la característica de modularidad y el área de Gestión y definición de activos (ADM) la pregunta sería:

   ¿Cuál es la estrategia que utiliza para que su SI continúe funcionando normalmente cuando uno o varios de sus procesos fallan durante su ejecución?
3. **Característica**: se hace referencia a las características claves del software resiliente como flexibilidad, complejidad, modularidad, eficiencia, entre otras.
4. **Técnica**: este campo hace alusión a las técnicas de elicitación tales como: entrevista, cuestionario, brainstorming, JAD, casos de uso y prototipo.
5. **Áreas**: contiene aquellas áreas que mantienen cierta relación con el objeto de la pregunta planteada. Las áreas deben estar desglosadas conforme al planteamiento de la metodología que es *área [metas]* puede ser sólo una meta o varias metas, así como también puede estar relacionada con una sola área o con varias áreas del CERT-RMM.
6. **Respuestas**: este campo propone varias alternativas, pero sólo aquella alternativa que satisfaga la pregunta debe ser la correcta. Las opciones de respuestas pueden

ser dicotómicas o de opción múltiple. Por ejemplo, tomando la pregunta anteriormente planteada, las respuestas serían:

	¿Cuál es la estrategia que utiliza para que su SI continúe funcionando normalmente cuando uno o varios de sus procesos fallan durante su ejecución?
	Desarrollar procesos adicionales que se utilicen como medidas alternas para reemplazar un proceso cuando falle de modo que no afecte el funcionamiento de las operaciones restantes del SI.
X	**Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.**
	Mantener independencias mínimas entre los componentes tecnológicos y los procesos que ejecuta el SI para conservar la continuidad en sus operaciones.
	Realizar análisis de amenazas, incluyendo modelos y patrones de ataque como medidas de control para proteger las operaciones que ejecuta el sistema de información.

Se observa cuatro posibles respuestas, pero sólo la resaltada de color rojo es la correcta, ya que complementa y satisface a la pregunta.

7. **Observación:** este campo describe el propósito de cada plantilla, lo que se desea conocer y conseguir con la pregunta planteada, con el objetivo de servir como guía para la determinación de los puntos clave que ayuden en el proceso de extracción de información, los cuales se describe en la siguiente sección.
8. **Mediciones - Área relacionada:** este campo se basa en el contenido de los campos *pregunta* y *áreas* con el objetivo de mencionar sugerencias que apoyen el proceso de resiliencia del SI que se está evaluando.

2.3.2. Desarrollo de plantillas.

Para desarrollar las plantillas que servirán como herramienta en la elicitación de requisitos de resiliencia se toma como base las secciones 2.2 correspondientes a las técnicas de elicitación y 4.3 que puntualiza las características de resiliencia del Estado del Arte, y las áreas de la metodología CERT-RMM en el punto 2.3 de esta sección.

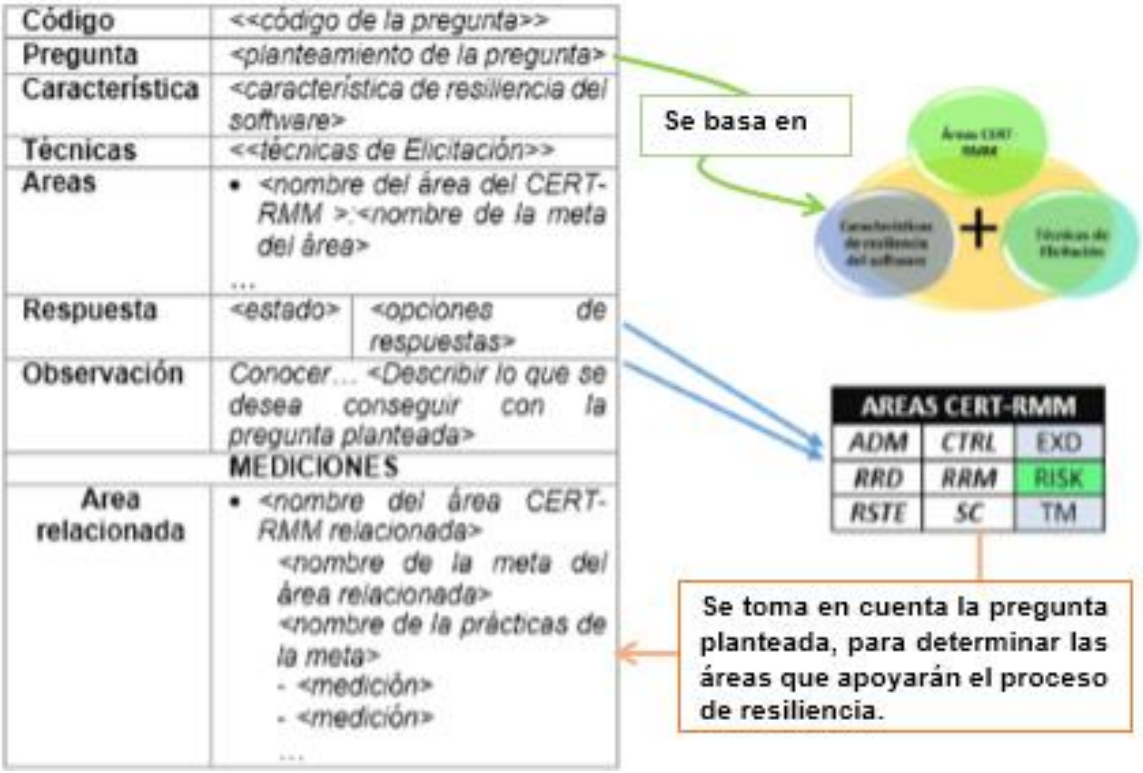


Figura 5. Estructura de la plantilla de elicitación de requerimientos de resiliencia.
Fuente: El autor.

Se plantea un cuestionario con el objetivo de indagar sobre la estructura y funcionamiento del software en base a información específica brindada por el usuario que responderá dicho cuestionario. El cuestionario engloba distintos planteamientos de preguntas entre los que se encuentran: abiertas o cerradas, a partir de las cuales se traza pautas que servirán de apoyo para el mejoramiento del software y aproximación a la resiliencia.

Las preguntas se encuentran organizadas de acuerdo a las áreas de proceso de la metodología CERT-RMM, de este modo se consigue facilitar la comprensión del ámbito al que se enfoca cada una de las plantillas para conocer el estado actual del SI y apoyar la propuesta de mejores prácticas que estimulen la inclusión de resiliencia en el software. En la figura 5 se muestra como se plantean las preguntas y mediciones que componen dicha plantilla.

Las preguntas y respuestas se definen en base a características de resiliencia y áreas del CERT-RMM ya que mantienen relación con el tema de estudio, y pueden ser utilizadas como estrategias para el proceso de elicitación que va permitir conocer información propia de cada SI evaluado. Sin embargo, las respuestas van en concordancia con las preguntas, es decir, cada una de las preguntas planteadas a más de realizarse en base a

las características de resiliencia y las áreas del CERT-RMM, estas deben satisfacer correctamente a la pregunta en el ámbito de resiliencia de software.

Se considera esencial aplicar todas las 44 preguntas, ya que se contará con más opciones y por lo tanto más posibilidades en las que el SI a evaluar presente rasgos de resiliencia. Cabe destacar, que el público al que va dirigido este trabajo y por lo tanto puede realizar este proceso son: analistas, desarrolladores, testers, etc. en fin usuarios empresariales que deseen conocer el estado de resiliencia de sus SI.

A continuación se encuentran desarrolladas las plantillas para la elicitación de requisitos de resiliencia, ordenadas por cada una de las 9 áreas de la metodología CERT-RMM.

AREA DE PROCESO: Gestión y Definición de Activos – ADM.

Código	**P01**	
Pregunta	¿Cuál es la estrategia que utiliza para que su SI continúe funcionando normalmente cuando uno o varios de sus procesos fallan durante su ejecución?	
Característica	Modularidad	
Técnica	Brainstorming	
Áreas de CERT-RMM	CERT-RMM: ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Establecer directrices para el desarrollo de soluciones técnicas resilientes.	
Respuesta		Desarrollar procesos adicionales que se utilicen como medidas alternas para reemplazar un proceso cuando falle de modo que no afecte el funcionamiento de las operaciones restantes del SI.
	X	**Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.**
		Mantener independencias mínimas entre los componentes tecnológicos y los procesos que ejecuta el SI para conservar la continuidad en sus operaciones.
		Realizar análisis de amenazas, incluyendo modelos y patrones de ataque como medidas de control para proteger las operaciones que ejecuta el sistema de información.
Observaciones	Conocer la acción que toma el SI para evitar que su funcionamiento se vea afectado por presencias de errores en sus componentes.	
MEDICIONES		
Ingeniería de Soluciones Técnicas Resilientes (RSTE)	SG1. Establecer directrices para el desarrollo de soluciones técnicas resilientes SG1.SP1 Identificar Directrices Generales - Determinar el alcance de la capacidad de recuperación en cada uno de los componentes del sistema de información de modo que asegure continuidad en las operaciones y servicios a los que apoye. - Comprender el entorno operativo y la definición de las limitaciones de operación para la capacidad de recuperación de los entornos en los que el software y los sistemas se implementarán.	

Código	**P02**	
Pregunta	¿Qué acción realiza cuando detecta que la base de datos de su sistema de información ha sido alterada?	
Característica	Conmutación	
Técnica	Entrevista, Brainstorming.	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión y Definición de Activos: Gestionar activos.	
Respuesta		Evaluar el impacto de los cambios en cuanto al sistema de información.
		Desarrollar un historial de cambios para justificar los cambios realizados.
	X	**Cargar el último backup hasta determinar la gravedad de los cambios en el sistema.**
Observaciones	Conocer si se realizan copias de seguridad como medida de protección para gestionar cambios no autorizados en la información de la base de datos.	
MEDICIONES		
Gestión y Definición de Activos (ADM)	SG3. Gestionar activos SG3.SP1 Identificar criterios de cambios - Establecer una línea de base fundamentándose en un inventario de activos para determinar cuáles han sido afectados por los cambios ejecutados. - Manejar respaldos de información como medida de seguridad que apoye el desarrollo y documentación de criterios para establecer cuando un cambio debe ser considerado. SG3.SP2 Mantener cambios a los activos e inventarios - Documentar los cambios del sistema de información en base a la actualización de los perfiles de los activos de modo que exista documentación como respaldo para la protección y el mantenimiento de los activos.	

Código	**P03**	
Pregunta	¿Cómo controla los cambios en los procesos del sistema de información sin causar interrupción en el cumplimiento de los objetivos de la organización?	
Característica	Independencia	
Técnica	Entrevista, Brainstorming.	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión y Definición de Activos: Gestionar activos. ➢ Gestión de Control: Analizar controles y evaluar la efectividad de controles.	
Respuesta		Utilizar una herramienta para controlar versiones del software.
		Establecer una línea de base a partir de la cual se medirán los cambios.
		Desarrollar planes de control de cambios.
	X	**Mantener independencia entre los procesos de cada componente del sistema de información.**
Observaciones	Conocer la estrategia que se utiliza para controlar que los cambios no afecte la ejecución de los procesos el sistema de información.	
MEDICIONES		
Gestión y Definición de Activos (ADM)	SG3. Gestionar activos SG3.SP2 Mantener cambios a los activos e inventarios - Mantener un historial de cambios como requisito para la justificación de la realización de los cambios. - Establecer canales de comunicación entre los responsables de cada componente del sistema de información para garantizar su responsabilidad individual por los cambios efectuados en los activos relacionados y su responsabilidad colectiva al evaluar el impacto de los cambios en todo el sistema de información.	
Gestión de Controles (CRTL)	SG3 Analizar Controles SG3.SP1 Analizar los controles - Identificar los cambios y aplicar controles para abordar las deficiencias en los activos relacionados con la ejecución del software.	
	SG4 Evaluar efectividad de los Controles SG4.SP1 Evaluar los controles - Evaluar el impacto de los cambios tanto en los controles existentes como en los nuevos controles de su sistema de información para seleccionar el ámbito donde se realizará la evaluación y abordar las áreas problemáticas.	

Código	**P04**	
Pregunta	¿Cómo determina cuáles son los activos que contribuirán en el desarrollo del sistema de información?	
Característica	Complejidad	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Definición y Gestión de Activos: Establecer activos organizacionales.	
Respuesta		Se identifica y establece qué servicios asociados a los activos son de alto valor.
		Se evalúa la estructura y orientación de los componentes del sistema de información.
		Se estipula los activos en base al tamaño del sistema de información.
	X	**Se realiza un inventario en base a los perfiles de los activos.**
Observaciones	Conocer cómo se determina el nivel de complejidad del sistema de acuerdo al perfil de los activos.	
MEDICIONES		
Gestión y Definición de activos (ADM)	ADM: SG1 Establecer activos organizacionales ADM: SG1.SP1 Inventario de activos - Identificar e inventariar el personal, información y componentes tecnológicos necesarios para el desarrollo del software de modo que se disponga de un repositorio de activos como base para establecer una fuente común para todos los activos de alto valor.	

AREA DE PROCESO: Gestión de Control - CTRL.

Código	**P01**	
Pregunta	¿Cuál es el tipo de control que utiliza para evitar actividades mal intencionadas o interrupciones no deseadas en el software?	
Característica	Operatividad	
Técnica	Entrevista	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión de Control: Establecer Controles y evaluar efectividad de los controles. ➢ Ingeniería de Soluciones Técnicas Resilientes: Desarrollar planes para el desarrollo de soluciones técnicas resilientes.	
Respuesta		Controles administrativos que aseguran una alineación con las intenciones de la gerencia e incluyen acciones tales como la gobernanza, el establecimiento de políticas, supervisión, auditoría, cumplimiento de la separación de funciones, y el desarrollo e implementación de planes de continuidad del servicio.
	X	**Controles técnicos que gestionan procesos automatizados y eficaces para la aplicación de necesidades de recuperación del software.**
		Controles físicos que proporcionan barreras físicas para el acceso aplicables a personas, tecnología y otros activos tangibles, como las instalaciones.
Observaciones	Conocer el control que se utiliza en el software para contrarrestar las interrupciones.	
MEDICIONES		
Gestión de Control (CTRL)	SG2. Establecer controles SG2. SP1 Definir controles - Definir controles técnicos como controles de acceso electrónicos, cortafuegos, cifrado y sistemas de detección de intrusos, durante el desarrollo del sistema de información, ya que dichos controles son gestionados por procesos automatizados que se manifiestan en software, sistemas, hardware, redes e infraestructuras de telecomunicaciones. - Confirmar o asignar la responsabilidad de la implementación de los controles a nivel de software para establecer controles de nivel de activos como: personal, información y recursos tecnológicos que apoyen la satisfacción de los objetivos de control.’	
Ingeniería de Soluciones Técnicas de resiliencia (RSTE)	SG2 Desarrollar planes para el desarrollo de soluciones técnicas resilientes SG2.SP1 Seleccionar y ajustar directrices - Identificar criterios de selección para las directrices de resiliencia en base a controles técnicos y físicos del software de modo que el proceso de selección de directrices y su posterior adaptación sea en un software específico.	

Código	**P02**	
Pregunta	¿Define estrategias de control jerárquico (por delegación de responsabilidades) como método de protección y mantenimiento de los activos del SI para asegurar la gestión de vulnerabilidades y amenazas?	
Característica	Redundancia	
Técnica	Entrevista	
Área	CERT-RMM: ➢ Gestión de Control: Establecer Objetivos de Control, establecer Controles. ➢ Gestión de Riesgos: Identificar Riesgos	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si el software es capaz de soportar eventos inesperados y continuar con su trabajo, sin dejar tiempos muertos de inactividad.	
MEDICIONES		
Gestión de Controles (CTRL)	CTRL:SG2 Establecer Controles CTRL:SG2.SP1 Definir los controles - Establecer controles de servicio y nivel de activos para satisfacer los objetivos de control, dichos controles pueden ser una combinación de los controles que ya existen, los controles que necesitan ser actualizados, y nuevos controles por cada componente del sistema de información de modo que los riegos que se susciten puedan ser resueltos independientemente del componente y no desequilibre el funcionamiento general del sistema de información.	
Gestión de Riesgos (RISK)	SG3 Identificar Riesgos SG3.SP1 Identificar riesgos a nivel de activos - Identificar herramientas, técnicas y métodos que la organización puede utilizar para identificar los riesgos en los activos que apoyan y son parte del sistema de información.	

Código	**P03**	
Pregunta	¿Cómo limita que usuarios no autorizados accedan a los componentes del sistema de información?	
Característica	Seguridad	
Técnica	Entrevista	
Área	CERT-RMM: ➢ Gestión de Controles: Establecer objetivos de control, establecer controles. ➢ Ingeniería de Soluciones Técnicas: Establecer lineamientos para el desarrollo de soluciones técnicas resilientes.	
Respuesta	**X**	**Se maneja objetivos de control como políticas, normas, privilegios, etc.**
		Se introduce criterios de decisión y autoridad para delimitar el ingreso.
		Se identifica y prioriza el control con el planteamiento de claves de seguridad.
		Se categoriza las funciones por prioridades de acceso.
Observaciones	Conocer la estrategia de control que se utiliza para restringir el ingreso en el sistema de información.	
MEDICIONES		
Gestión de Controles (CTRL)	SG1 Establecer objetivos de control SG1.SP1 Definir los objetivos de control - Definir y documentar los objetivos de control que se deriven de las directivas y directrices de gestión del software entre los que se incluyen el control de acceso, gestión de privilegios, cifrado, etc. - Priorizar los objetivos de control de modo que se determine los que mayor atención necesiten debido a su potencial para afectar la continuidad de las operaciones del sistema de información.	
Ingeniería de Soluciones Técnicas Resilientes (RSTE)	RTSE:SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes RTSE:SG1.SP2 Identificar las directrices de requisitos - Identificar e incluir requisitos de seguridad como controles de acceso, gestión de entidades, etc. en el desarrollo del sistema de información para limitar el acceso a dicho sistema.	

Código	**P04**	
Pregunta	¿Cuáles son las directivas y directrices en los que se basa para definir controles en los procesos de tecnología de información que aseguren el cumplimiento de los objetivos con una seguridad razonable?	
Característica	Integridad	
Técnica	Entrevista, Brainstorming	
Área	CERT-RMM: ➢ Gestión de Control: Establecer Objetivos de Control, establecer Controles. ➢ Gestión de Tecnología: Proteger los activos tecnológicos.	
Respuesta		Políticas, procedimientos, normas y directrices que la organización establece para promover comportamientos aceptables.
		Prácticas y declaraciones de códigos de ética e integridad.
		Objetivos y declaraciones de propensión a riesgos, la tolerancia y umbrales estratégicos.
	X	**Obligaciones de cumplimiento legal y reglamentario con el apoyo de las entrevistas con los auditores y el personal jurídico.**
Observaciones	Conocer las directivas y directrices que otorgan seguridad y por lo tanto coherencia en los procesos de tecnología de información del sistema.	
MEDICIONES		
Gestión de Controles (CTRL)	CTRL:SG2 Establecer Controles CTRL:SG2.SP1 Definir los controles - Asignar nuevos controles y líneas de negocio por parte de la unidad de organización que deberá llevarse a cabo a través de planes operativos en concordancia con sus responsables.	
Gestión de Tecnología (TM)	SG2. Proteger los activos tecnológicos SG2.SP2 Establecer e Implementar Controles - Seleccionar y diseñar controles basados en los requisitos de seguridad de los activos y la gama de condiciones que requieren una integridad de la configuración de los activos y la disponibilidad del activo para cumplir con su función.	

AREA DE PROCESO: Gestión de Dependencias Externas - EXD.

Código	**P01**	
Pregunta	¿Desarrolla planes de mitigación para gestionar los riesgos que podrían afectar el funcionamiento del sistema de información al mantener dependencias externas?	
Característica	Interdependencia e Interconexión	
Técnica	Entrevista	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión de Dependencias Externas: Administrar riesgos debido a dependencias externas. ➢ Ingeniería de Soluciones Técnicas Resilientes: Desarrollar planes para el desarrollo de soluciones técnicas resilientes ➢ Gestión de Riesgos: Mitigar y controlar el riesgo, implementar estrategias de riesgo.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si utiliza planes de mitigación de riesgos en la gestión del sistema de información como apoyo en las relaciones con dependencias/entidades externas.	
MEDICIONES		
Gestión de Dependencias Externas (EXD)	SG2. Administrar riesgos debido a dependencias externas SG2.SP2 Mitigar riesgos debido a dependencias externas - Desarrollar estrategias y planes para todos los riesgos que surgen por las dependencias externas que tienen una "mitigación" o disposición de "control" de reducción del riesgo en cada uno de los componentes del sistema de información. - Validar los planes de mitigación de riesgos comparándolos con las estrategias existentes para la protección y el mantenimiento del software de modo que la ejecución de sus procesos no sean interdependientes en su totalidad de las relaciones con dependencias externas.	
Ingeniería de Soluciones Técnicas (RSTE)	SG2 Desarrollar planes para el desarrollo de soluciones técnicas resilientes SG2.SP1 Seleccionar y ajustar directrices - Identificar los criterios de selección para las directrices de resiliencia en los que se incluye el grado en el que software o sistema aborda las medidas solicitadas en los planes de mitigación de riesgos de servicios, junto con los impactos y valoraciones de riesgo por cada interconexión.	
Gestión de Riesgos (RISK)	RISK:SG5 Mitigar y control el riesgo RISK:SG5.SP2 Implementar estrategias de riesgo - Implementar los planes de mitigación de riesgo y definir el compromiso continuo con los recursos por cada plan para permitir la ejecución exitosa de las actividades de gestión de riesgos.	

Código	**P02**	
Pregunta	¿Qué acción ejecuta para aplicar criterios consistentes y uniformes en la priorización de las dependencias externas relacionadas con el sistema de información?	
Característica	Complejidad	
Técnica	JAD	
Área	CERT-RMM: ➢ Gestión de Dependencias Externas: Identificar y priorizar dependencias externas y establecer relaciones formales.	
		Revisar la lista de los activos del SI para identificar los activos que están sujetos a las dependencias externas.
		Priorizar las dependencias externas de los activos en relación con los servicios, es decir, las dependencias externas asociadas a los servicios de alto valor son a las que se otorga máxima prioridad en cuanto a las actividades de resiliencia.
	X	**Revisar y actualizar con regularidad el establecimiento de prioridades y criterios para asegurarse de que el esquema de prioridades y la lista de dependencias externas priorizadas son apropiados para el entorno de riesgos y tolerancia a los que se adapta el SI.**
		Actualizar la lista de dependencias externas en una base regular de criterios aceptables de priorización.
Observaciones	Conocer las acciones que se realizan para aplicar criterios de priorización de dependencias externas que mantienen relación con la ejecución del software.	
MEDICIONES		
Gestión de Dependencias Externas (EXD)	EXD:SG1Identificar y priorizar dependencias externas EXD:SG1.SP1 Priorizar dependencias externas - Aplicar criterios de priorización con el apoyo de la lista de dependencias externas que promuevan el desarrollo de una lista de prioridades con la descripción de dependencias externas estrictamente necesarias para la ejecución exitosa de las actividades de seguridad, planes de continuidad y planes de restauración de servicios. - Actualizar periódicamente la lista de prioridades de las dependencias externas en base a los cambios de criterios y esquema de priorización, el entorno de funcionamiento, o la lista de dependencias externas.	

Código	**P03**	
Pregunta	¿En qué momento desarrolla el SLAs (acuerdo a nivel de servicio) al asociarse con una entidad externa?	
Característica	Confidencialidad	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Gestión de Dependencias Externas: Identificar y priorizar dependencias externas, establecer relaciones formales.	
Respuesta	**X**	**En última instancia, el SLA debe ser incorporado en el acuerdo contractual formal con la entidad externa.**
	X	**Es valioso desarrollar el SLA antes de entrar en una relación con una entidad externa de modo que el SLA se puede utilizar como parte del proceso de evaluación para seleccionar una entidad externa.**
		No se utiliza el SLAs.
		Se lo adapta conforme el sistema vaya necesitando dependencias.
Observaciones	Conocer el nivel de formalidad al mantener acuerdos con entidades externas.	
MEDICIONES		
Gestión de Dependencias Externas (EXD)	EXD:SG1Identificar y priorizar dependencias externas EXD:SG1.SP1 Identificar dependencias externas - Recopilar información para definir cada dependencia externa e incluir operaciones de seguridad que garanticen la protección de archivos confidenciales del sistema de información.	
	EXD:SG3 Establecer relaciones formales EXD:SG3.SP2 Establecer especificaciones de resiliencia para dependencias externas - Incluir características específicas de la entidad externa como experiencia en el sector, tecnología y arquitectura de los sistemas, controles de procesos, regulaciones, historial de cumplimiento, etc. para asegurar que el servicio o recurso que proporciona dicha entidad no provocará interrupciones en la ejecución normal de las operaciones del sistema de información.	

Código	**P04**	
Pregunta	¿Qué controles considera esenciales para proteger y mantener estables las operaciones del sistema al incluir entidades externas?	
Característica	Mantenibilidad	
Técnica	JAD	
Área	CERT-RMM: ➢ Gestión de Control: Establecer controles. ➢ Continuidad de Servicio: Preparar para la continuidad del servicio y Mantener planes de continuidad del servicio.	
Respuesta	**X**	**Desarrollar normas y directrices traducidas en un conjunto de especificaciones a nivel del software que se reflejan en los acuerdos con cada entidad externa para asegurar una implementación sin problemas.**
		Definir criterios de priorización y esquemas de las dependencias externas.
		Incluir requisitos de resiliencia en el desarrollo del software que gestione el mantenimiento de dependencias externas.
	X	**Desarrollar políticas relativas a la seguridad de la información o de tecnología de algunos de los activos, incluyendo el uso de las directrices de resiliencia en el desarrollo de software y de sistemas activos.**
Observaciones	Conocer las medidas que salvaguarda el software para proteger el acceso y mantener continuidad en los procesos del sistema de información al relacionarse con entidades externas.	
MEDICIONES		
Gestión de Control (CTRL)	CRTL:SG1 Establecer controles CRTL:SG1.SP1 Analizar controles - Determinar controles nuevos que se ajusten con el sistema de control interno, aunque exista cierta confusión entre las capas de control con la redundancia de control estos dos tipos de controles son necesarios durante el análisis de procesos conflictivos en el sistema de información al adaptar el sistema a una entidad externa.	
Gestión de Dependencias Externas (EXD)	EXD:SG3 Establecer relaciones formales EXD:SG3.SP2 Establecer especificaciones de resiliencia para dependencias externas - Las especificaciones de resiliencia de una dependencia externa debe cubrir con claridad las operaciones del sistema de información al que se encuentren asociadas, sin descuidar la misión de la organización.	

Código	**P05**	
Pregunta	¿Establece requisitos legales, estatutarios, reglamentarios y contractuales que requiere una organización y todas sus entidades externas en relación con los sistemas de información que manejan?	
Característica	Eficiencia	
Técnica	JAD	
Área	CERT-RMM: ➢ Gestión de Dependencias Externas: Formalizar las relaciones. ➢ Desarrollo de Requisitos de Resiliencia: Identificar requisitos empresariales.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si existe la suficiente seguridad en las relaciones con entidades externas que no afecten el sistema de información.	
MEDICIONES		
Desarrollar Requisitos de Resiliencia (RRD)	RRD:SG1 Identificar requisitos empresariales RRD:SG1.SP1 Establecer Requisitos de Resiliencia Empresarial - Identificar los requisitos legales, estatutarios, reglamentarios y contractuales que requiere una organización y todas sus entidades externas como: socios comerciales, contratistas y proveedores de servicios de acuerdo con los sistemas de información que manejen. - Definir los objetivos estratégicos de la organización, factores críticos de éxito, políticas u otros indicadores de importancia que podrían dar lugar a requisitos de resiliencia empresariales y de software, en apoyo a la seguridad de información y archivos confidenciales de sus sistemas.	
Gestión de Dependencias Externas (EXD)	SG3 Establecer relaciones formales SG3.SP4 Formalizar las relaciones - Seleccionar el tipo de contrato que mejor se ajusta a los estándares de desempeño requeridos por la organización y que se puede hacer cumplir en caso que surjan problemas con la ejecución de los procesos del sistema de información. - Asegurar acuerdos mutuos entre la organización y la entidad externa en todas las disposiciones del convenio y las especificaciones antes de la firma del contrato.	

AREA DE PROCESO: Definición de Requisitos de Resiliencia - RRD.

Código	**P01**	
Pregunta	¿Desarrolla mapas de servicios para detallar las relaciones entre los servicios, procesos de negocio y activos asociados al software?	
Característica	Interoperabilidad	
Técnica	Casos de uso	
Área	CERT-RMM: ➢ Desarrollo de Requisitos de Resiliencia: Identificar requisitos empresariales y desarrollar requisitos del servicio.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si debido a la asociación entre los servicios y los activos los requisitos de resiliencia de un servicio están representados esencialmente por los requisitos de resiliencia colectiva de los activos asociados.	
MEDICIONES		
Desarrollar Requisitos de Resiliencia (RRD)	RRD:SG1 Identificar requisitos empresariales RRD:SG1.SP1 Establecer Requisitos de Resiliencia Empresarial - Identificar los principios, objetivos y requisitos de software para el procesamiento, almacenamiento y transmisión de la información en base a los servicios que apoye la organización.	
	RRD:SG2 Desarrollar requisitos del servicio RRD:SG2.SP1 Establecer Requisitos de Resiliencia de Activos - Identificar los activos y el servicio asociado al que apoyan para el aseguramiento de la misión de los servicios que depende de la productividad coherente y eficaz del personal, recursos tecnológicos, información e instalaciones relacionadas con las del servicio a fin de guiar el desarrollo de los requisitos de resiliencia a nivel de activos.	

Código	**P02**	
Pregunta	¿Qué actividad realiza para asegurar el cumplimiento de la misión de los servicios que dependen del desarrollo coherente y eficaz del software con la intervención de personas, tecnología e información relacionadas?	
Característica	Continuidad	
Técnica	JAD	
Área	CERT-RMM: ➢ Desarrollo de Requisitos de Resiliencia: Desarrollar requisitos del servicio, analizar y validar requisitos. ➢ Gestión de Requisitos de Resiliencia: Gestionar requisitos.	
Respuesta	**X**	**Controlar que los requisitos estén alineados correctamente con los controladores de la organización y que van a proporcionar el nivel adecuado de seguridad cuando se traduce en controles de protección y planes de continuidad del servicio.**
		Asignar requisitos a nivel de empresa a los servicios y los activos asociados a la construcción del software.
		Realizar un análisis de afinidad entre los conductores estratégicos (como los factores críticos de éxito) y los requisitos de los activos durante el desarrollo del software.
		Establecer objetivos estratégicos que deben ser apoyados y promovidos por todas las funciones de organización en cuanto a la construcción del software.
Observaciones	Conocer las necesidades de los requisitos de continuidad y protección de los servicios de la organización, que se traducen en requisitos de resiliencia a nivel de activos, es decir requisitos aplicables en el sistema.	
MEDICIONES		
Desarrollo de Requisitos de Resiliencia (RRD)	SG3 Analizar y validar requisitos SG3.SP1 Establecer una definición de la funcionalidad requerida - Definir referencias de todos los servicios con los que se asocia el activo para establecer requisitos de resiliencia alineados a los controladores de la organización de modo que puedan proporcionar un recuperación ágil del sistema de información cuando sus operaciones se vean afectadas por la presencia de algún riesgo.	
Gestión de Requisitos de Resiliencia (RRM)	SG1 Gestionar requisitos SG1.SP5 Identificar Inconsistencias entre los requisitos de resiliencia y las actividades desarrolladas para satisfacer los requisitos - Revisar las actividades previstas o aplicadas en consistencia con los requisitos, para identificar irregularidades que podrían afectar el proceso de recuperación del software.	

Código	**P03**	
Pregunta	¿Establece requisitos de continuidad como medida de protección y apoyo en la ejecución de los procesos del software y el cumplimiento de los servicios organizacionales?	
Característica	Redundancia	
Técnica	JAD	
Área	CERT-RMM: ➢ Desarrollo de Requisitos de Resiliencia: Analizar y validar requisitos de resiliencia. ➢ Continuidad del Servicio: Preparar para la continuidad del servicio.	
Respuestas	**X**	**Verdadero**
		Falso
Observaciones	Conocer si se incluye requisitos de continuidad en el desarrollo del software de la organización.	
MEDICIONES		
Desarrollo de Requisitos de Resiliencia (RRD)	SG3 Analizar y validar requisitos SG3.SP3 Validar requisitos de resiliencia - Identificar los requisitos faltantes en cada componente del sistema de información y en alineación entre las necesidades y los conductores estratégicos de la organización para que conservar la normalidad de los procesos del sistema en general.	
Continuidad del Servicio (SC)	SG1 Preparar para la continuidad del servicio SG1.SP1 Planear la continuidad del servicio - Establecer requisitos de continuidad de los servicios relativos a la gestión de resiliencia en el software para definir los medios y actividades involucradas en la identificación e implementación de estrategias de continuidad en el sistema.	

Código	**P04**	
Pregunta	¿Cuál cree usted que es la importancia de los requisitos en el cumplimiento de los servicios a los que apoya el software?	
Característica	Mantenibilidad	
Técnica	JAD	
Área	CERT-RMM: ➢ Desarrollo de Requisitos de Resiliencia: Analizar y validar requisitos de resiliencia. ➢ Ingeniería de Soluciones Técnicas Resilientes: Desarrollar planes para el desarrollo de soluciones técnicas resilientes.	
Respuestas	**X**	**La alineación que deben mantener con los servicios ya que vincula las actividades a nivel prácticas realizadas en la seguridad y la continuidad del negocio.**
		Los vínculos explícitos e iterativos que se establecen entre los requisitos de servicio y los requisitos de los activos.
		Los procesos de desarrollo definidos y en uso para el software o el sistema.
		Pueden ser más estrictos que las exigencias que ya se ha establecido para un activo basado en su asociación con un servicio.
Observaciones	Conocer la alineación que vincula todas las actividades fundamentales en el desarrollo del software que reflejen las necesidades de servicio de la organización.	
MEDICIONES		
Desarrollo de Requisitos de Resiliencia (RRD)	SG3 Analizar y validar requisitos SG3.SP3 Validar requisitos de resiliencia - Asegurar que los requisitos de nivel de activos admiten la funcionalidad requerida de los componentes del software de acuerdo al servicio que apoyan.	
Ingeniería de Soluciones Técnicas Resilientes (RTSE)	SG2 Desarrollar planes para el desarrollo de soluciones técnicas resilientes SG2.SP1 Seleccionar y Ajustar Directrices - Identificar la prioridad de los objetivos y requisitos de resiliencia que deben ser satisfechos en cada fase del ciclo de vida del software o a las que se puede adaptar el software para corregir fallas en la ejecución de los procesos.	

AREA DE PROCESO: Gestión de Requisitos de Resiliencia - RRM.

Código	**P01**	
Pregunta	¿Cuál es la disponibilidad de los servicios que presta su sistema de información?	
Característica	Disponibilidad	
Técnica	Entrevista, Brainstorming	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión de Control: Establecer Controles y evaluar efectividad de los controles. ➢ Gestión de Requisitos de Resiliencia: Obtener un entendimiento común de los requisitos de resiliencia y mantener la trazabilidad de los requisitos de resiliencia	
Respuesta	**X**	**Todo el tiempo como apoyo a los sistemas y componentes de tecnología, información y datos, así como las instalaciones en las que estos activos sean accesibles y productivos.**
		Parcialmente, sólo los días laborables en apoyo de los activos que intervienen en el cumplimiento de la misión de la organización.
		Temporalmente, las ocasiones que sea necesario utilizarlo para apoyar los componentes de tecnología, información y datos e instalaciones en las que estos activos sean accesibles y productivos.
Observaciones	Conocer si el sistema puede tolerar las interrupciones durante el tiempo que el usuario se encuentra interactuando en el mismo. A menudo, no hay una simple relación de uno a uno entre el requisito y el activo, ya que, en la aplicación práctica, los requisitos son usualmente traducidos y se descomponen en el nivel más bajo.	
MEDICIONES		
Desarrollo de Requisitos de Resiliencia (RRD)	SG2 Desarrollar requisitos del servicio SG2.SP1 Establecer Requisitos de Resiliencia de Activos - Realizar una evaluación de riesgos de seguridad de información y analizar el impacto en el negocio para identificar los riesgos que deben reflejarse en los requisitos de los activos que apoyen la sostenibilidad de los servicios.	
Gestión de Control (CTRL)	SG2. Establecer Controles. SG2.SP1 Definir controles - Desarrollar una matriz de trazabilidad bidireccional que asigne objetivos de control, controles de servicio y de nivel de activos en apoyo a la gestión de peticiones de llamadas en los procesos que ejecuta el sistema de información.	

Código	**P02**	
Pregunta	¿Cómo apoyaría el análisis de resultados en las evaluaciones de riesgos cuando se identifica cambios en los requisitos del sistema de información?	
Característica	Seguridad	
Técnica	Entrevista, Brainstorming	
Área	CERT-RMM: ➢ Gestión de Requisitos de Resiliencia: Gestionar Requisitos ➢ Continuidad de Servicio: Mantener planes de continuidad del servicio.	
Respuesta		Determinar el alcance de la evaluación de riesgos en los requisitos.
		Desarrollar un registro de modificación de requisitos.
		Definir objetivos estratégicos y promoverlos en todas las funciones del software.
	X	**Desarrollar y documentar criterios para establecer cuándo un cambio en los requisitos debe ser considerado.**
Observaciones	Conocer si la gestión del cambio para los requisitos de resiliencia es un proceso continuo y si asigna una buena estrategia para controlarlo, de modo que se pueda rendir informes claros de ello.	
MEDICIONES		
Gestión de Requisitos de Resiliencia (RRM)	SG1 Gestionar Requisitos SG1.SP2 Gestionar los cambios en los requisitos de resiliencia - Desarrollar y documentar criterios para establecer cuándo un cambio en los requisitos debe ser considerado de modo que se asegure de que tales criterios sean acordes con la tolerancia al riesgo de la organización.	
Continuidad del Servicio (SC)	SG7 Mantener planes de continuidad del servicio SG7.SP1 Establecer criterios de cambio - Desarrollar y documentar las condiciones que pueden dar lugar a cambios en los requisitos de resiliencia para apoyar la identificación de nuevas vulnerabilidades en el software que afectan las condiciones de funcionamiento y protección.	

Código	**P03**	
Pregunta	¿Cómo monitorea el proceso de gestión del cambio durante la actualización de los requisitos a nivel de activos?	
Característica	Mantenibilidad	
Técnica	JAD, Casos de uso	
Área	CERT-RMM: ➢ Gestión de Control: Establecer controles, analizar controles y evaluar la efectividad de los controles. ➢ Gestión de Requisitos de Resiliencia: Gestionar los requisitos.	
Respuestas		Se identifica y documenta los cambios en los requisitos existentes (o la identificación de nuevas necesidades, si es necesario) ya que cualquier cambio en los controles existentes y la adición de nuevos controles puede resultar en la necesidad de una nueva evaluación.
		Se evalúa el impacto de los cambios en los requisitos de activos dado que la identificación de los activos asociados que puedan verse afectados por varios factores desencadenantes.
	X	**Se evalúa que de forma independiente el proceso de gestión del cambio esté en funcionamiento.**
Observaciones	Conocer si se gestiona los cambios que se realizan en los activos relacionados con el sistema de información, de modo que se actualice también los acuerdos con los encargados de ejecutar los servicios (custodios).	
MEDICIONES		
Gestión de Control (CTRL)	CRTL: SG2 Establecer controles CRTL: SG2.SP1 Definir los controles - Establecer controles a nivel de activos relacionados con el software para satisfacer objetivos de control en relación con los requisitos que pueden ser una combinación de los controles que ya existen, los controles que necesitan ser actualizados y controles nuevos que deben ponerse en práctica, de modo que faciliten la adaptabilidad del software en un entorno modificado.	
Gestión de Requisitos de Resiliencia (RRM)	RRM:SG1 Gestionar Requisitos RRM:SG1.SP3 Gestionar los cambios en los Requisitos de Resiliencia - Mantener un historial de cambios de requisitos que justifique la realización de los cambios y permita evaluar las actividades y compromisos para la protección y el mantenimiento de los bienes y servicios existentes.	

Código	**P04**	
Pregunta	¿Identifica e incluye requisitos de seguridad en cooperación y comprensión mutua entre los encargados de la ejecución de servicios y los encargados de la viabilidad de los activos para mejorar el software?	
Característica	Integridad	
Técnica	JAD, Casos de uso	
Área	CERT-RMM: ➢ Gestión de Requisitos de Resiliencia: Gestionar los requisitos. ➢ Definición y Gestión de Activos: Establecer activos organizacionales.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si existe una cooperación mutua y compartida de los requisitos que apoyan al software y el cumplimiento de las necesidades de la organización.	
MEDICIONES		
Gestión de Requisitos de Resiliencia (RRM)	SG1 Gestionar Requisitos SG1.SP1 Obtener un entendimiento de los Requisitos de Resiliencia - Establecer objetivos de evaluación y criterios de aceptación de los requisitos en coherencia con la misión de la organización y de los sistemas con los que opera, en los cuales se deberá incluir el cifrado de datos para apoyar el mejoramiento y protección del software. SG1.SP2 Obtener un compromiso con los Requisitos de Resiliencia - Documentar los requisitos en concordancia con los encargados de la ejecución de los servicios de modo que pueda fundamentarse la inclusión de los requisitos para mejorar el software.	
Definición y Gestión de Activos (ADM)	SG1 Establecer Activos Organizacionales SG1.SP2 Establecer un Entendimiento Común - Actualizar los perfiles de los activos para establecer y documentar la asociación de los activos a un servicio, de modo que los propietarios puedan asignar medidas de protección en las que se incluye el cifrado de datos en coherencia con las responsabilidades de los encargados de la ejecución de los servicios.	

Código	**P05**	
Pregunta	¿Cómo gestiona que los cambios en las necesidades asignadas a los custodios durante el desarrollo del software sean satisfechos y no se vean limitados?	
Característica	Redundancia	
Técnica	JAD	
Área	CERT-RMM: ➢ Gestión de Requisitos de Resiliencia: Gestionar Requisitos. ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Establecer lineamientos para el desarrollo de soluciones técnicas resilientes.	
Respuesta		Se utiliza normas de codificación segura para garantizar que los requisitos se cumplan y que las vulnerabilidades al realizar cambios en el software sean eliminados.
	X	**Se revisa las actividades previstas o aplicadas para la consistencia con los requisitos e identificar los cambios realizados en los requisitos.**
		Se identifica las inconsistencias de forma proactiva para negociar con los propietarios los cambios en los requisitos realizados por los custodios.
Observaciones	Conocer si el software es capaz de soportar eventos inesperados y continuar con su trabajo, sin dejar tiempos muertos de inactividad.	
MEDICIONES		
Gestión de Requisitos de Resiliencia (RRM)	SG1 Gestionar Requisitos SG1.SP5 Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos - Revisar las actividades previstas o aplicadas en el sistema en consistencia con los requisitos e identificar los cambios realizados en los mismos, de modo que los riesgos que puedan surgir con dichos cambios, puedan ser resueltos por cada activo antes que se ejecute los servicios a los que apoyan.	
Ingeniería de Soluciones Técnicas Resilientes (RTSE)	SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes SG1.SP4 Identificar las directrices de Implementación - Establecer revisiones, inspecciones y realizar análisis constantes del estado de los requisitos y así identificar los cambios no previstos y evaluar su impacto positivo o negativo en cuanto al cumplimiento de la misión del servicio al que se relaciona el software.	

AREA DE PROCESO: Ingeniería de Soluciones Técnicas Resilientes - RSTE.

Código	**P01**	
Pregunta	¿Cuál es la base o soporte de los criterios de inspección que utiliza para proporcionar un nivel aceptable de seguridad y confianza en el despliegue del software?	
Característica	Disponibilidad	
Técnica	JAD	
Áreas de CERT-RMM	CERT-RMM: ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Ejecutar el Plan. ➢ Gestión y Definición de Activos: Establecer Activos Organizacionales.	
Respuestas		La documentación de listas de pruebas en apoyo a los casos de garantía en el despliegue del software.
		Los resultados de los enfoques de prueba y montaje en las directrices de seguridad del software.
	X	**La disponibilidad completa y exhaustiva de la documentación de activos, incluyendo los inventarios de activos actualizados.**
		La satisfacción de los requisitos de seguridad en apoyo a los planes de continuidad de los servicios que soporta el activo a ser liberado.
Observaciones	Conocer el criterio fundamental y aplicable que puede tolerar el software para proceder a su despliegue en entornos de producción.	
MEDICIONES		
Ingeniería de Soluciones Técnicas de resiliencia (RSTE)	SG3 Ejecutar el Plan SG3.SP2 Entregar soluciones técnicas resilientes en producción - Inspeccionar el software y sistemas de manera predecible y repetible para asegurar que tengan criterios de inspección satisfechos antes de la liberación en un entorno de producción.	
Gestión y Definición de Activos (ADM)	SG1 Establecer Activos Organizacionales ADM:SG1.SP2 Establecer un entendimiento común - Crear un perfil para cada activo de alto valor y documentar la descripción donde se defina las diferencias e incluya información útil para facilitar la definición de los requisitos y la satisfacción de los mismos evaluados durante el despliegue del sistema.	

Código	**P02**	
Pregunta	¿Qué método utiliza para reflejar las directrices de mejora del plan de gestión de software?	
Característica	Redundancia	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Desarrollar planes para el desarrollo de soluciones técnicas resilientes. ➢ Continuidad de Servicio: Preparar para la continuidad del servicio.	
Respuesta	**X**	**La definición de procesos de desarrollo que incluye medidas de progreso, establecimiento y presentación de objetivos, y la asignación de recursos (personal, fondos, bienes de equipo, etc.) para poner en práctica las directrices de resiliencia.**
		La definición de criterios de decisión y autoridad en el desarrollo del plan, aplicables en los hitos principales del sistema de información.
		La identificación de los conceptos operacionales y escenarios asociados a la capacidad de recuperación del software.
Observaciones	Conocer el método que utiliza para reflejar las directrices de resiliencia en el sistema de información.	
MEDICIONES		
Ingeniería de Soluciones Técnicas Resilientes (RTSE)	SG3 Ejecutar el Plan SG3.SP1 Monitorear la ejecución del plan de desarrollo - Monitorear el desempeño del software y documentar los procesos que apoyan y mejoran la seguridad, rendimiento, disponibilidad, continuidad y seguridad del sistema para garantizar la ejecución normal del sistema de información.	
Continuidad del Servicio (SC)	SG1 Preparar para la continuidad del servicio SG1.SP2 Establecer estándares y directrices para la continuidad del servicio - Desarrollar y comunicar las directrices y normas de continuidad del servicio considerando: la propiedad y responsabilidad del plan, requisitos de documentación para los planes, requisitos de prueba para los planes incluyendo los intervalos y presentación de informes de resultados de las pruebas, etc.	

Código	**P03**	
Pregunta	¿Somete el software a una inspección formal en base a criterios documentados para asegurar que se ha cumplido con las directrices de mejora antes de ser liberados en un entorno de producción?	
Característica	Continuidad	
Técnica	Entrevista, Brainstorming	
Área	CERT-RMM: ➢ Gestión de Requisitos de Resiliencia: Gestionar requisitos. ➢ Ingeniería de Soluciones Técnicas Resilientes: Desarrollar planes para el desarrollo de soluciones técnicas resilientes.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si el resultado satisfactorio de los criterios de inspección es la aprobación para el despliegue del software.	
MEDICIONES		
Gestión de Requisitos de Resiliencia (RRM)	SG1 Gestionar requisitos SG1.SP4 Mantener la trazabilidad de los requisitos de resiliencia - Desarrollar un documento que detalle el origen y función de los requisitos, que incluya además como cambian dichos requisitos para asegurar que refleje las necesidades actuales del sistema antes del despliegue. SG1.SP5 Identificar inconsistencias entre los requisitos de resiliencia y las actividades desarrolladas para satisfacer los requisitos - Documentar las restricciones de custodia que puedan impedir la actualización de los requisitos en caso de ser necesario, así como la satisfacción de las necesidades del sistema obstaculizando la continuidad de sus operaciones.	
Ingeniería de Soluciones Técnicas (RSTE)	RTSE:SG2 Realizar planes para el desarrollo de soluciones técnicas resilientes RTSE:SG2.SP1 Seleccionar y ajustar directrices - Identificar los criterios de selección para las directrices de resiliencia, como el valor relativo del software, prioridad de los objetivos y requisitos de resiliencia, etc., que de una u otra forma influyen en el proceso de recuperación del software.	

Código	**P04**	
Pregunta	¿Qué directrices de codificación utiliza en su software para superar situaciones de estrés?	
Característica	Interoperabilidad	
Técnica	Brainstorming, Casos de uso	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión de Riesgos: Establecer Controles. ➢ Ingeniería de Soluciones Técnicas Resilientes: Establecer lineamientos para el desarrollo de soluciones técnicas resilientes.	
Respuesta	**X**	**Normas de codificación segura y herramientas de análisis de código estático y dinámico.**
		Patrones de diseño en el nivel de arquitectura y diseño.
		Evaluación de la superficie de ataque y mitigación de vulnerabilidades.
		Monitoreo y auditorias durante la codificación.
Observaciones	Conocer si el software cuenta con normas y herramientas que aseguren la operatividad de los procesos durante las actividades normales y en momentos de estrés.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG6. Utilizar la Información de los Riesgos para Gestionar la Resiliencia. SG6.SP1 Revisar y ajustar estrategias para proteger los activos y servicios - Revisar los controles existentes o desarrollar e implementar controles adicionales que son necesarias para mitigar los riesgos a los que está propenso el sistema.	
Ingeniería de Soluciones Técnicas Resilientes (RSTE)	SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes SG1.SP3 Identificar las directrices de arquitectura y diseño - Identificar directrices de arquitectura y diseño para el desarrollo de sistemas de información, de manera que dichas directrices apoyen la estabilidad del sistema cuando exista inconvenientes. - Realizar análisis de código abierto, COTS, incluyendo la verificación de la conducta funcional, la resistencia requerida y la ausencia de contenido malicioso en el sistema de información.	

Código	**P05**	
Pregunta	¿Cuál de las siguientes opciones considera que es correcta al definir la arquitectura y diseño del software?	
Característica	Integridad	
Técnica	JAD	
Área	CERT-RMM: ➢ Ingeniería de Soluciones Técnicas Resilientes: Establecer lineamientos para el desarrollo de soluciones técnicas resilientes. ➢ Gestión de Tecnología: Gestionar la integridad de los activos de tecnología	
Respuestas	**X**	**Construir estrategias que conserven la flexibilidad en la arquitectura para asegurar el funcionamiento de los servicios en momentos de estrés o después de eventos disruptivos.**
		Incluir temas de interconexión, interoperabilidad, continuidad del servicio, escalabilidad y complejidad en los componentes del software.
		Evaluar las posibles debilidades en el diseño que podrían ser explotadas al culminar la implementación del sistema.
		Identificación y priorización de control durante la arquitectura y el diseño.
Observaciones	Conocer la importancia que se otorga al planificar y desarrollar la arquitectura y diseño del sistema de información.	
MEDICIONES		
Ingeniería de Soluciones Técnicas Resilientes (RSTE)	RTSE:SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes RTSE:SG1.SP3 Identificar las directrices de Arquitectura y Diseño - Desarrollar patrones de diseño que garanticen seguridad en la arquitectura y diseño de los sistemas de información. - Analizar la complejidad y la escala del sistema, incluyendo los procesos de negocio de extremo a extremo y análisis de la vulnerabilidad del servicio.	
Gestión de Tecnología (TM)	TM:SG4 Gestionar la integridad de los activos de tecnología TM:SG4.SP2 Ejecutar la gestión de la configuración - Definir estándares de tecnología, directrices y políticas para la gestión de la configuración e Implementar seguridad en sus activos con el uso de la encriptación y administración de credenciales.	

Código	**P06**	
Pregunta	¿Considera usted que el incrementar medidas de seguridad en el desarrollo de software en lugar de capacitar al personal contrarresta el error humano y disminuye posibilidades de riesgo?	
Característica	Operatividad	
Técnica	JAD	
Área	CERT-RMM: ➢ Gestión de Control: Establecer objetivos de control. ➢ Ingeniería de Soluciones Técnicas: Establecer lineamientos para el desarrollo de soluciones técnicas resilientes	
Respuesta		Verdadero
	X	**Falso**
Observaciones	Conocer si la capacitación al personal es tomando en consideración como medida de seguridad para realizar archivos con un alto nivel de operatividad.	
MEDICIONES		
Gestión de Control (CTRL)	CRTL: SG1 Establecer objetivos de control CRTL: SG1.SP1 Definir objetivos de control - Determinar estándares que ayuden al personal en el desarrollo correcto del sistema, en los cuáles se incluya adicionalmente códigos de ética e integridad en la ejecución de los procesos asignados.	
Ingeniería de Soluciones Técnicas (RSTE)	RSTE: SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes RSTE: SG1.SP2 Identificar directrices de Requisitos - Identificar pautas para el desarrollo de software y sistemas resilientes como: recolección de requisitos de resiliencia, análisis de riesgos y requisitos de compensación, control de acceso, gestión de entidades, etc. y además capacitar a ingenieros de software y administradores de proyectos para gestionar e incluir la resiliencia en los sistemas de información.	

AREA DE PROCESO: Gestión de Riesgos - RISK.

Código	**P01**	
Pregunta	¿Identifica y prioriza los servicios para definir los riesgos que deberán gestionarse con la ayuda del planteamiento de requisitos con el objetivo de mejorar el software?	
Característica	Escalabilidad	
Técnica	JAD, Brainstorming	
Áreas de CERT-RMM	CERT-RMM: ➢ Desarrollo de Requisitos e Resiliencia: Desarrollar requisitos del servicio. ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Establecer lineamientos para el desarrollo de soluciones técnicas resilientes. ➢ Gestión de Riesgos: Utilizar la Información de los Riesgos para Gestionar la Resiliencia.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si en el sistema la identificación y priorización los servicios son vitales para el cumplimiento de la misión operativa, de modo que se identifique las necesidades específicas de los activos.	
MEDICIONES		
Desarrollo de Requisitos de Resiliencia (RRD)	SG2 Desarrollar requisitos del servicio SG2.SP1 Establecer Requisitos de Resiliencia de Activos - Realizar la evaluación de riesgos para identificar aquellos que deben reflejarse en los requisitos de los activos y comunicar los requisitos que afectan a todas las unidades de la organización y líneas de negocio para que puedan gestionarse.	
Ingeniería de Soluciones Técnicas de resiliencia (RSTE)	SG2 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes SG1.SP2 Identificar las directrices de Requisitos - Identificar requisitos para el desarrollo de software y sistemas resilientes, como el análisis de riesgos durante la ingeniería de requisitos para priorizar riesgos, requisitos de compensación que incluyen lo que necesita el propietario del servicio, las necesidades de las partes interesadas, las consideraciones ambientales, etc. - Revisar las especificaciones de los requisitos para definir los medios de validación de los niveles escalables del software.	
Gestión de Riesgos (RISK)	RISK: SG6. Utilizar la Información de los Riesgos para Gestionar la Resiliencia. RISK: SG6.SP2 Revisar y ajustar las estrategias para mantener los servicios. - Validar los planes a través de los riesgos identificados para garantizar la efectividad del plan al cubrir una serie de posibles amenazas, riesgos operacionales y de software.	

Código	**P02**	
Pregunta	¿Cómo controla el equilibrio en la comunicación de los procesos cuando se presentan riesgos?	
Característica	Continuidad	
Técnica	Entrevista	
Área	CERT-RMM: ➢ Gestión de Riesgos: Análisis de riesgos. ➢ Ingeniería de Soluciones Técnicas Resilientes: Desarrollar planes para el desarrollo de soluciones técnicas resilientes.	
Respuesta	**X**	**Se gestiona tiempos de interrupción mínimos.**
		Se desarrolla planes de mitigación de riesgos.
		Se desarrolla un plan de comunicaciones.
Observaciones	Conocer si el sistema a pesar de la presencia de inconvenientes puede continuar con el funcionamiento normal de sus operaciones.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG6 Usar información de riesgo para gestionar la resiliencia SG6.SP1 Revisar y ajustar estrategias para proteger los activos y servicios. - Revisar y ajustar las lecciones aprendidas en la gestión de riesgos para validar los planes a través de los riesgos identificados para conservar la continuidad en los procesos del sistema de información y en los servicios que presta.	
Ingeniería de Soluciones Técnicas (RSTE)	SG2 Desarrollar planes para el desarrollo de soluciones técnicas resilientes SG2.SP2 Integrar las directrices seleccionadas con un proceso definido de desarrollo de software y sistemas - Determinar riesgos nuevos introducidos por las directrices de resiliencia y elevar los riesgos identificados en la actualidad a una prioridad más alta, de manera que la resolución de los mismos sea en tiempos mínimos que no alteren la ejecución de procesos del sistema de información.	

Código	**P03**	
Pregunta	¿Qué consideraciones de gestión de riesgo utiliza para mejorar y mantener estable el control interno del sistema?	
Característica	Modularidad	
Técnica	Entrevista, Brainstorming	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión de Riesgos: Utilizar Información de Riesgos para Administrar la Resiliencia. ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Establecer directrices para el desarrollo de soluciones técnicas resilientes. ➢ Continuidad del Servicio: Desarrollar Planes de Continuidad de Servicio.	
Respuesta	**X**	**El uso de lecciones aprendidas en la gestión de riesgos que ayuda al sistema al aplicar controles faltantes y actualizar los controles existentes para considerar los riesgos nuevos y emergentes por cada componente del sistema.**
		Comparar los planes de mitigación de riesgo con los sistemas de control interno en activos y servicios afectados de los componentes del sistema de información.
		Revisar los controles existentes en los componentes del sistema de información o desarrollar controles adicionales necesarios para mitigar los riesgos.
		Definir un plan de continuidad del servicio para mantener estabilidad en las operaciones del sistema de información.
Observaciones	Conocer si la información obtenida a partir de la identificación, análisis y mitigación de riesgos se utiliza para mejorar el proceso de gestión de resiliencia en el software.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG6. Utilizar Información de Riesgos para Administrar la Resiliencia SG6.SP1 Revisar y ajustar las estrategias para proteger los bienes y servicios - Revisar y ajustar las lecciones aprendidas durante la gestión de riesgos para identificar e implementar controles faltantes en los componentes del sistema de información.	
Ingeniería de Soluciones Técnicas de Resiliencia (RTSE)	SG1. Establecer directrices para el desarrollo de soluciones técnicas resilientes SG1.SP1 Identificar Directrices Generales - Determinar el alcance de la resiliencia en el software con la presencia de riesgos mediante el control de la continuidad de las operaciones para el o los servicios que el software apoya.	
Continuidad del Servicio (SC)	SG3. Desarrollar Planes de Continuidad de Servicio SG3. SP1 Desarrollar y Documentar Planes de Continuidad de Servicio - Definir estrategias para conservar la independencia entre los componentes del software de manera que se mantenga estabilidad en los servicios que apoya.	

Código	**P04**	
Pregunta	¿Realizar la evaluación de riesgos y analizar el impacto en el negocio ayuda a identificar los conflictos que podrían presentarse con la inclusión de normas internas adicionales y herramientas para el desarrollo del sistema de información?	
Característica	Interoperabilidad	
Técnica	Entrevista, Brainstorming	
Áreas de CERT-RMM	CERT-RMM: ➢ Definición de Requisitos de Resiliencia: Analizar y validar requisitos. ➢ Gestión de Riesgos: Identificar el Riesgo.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si el sistema puede tolerar las interrupciones durante el tiempo que el usuario se encuentra interactuando en el mismo.	
MEDICIONES		
Desarrollo de Requisitos de Resiliencia (RRD)	SG3 Analizar y validar requisitos SG3.SP1 Analizar requisitos de resiliencia de activos - Analizar los requisitos de activos en contra de la funcionalidad de los activos de referencia y realizar ajustes en los mismos que apoyen el tratamiento de los riesgos según sea necesario.	
Gestión de Riesgos (RISK)	SG3 Identificar el riesgo SG3.SP1 Identificar los niveles de riesgo en los activos - Identificar las herramientas, técnicas y métodos que la organización puede utilizar para identificar los riesgos operativos que afecten el funcionamiento de los sistemas de información.	

Código	**P05**	
Pregunta	¿Cómo determina la resistencia de los controles del sistema de información en base al análisis de riesgos?	
Característica	Rendimiento	
Técnica	Entrevista, Brainstorming	
Áreas de CERT-RMM	CERT-RMM: ➢ Gestión de Control: Evaluar efectividad de los controles. ➢ Gestión de Riesgos: Utilizar la Información de los Riesgos para Gestionar la Resiliencia.	
Respuesta		Se dispone los controles en capas para evaluar el cumplimiento de los objetivos de control establecidos.
	X	**Se identifica los cambios en los controles existentes, propuestas de nuevos controles y otros métodos para abordar las deficiencias de control en el menor tiempo posible.**
		Se define los riesgos que podrían surgir como resultado de los vacíos que aún persisten, incluso cuando los controles están operando de manera efectiva.
		Se identifica controles en conflicto y se los sustituye o se procede a eliminarlos cuando sea posible.
Observaciones	Conocer si se identifica los cambios en la administración de los controles de para enfrentar riesgos en tiempos mínimos de modo que no se interrumpa las ejecución de operaciones del sistema de información.	
MEDICIONES		
Gestión de Control (CTRL)	SG4. Evaluar efectividad de los controles. SG4.SP1 Evaluar los controles - Ejecutar la evaluación de controles utilizando diversas técnicas que van desde las auto-evaluaciones informales y evaluaciones formales más estructuradas contra las normas establecidas proporcionando mayor rapidez en la ejecución de procesos. - Identificar cambios en los controles existentes y los nuevos controles propuestos para abordar las áreas problemáticas y reducir el coste de los controles.	
Gestión de Riesgos (RISK)	SG5 Mitigar y controlar el Riesgo SG5.SP2 Implementar estrategias de Riesgo - Desarrollar un método para el seguimiento de los riesgos e implementarlo en los planes de mitigación de riesgo que recoge medidas de rendimiento en el proceso de gestión de riesgos.	

Código	**P06**	
Pregunta	¿Qué estrategia utiliza para la selección y la aplicación de estrategias de control de riesgos frente a los bienes y servicios asociados a la continuidad de las operaciones del sistema de información?	
Característica	Redundancia	
Técnica	Entrevista, Brainstorming	
Área	CERT-RMM: ➢ Gestión de Riesgos: Mitigar y controlar el riesgo. ➢ Continuidad de Servicio: Desarrollar planes de continuidad del servicio, validar planes de continuidad del servicio y ejercer planes de continuidad del servicio.	
Respuesta		Diseñar e implementar los requisitos de seguridad en los bienes y servicios para conservar la continuidad del software.
		Utilizar herramientas, técnicas y metodologías, como las evaluaciones de riesgos en la seguridad de la información.
		Utilizar lecciones aprendidas de bases de datos, como la base de conocimiento de incidentes para proteger la continuidad del sistema de información.
	X	**Desarrollar planes de continuidad del servicio que mantendrán la continuidad del software si se ve afectado por la presencia de riesgos.**
Observaciones	Conocer la estrategia utilizada para que el software conserve la continuidad de sus operaciones aún con la presencia de riesgos.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG5 Mitigar y control el Riesgo SG5.SP2 Implementar estrategias de Riesgo - Plantear el compromiso continuo de los recursos para cada plan en apoyo a la ejecución exitosa de las actividades de gestión de riesgos en el sistema de información.	
Continuidad del Servicio (SC)	SC:SG3 Desarrollar planes de continuidad del servicio SC: SG3.SP1 Identificar los planes a ser desarrollados - Desarrollar planes de continuidad de servicios como parte del proceso de análisis de impacto en el negocio a fin de apoyar el cumplimiento de las actividades de auditoría en los procesos del sistema de información. SC:SG3.SP2 Desarrollar y documentar los planes de continuidad del servicio - Documentar el plan de continuidad del servicio a través de plantillas disponibles e identificar los grupos de interés de los planes específicos de continuidad del servicio.	

Código	**P07**	
Pregunta	¿Qué parámetros de riesgos utiliza en su sistema de información para la medición consistente de las vulnerabilidades a las que está expuesto durante su desarrollo?	
Característica	Operatividad	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Gestión de Riesgos: Establecer parámetros y enfoque de riesgos. ➢ Ingeniería de Soluciones Técnicas Resilientes: Desarrollar planes para el desarrollo de soluciones técnicas resilientes.	
Respuestas		Se utiliza taxonomías y escenarios de riesgos.
		Se revisa los catálogos o historial de vulnerabilidades.
		Se realiza auditorías y revisiones internas de riesgos durante la codificación.
	X	**Definir umbrales de riesgo para cada categoría de riesgo en el desarrollo del software.**
Observaciones	Conocer si se gestiona umbrales de riesgo para la protección del software, puesto que si los riesgos sobresalen a los umbrales se consideran inaceptables, y se deberán tomar medidas para mitigar los riesgos.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG2 Establecer parámetros y enfoque de riesgos SG2.SP1 Definir parámetros de riesgo - Definir umbrales de riesgo para cada categoría de riesgo al definir la probabilidad de que se presenten riesgos durante el desarrollo del sistema de información.	
Ingeniería de Soluciones Técnicas Resilientes (RSTE)	SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes SG1.SP4 Identificar las directrices de Implementación - Identificar las directrices de codificación para el desarrollo de software resiliente como: análisis de riesgos y amenazas durante la codificación, evaluación y mitigación de la superficie de ataque, definición de patrones de diseño seguras en el nivel de ejecución, inclusión de estándares de codificación de software seguro, etc.	

Código	**P08**	
Pregunta	¿Cómo categoriza los riesgos del software en cuanto a los activos de tecnología?	
Característica	Confidencialidad	
Técnica	Entrevista, Brainstorming	
Área	CERT-RMM: ➢ Gestión de Riesgos: Preparación para la Gestión de Riesgos ➢ Desarrollo de Requisitos de Resiliencia: Identificar requisitos empresariales y desarrollar requisitos del servicio.	
Respuesta		Se determina las fuentes de riesgo como herramienta para la gestión de riesgos de forma continua a las condiciones de operación que cambian y evolucionan.
		De acuerdo a las acciones involuntarias de personas, tales como divulgaciones accidentales o modificaciones de la información.
	X	**Se realiza en cuanto a los fallos de la tecnología, tales como los resultados previstos de la ejecución del software y el fracaso de los componentes de hardware, tales como servidores y telecomunicaciones.**
		Se toma en cuenta los eventos y las fuerzas externas, tales como desastres naturales, fallas de la infraestructura pública, y los inconvenientes suscitados en la cadena de suministro de la organización.
Observaciones	Conocer la forma en la que se categoriza los riesgos del software que afectan los activos de tecnología.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG1 Preparación para la Gestión de Riesgos SG1.SP1 Determinar las categorías y fuentes de riesgo - Determinar las fuentes de riesgo como: malos diseños, acciones involuntarias de personas, fallas de tecnología, etc., para definir las categorías de riesgo que facilitan el proceso de análisis y mitigación.	
Gestión de Tecnología (TM)	SG3 Gestionar riesgos de los activos de tecnología SG3.SP1 Identificar y evaluar los riesgos de activos de tecnología - Monitorear el riesgo y la estrategia de riesgo sobre una base regular para asegurarse de que no representa una amenaza adicional en los procesos del software.	

AREA DE PROCESO: Gestión de Tecnología - TM.

Código	**P01**	
Pregunta	¿Qué políticas y procedimientos de gestión de acceso establece para aprobar privilegios de acceso a los activos de tecnología?	
Característica	Seguridad	
Técnica	JAD, Casos de uso	
Área	CERT-RMM: ➢ Gestión de Tecnología: Gestionar la integridad de los activos de tecnología. ➢ Definición de Requisitos de Resiliencia: Desarrollar requisitos del servicio.	
Respuesta		Solicitar un inventario de activos de tecnología y para priorizar los activos en relación con los requisitos de seguridad del sistema de información.
	X	**Desarrollar directrices claras para las solicitudes de acceso que se incluyen el tipo y el grado de acceso que se les entregará a los objetos, como los sistemas y procesos.**
		Seleccionar un nivel de control de configuración en base a los objetivos, riesgos y recursos que varían en relación con el ciclo de vida del proyecto.
Observaciones	Conocer las políticas para gestionar el acceso en los activos de tecnología que se encuentran relacionados con los sistemas de información.	
MEDICIONES		
Definición de Requisitos de Resiliencia (RRM)	SG2 Desarrollar requisitos del servicio SG2.SP1 Establecer requisitos de resiliencia de activos - Entrevistar a los propietarios de activos para determinar las necesidades específicas de acceso en el sistema de información.	
Gestión de Tecnología (TM)	TM:SG4 Gestionar la integridad de los activos de tecnología TM:SG4.SP1 Controlar el acceso a los activos de tecnología - Establecer políticas y procedimientos de administración de solicitudes de acceso y aprobación de privilegios en los activos de tecnología para el establecimiento de herramientas organizativamente aceptables, así como técnicas y métodos para controlar el acceso al software.	

Código	**P02**	
Pregunta	¿Cómo planifica el mantenimiento de los recursos tecnológicos integrados en el desarrollo del software para el cumplimiento de los servicios de la organización?	
Característica	Disponibilidad	
Técnica	Entrevistas, JAD	
Áreas de CERT-RMM	CERT-RMM: ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Realizar planes para el desarrollo de soluciones técnicas resilientes ➢ Gestión de Tecnología: Gestionar la disponibilidad de los activos de tecnología.	
Respuesta	**X**	**Se puede optar por desarrollar planes de continuidad del servicio para la aplicación en los sistemas como parte del desarrollo de los servicios de alto valor.**
		Se analiza el impacto de vulnerabilidades en los componentes del software que podrían afectar los activos de tecnología y en base al resultado establecer estrategias de protección para los activos.
		Se evalúa la disponibilidad de métricas para la tecnología y los servicios relacionados en el mantenimiento de los activos tecnológicos.
Observaciones	Conocer la planificación para el mantenimiento de los activos de tecnología que pueden influir positiva o negativamente en caso de presentarse un inconveniente en el software.	
MEDICIONES		
Ingeniería de Soluciones Técnicas de resiliencia (RSTE)	RTSE:SG2 Realizar planes para el desarrollo de soluciones técnicas resilientes RTSE:SG2.SP1 Seleccionar y ajustar directrices - Seleccionar y adaptar directrices que se ajusten al valor relativo del otorgando prioridad a la protección de los activos tecnológicos en los que se apoya el sistema.	
Gestión de Tecnología (TM)	TM:SG5 Gestionar la disponibilidad de los activos de tecnología TM:SG5.SP1 Ejecutar la planeación para el sostenimiento de activos de tecnología - Establecer indicadores de disponibilidad en activos de tecnología de alto valor, de modo que se establezcan objetivos que disminuyan el tiempo que tarda el software en recuperar su estado normal.	

Código	**P03**	
Pregunta	¿Desarrolla planes de continuidad por cada tipo de software que utiliza en su organización o los agrupa con el desarrollo de planes de continuidad de servicio?	
Característica	Complejidad	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Gestión de Tecnología: Proteger los activos tecnológicos y gestionar la disponibilidad de los activos de tecnología. ➢ Continuidad del Servicio: Desarrollar planes de continuidad del servicio.	
Respuesta		Se desarrolla planes de continuidad por cada tipo de software.
		Se agrupa los planes de continuidad de los activos con los planes de continuidad del servicio.
	X	**Se realiza las dos acciones, evaluando el ambiente y estructura de los activos.**
		No se desarrolla planes de continuidad.
Observaciones	Conocer cómo se vinculan los activos entre sí a más de los servicios que tienen asociados y determinar cuál será su enfoque de planificación para sostener dichos activos.	
MEDICIONES		
Gestión de Tecnología (TM)	TM: SG2Proteger los activos tecnológicos. TM:SG2.SP1 Asignar Requisitos de Resiliencia a los Activos de Tecnología - Desarrollar, implementar y administrar un nivel adecuado de controles administrativos, técnicos y físicos para manejar las condiciones que podrían causar la interrupción de los activos, tomando en cuenta la naturaleza compartida de la tecnología	
Continuidad del Servicio (SC)	SG3 Desarrollar planes de continuidad del servicio SG3.SP1 Identificar los planes a ser desarrollados - Identificar los grupos de interés de los planes específicos de continuidad del servicio, que pueden ser gerentes de nivel superior y dueños de los activos.	

Código	**P04**	
Pregunta	¿Cuenta con un sistema de control interno para proteger el funcionamiento continuo de los recursos tecnológicos que forman parte del sistema de información?	
Característica	Operatividad	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Gestión de Control: Establecer objetivos de control. ➢ Gestión de Tecnología: Proteger los activos tecnológicos.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si se utiliza controles para proporcionar un nivel aceptable de protección sobre los activos de tecnología que apoyan el desarrollo y funcionamiento del software.	
MEDICIONES		
Gestión de Control (CTRL)	SG1 Establecer objetivos de control SG1.SP1 Definir objetivos de control - Otorgar prioridades en los controles que se derivan de las directivas y directrices de gestión de los recursos tecnológicos que forman parte del sistema de información.	
Gestión de Tecnología (TM)	SG2 Proteger los activos de tecnología SG2.SP2 Establecer e implementar controles - Seleccionar y diseñar controles basados en los requisitos de capacidad de recuperación de los activos y la gama de condiciones que requieren integridad en la configuración de los activos y la disponibilidad del activo para cumplir con su función.	

AREA DE PROCESO: Continuidad de Servicio - SC.

Código	**P01**	
Pregunta	¿Cuáles son las consideraciones que toma en cuenta al desarrollar y comunicar las directrices y normas de continuidad del servicio a los interesados en el sistema de información?	
Característica	Flexibilidad	
Técnica	JAD	
Áreas de CERT-RMM	CERT-RMM: ➢ Ingeniería de Soluciones Técnicas de Resiliencia: Ejecutar el Plan. ➢ Continuidad de Servicio: Mantener planes de continuidad de servicio.	
Respuesta		Propiedad y responsabilidad del plan.
	X	**Requisitos de prueba para los planes, incluyendo los intervalos y presentación de informes de resultados de las pruebas.**
		Identificación y participación de los interesados en el sistema de información.
		Plan de control de versiones, repositorios y seguridad.
Observaciones	Conocer si utiliza alguna estrategia para apoyar la mantenibilidad del proceso de comunicación entre los interesados del software y por ende sustente el equilibrio de los procesos.	
MEDICIONES		
Ingeniería de Soluciones Técnicas de Resiliencia (RSTE)	SG3. Ejecutar el Plan SG3.SP2 Liberar las Soluciones Técnicas de Resiliencia en la Producción - Disponer de documentación de activos completa y exhaustiva para satisfacer las necesidades de recuperación del software demostrada en general en apoyo de los planes de continuidad del servicio para los servicios que soporta el sistema.	
Continuidad de Servicio (SC)	SG2 Identificar y priorizar servicios de alto valor SG2.SP1 Identificar los servicios de alto valor para la organización - Identificar los servicios de la organización de alto valor, los activos y actividades asociadas para facilitar el acoplamiento de los activos para el soporte del software.	

Código	**P02**	
Pregunta	¿Qué beneficio cree usted que brinda el plan de continuidad al gestionar riesgos del sistema de información?	
Característica	Integridad	
Técnica	JAD	
Área	CERT-RMM: ➢ Continuidad del Servicio: Identificar y priorizar servicios de alto valor, desarrollar planes de continuidad del servicio. ➢ Gestión de Riesgos: Analizar el riesgo.	
Respuesta		Guarda y protege los resultados de los planes de continuidad de servicio en un almacén de datos.
	X	**Permite asegurar el acceso al sistema de información y proporciona un lugar centralizado para archivar planes y controla las versiones.**
		Identifica las necesidades de formación especializada para las actividades que se describe en el plan.
		Los planes de continuidad de negocio se centran en la continuación de la prestación de un servicio en condiciones degradadas.
	X	**Controlar las consecuencias del riesgo realizado y asegurar la integridad de los archivos sensibles del sistema de información**
Observaciones	Conocer las medidas para el aseguramiento de la información tanto para la conservación como para el acceso.	
MEDICIONES		
Gestión de Riesgos (RISK)	SG4 Analizar el riesgo SG4.SP3 Asignar disposición al Riesgo - Asignar una disposición riesgo para cada declaración de riesgos basado en la valoración de riesgos y el establecimiento de prioridades.	
Continuidad del Servicio (SC)	SG3 Desarrollar planes de continuidad del servicio SG3.SP4 Almacenar y asegurar los planes de continuidad del servicio - Establecer un inventario del plan de continuidad del servicio y guardarlo en una base de datos como medida de protección de la información y asegurar que los planes de continuidad de servicio estén debidamente protegidos pero accesibles a la petición de aquellos usuarios que tienen la debida autorización.	

Código	**P03**	
Pregunta	¿Incluye planes de continuidad de servicios para controlar los cambios que se incrementan de acuerdo a los protocolos y las normas de control de versiones del software?	
Característica	Escalabilidad	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Gestión de Control: Establecer objetivos de control, establecer controles, analizar controles y evaluar la efectividad de controles. ➢ Continuidad del Servicio: Mantener planes de continuidad del servicio.	
Respuesta	**X**	**Verdadero**
		Falso
Observaciones	Conocer si los cambios en el software se realizan en base a los criterios de cambio establecidos en los planes.	
MEDICIONES		
Gestión de Control (CRTL)	CRTL: SG4 Evaluar la efectividad de controles CRTL: SG4.SP1 Evaluar la efectividad de controles - Identificar cambios en los controles existentes y los nuevos controles propuestos para abordar las áreas problemáticas que podrían ocasionar problemas al incrementar nuevas funcionalidades en el sistema.	
Continuidad del Servicio (SC)	SG7 Mantener planes de continuidad del servicio SG7.SP2 Mantener los cambios a los planes - Incrementar versiones en los planes de continuidad de servicio en el inventario o plan de base de dato y comunicar los planes actualizados a los interesados conforme a lo prescrito, de modo que el sistema pueda ser escalable.	

Código	**P04**	
Pregunta	¿Cuáles son los factores que considera importantes en la elaboración de criterios para la selección de una entidad externa en apoyo a la operatividad del sistema de información?	
Característica	Interdependencia e Interconexión	
Técnica	Brainstorming	
Área	CERT-RMM: ➢ Gestión de Dependencias Externas: Establecer relaciones formales ➢ Continuidad del Servicio: Identificar y priorizar servicios de alto valor.	
	X	**La naturaleza del activo a medida en que el software o información sea compatible con un servicio de alto valor o sea un elemento esencial que llevará a cabo el servicio.**
		La capacidad de la entidad externa para participar en la supervisión, pruebas y actividades de verificación en el sistema de información.
		Si la entidad externa es capaz de proporcionar sus servicios durante períodos de uso concurrente.
	X	**Niveles de soporte en el cual dependen los servicios con el fin de desarrollar planes eficaces e integrales de continuidad del servicio.**
Observaciones	Conocer los criterios que deben incluir las medidas de la entidad externa candidata para cumplir con las especificaciones establecidas en la resiliencia del software.	
MEDICIONES		
Continuidad del Servicio (SC)	SG2 Identificar y priorizar servicios de alto valor SG2.SP2 Identificar dependencias e interdependencias internas y externas - Identificar y documentar los servicios de las entidades externas que depende la organización y desarrollar una lista de contactos clave que podrían interconectarse con los sistemas de información a fin de lograr un sistema seguro y sostenible.	
Gestión de Dependencias Externas (EXD)	SG3 Establecer relaciones formales SG3.SP3 Evaluar y seleccionar entidades externas - Establecer criterios de selección de entidades externas en función de sus capacidades para cumplir con las especificaciones de resiliencia y de acuerdo con los criterios de selección establecidos en el sistema.	

2.4. Beneficios de la guía

Los beneficios que brinda el implantar la guía en un sistema de información son los siguientes:

- Evalúa el nivel de resiliencia en los SI.
- Incentiva a las organizaciones a incluir características de resiliencia en sus sistemas de información.
- Propone estrategias de seguridad y continuidad que pueden implementarse desde las fases iniciales del ciclo de vida del software.
- Permite evaluar SI para conocer si mantienen un estado resiliente o no resiliente.
- Brinda recomendaciones en base a la resiliencia de software para el mejoramiento de su sistema de información.

2.5. Aplicaciones de la guía

Esta guía metodológica es aplicable si se dirige a los interesados en conocer el estado actual de los SI y además si la organización está dispuesta adoptar prácticas de mejoras en base a resiliencia, esto en cuanto a la seguridad del software durante su ciclo de vida, así como en la continuidad de los servicios en la organización.

CAPITLO III: IMPLEMENTACIÓN DE LA GUÍA A TRAVÉS DE UN SISTEMA DE INFORMACIÓN

3.1. Tipo de aplicación

Estamos inmersos en la sociedad de la información que trae consigo herramientas potentes como la web 2.0 que marcó el inicio de la red de comunicaciones a través del Internet y actualmente en su nueva versión 3.0 donde se puede recalcar el uso de Data Web e Inteligencia Artificial en el gestionamiento de la interacción del usuario y las funcionalidades de cada plataforma. Es así, que las interfaces web se están convirtiendo en elementos clave de las aplicaciones para facilitar la comunicación entre proveedores, socios, compradores, etc., todos estos acontecimientos marcan una notable evolución en cuanto a la tecnología de la información. Por tales razones, se considera conveniente desarrollar una aplicación web como herramienta de apoyo al proceso de elicitación, en el cual se enfoca la presente guía metodológica.

3.2. Metodología RUP

Buscando una metodología ordenada que contribuya en el desarrollo eficiente y eficaz del SI, se toma la metodología RUP[15] ya que ofrece mejores garantías de funcionamiento al orientarse especialmente hacia el desarrollo de casos de uso, gestión de riesgos, diseño de una arquitectura consistente y un proceso de retroalimentación.

Dentro de la metodología se cree conveniente la gestión tanto del proyecto en general como del producto que es el software que se desarrollará.

3.2.1. Gestión del proyecto.

Para lograr un proyecto de software provechoso se debe mantener una idea clara del trabajo a realizar, los riesgos a enfrentar, recursos necesarios, las tareas-actividades a llevar a cabo, el esfuerzo en tiempos y costos a consumir y el plan a seguir.

Entregables: forman

- Estructura de Desglose de Trabajo (WBS[16]) (Anexo B)
- Cronograma (Anexo C)

[15] RUP: Rational Unified Process, es un marco de desarrollo que indica una forma de enfocar un proyecto de desarrollo del software.

[16] WBS: Work Breakdown Structure, es una herramienta que se utiliza para desglosar los componentes de trabajo que constituyen el objetivo de un proyecto.

3.2.2. Gestión del producto/software.

3.2.2.1. ETAPA 1: Iniciación.

Define el ámbito y objetivos del proyecto, establece alcance, riesgos, arquitectura y termina con el plan de iteraciones.

Lo que se pretende realizar en esta etapa toma las siguientes fases:

1. *Modelado de Negocio.*

   Consiste en una descripción del problema a solucionar, se describirá los procesos existentes u observados generalmente con la captura de requisitos, con el fin de comprenderlos y establecer reglas que sirvan como delimitantes.

2. *Captura de Requisitos.*

   Se extrae los requisitos del cliente, separando los funcionales de los no funcionales.

Entregables:

- Documento de Visión, documenta los requisitos básicos del proyecto, las funciones y limitaciones principales. (Anexo D)
- Especificación de Requisitos, describe las necesidades del proyecto. (Anexo E)
- Modelo de Caso de Uso, identifica las actividades y los actores que intervienen para llevar a cabo un proceso. (Anexo F)
- Especificación de Casos de Uso. (Anexo G)

3.2.2.2. ETAPA 2: Elaboración.

Se determina la línea base lo cual garantiza que la arquitectura, requisitos y planes son los suficientemente estables, y así se pueda hacer frente (mitigar) los riesgos de gran importancia arquitectónica del proyecto.

Las fases que se utilizarán de esta etapa son:

1. *Análisis.*

   Detalla el flujo del trabajo realizando los casos de uso, incluyendo la identificación de clases, atributos y relaciones.

2. *Diseño.*

   Transforma los requisitos al diseño del sistema, se desarrolla la arquitectura, y adapta el diseño para conseguir consistencia en el entorno de implementación.

Entregables:

- Diagrama de Clases. (Anexo H)
- Diagrama de Secuencia. (Anexo I)
- Diagrama de Actividades. (Anexo J)

3.2.2.3. ETAPA 3: Construcción.

Completa la funcionalidad del sistema con la elaboración de un producto totalmente operativo y en la elaboración del manual de usuario.

Las fases que se utilizarán de esta etapa son:

1. *Implementación.*

Se desarrolla el sistema, implementando las clases y objetos, se reportará errores en caso de encontrarlos en el diseño. El resultado final es un sistema ejecutable.

2. *Pruebas.*

Se evalúa la calidad del producto que incluye las funciones del mismo, verificando que los requisitos hayan sido implementados exitosamente y documenta los defectos encontrados.

Entregables:

- Ejecutable, se construye el sistema y se lo deja listo para comenzar las pruebas.
- Reporte de pruebas.

3.2.2.4. ETAPA 4: Transición.

Esta etapa asegura que el software esté disponible para los usuarios finales, se ajusta errores y defectos encontrados en las pruebas de aceptación, se capacita a los usuarios y provee el soporte técnico necesario. En sí, se verifica que el producto cumpla con las especificaciones entregadas por las personas involucradas en el proyecto.

Las fases que se utilizarán de esta etapa son:

1. *Despliegue.*

Se evalúa e instala el software, además de brindar asistencia y ayuda a los usuarios.

Entregables:

- Manual de Usuario, se completa el material iniciado en la fase construcción, ya que ayudan al usuario final en el aprendizaje, uso, operación y mantenimiento del producto, de acuerdo con los requisitos planteados en la fase de iniciación. (ANEXO K)

3.3. Herramientas para el desarrollo del SI

Lenguaje de programación.

El lenguaje de programación que se utiliza es Procesador de Hipertexto (PHP) ya que está diseñado para el desarrollo web generalmente dinámico, multiplataforma y soportado por la mayoría de servidores web.

Base de Datos.

Se utiliza MySQL como base de datos relacional por su facilidad de gestionamiento y su enfoque en el desarrollo web por lo cual está muy ligada a PHP que es el lenguaje de programación definido para la codificación del sistema de información.

3.4. Prototipo del SI

3.4.1. Interfaz del SI.

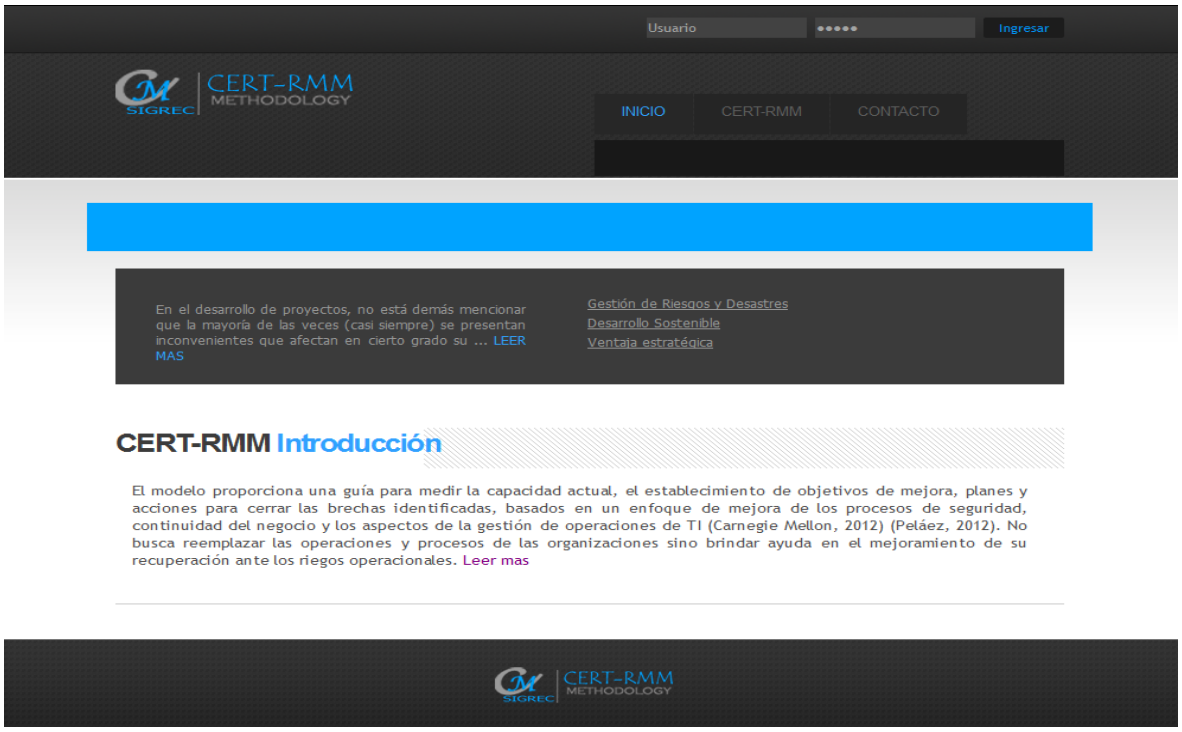


Figura 6. Interfaz del SISGRES.
Fuente: El autor.

En la portada del SI se encuentra la sección del autenticación y un menú navegable que presenta información acerca de resiliencia, la metodología CERT-RMM y datos de contacto como se muestra en la figura 6. De esta manera, los usuarios podrán informarse mejor acerca de esta metodología.

3.4.2. Funcionalidades.

En vista del objetivo de este trabajo el SI, se gestiona dos tipos de usuarios que son un administrador (Ver figura 7 y 10) y un cliente (Ver figura 17), en base a los cuales se deberá realizar las siguientes funcionalidades:

3.4.3. Administrador.

Gestionar usuarios.

Figura 7. Interfaz principal de gestión de usuarios.
Fuente: El autor.

Se presenta una lista con todos los usuarios registrados en el SI y además muestra opciones para actualizar (Ver figura9) su información, eliminar e incluso registrar usuarios nuevos (Ver figura 8).

<u>Registrar usuario</u>

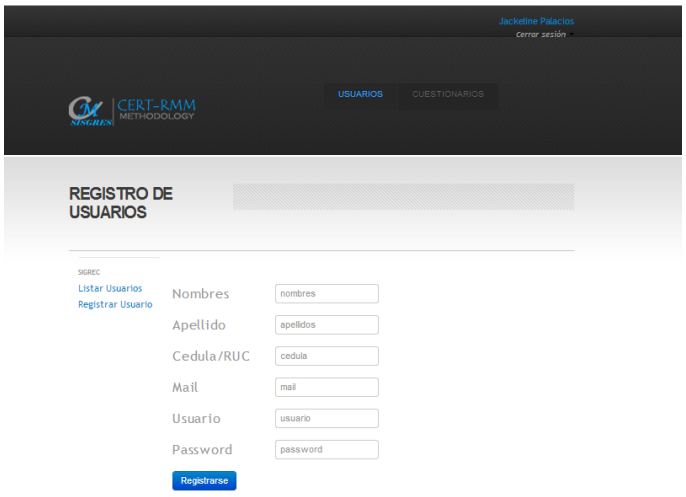


Figura 8. Formulario para registrar usuarios.
Fuente: El autor.

Actualizar usuario

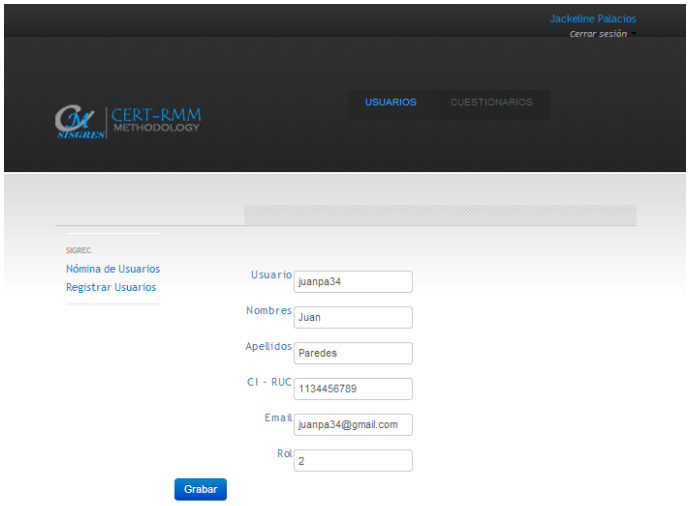


Figura 9. Formulario de actualización de datos del usuario.
Fuente: El autor.

Gestionar cuestionarios

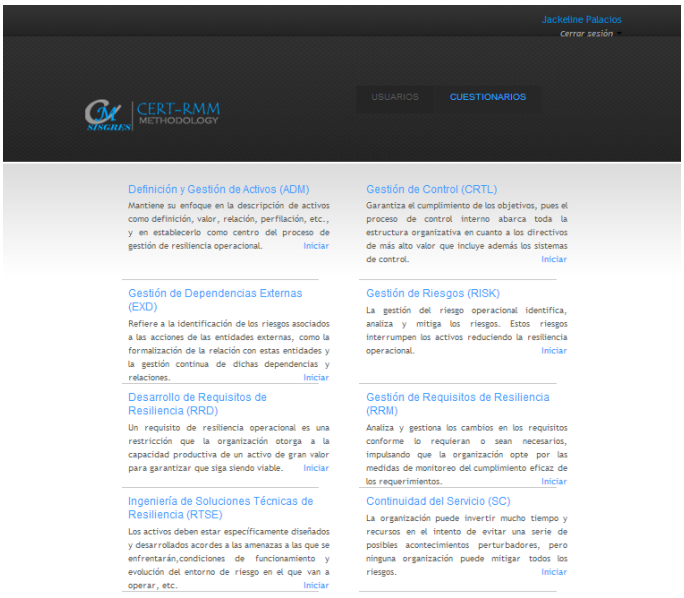


Figura 10. Áreas de la Metodología CERT-RMM.
Fuente: El autor.

Se presenta en la figura 10 una lista con las 9 áreas de la Metodología CERT-RMM, cada una con su descripción y una opción denominada <<Iniciar>> para visualizar el cuestionario perteneciente a cada área.

Cuestionarios

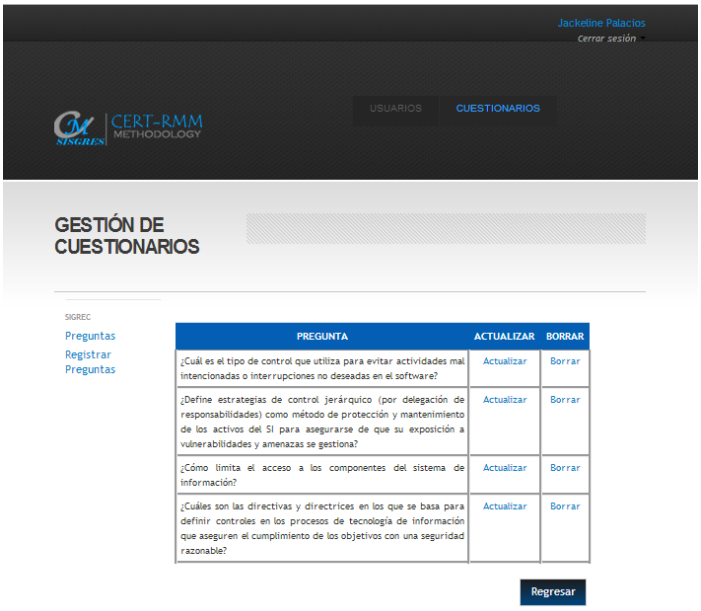


Figura 11. Pantalla principal para la gestión de cuestionarios.
Fuente: El autor.

Al igual que en la gestión de usuarios, se realiza las operaciones básicas de actualización (Ver figura 13), eliminación y registro de preguntas (Ver figura 12).

Registrar preguntas

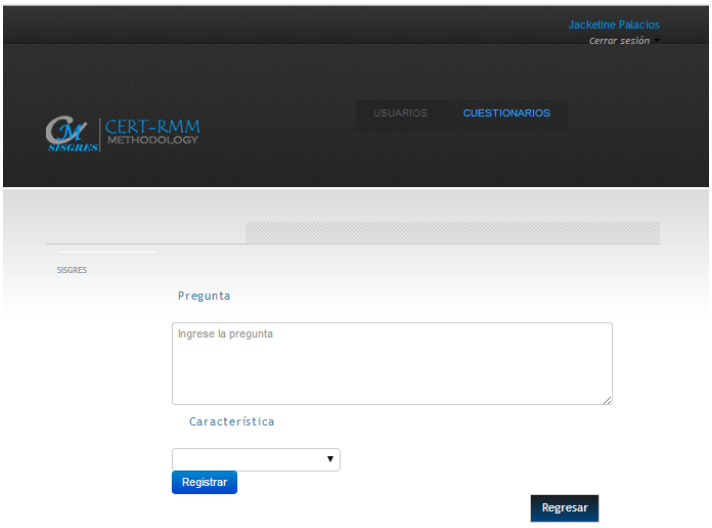


Figura 12. Formulario para el registro de preguntas nuevas.
Fuente: El autor.

Actualizar preguntas

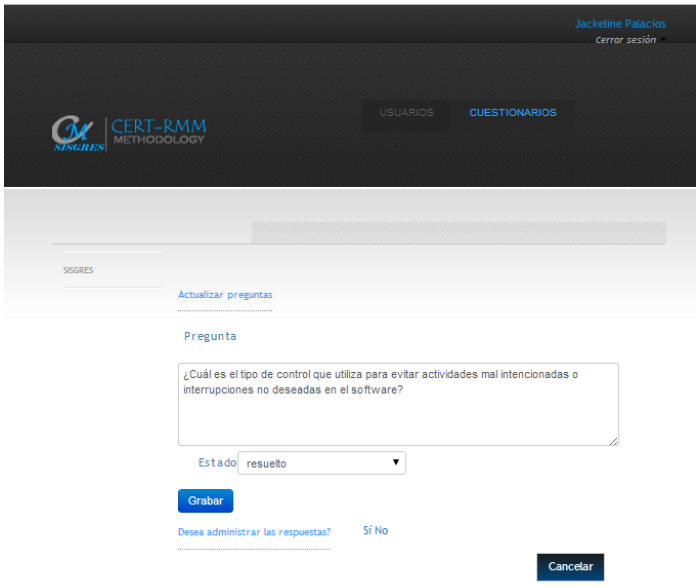


Figura 13. Formulario de actualización de información de preguntas.
Fuente: El autor.

Se puede actualizar el contenido y estado de la pregunta, así como las respuestas asociadas (Ver figura14).

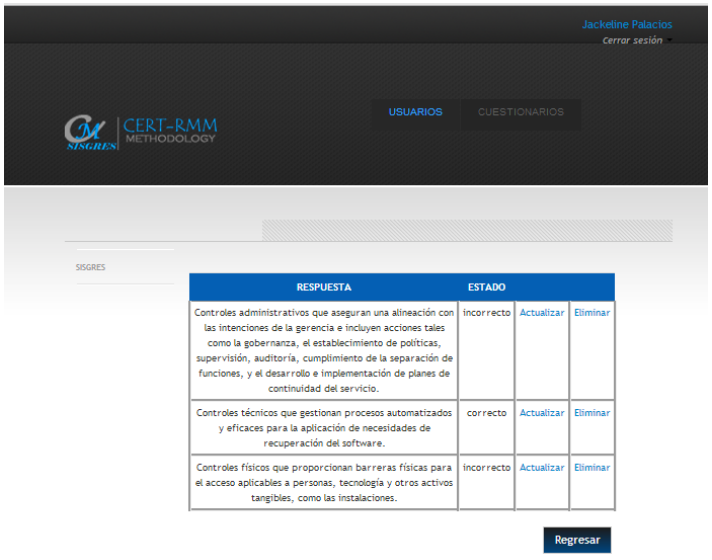


Figura 14. Lista de respuestas de la pregunta seleccionada.
Fuente: El autor.

Con las respuestas también se pueden realizar las operaciones básicas (actualizar (Ver figura 16), borrar, registrar (Ver figura 15)), como se muestra a continuación:

Registrar respuesta

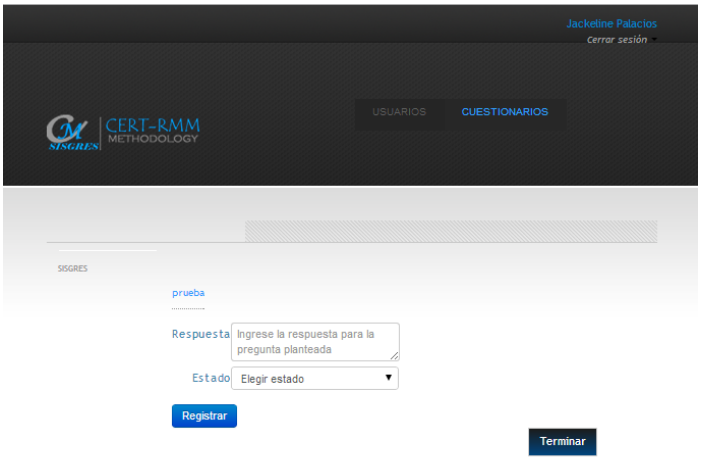


Figura 15. Formulario para el registro de respuestas.
Fuente: El autor.

Actualizar respuesta

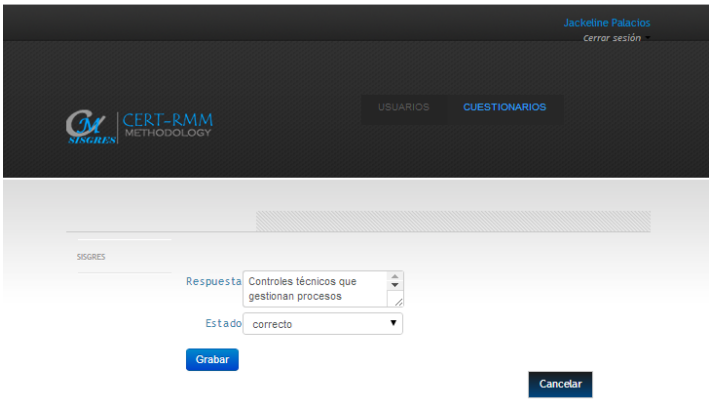


Figura 16 Formulario para la actualización de respuestas.
Fuente: El autor.

Las operaciones que se muestra en las figuras son las operaciones que puede realizar el usuario registrado como administrador.

3.4.4. Cliente.

Empieza con un mensaje de confirmación según se puede observar en la figura 13 donde se explica que encontrará el usuario al aceptar el mensaje y lo que conseguirá al finalizar la evaluación.

Figura 17. Mensaje de bienvenida.
Fuente: El autor.

Al aceptar el mensaje de confirmación se presenta un menú con las áreas del CERT-RMM involucradas con la resiliencia del software, como se muestra en la figura 18.

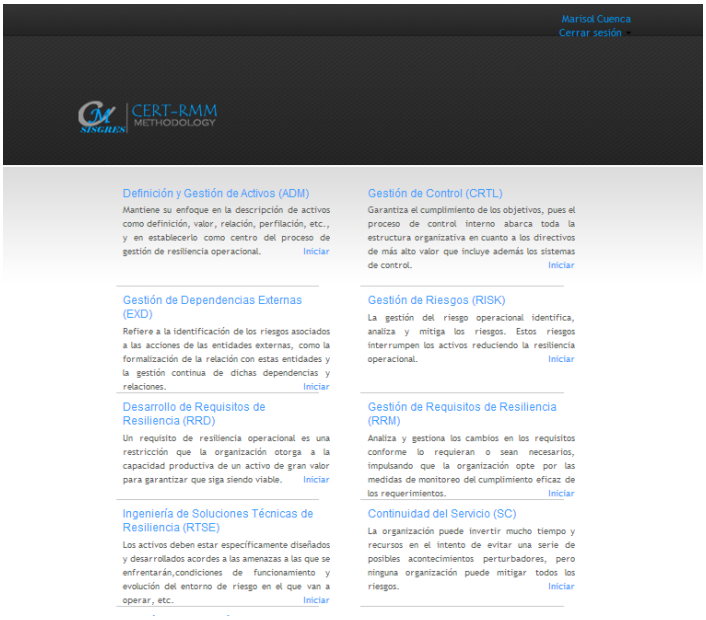


Figura 18. Guía de las áreas de la metodología CERT-RMM.
Fuente: El autor.

Y dentro de cada opción (área) se muestran las preguntas desarrolladas para obtener requisitos de resiliencia (Ver figura 19).

Figura 19. Preguntas y respuestas del área de CTRL.
Fuente: El autor.

Al terminar de responder las preguntas de todas las opciones (áreas) se procede con el siguiente paso (Ver figura 20) que son los resultados, donde se presenta el número de aciertos y fallas en las preguntas para cumplir con las características del software resiliente.

Caracteristica	P. Correctas	P. Incorrectas	Sugerencias
Modularidad	1	1	Revisar...
Independencia	0	1	Revisar...
Disponibilidad	2	3	Revisar...
Flexibilidad	0	1	Revisar...
Redundancia	1	3	Revisar...
Seguridad	2	0	Revisar...
Confidencialidad	1	2	Revisar...
Operatividad	0	2	Revisar...
Continuidad	1	3	Revisar...
Complejidad	1	2	Revisar...
Mantenibilidad	2	2	Revisar...
Interdependencia e Interconexión	0	0	Revisar...
Conmutación	1	0	Revisar...
Eficiencia	0	0	Revisar...
Interoperabilidad	0	1	Revisar...
Manejabilidad	0	0	Revisar...
Rendimiento	0	0	Revisar...

Figura 20. Aciertos y errores por cada característica del software resiliente.
Fuente: El autor.

Por cada una de las características se presenta sugerencias claves para que puedan mejorar o alcanzar la resiliencia en su SI (Ver figura 21).

Figura 21. Lineamientos sugeridos en base a la metodología CERT-RMM para mejorar la característica de modularidad.
Fuente: El autor.

Además se puede obtener un reporte con los resultados de la evaluación según se muestra en la figura 22, un informe general en base a las áreas de la Metodología CERT-RMM presentado en la figura 23. Cabe mencionar que se cuenta con opción para visualizar el reporte en versión pdf.

Reporte.

Definición y Gestión de Activos

Pregunta	Lineamiento Sugerido	Lineamiento Marcado	Resultado
¿Cuál es la estrategia que utiliza para que su SI continúe funcionando normalmente cuando una o varias de sus procesos fallan durante su ejecución?	Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.	Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.	correcto
¿Qué acción realiza cuando detecta que la base de datos de su sistema de información ha sido alterada?	Cargar en el sistema el último backup hasta determinar la gravedad de los cambios.	Cargar en el sistema el último backup hasta determinar la gravedad de los cambios.	correcto
¿Cómo controla los cambios en los procesos del sistema de información sin causar interrupción en el cumplimiento de los objetivos de la organización?	Mantener independencia entre los procesos de cada componente del sistema de información.	Desarrollar planes de control de cambios.	incorrecto
¿Cómo determina cuáles son los activos que contribuirán en el desarrollo del sistema de información?	Se realiza un inventario en base a los perfiles de los activos.	Se realiza un inventario en base a los perfiles de los activos.	correcto

Figura 22. Historial del estado de las preguntas resueltas en la evaluación
Fuente: El autor.

Informe General.

Areas	Total	L. Correctas	L. Incorrectas
Definición y Gestión de Activos	4	0	4
Gestión de Control	4	1	3
Gestión de Dependencias Externas	5	5	0
Gestión de Riesgos	4	2	2
Desarrollo de Requerimientos de Resiliencia	5	2	3
Gestión de Requerimientos de Resiliencia	6	3	3
Ingeniería de Soluciones Técnicas de Resiliencia	8	2	6
Continuidad del Servicio	4	2	2
Gestión Tecnológica	4	3	1
Respuestas	44	20	24

NIVEL DE RESILIENCIA: 8.8%

Regresar

Figura 23. Resumen de la evaluación por cada área.
Fuente: El autor.

3.4.5. Resultados esperados.

Lo que se desea conseguir es un SI que apoye el proceso de elicitación de requisitos de resiliencia de software en base a encuestas desarrolladas con relación a la metodología CERT-RMM y sus áreas que se enfocan en el software resiliente.

3.5. Construcción del SI

El SI se lo realiza en base a una arquitectura cliente-servidor como se presenta en la figura 24.

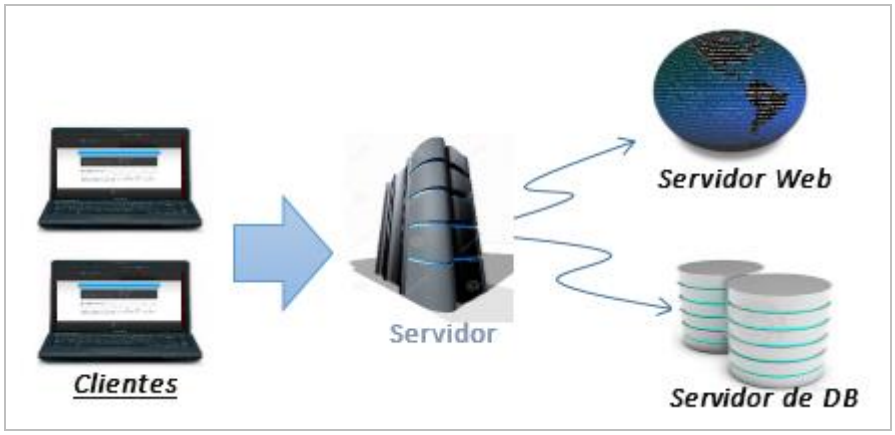


Figura 24. Arquitectura cliente-servidor.
Fuente: El autor.

3.5.1. Control de acceso.

Se realiza un formulario de autenticación con el cual se limita el acceso únicamente a usuarios registrados en el SI sean de tipo administrador o cliente.

3.5.2. Carga de datos.

En la base de datos se almacena toda la información que necesita el SI como es: áreas, preguntas, respuestas, resultados, sugerencias, etc. En la figura 25 se presenta el modelo de base de datos relacional que utiliza el SI.

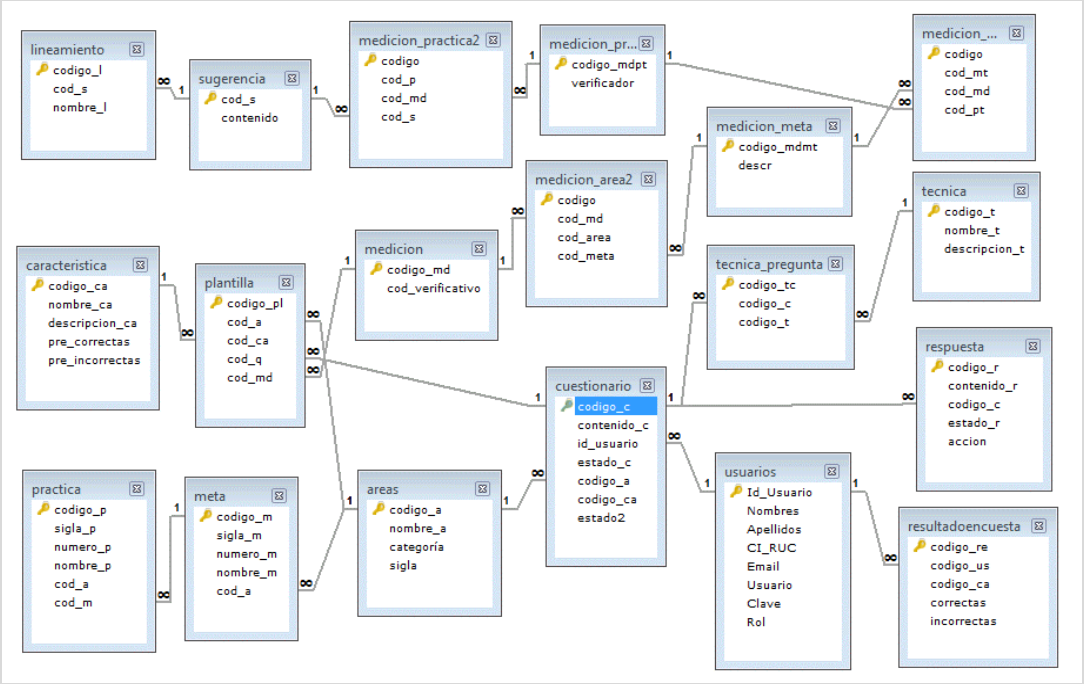


Figura 25. Base de datos del SISGRES.
Fuente: El autor.

3.5.3. Presentar datos.

Se traba con sentencias Sql para extraer la información de la base de datos y presentarla en la interfaz de usuario. Esta acción se aplica para presentar lista de usuarios, áreas, preguntas, respuestas, resultados y sugerencias.

3.5.4. Calcular datos.

En base a la información recogida por el usuario y la información almacenada en la base de datos, se realiza comparaciones para presentar los resultados que abarca las características de resiliencia alojadas en la *tabla característica* y se realiza el cálculo de la cantidad de preguntas correctas e incorrectas según las respuestas del usuario.

3.5.5. Guardar datos.

La información que se recoge con cada sesión de usuario se almacena directamente en la base de datos, que mantiene un historial de las sesiones de los usuarios y el resultado de su evaluación.

3.6. Pruebas del SI

Para comprobar que el SI desarrollado funciona se lo aplica en SI externos y en base a sus respuestas se podrá realizar una comparativa para verificar el funcionamiento eficaz.

CAPITULO IV: VERIFICACIÓN DE LA APLICABILIDAD DE LA GUÍA METODOLÓGICA

4.1. Parte I: Estadística descriptiva para la totalidad de sistemas encuestados

El trabajo se lo aplicó en organizaciones adyacentes a la UTPL, así como también en organizaciones externas como Funeraria Jaramillo y Electrictelecom, en las cuales se determinó que la mayoría ha desarrollado y desarrolla SI transaccionales, mientras que en la otra parte corresponde al desarrollo de sistemas estratégicos y de apoyo a la toma de decisiones, como se muestra en la figura 26.

Cabe mencionar que se tomó en cuenta personas que desarrollaron alguna alternativa de software o que actualmente están desarrollando una, ya sea enfocado en el ámbito financiero o administrativo, no se hizo distinción alguna con respecto a la profesión, puesto en el que trabaja, edad o sexo.

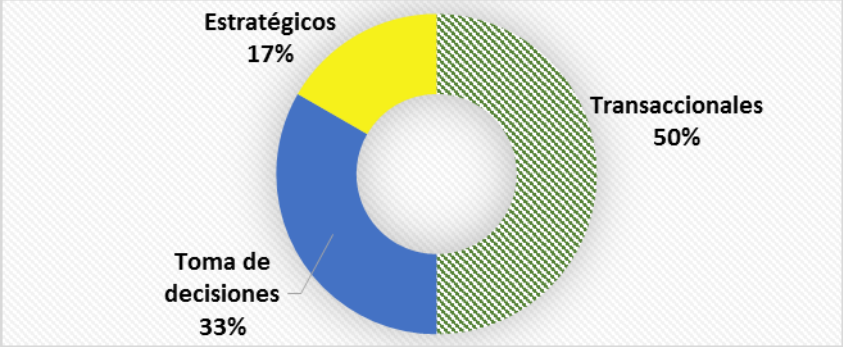


Figura 26. Tipos de Sistemas de Información.
Fuente: El autor.

Tomando en cuenta las características propias de los sistemas seleccionados para responder la encuesta, en la figura 27 se muestra que son cuatro niveles de experiencia por los que se caracterizan los encuestados, denotando que la mayoría posee un alto nivel de experiencia en el desarrollo de sistemas y en cuanto al nivel medio son pocos los desarrolladores que poseen dicha característica.

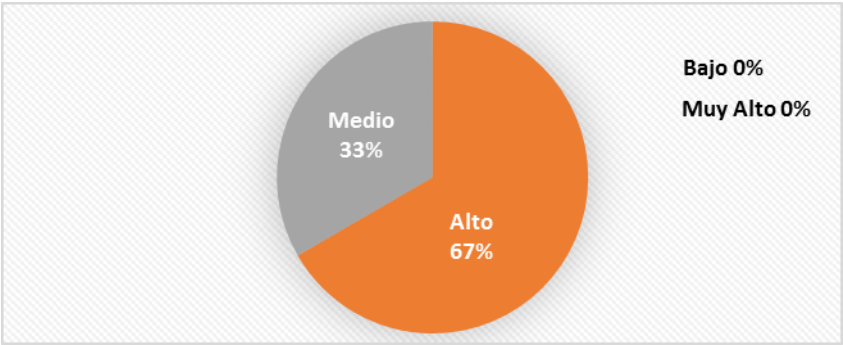


Figura 27. Nivel de experiencia de las personas encuestadas.
Fuente: El autor.

(Caralli, Allen, & White, 2010) mencionan que el triunfo de la misión de una organización se basa en el éxito de cada servicio en el logro de su misión. A su vez, la garantía de la misión de los servicios depende de algunas características que deben cumplirse. Es así que se evalúa la resiliencia de software por cada área de la Metología CERT-RMM.

Iniciamos con el área de Definición y Gestión de Activos. Se decidió indagar sobre la estrategia que se utiliza para que el SI continúe funcionando normalmente cuando una o varias de sus procesos fallan durante su ejecución, dentro de las respuestas obtenidas la figura 28 muestra que segmentar el software en módulos es la estrategia que la mayoría de encuestado utiliza en el desarrollo de los sistemas de información para conservar el funcionamiento normal de sus procesos.

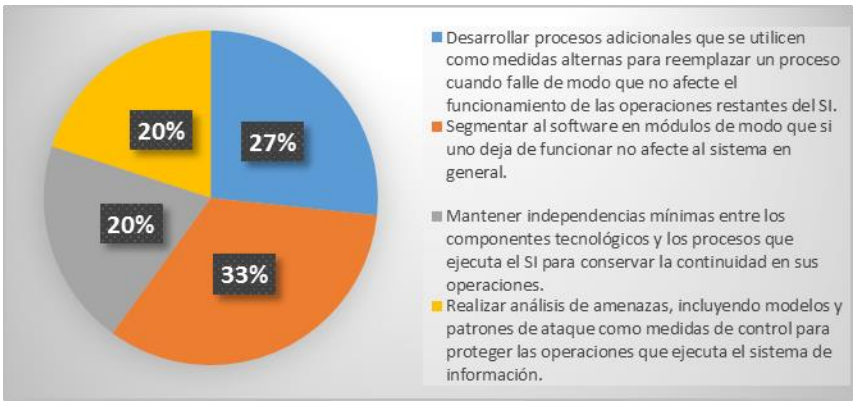


Figura 28. Estrategias para proteger el funcionamiento normal del SI.
Fuente: El autor.

La figura 29 muestra las acciones que realizan cuando se detecta alteraciones en la base de datos del SI siendo el historial de cambios la estrategia que mayormente se utiliza para el control de cambios.

Figura 29. Acciones para gestionar cambios no autorizados en la base de datos.
Fuente: El autor.

La figura 30 denota que las herramientas para el control de versiones es la estrategia que la mayoría se utiliza para controlar los cambios en los procesos del SI sin causar interrupción en el cumplimiento de los objetivos de la organización.

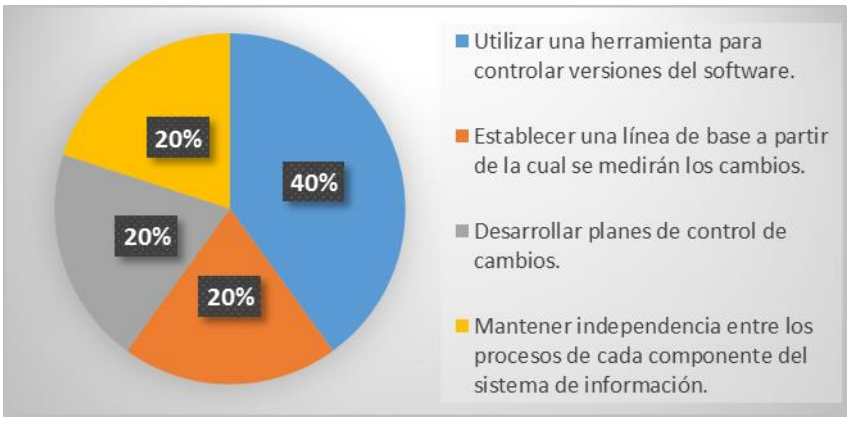


Figura 30. Estrategias de control de cambios en el SI.
Fuente: El autor.

La figura 31 muestra cómo se determina los activos que contribuirán en el desarrollo del sistema de información donde el 38% afirma que primero se evalúa la estructura y orientación de los componentes del sistema de información antes de identificar los servicios, definir el tamaño e incluso realizar el inventario de activos

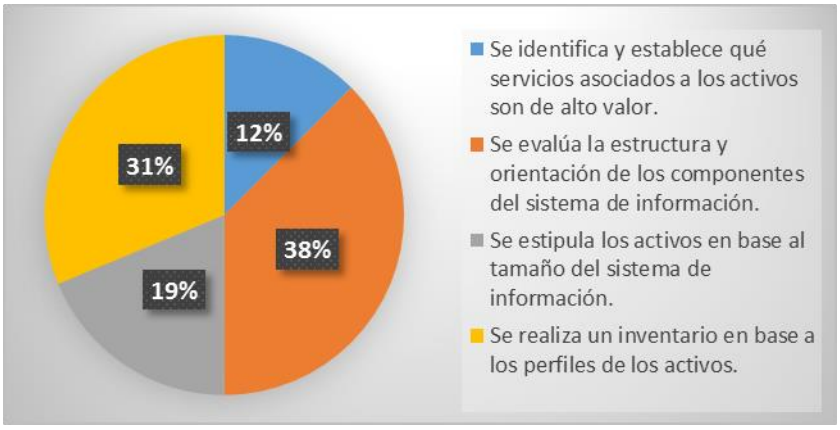


Figura 31. Definición de activos en el SI.
Fuente: El autor.

El proceso de control generalmente se refleja en el sistema de control interno por ello se aborda el área de Gestión de Control, iniciando con el tipo de control que se utiliza para evitar actividades o interrupciones no deseadas en el software. En base al estudio realizado se menciona que los controles administrativos rara vez son utilizados de acuerdo a los resultados de la figura 32, donde sobresale los controles físicos que

protegen el acceso al SI, aplicables a personas, tecnología y otros activos tangibles, como instalaciones.

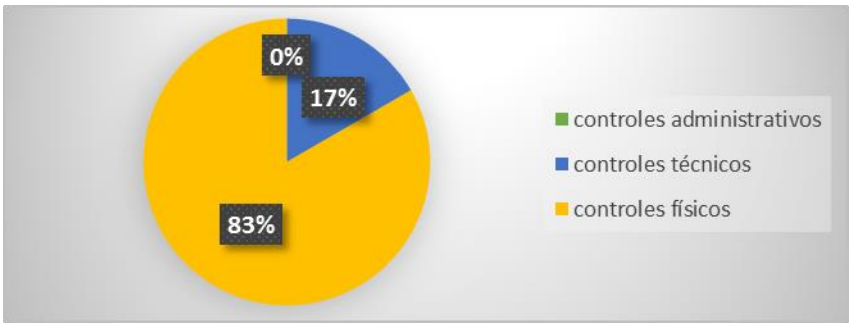


Figura 32. Tipos de controles en el SI.
Fuente: El autor.

Para proteger el SI según la figura 33 solamente el 33% utiliza una buena estrategia de protección ya que si adoptan la estrategia de control jerárquico.

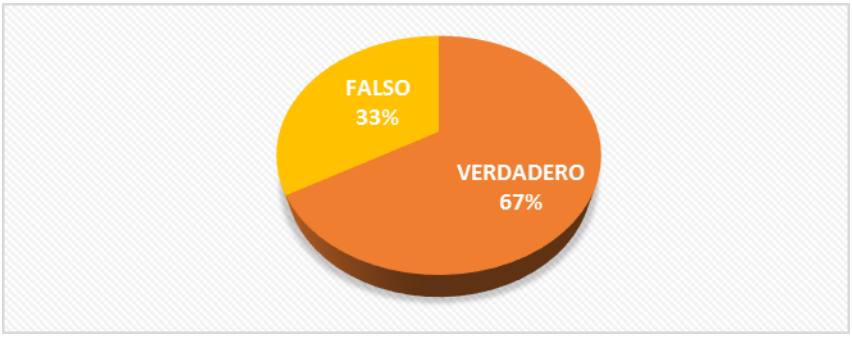


Figura 33. Nivel de control jerárquico.
Fuente: El autor.

La figura 34 muestra las estrategias para limitar el acceso a los componentes del SI, donde los criterios de decisión y autoridad son las estrategias de control que se utilizan para delimitar las funciones que puede ejecutar el usuario en el software.

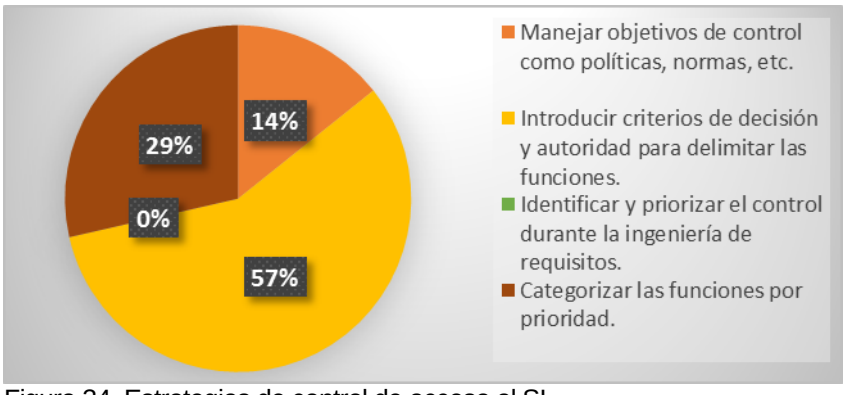


Figura 34. Estrategias de control de acceso al SI.
Fuente: El autor.

En la figura 35 se muestra las directivas y directrices en los que se basan los analistas para definir controles en los procesos de tecnología de información para asegurar el cumplimiento de los objetivos, que incluye políticas, procedimientos y directrices que la organización establece para promover comportamientos aceptables otorgando seguridad y por lo tanto coherencia en los procesos de tecnología de información del sistema.

Figura 35. Directrices de control en procesos de tecnología.
Fuente: El autor.

Se aborda el área de Gestión de Dependencias externas, que evalúa la acción para desarrollar criterios consistentes en la priorización de las dependencias externas y para su aplicabilidad uniforme en todo el sistema de información, en la figura 36 se muestra que la mayoría de las organizaciones desarrolla planes de mitigación para minimizar los riesgos al mantener dependencias, mientras que el 33% no lo hace.

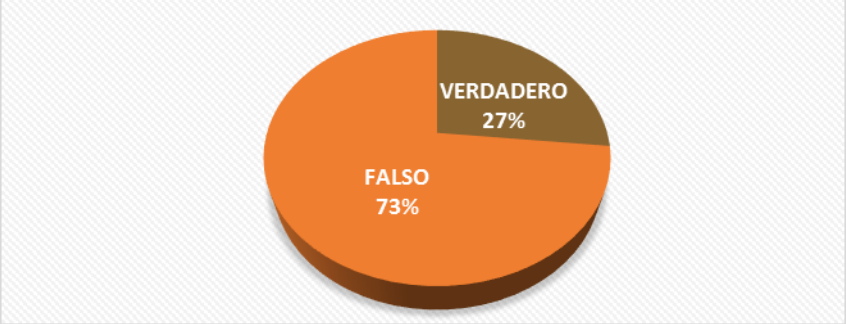


Figura 36. Incidencia de los planes de mitigación de riesgos con dependencias externas.
Fuente: El autor.

Revisar y actualizar con regularidad el establecimiento de prioridades y criterios para asegurarse de que el esquema de prioridades y la lista de dependencias externas priorizadas son apropiados para el entorno de riesgos y tolerancia del software son las acciones que en su mayoría realizan al priorizar las dependencias según lo muestra la figura 37.

Figura 37. Acciones para priorizar dependencias externas.
Fuente: El autor.

La figura 38 denota que el SLAs no se desarrolla al inicio o final de una relación con una entidad externa, sino que lo van adaptando conforme el sistema vaya necesitando asociarse a una dependencia.

Figura 38. Desarrollo de SLAs.
Fuente: El autor.

En la figura 39 se muestra los controles esenciales para la protección y el mantenimiento de las operaciones del sistema cuando se incluye entidades externas, son las normas y directrices las que obtuvieron mayor número de respuestas con el 50% que afirman utilizarla de modo que salvaguardan el software y mantienen continuidad en los procesos del sistema de información al relacionarse con entidades externas.

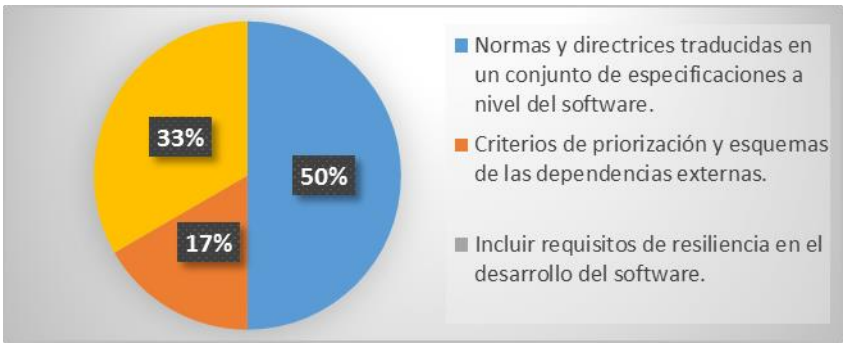


Figura 39. Controles para la protección y el mantenimiento de las operaciones del sistema.
Fuente: El autor.

Establecer requisitos legales, estatutarios, reglamentarios y contractuales que requieren una organización y todas sus entidades externas en relación con los sistemas de información lo realiza el 67% de los encuestados mientras que el 33% no lo realiza ya sea por falta de conocimiento o experiencia en este ámbito (Ver figura 40).

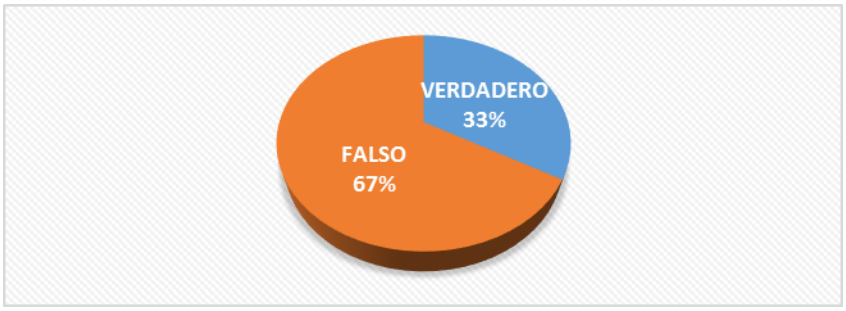


Figura 40. Nivel de administración de requisitos con relaciones externas.
Fuente: El autor.

Se evalúa el área de Definición de Requisitos de Resiliencia, iniciando con el desarrollo de mapas de servicios, acción que la realizan la mayoría de los encuestados para detallar las relaciones entre los servicios, procesos de negocio y activos asociados al software (Ver figura 41).

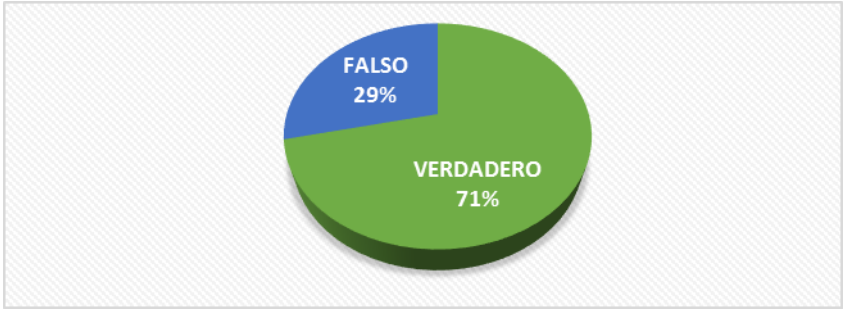


Figura 41. Nivel de desarrollo de mapas de servicios.
Fuente: El autor.

En la figura 42 muestra que la acción que se realiza para asegurar el cumplimiento de la misión de los servicios es identificar requisitos aplicables a cada servicio y activos asociados a la construcción del software según la mayoría de los encuetados, ya que además dependen del desarrollo coherente y eficaz del software, con la intervención de personas, tecnología e información relacionadas.

Figura 42. Actividades de apoyo al cumplimiento de objetivos de los servicios.
Fuente: El autor.

En la figura 43, la mayoría de los encuestados no establecen requisitos de continuidad, sin embargo en un porcentaje menor, aunque bastante notorio, un 40% supo manifestar que si aplican requisitos de continuidad como medidas de apoyo para la ejecución de los procesos del software y el cumplimiento de los servicios organizacionales.

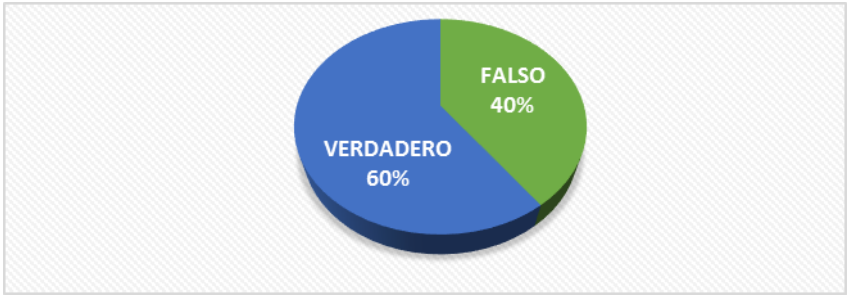


Figura 43. Actividades de dependencia de requisitos y activos.
Fuente: El autor.

En cuanto a la importancia de los requisitos en el cumplimiento de los servicios a los que apoya el software, según muestra la figura 44 se destacan los vínculos entre los requisitos de activos y servicios con el 37% como aquella característica que apoyan a los requisitos ya que es importante conocer la alineación que relaciona todas las actividades fundamentales que reflejen las necesidades de servicio de la organización en el desarrollo del software.

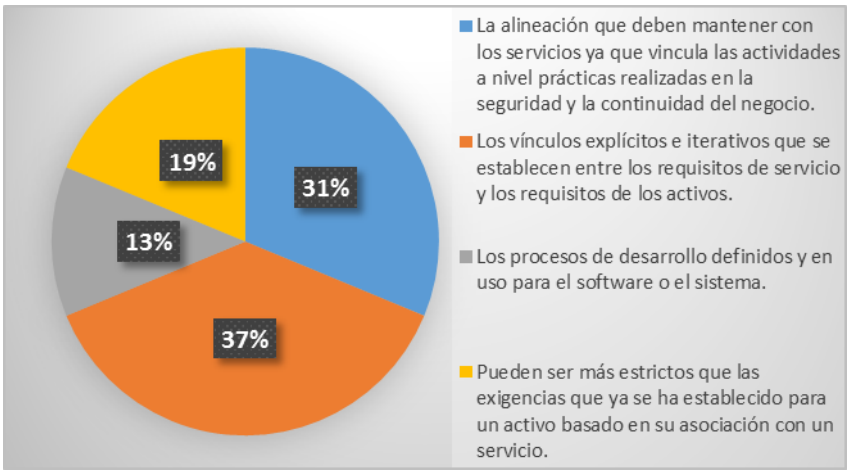


Figura 44. Importancia de los requisitos en los servicios.
Fuente: El autor.

Se evalúa el área de Gestión de Requisitos de Resiliencia. En cuanto a la disponibilidad del servicio que debería ofrecer un SI la mayoría concuerda en un 57% que todo el tiempo debe estar disponible el servicio como apoyo a los sistemas y componentes de tecnología, información y datos, así como las instalaciones en las que estos activos sean accesibles y productivos (Ver figura 45).

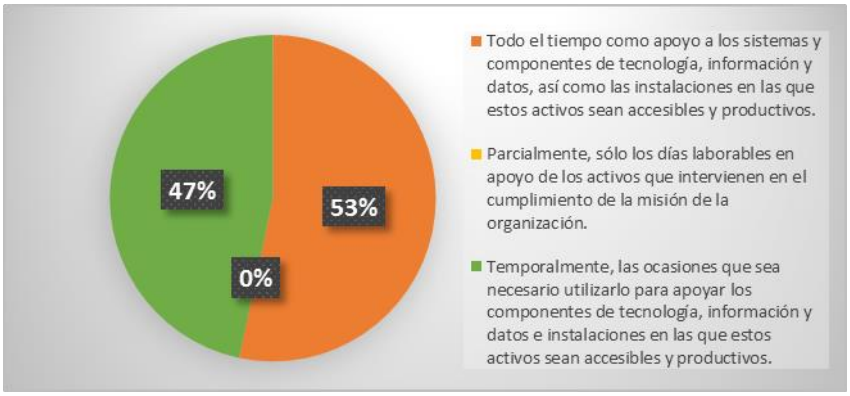


Figura 45. Disponibilidad del servicio.
Fuente: El autor.

En la figura 46 se muestra alternativas que se podría tomar para apoyar el análisis de resultados de las evaluaciones de riesgos al identificar cambios en los requisitos del SI, de las cuales se podría decir que la alternativa que mayor demanda presenta es el desarrollar un registro de modificación de requisitos para el apoyo de dicho análisis.

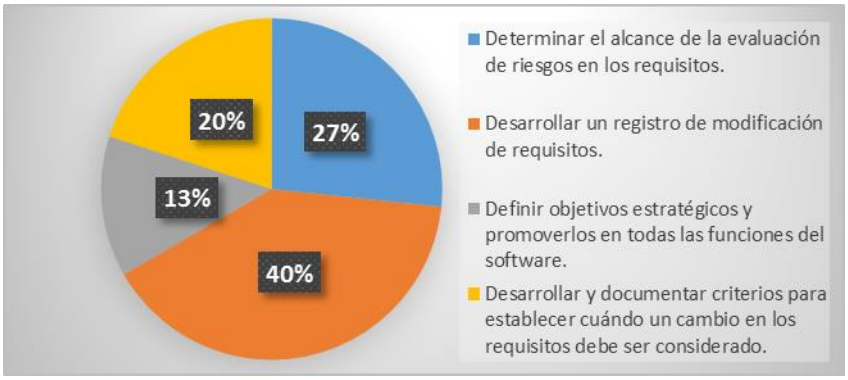


Figura 46. Estrategias de apoyo al análisis de resultados.
Fuente: El autor.

Para monitorear el proceso de gestión del cambio en cuanto a la actualización de los requisitos a nivel de activos, en la figura 47 se muestra que identificar y documentar los cambios en los requisitos existentes es el proceso que mayormente se realiza.

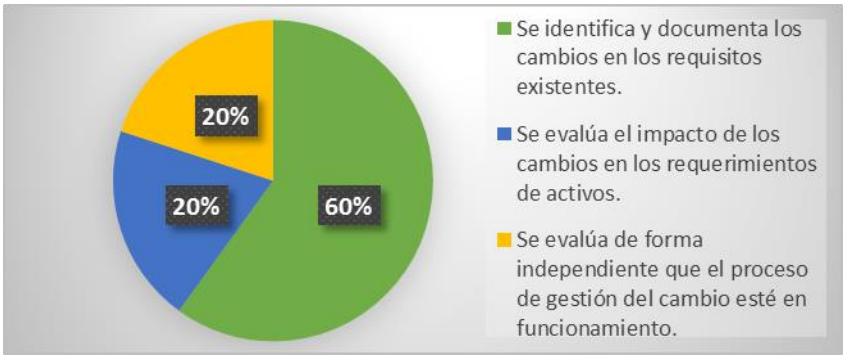


Figura 47. Lineamientos para el monitoreo de la gestión de cambios.
Fuente: El autor.

En la figura 48, con enfoque en el mejoramiento del software el 71% de los encuestados afirman que se requiere la identificación e inclusión de requisitos de seguridad con la cooperación y comprensión mutua entre los propietarios de servicios y activos, y los custodios de los mismos, puesto que es importante conocer si existe una cooperación mutua y compartida de los requisitos que apoyan al software y el cumplimiento de las necesidades de la organización.

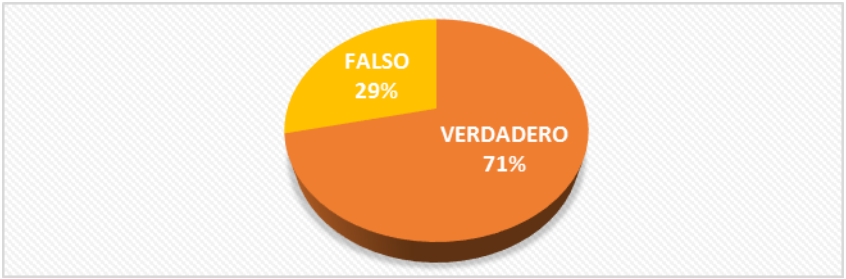


Figura 48. Nivel de inclusión de requisitos de seguridad en el software.
Fuente: El autor.

Para gestionar que los cambios en las necesidades asignadas a custodios durante el desarrollo del software, la mayoría utiliza normas de codificación segura en garantía del cumplimiento de los requisitos y que las vulnerabilidades sean eliminadas como se presenta en la figura 49.

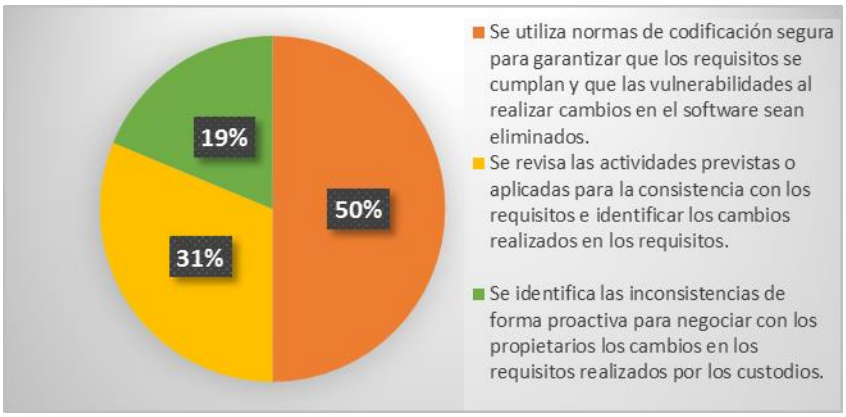


Figura 49. Estrategias de gestión de cambios en las necesidades de custodios de servicios.
Fuente: El autor.

A continuación se aborda el área de Ingeniería de Soluciones Técnicas Resilientes que inicia con el análisis de lineamientos que podrían ser la base o soporte de los criterios de inspección para proporcionar un nivel aceptable de seguridad y confianza en el despliegue del software, es así que según muestra la figura 50 existe cierta discrepancia entre el desarrollar documentación de listas de pruebas y la satisfacción de los requisitos de seguridad presentando en los dos casos un 29% de probabilidad.

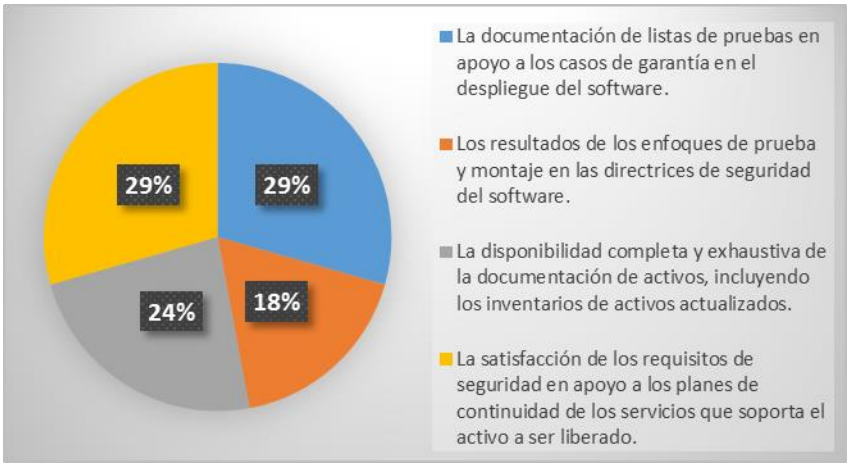


Figura 50. Criterios de seguridad y confianza en el despliegue del software.
Fuente: El autor.

Las directrices de mejora se muestran en la figura 51 donde los criterios de decisión y autoridad constituyen el método que mayormente se utiliza en el desarrollo del plan de gestión del software.

Figura 51. Métodos para reflejar directrices de mejorar de un plan de gestión de software.
Fuente: El autor.

El software según muestra la figura 52, el 57% de los encuestados afirma que se debe someter a una inspección formal con criterios documentados para asegurar que han cumplido con las directrices de mejora antes de ser liberados en un entorno de producción, mientras que el 43% restante no está de acuerdo con esta afirmación.

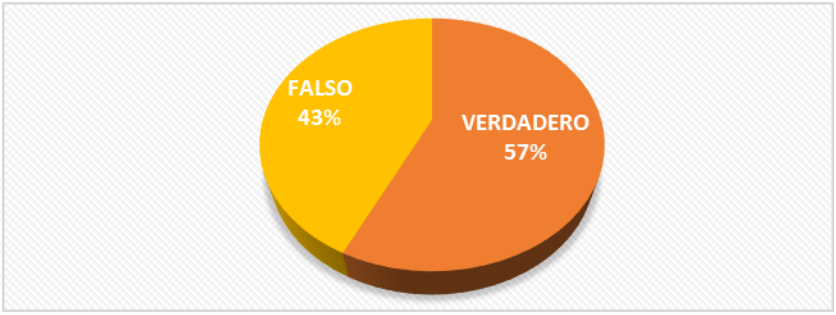


Figura 52. Nivel de inspección formal a la que debe someterse el software.
Fuente: El autor.

Las directrices de codificación para superar situaciones de estrés se muestran en la figura 53 resaltando que el 38% ha manifestado que en su software realizan la evaluación de la superficie de ataque de los riesgos para superar dichas situaciones mientras que la inclusión de normas y herramientas de codificación segura que podrían ayudar mejor en la protección del software presenta un 31%.

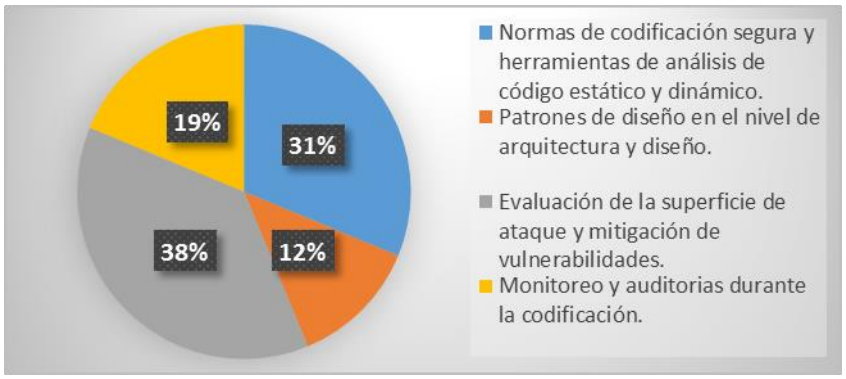


Figura 53. Directrices de codificación para superar situaciones de estrés.
Fuente: El autor.

En la figura 54 se muestra las opciones para definir la arquitectura y diseño del software, donde la opción más utilizan es una arquitectura flexible que asegure que los servicios estén en funcionamiento en momentos de estrés, aunque también se usa temas de interconexión, interoperabilidad, continuidad del servicio, priorización, pero la flexibilidad apoya mejor la resiliencia en el software.

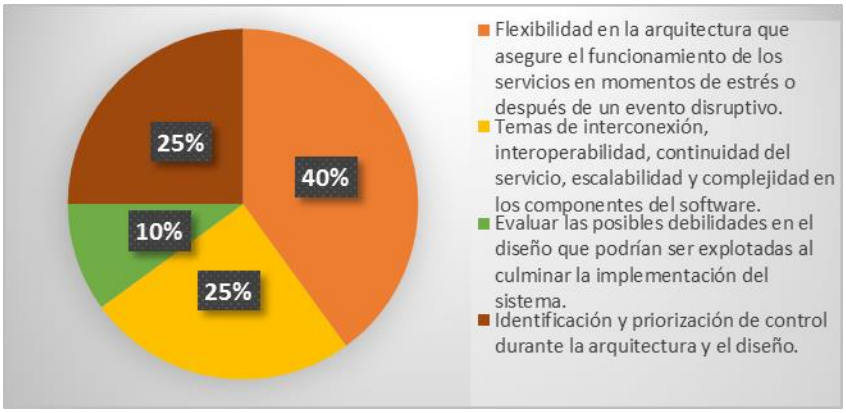


Figura 54. Definiciones de arquitectura y diseño del software.
Fuente: El autor.

En la figura 55, se puede observar que es el 62% de los encuestados quienes están de acuerdo que el incrementar medidas de seguridad en el desarrollo de software en lugar de capacitar al personal si contrarresta el error humano y disminuye las posibilidades de riesgo en el software, mientras que el 38% no concuerda con esta afirmación.

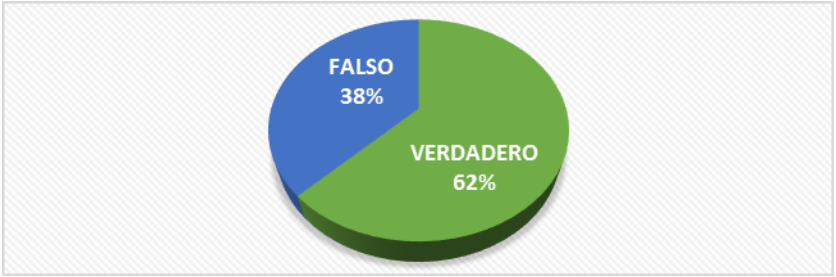


Figura 55. Niveles de medidas de seguridad en el desarrollo de software.
Fuente: El autor.

En cuanto al área de Gestión de Riesgos esta inicia con la identificación y priorización de servicios y según los indicadores de la figura 56 no existe gran apoyo ya que el 63% de los encuestados no están de acuerdo que sea de vital importancia para identificar los riesgos y que deban gestionarse con la ayuda del planteamiento de requisitos para mejorar el software.

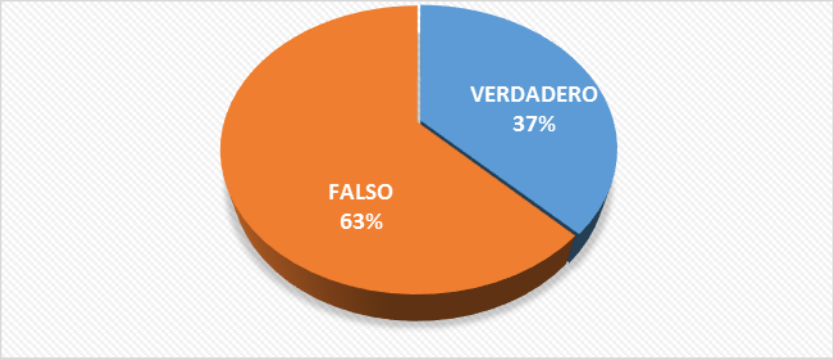


Figura 56. Niveles de identificación y priorización del servicio.
Fuente: El autor.

En la figura 57 se denota que es el plan de mitigación de riesgos el que mayor uso tiene con un 43% dejando de lado el plan de comunicaciones y la gestión de tiempos mínimos para controlar el equilibrio en la comunicación de los procesos cuando se presenten riesgos.

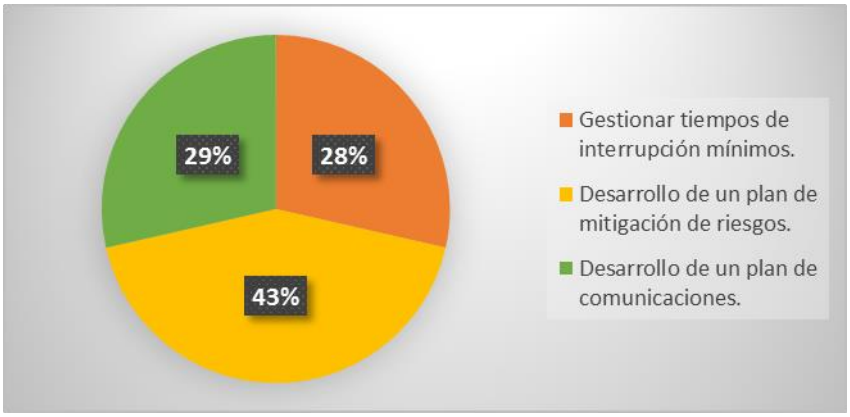


Figura 57. Estrategias de control del equilibrio en la comunicación.
Fuente: El autor.

Las consideraciones de gestión de riesgo pueden ayudar a mejorar y mantener estable el control interno del sistema, en la figura 58 muestra que no se compara los planes de mitigación de riesgos sino que se revisa los controles existentes en los componentes del SI o desarrolla controles adicionales necesarios para mitigar los riesgos.

Figura 58. Niveles de identificación y priorización del servicio.
Fuente: El autor.

Según los indicadores de la figura 59 es el 75% el que denota el uso de la evaluación de riesgos para la seguridad de información y el análisis de impacto en el negocio puesto que también ayuda a identificar los conflictos que podrían presentarse con la inclusión de nuevas normas internas y herramientas para el desarrollo del sistema de información, mientras que sólo un 25% no realizan la evaluación de riesgos antes de incluir normas y herramientas adicionales.

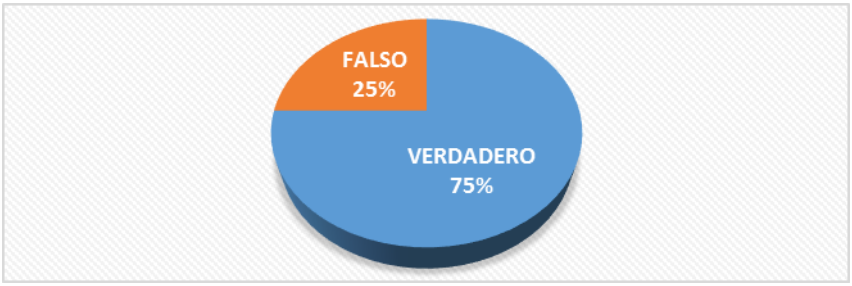


Figura 59. Niveles de evaluación de riesgos.
Fuente: El autor.

Para determinar la resistencia de los controles del sistema la figura 60 muestra que se puede determinar mediante la definición de riesgos cuando los controles sufran inconvenientes o incluso cuando los controles estén operando de manera efectiva.

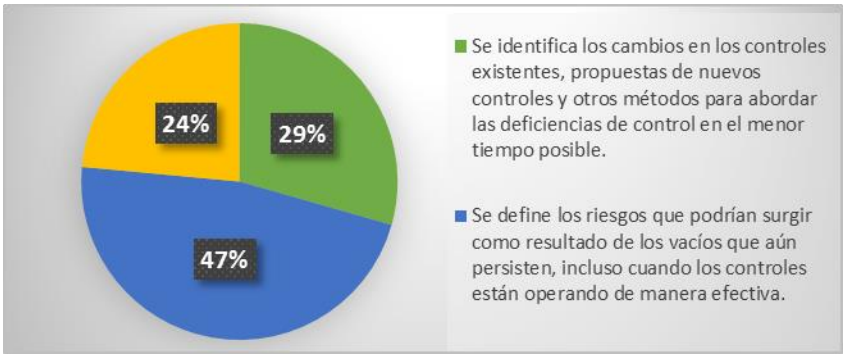


Figura 60. Alternativas para la determinación de resistencia de los controles.
Fuente: El autor.

En cuanto a las mediciones de vulnerabilidades la figura 61 muestra parámetros de riesgos para una medición consistente donde la mayoría se inclina por el desarrollo de auditorías y revisiones internas de riesgos durante la codificación para la ejecución de tales mediciones.

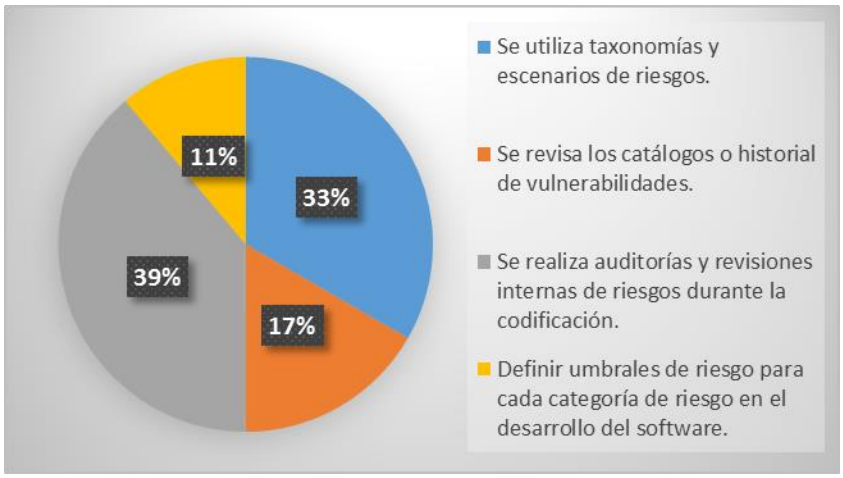


Figura 61. Parámetros de medición de vulnerabilidades.
Fuente: El autor.

En la figura 62 muestra que el 42% de los encuestados categoriza los riesgos del software en cuanto a los activos de tecnología tomando en cuenta los eventos y las fuerzas externas, tales como desastres naturales, fallas de la infraestructura pública, y los inconvenientes suscitados en la cadena de suministro de la organización.

Figura 62. Alternativas de categorización de riesgos.
Fuente: El autor.

Continuando con el área de Gestión de Tecnología; en la figura 63 muestra las políticas y procedimientos de gestión de acceso donde el 53% es desarrolla directrices claras para resolver las solicitudes que incluyen el tipo y el grado de acceso que se les entregará a los objetos como sistemas y procesos, dejando a un lado los inventarios y niveles de control que también son importantes en la gestión de activos de tecnología.

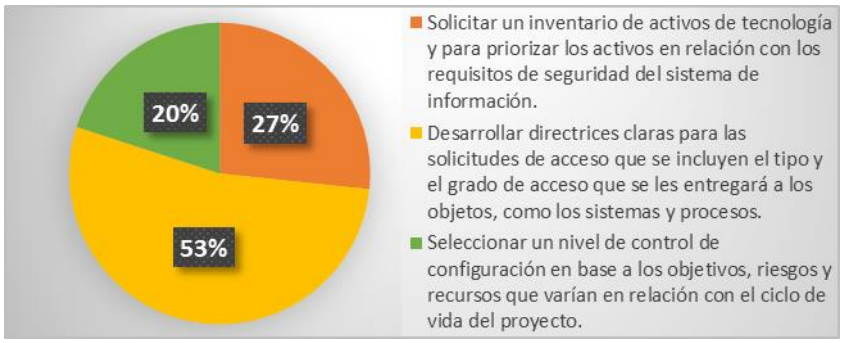


Figura 63. Políticas y procedimientos de gestión de acceso en activos de tecnología.
Fuente: El autor.

Para el mantenimiento de los recursos tecnológicos integrados en el desarrollo del software se opta por desarrollar planes de continuidad de servicio para el cumplimiento de los servicios de la organización, según muestra la figura 64.

Figura 64. Estrategias para el mantenimiento de recursos tecnológicos.
Fuente: El autor.

Como alternativa para el desarrollo de planes de continuidad amerita mencionar que según muestra la figura 65 los encuestados manifiestan en su mayoría que desarrollan planes de continuidad por cada tipo de software de modo que existan un soporte individual para cada uno en el caso de presentarse alguna situación de estrés que amenace el cumplimiento del servicio al que apoya.

Figura 65. Alternativas para el desarrollo de planes de continuidad.
Fuente: El autor.

Quienes cuentan con un sistema de control interno según la figura 66 superan el 50% ya que aplican este tipo de control para el funcionamiento continuo de los recursos tecnológicos que conforman un SI.

Figura 66. Indicadores del uso de control interno en recursos tecnológicos.
Fuente: El autor.

Y finalmente en el área de Continuidad del Servicio las consideraciones que se toma en cuenta al desarrollar y comunicar las directrices y normas de continuidad a los interesados según la figura 67 muestra que el 40% se inclina por el desarrollo de planes de control de versiones, repositorios y de seguridad como mejor alternativa.

Figura 67. Lineamientos para el desarrollo y comunicación de directrices y normas de continuidad del servicio.
Fuente: El autor.

En la figura 68 se afirma que el beneficio del plan de continuidad lo atribuyen a la prestación de un servicio de forma continua en condiciones degradadas.

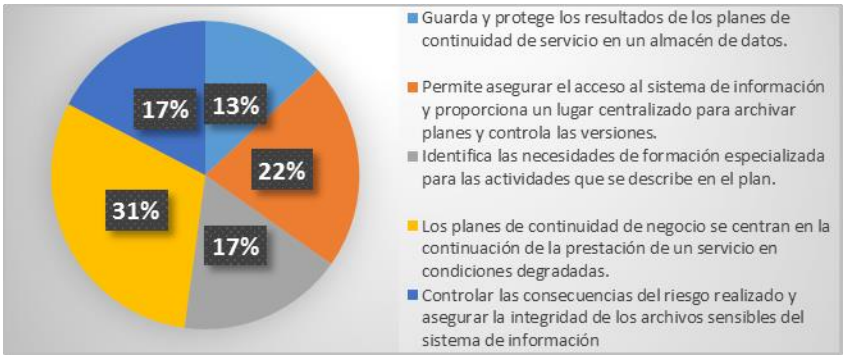


Figura 68. Beneficios del plan de continuidad de servicios.
Fuente: El autor.

En la figura 69 se muestra que el 60% de las personas que respondieron la encuesta no incluye planes de continuidad de servicios para controlar los cambios en el software y que se incrementan de acuerdo a los protocolos y las normas de control de versiones.

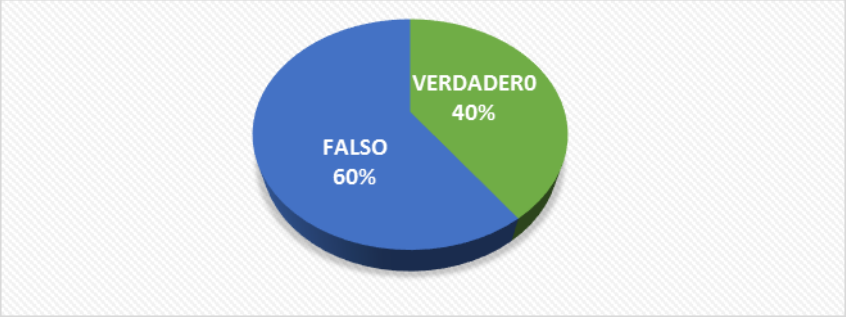


Figura 69. Indicadores de la inclusión de planes de continuidad en el control de cambios del software.
Fuente: El autor.

Finalmente en la figura 70 para considerar una relación con entidades externas el 39% ha sabido manifestar que primero se debe identificar si la entidad seleccionada es capaz de proporcionar sus servicios durante periodos de tiempo concurrente, luego se podría considerar la capacidad de supervisión, test, compatibilidad y por último el nivel de soporte en el cual dependen los servicios.

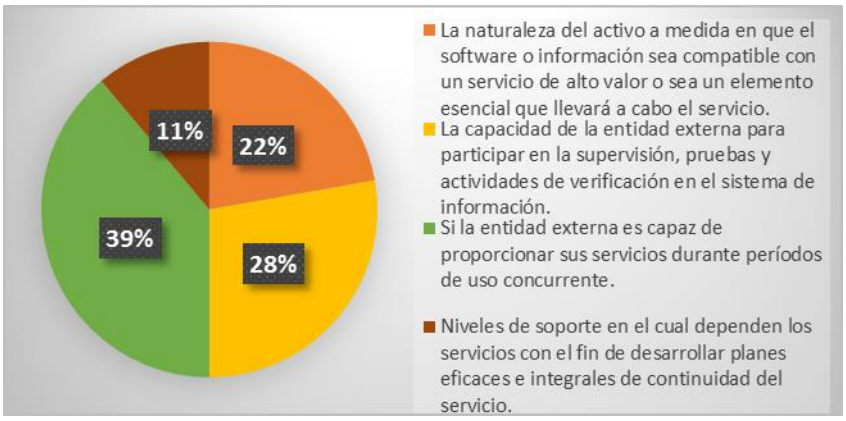


Figura 70. Factores de selección para entidades externas.
Fuente: El autor.

4.2. Parte II: Estudio comparativo del proceso de elicitación de requerimientos entre tipos de software

4.2.1. Parte II - 1: Tipos de software y técnicas utilizadas para el proceso de elicitación de requerimientos.

En la siguiente tabla se muestra una comparación de las técnicas utilizadas para la elicitación de requisitos de software resilientes y no resilientes.

Tabla 7. Comparación técnicas de elicitación de requisitos en Software resiliente y no resiliente.

TÉCNICAS DE ELICITACIÓN	SOFTWARE NO RESILIENTE			SOFTWARE RESILIENTE		
	Alto	Medio	Bajo	Alto	Medio	Bajo
ENTREVISTAS	X					X
ENCUESTAS/CUESTIONARIOS	X				X	
JAD	X					X
BRAINSTORMING		X				X
CASOS DE USO	X					X
PROTOTIPOS		X			X	

Fuente: El autor.

En la tabla 7 se observa que se encontraron diferencias estadísticamente significativas con respecto al nivel de extracción de las técnicas más utilizadas para la elicitación de requisitos cuando se comparan aquellas más usadas en el software no resiliente respecto al software resiliente. Se puede mencionar que las técnicas de elicitación listadas tienen mayor incidencia sobre el software resiliente ya que su nivel de extracción es en la mayoría de las técnicas de *alto nivel* con respecto al software resiliente, que en este caso presentan un *bajo nivel* a diferencia de dos técnicas que parecen tener un *nivel medio* de aceptación en el proceso de elicitación, dichas técnicas son: encuestas/cuestionarios y los conocidos prototipos. Son técnicas comunes (al igual que las demás técnicas listadas) pero con las peculiaridades de anonimato (protege la integridad de la persona encuestada al obtener los requisitos) atribuida a las encuestas/cuestionarios y la visión futurista del sistema de cómo se funcionaría antes de ser desarrollado ya que además consisten en un modelo fácilmente aplicable y modificable atribuida a los prototipos.

Se puede concluir que las Encuestas/Cuestionarios y la Prototipación se identificaron como técnicas de elicitación que más se utilizan en este trabajo. Sin embargo las Entrevistas, JAD, Brainstorming y Casos de Uso son técnicas de elicitación estadísticamente asociadas a los requisitos funcionales.

4.2.2. Parte II - 2: Requisitos de resiliencia de software en sistemas resilientes y sistemas no resilientes.

En la figura 71 se observa el nivel de cumplimiento del software que se considera como resiliente y el software que no es resiliente en cuanto a los requisitos de resiliencia.

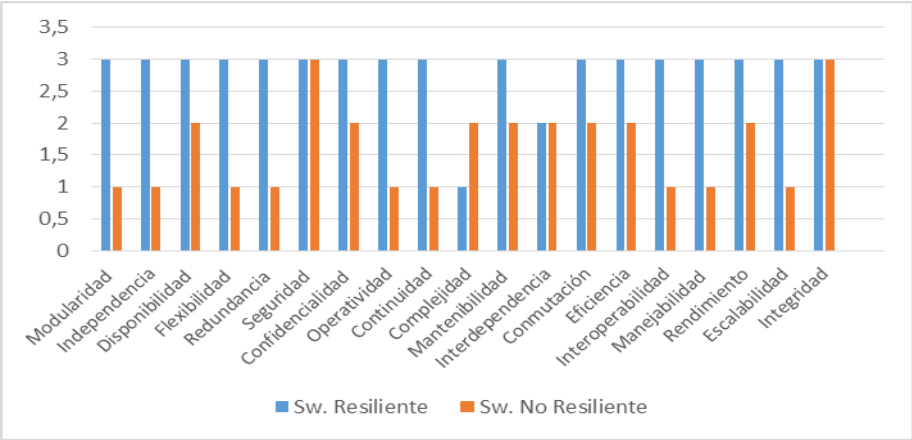


Figura 71. Nivel de cumplimiento de requisitos de resiliencia de software en sistemas resilientes y no resilientes.
Fuente: El autor.

Niveles de cumplimiento: Alto (3), Medio(2) y Bajo (1).

Como se puede observar ninguno de los dos tipos de software cumple a la perfección los requisitos de resiliencia, entonces si uno de los dos tipos de software que se está evaluando se dice que es resiliente, acaso ¿no debería cumplir con todos los requisitos de resiliencia de software mencionados? Según el estudio realizado los SI resiliente cumplen en altos porcentajes los requisitos de resiliencia listados, salvo el caso de dos de ellos como son: la Complejidad y la Interdependencia e Interconexión, puesto que la complejidad como se la mencionado anteriormente define un nivel de dificultad mínimo en cuanto a la arquitectura del SI facilitando la inclusión de la resiliencia en el desarrollo de sistemas individuales, por lo cual no puede mantener un nivel de cumplimiento alto; y la interdependencia e interconexión gestiona que la dependencia a otros sistemas se de en porcentajes mínimos, por lo tanto no puede existir un alto nivel de interdependencia y conexión entre los sistemas, ya que además no se cumpliría con las características de independencia que también es un requisito de resiliencia y este si debe cumplirse en alto nivel.

Se puede observar también la existencia de requisitos de resiliencia con un nivel de cumplimiento alto en cuanto a SI no resiliente, pero este hecho no es suficiente para que sea considerado como resiliente, puesto que debe constar con la mayoría de requisitos de

resiliencia que se muestran en la figura 71, cada uno con su respectivo nivel de cumplimiento. Ahora, existen dos características que también llegan a un alto nivel en los sistemas no resilientes como son: la Seguridad e Integridad ¿por qué sucede esto? Las dos características son comunes en los sistemas y aunque no todos las gestionan eficazmente, se incluyen dentro de los requisitos no funcionales; la seguridad enfocada en controles de acceso y gestión de privilegios, que van de la mano con la integridad ya que maneja la coherencia de los datos y programas mediante la protección del cifrado de datos. De hecho, lo que se podría deducir es que el software no resiliente presenta cierto nivel de resiliencia de software, por las características de seguridad, pero no es completamente resiliente.

Si se observa nuevamente la figura 71 se puede apreciar que entre los requisitos de resiliencia listados están los términos de seguridad de la información como son: confidencialidad, disponibilidad y nuevamente la integridad. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles que radican en el enfoque y metodologías con las que trabajan.

Los SI por lo general incluyen conceptos de confidencialidad, integridad y disponibilidad conocidos como requisitos de seguridad de la información, los cuales son parte de la resiliencia –desde ese momento ya presentan cierto grado de resiliencia–, en cambio los SI resilientes a más de los requisitos de seguridad presentan en su estructura características de modularidad, independencia, redundancia, interoperabilidad, etc., conocidos como requisitos de resiliencia y tomando como base el estudio realizado se determinó que tales requisitos deben cumplirse en su mayoría.

Al contar con un sistema que no incluye características de resiliencia pero que cumple eficazmente con las necesidades para las que fue creado se habla de un sistema de calidad y por lo tanto es útil. En sí, el papel de la resiliencia es dar un agregado especial al software que no es la funcionalidad, sino la capacidad de enfrentar los riesgos y de recuperar el estado normal de los procesos cuando sean intermitentes o afectados por algún inconveniente de modo que puedan conservar la continuidad en sus operaciones.

Resultados obtenidos: como resultado del presente trabajo de tesis se logró la publicación del artículo “Elicitación de Requisitos de Resiliencia para Sistemas de Información basado en el modelo CERT-RMM”, en el evento CISTI 2014 9na. Conferencia Ibérica de Sistemas y Tecnologías de Información, el cual tuvo el agrado de ser aceptado.

CONCLUSIONES

- Según el trabajo realizado en cuanto al proceso de elicitación se concluye que los requisitos no funcionales y de seguridad son los enfoques claves que apoyan la resiliencia, además se determinó que la mayoría de las técnicas de elicitación permiten obtener requisitos de resiliencia.

- En el estudio de la metodología CERT-RMM se dedujo 9 áreas que gestionan la resiliencia en el software, sin embargo la Ingeniería de Soluciones Técnicas Resilientes y Continuidad del Servicio son las áreas que mayor énfasis presentan al estar relacionadas con características de resiliencia como: flexibilidad, operatividad, continuidad, interdependencia e interconexión, interoperabilidad, escalabilidad, etc., las cuales sirven de gran ayuda agilizando la identificación de conflictos a nivel de activos.

- La gestión de riesgos, como área de la metodología CERT-RMM une los enfoques de resiliencia de software y resiliencia operacional, ya que gestiona medidas de protección en base a la información recogida durante el proceso de evaluación para brindar seguridad a los SI como a la organización, adicionalmente en base al trabajo realizado se obtuvo que la mayoría de características de resiliencia de software se tratan en esta área, la cual mantiene estrategias óptimas para proteger y mantener la normalidad en las operaciones que realiza el SI y de hecho, evita la ejecución de interrupciones potenciales que podrían interferir en el cumplimiento de la misión y reducir su estado de resiliencia.

- La característica de resiliencia que es tratada por la mayoría de las áreas del CERT-RMM en base al trabajo realizado se determinó la redundancia ya que se utiliza como medida de protección para contrarrestar las fallas antes que se conviertan en vulnerabilidades para el SI.

- De la familia ISO 27000 son 3 estándares que apoyan la gestión de resiliencia de software con cierta analogía a las áreas de la metodología CERT-RMM que mantienen el mismo enfoque, donde según el estudio realizado se ha demostrado que los estándares ISO 27001 y 27005 van de la mano con las áreas de Gestión de Activos, Requisitos, Riesgos, Soluciones Técnicas y Continuidad, pues implementan estrategias de gestión de riesgos y seguridad para proteger y mantener establece el SI.

- Para integrar seguridad en el ciclo de vida de los SI se realizó el estudio del estándar ISO 27034, el cual denota varias relaciones con todas las áreas del CERT-RMM partiendo con

la identificación de procesos, personas, datos, etc., hasta administrar la tecnología para facilitar el desarrollo y satisfacción de los requisitos de resiliencia, además se basa en el enfoque de gestión de riesgos y controles de seguridad definidos en los estándares ISO 27001 e ISO 27005.

- Según el trabajo realizado la mayoría de SI de las organizaciones evaluadas presentan un nivel de resiliencia que oscila en un aproximado del 8.8% al 43%, y en base a los resultados del estudio se ha demostrado que son pocas las características que permiten identificar la resiliencia en los SI, por tal razón se debería incluir características de continuidad, flexibilidad, independencia, manejabilidad y rendimiento en sus operaciones para que puedan conseguir ser resilientes.

- En base a los resultados de la evaluación se demostró que son pocas las organizaciones en las que se considera la presencia de ciertos rasgos de resiliencia de software, ya que software resiliente como tal se encontró en proporciones menores, por lo cual se concluye que el software no resiliente mantiene cierta predominación actualmente en el mercado informático.

- La importancia de la resiliencia en los SI radica en el cumplimiento de las características del software resiliente, puesto que existen por una razón que es la de ayudar en el mejoramiento del proceso de recuperación ante riesgos, sean estos altos o moderados.

- Tomando como base el estudio realizado se determinó que los requisitos de resiliencia deben cumplirse en su mayoría salvo el caso de la complejidad y la interdependencia e interconexión, las cuales deben cumplirse en niveles mínimos por el conflicto que representan para los demás requisitos.

RECOMENDACIONES

- No se debe confundir un SI seguro como un SI resiliente puesto que las características de seguridad que presenta un software seguro tan sólo son algunas de las peculiaridades que se considera en la resiliencia, y de hecho la seguridad es solamente uno de los requisitos que caracterizan a un software como resiliente.
- Se recomienda que dentro del proceso de elicitación de requisitos no se debe olvidar incluir características de seguridad como parte de los requisitos no funcionales.
- Para implementar requisitos de resiliencia en los SI, estos deben estar acordes a una metodología que mantenga el mismo enfoque por lo cual se recomienda utilizar la metodología CERT-RMM.
- Para incentivar a las organizaciones a incluir requisitos de resiliencia en el desarrollo de sus SI se debe realizarlo con la ayuda de las áreas de Definición y Gestión de Requisitos de Resiliencia del CERT-RMM.
- Se debe utilizar las áreas de Ingeniería de Soluciones Técnicas Resilientes y Continuidad de Servicio del CERT-RMM para definir estrategias de seguridad y continuidad en las operaciones que realiza el SI.
- Se debe evaluar la complejidad del SI con el apoyo del área de Gestión de Control ya que la resiliencia de software generalmente se adhiere mejor en sistemas poco complejos.
- Durante las fases iniciales del ciclo de vida de software se debe incluir la resiliencia en base a los lineamientos que presentan las áreas de la metodología CERT-RMM, dado que durante la etapa de implementación sería más complejo, costoso y poco eficiente.
- Para garantizar la realización eficaz y eficiente de los objetivos del software se debe usar las áreas de Gestión de Activos y Control del CERT-RMM.
- Se debe tener presente el área de Gestión de Tecnología ya que los activos tecnológicos son utilizados directa o indirectamente en la automatización de los servicios y facilita el cumplimiento de la misión del SI.
- No se debe aplicar lineamientos de resiliencia operacional al definir a un software resiliente ya que cambiaría su enfoque, a excepción del área de Gestión de Riesgos que gestiona los dos enfoques de resiliencia.

BIBLIOGRAFÍA

Ambrosone, M. (2004). La Administración del Riesgo Empresarial: Una responsabilidad de todos - El enfoque COSO. 24.

Antón, A. I. (1997). *Goal Identification and Refinement in the Specification of Software-Based Information Systems.* Georgia.

Antonelli, L., & Oliveros, A. (2002). Fuentes utilizadas por desarrolladores de software en Argentina para elicitar requerimientos. 11.

Axelrod, C. W. (Septiembre de 2009). Investing in Software Resiliency. 6.

Bastani, F. B., Fu, J., & Yen, I.-L. (2008). *Model-Driven Prototyping Based Requirements.* Dallas, Texas.

Black, P. E., & Windley, P. J. (January de 1997). Verifying resilient software. In. *System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on, Vol. 5*, pp. 262-266. IEEE.

Borland. (2005). MITIGATING RISK WITH EFFECTIVE REQUIREMENTS ENGINEERING. 14.

Braude, E. J. (2003). *Software Engeeniering, An Object-Oriented Perspective.* México: Alfaomega.

Caralli, R. A., Allen, J. H., & White, D. W. (2010). *CERT Resilience Management Model.* Boston: Pearson Education.

Caralli, R. A., Allen, J. H., & White, D. W. (2011). *CERT Resilience Management Model.* Boston: Pearson Education.

Caralli, R. A., Allen, J. H., Curtis, P. D., White , D. W., & Young, L. R. (2010). *CERT® Resilience Management Model.* CarneigeMellon.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young , L. R. (2010). Resilience Requirements Management (RRM). *CERT® Resilience Management Model*, 24.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Asset Definition and Management (ADM). *CERT® Resilience Management Model*, 29.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Controls Management (CTRL). *CERT® Resilience Management Model*, 31.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Enterprise Focus (EF). *CERT® Resilience Management Model*, 35.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). External Dependencies Management (EXD). *CERT® Resilience Management Model*, 42.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Improving Operational Resilience Processes. *CERT® Resilience Management Model, Version 1.0*, 259. Obtenido de http:// www.cert.org/resilience/

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Resilient Technical Solution Engineering (RTSE). *CERT® Resilience Management Model*, 41.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Risk Management (RISK). *CERT® Resilience Management Model*, 32.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Service Continuity (SC). *CERT® Resilience Management Model*, 40.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010). Technology Management (TM). *CERT® Resilience Management Model*, 49.

Caralli, R. A., Allen, J. H., Cutis, P. D., White, D. W., & Young, L. R. (2010). Resilience Requirements Development (RRD). *CERT® Resilience Management Model*, 25.

Cheema, A. (3 de January de 2014). *Brain Book*. Obtenido de ISO/IEC 27001 DOMAINS: http://arfanahmedcheema.blogspot.com/2014/01/isoiec-27001-domains.html

Davies, S. (1993). Are Coping Strategies a Cop Out? En *IDS Bulletin* (págs. 60-72). Brighton: Institute of Development Studies.

Deming, W. E. (22 de Noviembre de 2012). *Universidad de Antioquía.* Obtenido de CICLO PHVA: http://guajiros.udea.edu.co/fnsp/cvsp/Practica%20procesos/Metodologias%20procesos/CicloPHVA.pdf

Devanbu, P., & Stubblebine, S. (2013). *Software Engineering for Security: a Roadmap.* USA: University of California.

Ducón , K. E., & Carrillo, J. D. (2013). *Guía para la Implementación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores Prácticas.* Madrid: Universidad Politécnica de Madri.

Durán, A., & Bernárdez, B. (2000). *Metodología para la Elicitación de Requisitos de Sistemas Software.* Sevilla, España.

Fernández, C., Mendoza, A., Martínez, D., Mendoza, E., & Sumano, P. (2003). XVI Congreso Nacional y II Congreso Internacional de Informática y Computación. *Ingeniería de Requerimientos aplicada a la Universidad Virtual de la UTM*, (pág. 6). México, Zacatecas.

Hadad, G. D., Doorn, J. H., Kaplan, G. N., & Sampaio, J. (2003). Enfoque Middle-Out en la Construcción e Integración de Escenarios. 16.

Hernández, J. G. (15 de Enero de 2013). Obtenido de http://www.jesusgilhernandez.com/2013/01/15/software-resilience/

Huhn, R. (06 de 06 de 2013). *InfoQ*. Obtenido de Creating Resilient Software with Akka: http://www.infoq.com/articles/resilient-software-with-akka

Ian, S., & Pete, S. (1997). *Requirements Engineering A good practice guide.* Chichester: Wiley, 2004.

Ibrahim, N., Wan Kadir, W. N., & Deris, S. (2008). Comparative Evaluation of Change Propagation Approaches towards Resilient Software Evolution. *Software Engineering Advances, 2008. ICSEA '08.* , 7.

ISO/IEC. (2011). ISO/IEC 27034 Information technology — Security techniques — Application security. *ISO/IEC 27034*, 67.

Kotonya, G., & Ian, S. (1997). *Requirements Engineering: Processes and Techniques.* (J. Wiley, Ed.) New York: Chichester.

Lamswerde, A. (2003). *From System Goals to Software Architecture.* Louvain: Université catholique de Louvain.

Loucopoulos, P., & Karakostas, V. (1995). *System Requirements Engineering.* New York: McGraw-Hill.

Manyena, S. B. (Diciembre de 2006). The concept of resilience revisited. *Disasters*, 434-450.

Maña, A., May, D., Sánchez, F., & Yague, M. I. (s.f.). Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software. 10.

Marcus, E., & Stern, h. (s.f.). Blueprints for high availability: designing resilient distributed systems.

Merkow, M. S., & Raghavan, L. (2011). *Secure and Resilient Software: Requirements, Test Cases, and Testing Methods.* Boca Raton: Taylor & Francis Group.

Mitchell, T., & Harris, K. (January de 2012). Resilience: A risk management approach. 7.

Oloriz, M. G. (Agosto de 2004). *Elicitación de Requerimientos.* Obtenido de http://www.slidefinder.net/e/elicitaci%C3%B3n_requerimientos_lic_mario_oloriz/elicitaciondererequerimientos%282%29/30219395

Peláez, R. (2012). Manejo de la capacidad de recuperación en el modelo RMM del CERT. *Universitat Oberta de Catalunya*, 12. Obtenido de http://hdl.handle.net/10609/14730

Pressman, R. S. (2005). *Ingeniería del Software, Un enfoque práctico* (Sexta ed.). México: Edamsa Impresiones, S.A. de C.V.

Rumbaugh, J., Blaha, M., Premerlani, W., Eddy, F., & Lorensen, W. (1996). *Modelado y Diseño Orientado a Objetos: Metodología OMT y OMT II.* New York.

Sharmila, P., & Umarani, R. (2011). *A walkthrough of Requirement Elicitation Techniques.* Tamilnadu, India.

Sim Abdullah, N. A., & Md Noor, N. L. (2013). *Resilient Organization: Modelling The Capacity for Resilience.* Shah Alam, Malaysia: Universiti Teknologi Mara.

Sommerville, I. (2006). *Ingeniería del Software.* España: Pearson Education.

Sommerville, I. (2011). *Ingeniería de Software.* Mexico: Pearson Education.

Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise Resilience: Managing Risk in the Networked. 3.

SWEBOK. (2004). Guide to the Software Engineering Body of . *A project of the IEEE Computer Society* , 202.

Vanthinking. (2013). *Vanthinking Online Professional Skills Development*. Obtenido de Resilience Management: http://main.vanthinking.com/index.php/The-aspects-of-Resilience-Management.html

ANEXOS

A. CERT-RMM

Definición y gestión de activos (ADM).

Mantiene su enfoque en la descripción de activos como definición, valor, relación, perfilación, etc., y en establecerlo como centro del proceso de gestión de resiliencia operacional.

En cuanto a la organización, también define y gestiona el proceso para mantener la corriente del inventario de activos y asegura que los cambios en el inventario no den lugar a deficiencias en las estrategias para la protección y el mantenimiento de los activos (Caralli R. A., Allen, Curtis, White, & Young, Improving Operational Resilience Processes, 2010). Los aspectos de resiliencia de estos activos se abordan en las zonas de activos específicos del proceso.

Objetivos y prácticas específicas.

ADM: SG1 Establecer activos organizacionales.

Dentro de la resilencia los activos son: personas, información, tecnología e instalaciones; cada uno de ellos cumple una función, que en forma general son actividades correspondientes a operar, controlar, alimentar, automatizar, apoyar y ejecutar los servicios.

¿Qué son los servicios? Constituye un servicio aquellas actividades que apoyan el cumplimiento de los objetivos organizacionales.

Con el fin de determinar adecuadamente las necesidades de resiliencia la organización define estos activos desde una perspectiva de servicio y establece la propiedad y la responsabilidad de su capacidad de recuperación (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010).

ADM: SG1.SP1 Activos de inventario

Los activos constituyen la parte primordial de la organización, pero su incumplimiento en lugar de ser un apoyo se convertiría en problemas que ofuscan la capacidad de recuperación operativa.

¿Cuál es el primer paso a tomar con los activos? Es identificarlos y luego definir los de alto valor, pero ¿Qué se gana con esto? Al realizar esto se logrará satisfacer los requisitos

de resiliencia y mantener la “estructura y orientación para el desarrollo de un inventario de los activos de alto valor” (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010).

ADM: SG1.SP2 Establecer un entendimiento común

Define el alcance de los activos, importantes para "decidir cuanta información es útil facilitando la satisfacción de necesidades" (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010).

En prácticas posteriores donde se habla de los requisitos, se menciona la importancia de documentarlos, pues bien dentro de la resiliencia nuevamente vuelve a tomar vigor en este caso como un perfil activo, esencial para la comunicación y actualización de los mismos.

ADM: SG1.SP3 Establecer propiedad y custodia

Bien, se habla de activos y servicios que se clasifica y documenta, pero ahora estos activos serán controlados, lo cual dentro de la resiliencia se lo conoce como propietarios y custodios.

¿Qué son los propietarios y custodios? Los propietarios se consideran a "las personas o unidades organizativas internas o externas a la organización, que tienen la responsabilidad principal de la viabilidad, productividad y capacidad de recuperación de los activos" (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010), a diferencia los custodios que se encargan de implementar y controlar los activos que se les haya otorgado.

La identificación de los custodios de los activos de alto valor también ayudará a identificar el entorno operacional de los activos donde los riesgos pueden surgir y para lo cual se implementará planes de continuidad (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010).

ADM: SG2 Establecer la relación entre los activos y servicios.

Al contar con activos y servicios trabajando independientemente sin relación alguna, en lo único que pueden ayudar es a crear problemas. Es así, que para que sirvan de apoyo a la organización deben “desarrollar, implementar y administrar estrategias de resiliencia”

(Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010) acordes a cada operación organizacional.

ADM: SG2. SP1 Asociar activos con servicios

Se habla del inventario de activos y de la relación que deben mantener con los servicios, pero esta práctica presenta algo diferente, pues se enfoca en el refortalecimiento de los activos manejando la Gestión de Riesgos con el fin de: identificar servicios de alto valor sometiéndolos a una validación con respecto a los activos que están vinculados y crean listas, perfiles y bases de datos actualizadas y de calidad.

ADM: SG2.SP2 Analizar dependencias de activos y servicios

A más de una relación entre activos y servicios, estos ¿Mantienen dependencias? Pues sí, ya que apoyan el proceso de resiliencia durante el desarrollo de requisitos, estrategias de protección y al definir entornos compartidos, ayudando en la mitigación de riesgos. Es interesante la explicación que dan (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010) "cuando las dependencias dan lugar a un entorno compartido de un activo, se debe prestar atención a los efectos que esta situación tendrá sobre la satisfacción de las necesidades de capacidad de recuperación en el nivel de servicio. Por ejemplo, si los requisitos de resiliencia se establecen para una instalación y más de un servicio se lleva a cabo en dicha instalación, los requisitos para la protección y el mantenimiento de la instalación deben ser suficientes para satisfacer las necesidades de los servicios que comparten las instalaciones. Al identificar estos conflictos potenciales con tiempo, una organización puede mitigar activamente (mediante la revisión de los requisitos u otras acciones) antes de que se conviertan en un riesgo que afecta a la capacidad de recuperación operativa de los servicios afectados".

ADM: SG3 Gestión de activos.

El software se caracteriza por un ciclo de vida propio con objetivos a cumplir, pues bien los activos no se quedan atrás ya que también mantienen un ciclo de vida, que no está libre de sufrir cambios que debilitan la protección de los mismos, dejando tanto los inventarios de los bienes y servicios como sus requisitos desprotegidos lo cual descontrola el alcance de la organización.

ADM: SG3.SP1 Identificar Criterios de Cambio

Hay que empezar por lo primordial ¿Qué es un criterio? Se considera como criterio a una regla o norma que determina la calidad de los procesos evaluados, el cual deberá ser válido, fiable y apropiado. Ahora al incluirse en la capacidad de recuperación este abarca además de los activos, las áreas que se mencionan anteriormente como el personal, la tecnología, la información y las instalaciones; donde todos los cambios efectuados tienen mayor impacto en los requisitos que pueden ser modificados o eliminados.

ADM: SG3.SP2 Mantener cambios en activos e inventario

Los cambios constantes de los activos en la organización sean por cambios en el personal, información, tecnología e instalaciones, así como la inserción de nuevos activos hace que esta práctica se ocupe de estas situaciones en las que incluye los detalles y composición de los activos.

¿Qué es lo que puede cambiar en los activos? Lo que puede cambiar es el valor, la custodia y propiedad; pero ¿Y el inventario? Este se actualiza guardando el perfil de los activos, pues cuando se realizan los cambios “siempre que los bienes se eliminan, los propietarios de dichos activos deben asegurarse de que sus necesidades de resiliencia se eliminan (si es posible) o se transfieren y se actualizan con los activos en lugar de reemplazarlos” (Caralli R. A., Allen, Curtis, White, & Young, Asset Definition and Management (ADM), 2010).

Gestión de Control (CTRL).

Garantiza el cumplimiento de los objetivos, pues el proceso de control abarca toda la estructura organizativa desde los directivos de más alto valor hasta los sistemas de control interno y registros financieros, todo lo mencionado desde el punto de vista organizacional. Ahora, visto desde la perspectiva de resiliencia operativa este proceso ayuda en el mantenimiento, protección y prevención de interrupción de los activos, y continuidad de los servicios.

Objetivos y Prácticas Específicas.

CTRL: SG1 Establecimiento de objetivos de control.

La organización utiliza los objetivos de control como medio de selección, análisis y gestión de un nivel adecuado de control para lograr los objetivos estratégicos de la organización.

En estos objetivos de control se asegurará la prevención ante fraudes, gestión de líneas de negocio y en sí las directrices de gestión de la organización.

CTRL: SG1.SP1 Definir objetivos de control

Los objetivos de control se definen generalmente sobre comportamientos aceptables de control, "se impulsan por las estrategias para la protección y el mantenimiento de los activos relacionados con el servicio para asegurarse de que su exposición a vulnerabilidades y amenazas se gestiona" (Caralli R. A., Allen, Curtis, White, & Young, Controls Management (CTRL), 2010).

Es así que estos objetivos de control se seleccionan, analizan y gestionan para garantizar su cumplimiento.

CTRL: SG2 Establecer controles.

Un control es una política, procedimiento, método, tecnología o herramienta que satisface un objetivo de control establecido (Caralli R. A., Allen, Curtis, White, & Young, Controls Management (CTRL), 2010).

Dentro de la resilencia operacional se busca que los controles disminuyan la exposición de los activos a vulnerabilidades en la organización.

Para mantener mayor efectividad de los controles en los ámbitos que los requieran, se tiene tres tipos:

- Controles administrativos, se aseguran que la gerencia direccione la organización conforme a políticas, planes de continuidad, la gobernanza y demás acciones establecidas para alcanzar los requisito no-funcionales unidos a los requisitos de resiliencia.
- Controles técnicos, se manifiestan en los activos de tecnología incluido las redes y telecomunicaciones, estos "son eficaces para la aplicación de todo tipo de necesidades de resiliencia" (Caralli R. A., Allen, Curtis, White, & Young, Controls Management (CTRL), 2010).
- Controles físicos, se aplican a los activos tangibles como son personas, tecnología e instalaciones que utilizan material físico para realizar el control, aunque "es más eficaz para aplicar los requisitos de integridad y disponibilidad, pero también se pueden utilizar para asegurar la confidencialidad" (Caralli R. A., Allen, Curtis, White, & Young, Controls Management (CTRL), 2010).

CTRL: SG2.SP1 Definir controles

Los controles a nivel empresarial se basan en el cumplimiento de reglamentos, identificación de riesgos, atributos de calidad, objetivos estratégicos, requisitos de control externo en los que opera la organización y por lo tanto deberán de cumplir las distintas unidades organizativas que lo componen.

En cuanto a controles a nivel de servicio se mantiene un proceso donde se identifican, otorgan prioridad y finalmente se comunican con el área de proceso EF (Enfoque Empresarial), para su desenvolvimiento total se derivan de los controles de nivel de activos, ahora estos controles de nivel de activos se encargan del cumplimiento de la misión del servicio.

CTRL: SG3 Analizar controles.

Se evalúa los controles, esto en cuanto a los ya existentes y los nuevos (en caso de haberlos) basados en los requisitos de resiliencia y cumpliendo los objetivos de resiliencia de servicios y activos.

CTRL: SG3.SP1 Analizar controles

Ayuda a la organización en la identificación de riesgos y deficiencias de control que impidan el cumplimiento de los objetivos de control, opaquen la capacidad de recuperación de los activos y servicios, de modo que se implemente controles actualizados determinando el grado de análisis necesario.

Surgen nuevos controles como el de capas que reúne uno o más objetivos de control para su ejecución y el control de redundancia que se utiliza cuando hay más de un tipo de control por cumplir.

CTRL: SG4 Evaluar la efectividad de los controles.

El nivel de deficiencias dentro de la organización deberá ser mínimo para que la efectividad de los controles por medio de actividades de resiliencia satisfaga los objetivos de control, estrategias de protección y mantenimiento, inclusive los requisitos de resiliencia.

Esta práctica captura el monitoreo continuo, revisión y mejora de las actividades que son esenciales para asegurar que los controles siguen siendo eficaces (Caralli R. A., Allen, Curtis, White, & Young, Controls Management (CTRL), 2010).

CTRL: SG4.SP1 Evaluar los controles

La realización de la evaluación periódica del sistema de control interno se hace necesario para asegurar el cumplimiento continuo de los objetivos de control y la inclusión de estrategias para la protección y el mantenimiento de los servicios (y sus activos de apoyo), y que los requisitos de resistencia se están cumpliendo (Caralli R. A., Allen, Curtis, White, & Young, Controls Management (CTRL), 2010).

Se identifica las áreas que necesitan mayor atención en el cumplimiento de sus obligaciones, de modo que los controles redundantes y conflictos entre controles se eliminen ahorrando costos en la resiliencia operacional.

Gestión de dependencias externas (EXD).

Esta área se refiere a la identificación de los riesgos asociados a las acciones de las entidades externas, como la formalización de la relación con estas entidades y la gestión continua de dichas dependencias y relaciones, todo de manera que asegure las medidas de resistencia apropiadas para proteger y mantener los servicios y bienes que dependen de este tipo de acciones y entidades de la organización (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010).

El outsourcing toma parte en esta área del CERT, que implica cambios estructurales en la organización, pero se mantendrá la misión de los servicios a pesar de constituirse como una dependencia externa, busca agilizar los procesos (gestión de resiliencia).

Objetivos y prácticas específicas.

EXD: SG1 Identificar y priorizar las dependencias externas.

Se diferencia las dependencias que son de mayor valor las cuales deberán ser identificadas para obtener una resiliencia operacional adecuada de los bienes y servicios que apoyan.

EXD: SG1.SP1 Identificar dependencias externas

Cualquier bien o servicio que es objeto de las acciones de una entidad externa es la fuente de una dependencia externa (Caralli R. A., Allen, Curtis, White, & Young, 2010).

El momento que una organización subcontrata una entidad externa o cuando la organización permite el acceso a los usuarios a sus activos de alto valor, es ahí cuando se producirá una dependencia externa.

EXD: SG1.SP2 Priorizar dependencias externas

El hecho de priorizar las dependencias externas asegurará que la organización mantenga una buena dirección de sus recursos, dando más importancia a los servicios de alto valor en cuanto a las operaciones de resiliencia.

El establecimiento de prioridades y criterios deberán revisarse y actualizarse con regularidad para garantizar que el esquema de prioridades y la lista de dependencias externas priorizadas sean apropiados para el entorno de riesgos de la organización y la tolerancia (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010).

EXD: SG2 Gestionar los riesgos debido a dependencias externas.

Cuando la organización mantiene muchas dependencias externas será más propensa a sufrir riesgos adicionales que intervienen en el incumplimiento de sus metas.

EXD: SG2.SP1 Identificar y evaluar riesgos debido a dependencias externas

Cada riesgo en la organización sea de cualquier tipo, deberá ser identificado y evaluado para mantener en este caso la resiliencia operacional de los servicios.

EXD: SG2.SP2 Mitigar riesgos debido a dependencias externas

Al mitigar los riegos se ayudará en el desarrollo de estrategias y planes que apoyen la inclusión de controles reduciendo el impacto en la organización.

EXD: SG3 Establecer relaciones formales.

Una relación formal se constituirá a base de requisitos relacionados con las entidades externas y la organización.

Estos acuerdos se actualizan durante todo el ciclo de vida de la relación con la entidad externa, según sea necesario (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010).

EXD: SG3.SP1 Establecer especificaciones empresariales para dependencias externas

Para proteger el funcionamiento de la organización se cuenta con valores y comportamientos reflejados en las políticas organizacionales traducidas a un conjunto de condiciones a nivel de la organización, de este modo se permitirá la implementación eficaz de las estrategias de resiliencia operacional.

EXD: SG3.SP2 Establecer especificaciones de resiliencia para dependencias externas

Los bienes y servicios de alto valor en la organización mantienen requisitos que establecen especificaciones a partir de los cuales surgen las dependencias externas que apoyan la resiliencia operacional.

Las especificaciones para una dependencia externa específica y de las entidades incluyen, en su caso, las características requeridas por la entidad externa (por ejemplo, la situación financiera y la experiencia), los comportamientos requeridos de la entidad externa (por ejemplo, la seguridad y las prácticas de formación), y los parámetros de rendimiento que deberán ser exhibidos por la entidad externa (por ejemplo, el tiempo de recuperación después de un tiempo de incidentes y respuesta a llamadas de servicio) (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010).

EXD: SG3.SP3 Evaluar y seleccionar las entidades externas

El proceso y los criterios de selección se diseñarán para garantizar que la entidad seleccionada puede satisfacer plenamente las especificaciones de la organización (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010), aunque si existieran especificaciones no cubiertas se podrá cambiar las acciones de dependencia y en caso de no poder cambiarlas se los tratará como riesgos.

EXD: SG3.SP4 Relaciones formales

Se mantienen contratos, memorandos y órdenes con entidades externas que describirán disposiciones y acuerdos, dependiendo de la forma, según lo destacan (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010):

- Tipo de relación entre la organización y la entidad externa.

- Tipo de productos o servicios (dependencias externas) que suministra la entidad externa (sobre todo si los servicios son para mantener la seguridad y capacidad de recuperación en lugar de servicios generales)
- Nivel de integración de la entidad externa para el servicio (es decir, el grado en que la organización se basa en la entidad externa para cumplir con la misión de servicio).

Grado al cual la entidad externa se hace con la custodia de los activos de la empresa(s) con el fin de proporcionar productos y servicios necesarios.

EXD: SG4 Gestionar el rendimiento de la entidad externa.

La organización deberán gestionar las entidades externas mediante el control de rendimiento de las especificaciones y tomar las medidas correctivas apropiadas (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010).

EXD: SG4.SP1 Monitor de rendimiento de la entidad externa

Es necesario mantener un control periódico del desempeño de las entidades externas para su impacto potencial en los procesos resilientes en la organización.

Para asegurarse de que la supervisión del rendimiento se llevará a cabo de manera oportuna y constante, la organización debe establecer procedimientos que determinen la frecuencia, el protocolo y la responsabilidad de supervisar una entidad externa particular (Caralli R. A., Allen, Curtis, White, & Young, External Dependencies Management (EXD), 2010).

EXD: SG4.SP2 Corregir el rendimiento de la entidad externa

Las acciones correctivas se basan en las dependencias externas, estas se “establecen en acuerdo con la entidad externa, y con una evaluación de las alternativas pues deberá ser completado antes de la implementación de acciones correctivas (Caralli R. A., Allen, Curtis, White, & Young, 2010)”.

Gestión de riesgos (RISK).

La gestión del riesgo operacional identifica, analiza y mitiga los riesgos. Estos riesgos interrumpen los activos reduciendo la resiliencia operacional.

¿Cómo mitigar los riesgos? Requiere mantener las estrategias equilibradas tanto en la protección como mantenimiento de los bienes y servicios organizacionales.

El medir el impacto es una tarea que corresponde a los criterios de evaluación, los cuales a través de la evaluación de los riesgos obtienen información valiosa para el mejoramiento y protección de los activos y servicios.

Objetivos y prácticas específicas.

RISK: SG1 Preparar la gestión de riesgos.

Generalmente se establece un plan de riesgos para un monitoreo continuo de los riesgos que atacan la resiliencia de los activos de la organización.

RISK: SG1.SP1 Determinar las fuentes y categorías de riesgos

Para determinar y clasificar los tipos de riesgos están las fuentes de riesgos que afectan al funcionamiento tanto de activos y servicios de la organización.

Una vez que son clasificados los tipos de riesgos es necesario recopilarlos y organizarlos por categorías de riesgos de modo que se facilite la mitigación de los mismos.

RISK: SG1.SP2 Establecer una estrategia de gestión del riesgo operacional

Dentro de los parámetros esenciales que una estrategia de riesgo operacional (Caralli R. A., Allen, Curtis, White, & Young, 2010) menciona artículos típicos de los cuales se toma los más importantes:

• El alcance de las actividades de gestión de riesgo operacional.

• Los métodos que se utilizarán para la identificación del riesgo operacional.

• Las fuentes de riesgo operativo.

• Parámetros para medir y tomar medidas sobre los riesgos operativos.

• Las técnicas de mitigación del riesgo que se utilizarán, como el desarrollo de los controles administrativos, técnicos, físicos de capas y el desarrollo de planes de continuidad de servicio.

• El personal involucrado en la gestión del riesgo operacional y el alcance de su participación en las actividades se señaló anteriormente.

Todos estos artículos deben ser documentados para que las partes interesadas (internas y externas) puedan estar informados de todas las actividades de gestión de riesgo operacional.

RISK: SG2 Establecer parámetros y enfoques de riesgos.

Proporcionan criterios comunes y coherentes para la comparación de riesgos y para caracterizar la gravedad de las consecuencias para la organización si el riesgo se realiza (Caralli R. A., Allen, Curtis, White, & Young, 2010).

RISK: SG2.SP1 Definir parámetros de riesgo

Se determina el estado del riesgo, si este está controlado o si ha sobrepasado el nivel de tolerancia, que reflejan la aversión del riesgo en la organización.

Parámetros de riesgo también establecen la filosofía de la organización en la gestión de riesgos, cómo se controlan los riesgos, que está autorizado para aceptar riesgos en nombre de la organización, y con qué frecuencia y en qué grado de riesgo operacional deben ser evaluados (Caralli R. A., Allen, Curtis, White, & Young, 2010).

RISK: SG2.SP2 Establecer criterios de medición de riesgo

Criterios de medición de riesgo son los criterios objetivos que la organización utiliza para evaluar, categorizar y priorizar los riesgos operacionales (Caralli R. A., Allen, Curtis, White, & Young, 2010). Además se determinan las áreas de impacto donde se ejecutan los riesgos.

Cuando se define y documenta la medición de los riesgos proporciona una visión del nivel de gravedad del impacto y se identifica cuáles son las probabilidades que impacten nuevamente o que surjan nuevos riesgos operativos.

RISK: SG3 Identificar el riesgo.

El impacto de los riesgos puede causar daños severos que pueden llegar hasta el cierre de la organización, para ello se considera conveniente el identificar con anterioridad los riesgos evitando estas consecuencias.

RISK: SG3.SP1 Identificar los riesgos del nivel de activos

Al igual que en las prácticas de las demás áreas dentro de la gestión del riesgo se establece una línea base, esta vez con los riesgos identificados. Estos riesgos riegos pueden afectar los activos (personas, información, tecnología e instalaciones) de la organización perturbando la resiliencia operativa.

Se puede utilizar taxonomías de riesgos, cuestionarios, metodologías, listas de vulnerabilidades y procesos de control como herramientas complementar la identificación de riesgos.

RISK: SG3.SP2 Identificar los riesgos de nivel de servicio

Los riesgos asociados a los activos de la organización deben examinarse en el contexto de estos servicios, para determinar si hay un impacto potencial en la garantía de la misión, que a su vez podría afectar la capacidad de la organización para cumplir su misión (Caralli R. A., Allen, Curtis, White, & Young, 2010).

Para reflejar el estado de la declaración de riesgos se deberá identificar los servicios asociados, que determinan el efecto y la gravedad sobre el mismo servicio al ejecutarse los riesgos a nivel de activos.

RISK: SG4 Analizar riesgos.

El análisis de riesgos se lleva a cabo por la organización para determinar la importancia relativa de cada riesgo operacional identificados y se utiliza para facilitar la disposición de riesgos de la organización y las actividades de mitigación (Caralli R. A., Allen, Curtis, White, & Young, 2010).

RISK: SG4.SP1 Evaluar el riesgo

Dado que los riesgos son los mismos en todas las organizaciones, por ende, la manera de tratarlos es distinta. Cada riesgo se evalúa en función de los criterios de medición y prioridades de impacto.

Existen dos formas de evaluar los riesgos están son cualitativa que determina un nivel bajo, medio y alto, o cuantitativa que asigna puntuaciones.

RISK: SG4.SP2 Categorizar y priorizar riesgos

Con la categorización se logra priorizar los riesgos para manejarlos de manera eficiente, en el proceso de mitigación.

RISK: SG4.SP3 Asignar disposiciones de riesgo

Las intenciones que toma la organización para hacer frente a los riesgos se considera como disposiciones de riesgo, acompañadas del desarrollo de estrategias para reducir al mínimo los riesgos.

Los riesgos que deben ser investigados o aplazados, serán examinados cuidadosamente para asegurar que no dará lugar a retrasos en la realización de la mitigación del riesgo o de los efectos sobre la resiliencia operativa (Caralli R. A., Allen, Curtis, White, & Young, 2010).

RISK: SG5 Mitigar y controlar riesgos.

La mitigación del riesgo consiste en el desarrollo de estrategias que buscan minimizar el riesgo a un nivel aceptable (Caralli R. A., Allen, Curtis, White, & Young, 2010).Los requisitos de resiliencia se revisan en la mitigación para evaluar su cumplimiento.

La mitigación del riesgo requiere a la organización para llevar a cabo dos acciones distintas: (1) desarrollar planes de mitigación de riesgo y (2) aplicar y supervisar estos planes para la eficacia (Caralli R. A., Allen, Curtis, White, & Young, 2010).

RISK: SG5.SP1 Desarrollar planes de mitigación de riesgos

El mantenimiento de activos y servicios se torna fundamental en la resiliencia operacional, ahora con la presencia de riesgos, el resultado de su evaluación "puede ser muy costoso en planes y actividades de reducción del riesgo, por lo que la organización debe tener en cuenta estos costos en el desarrollo del plan (Caralli R. A., Allen, Curtis, White, & Young, 2010)".

RISK: SG5.SP2 Implementar estrategias de riesgos

En el plan de mitigación se abarca la mayoría de riesgos categorizados, pero ¿Qué pasa cuando no constan algunos riesgos? Estos deben ser evaluados y revisados de forma periódica e incluso pueden necesitar disposiciones nuevas.

En la estrategia de gestión de riesgos se definen los intervalos en los que debe revisarse la situación de las estrategias de riesgo (Caralli R. A., Allen, Curtis, White, & Young, 2010).

RISK: SG6 Utilizar información de riesgos para administrar la resiliencia.

La información de riesgos que atentan contra la organización es un importante aporte a la validación de la seguridad y estrategias de resiliencia.

RISK: SG6.SP1 Revisar y ajustar las estrategias para proteger activos y servicios

Mejorar y mantener la resiliencia operacional de la organización depende de las lecciones aprendidas en la gestión de riesgos que se mejore los controles mediante la implementación de controles que faltan y actualizan los controles existentes para considerar los riesgos nuevos y emergentes (Caralli R. A., Allen, Curtis, White, & Young, 2010). Así al comparar los planes se detectan los controles que no mantienen un funcionamiento eficiente.

RISK: SG6.SP2 Revisar y ajustar las estrategias para mantener los servicios

Se mantienen los servicios si estos se consideran parte del plan de mitigación que se encarga de controlarlos.

La validación de los planes a través de los riesgos identificados también proporciona otro medio para garantizar la efectividad del plan para cubrir una amplia gama de posibles amenazas y riesgos operacionales (Caralli R. A., Allen, Curtis, White, & Young, 2010).

Desarrollo de requisitos de resiliencia (RRD).

Un requisito de resiliencia operacional es una restricción que la organización otorga a la capacidad productiva de un activo de gran valor para garantizar que siga siendo viable y se pueda sostener cuando está cargado en la producción para apoyar un servicio de alto valor (Caralli R. A., Allen, Cutis, White, & Young, 2010).

Los requisitos se caracterizan como restricciones que se deben de cumplir conjuntamente con los atributos de calidad (confidencialidad, integridad, disponibilidad) y los tipos de activos (personas, información, tecnología e instalaciones) propios de la resiliencia.

Objetivos y prácticas específicas.

RRD: SG1 Identificación de los requisitos empresariales.

Los requisitos empresariales se constituyen a partir de los requisitos que la organización impone en cuanto a funciones y actividades en base a las necesidades identificadas.

RRD: SG1.SP1 Establecer los requisitos de resiliencia empresarial

La identificación de riesgos e análisis de impacto generan resultados que servirán de guía para el establecimiento de requisitos, los cuales incluyen adicionalmente reglamentos, afiliaciones de negocios, políticas, convenios para el mantenimiento de datos y

restricciones, todos estos componentes forman y refuerzan la capacidad de recuperación de la empresa.

RRD: SG2 Desarrollar requisitos de servicio.

Existe cierta dependencia para el logro de la capacidad de recuperación, es así, que los servicios dependen de los activos asociados y de estos activos depende que se logre la misión del servicio, considerándose todos los tipos de activos como personas, información, tecnología e instalaciones. Ahora como fuentes para que se desarrolle los requisitos de servicio están los propietarios de los servicios los cuales para cumplir la resiliencia deberán trabajar conjuntamente con los propietarios de activos y en sí los requisitos de activos.

RRD: SG2.SP1 Establecer requisitos de resiliencia de activos

Los requisitos de activos se determinan en base a la contribución de los activos y el apoyo de los servicios resaltando así las necesidades de protección y continuidad que aseguran la coherencia y eficacia en la misión.

RRD: SG2.SP2 Asignar requisitos de resiliencia empresarial a servicios

Los requisitos de resiliencia empresarial son más rígidos que los requisitos de activos, pero cuando las necesidades empresariales se unen con los requisitos de activos pueden modificar dichos requerimientos.

RRD: SG3 Analizar y validar los requisitos.

Se garantiza la especificación correcta del nivel de resistencia de sus activos y la contribución a los servicios que se asocian.

RRD: SG3.SP1 Establecer una definición de los requisitos funcionales

Los requisitos se asocian con los controladores de la organización acorde a los servicios que apoyan y luego se traducen en planes de control de protección y continuidad.

RRD: SG3.SP2 Analizar los requisitos de resiliencia

Se analiza los requisitos de resiliencia para solventar conflictos entre las necesidades y funcionalidades que requieren los activos (información, tecnología e instalaciones) de modo que se identifique las necesidades que no se pueden cumplir.

RRD: SG3.SP3 Validar los Requisitos de Resiliencia

Se asegura la protección y sostenibilidad de los requisitos en cuanto a los activos y servicios asociados, lo cual implica riesgos que naturalmente son tratados.

Gestión de requisitos de resiliencia (RRM).

Busca garantizar que los requisitos del área de Desarrollo de Requisitos de Resilencia (RRD) permanezcan viables para cada activo de alto valor asociado con un servicio de alto valor hasta que se retiró, o hasta que se cambie debido a uno o más factores desencadenantes de organización

(Caralli R. A., Allen, Curtis, White, & Young , Resilience Requirements Management (RRM), 2010). Además, analiza y gestiona los cambios en los requisitos conforme lo requieran o sean necesarios, impulsando que la organización opte por las medidas de monitoreo del cumplimiento eficaz de los requisitos.

Objetivos y prácticas específicas.

RRM: SG1 Gestionar los requisitos.

Se identifica la existencia de inconsistencias en los requisitos, de modo que se pueda gestionar los cambios con las medidas correctivas apropiadas otorgando una visión general y compartida tanto a los propietarios como custodios, sin olvidar la relación entre los bienes y servicios.

RRM: SG1.SP1 Obtener un entendimiento de los requisitos de resiliencia

Se basa en el entendimiento que mantengan los propietarios y custodios de activos, así como los propietarios de servicios, esto en cuanto a la identificar y compartir necesidades. De hecho, es crucial el entendimiento común que deberán mantener los propietarios y custodios para la protección y mantenimiento del valor de los activos.

RRM: SG1.SP2 Obtener el compromiso de requisitos de resiliencia

Se mencionan dos acciones que garantizan la aplicación de los requisitos de resiliencia:

- Comunicarse a todos los custodios.
- Manejar la aplicación y gestión de los requisitos de resiliencia mediante un compromiso con los custodios.

Los propietarios deben asegurarse que los compromisos se han obtenido por parte de los custodios, tanto internos como externos a la organización para cumplir los requisitos

según lo previsto y lograr los requisitos a medida que cambian y evolucionan (Caralli R. A., Allen, Curtis, White, & Young , Resilience Requirements Management (RRM), 2010).

RRM: SG1.SP3 Gestionar cambios en los requisitos de resiliencia

Los cambios precipitan la capacidad de recuperación de activos por lo cual se identifica los factores que incitan el cambio evitando que se generen, pues se evalúa el impacto de los cambios en los requisitos de activos, se documentan y comunican a los custodios respectivos.

RRM: SG1.SP4 Mantener la trazabilidad de los requisitos de resiliencia

Esta práctica especifica la capacidad de la organización de rastrear las fuentes de sus requisitos de resiliencia, de modo que se pueda descubrir las relaciones de activos y requisitos de resiliencia en sus cardinalidades sea uno a uno, uno a muchos o inclusive muchos a muchos, así se evitará conflictos y se apoyará la productividad de la organización.

RRM: SG1.SP5 Identificar inconsistencias entre los requisitos de resiliencia y las actividades realizadas para cumplir los requisitos

Intervienen en gran medida los custodios como responsables de los requisitos asignados e implementar controles que identifiquen conflictos ayudando al mantenimiento de activos, "puesto que los activos pueden derivar los requisitos de más de una fuente (Caralli R. A., Allen, Curtis, White, & Young , Resilience Requirements Management (RRM), 2010) ".

Ingeniería de Soluciones Técnicas de Resiliencia (RTSE).

Los activos deben estar específicamente diseñados y desarrollados con la consideración del tipo de amenazas a las que se enfrentarán, las condiciones de funcionamiento y evolución del entorno de riesgo en el que van a operar determinando las prioridades y necesidades para mantener los servicios que apoyan (Caralli R. A., Allen, Curtis, White, & Young, Resilient Technical Solution Engineering (RTSE), 2010).

La mayoría de los software se desarrollan siguiendo los requisitos funcionales donde se especifica lo que el sistema debe hacer y como lo debe hacer tanto en la definición como en el diseño del sistema, pero los requisitos no funcionales también son de gran importancia y por lo tanto deben ser considerados al inicio del ciclo de vida del software y

no en la parte de ejecución donde por lo general para conseguirlos su costo es elevado, con menor eficacia y a un alto nivel de riesgo operacional.

Esto ocasiona que se disminuya la vida útil del software, así como su capacidad de recuperación, decepcionando el rendimiento esperado en la inversión.

¿Cómo se integrará la resiliencia? Se empieza con el desarrollo e integración de un plan de resiliencia en los procesos específicos del ciclo de vida del software, así conformará parte de la organización; se integra los atributos de calidad juntamente con los requisitos funcionales lo cual servirá para la identificación de requisitos de resiliencia y el diseño de arquitecturas que reflejen la capacidad de recuperación, seguridad, sostenibilidad, operatividad y sistema de activos.

¿Cómo se conseguirá la continuidad del sistema? Los controles servirán de pilar para asegurar la resiliencia, pues se mantendrá controles basados en la especificación de requisitos y diseño, de hecho se llegan a integrar los planes de continuidad del sistema como los planes de continuidad del servicios para asegurar la sostenibilidad de software, hardware y tecnología.

El desarrollo de requisitos, que analiza lo que desea el cliente en cuanto al software, lo que necesita el software para cumplir las necesidades del cliente y las características de los componentes finales, y la “solución técnica, cuyo objetivo es diseñar, desarrollar e implementar soluciones a los requisitos de software y del sistema” (Caralli R. A., Allen, Curtis, White, & Young, Resilient Technical Solution Engineering (RTSE), 2010), constituyen dos modelos de madurez del CMMI que se estudian en esta área.

Objetivos y prácticas específicas.

RTSE: SG1 Establecer directrices para el desarrollo de una solución técnica resiliente.

La seguridad y continuidad de procesos en el software se consideran como soluciones técnicas resilientes. De hecho, si se desea incorporar la resiliencia en el ciclo de vida del software, no es tarea fácil puesto que los requisitos de resiliencia deben ser relevantes, tratados tempranamente, analizados y planificados para y durante todo el ciclo de vida, el diseño del software y sistema, a más de satisfacer los requisitos de resiliencia deben ser prácticos y operacionales libres de amenazas, mantenidos a través del monitoreo constante y con la ayuda de la gestión de cambios y configuración.

Sin embargo, se obtendrá una base consistente cuando se institucionalice la resiliencia en el proyecto de software que exige la documentación de requisitos según las directrices planteadas garantizando coherencia y cumplimiento de los requisitos de resiliencia de la organización.

RTSE: SG1.SP1 Identificar directrices generales

Estas directrices se tratan durante todo el ciclo de vida del software, siendo una directriz diferente por cada etapa basadas en el entorno de producción, la continuidad de las operaciones, análisis de riesgos, y más aspectos que incumbe la resiliencia.

RTSE: SG1.SP2 Identificar directrices de requisitos

Los requisitos se identifican y refinan de acuerdo a las necesidades que el desarrollo del software necesita, pues el sistema resultante deberá apoyar la continuidad del servicio, además será necesario el desarrollo de métodos y escenarios que traten las amenazas y validen los requisitos funcionales, lo cual evitará los ataques y apoyará capacidad de recuperación.

RTSE: SG1.SP3 Identificar directrices de arquitectura y diseño

Dada la existencia de condiciones y ambientes cambiantes hacen necesario que la arquitectura y diseño de directrices sea eficaz, lo cual orientará y apoyará la toma de decisiones, interoperabilidad, continuidad del servicio, y de más operaciones que garanticen el funcionamiento de los servicios de alto valor en momentos de estrés.

RTSE: SG1.SP4 Identificar directrices de implantación

En la implantación se garantiza que los requisitos de resiliencia se cumplen y se valida la arquitectura y diseño del sistema. Este incluye normas, herramientas que validan el cumplimiento de las normas y elimine vulnerabilidades. Puesto que esta fase va de la mano con las pruebas, se utiliza varias técnicas de prueba, como las de caja negra y caja blanca, que son las más utilizadas para comprobar que los requisitos de resiliencia se cumplen.

RTSE: SG1.SP5 Identificar directrices de montaje y de integración

Los límites de capacidad de recuperación nacen como respuesta a los servicios "just-in-time" que incrementan la eficiencia y eficacia empresarial, de esta manera se evita errores en el montaje de integración del diseño, gestión inadecuada de servicios, desajustes

arquitectónicos, el uso de activos en entorno imprevistos, desconfianza en el uso de redes, y demás preocupaciones sobre la privacidad y aseguramiento de la información de los usuarios.

RTSE: SG2 Desarrollar planes de desarrollo de soluciones técnicas de resiliencia.

Los planes deberán ser conocidos dentro del ciclo de vida de desarrollo del software, ya que describe las directrices propias para hacer frente a la resiliencia y monitorear el nivel de consideración y cumplimiento de los requisitos de resiliencia en las etapas de diseño y ejecución, incluyendo previamente el montaje y la integración que se habla en la práctica anterior.

RTSE: SG2.SP1 Seleccionar y adaptar directrices

Al mantener buenos criterios, estables sobre todo, la adaptación de directrices en el ciclo de vida de desarrollo de software será menos complicados al contar con valores relativos de activos y requisitos de resiliencia logrando más eficiencia.

RTSE: SG2.SP2 Integrar la selección de directrices con una definición de software y procesos de desarrollo de sistemas

Los modelos de procesos de software generalmente no incluyen la resiliencia por lo que son incapaces de resistir y recuperarse ante eventos perjudiciales afectando los servicios y procesos, entonces se define, gestiona y mejora el software al incluir planes de continuidad asegurando la capacidad de recuperación que ofrece la resiliencia operacional.

RTSE: SG3 Ejecutar el plan.

Por medio del plan se controla el ciclo de vida de desarrollo, presentando informes de ejecución en cada hito, ya que se mantiene el monitoreo periódico que comprueba el cumplimiento de los requisitos de resiliencia.

RTSE: SG3.SP1 Supervisar la ejecución del plan de desarrollo

La desviación del plan con respecto a la capacidad de recuperación debe ser analizada para comprender el impacto potencial sobre el proyecto, el software, el sistema y la organización (Caralli R. A., Allen, Curtis, White, & Young, Resilient Technical Solution Engineering (RTSE), 2010).

Durante la ejecución del plan se pueden presentar algunos inconvenientes, por lo cual la organización evaluará la consistencia de los procesos y actividades asegurando la capacidad de recuperación.

RTSE: SG3.SP2 Liberar soluciones técnicas resilientes en producción

Generalmente los criterios son documentados, sin documentación no se puede formalizar ningún criterio o directriz, ahora antes de liberar producciones se utilizará los casos de prueba para evaluar si cumplen con los requisitos de resiliencia.

Continuidad del servicio (SC)

La organización puede invertir mucho tiempo y recursos en el intento de evitar una serie de posibles acontecimientos perturbadores, pero ninguna organización puede mitigar todos los riesgos.

Sin embargo la organización debe estar preparada para enfrentar las posibles interrupciones que se presenten, es así que para mantener un servicio de alto valor están los planes de contingencia y para regresar los servicios a un estado inicial aceptable en el que se encuentran los planes de recuperación y restauración.

Objetivos y prácticas específicas.

SC: SG1 Prepararse para la continuidad del servicio.

Se establece métodos para preparar a la organización para acoger e implementar la continuidad guardando coherencia y sostenibilidad.

SC: SG1.SP1 Plan de continuidad del servicio

Asegura que se cumpla con la misión de la organización a pesar que existan interrupciones internas o externas en los servicios.

Al alinearse con los objetivos estratégicos, se hace necesario el mantenimiento de activos y servicios, pues necesita patrocinio por parte de la organización, además su estructura deberá ser escalable y flexible de modo que pueda ser implementado y administrado como un programa de continuidad de servicio.

SC: SG1.SP2 Establecer criterios y directrices para la continuidad del servicio

Directrices y normas también proporcionan a la organización una capacidad de ver la continuidad del servicio a nivel empresarial y gestionar esta función para cumplir con las

metas organizacionales (Caralli R. A., Allen, Curtis, White, & Young, Service Continuity (SC), 2010).

Además de proporcionar estándares y documentar la conformidad de elementos de continuidad del servicio.

SC: SG2 Identificar y priorizar los servicios de alto valor.

Se torna importante el identificar dependencias de servicios y priorizar servicios antes del desarrollo del plan de continuidad de modo que sirvan también como línea base; a partir de la cual se puede evaluar la eficacia del plan y en la resiliencia operacional se analiza lo que es el coste de su gestión.

SC: SG2.SP1 Identificar servicios de calidad de la organización

Identificación de servicios de calidad, sus activos asociados, así como las actividades que soportan estos servicios deben realizarse antes que la organización intente desarrollar planes de continuidad del servicio (Caralli R. A., Allen, Curtis, White, & Young, Service Continuity (SC), 2010). Donde se incluye también la priorización de servicios de alto valor disminuyendo el impacto de riesgos fortaleciendo la seguridad.

SC: SG2.SP2 Identificar dependencias e interdependencias internas y externas

Se determina los niveles de dependencia activos y servicios, así como alianzas externas, que serán considerados en el plan de continuidad de servicio en la organización.

SC: SG2.SP3 Identificar registros y bases de datos vitales de la organización

Los activos de información de alto valor (registros civiles y bases de datos) son esenciales para el desarrollo de los planes de continuidad.

Cuando se produce una interrupción, para proteger derechos legales y financieros tanto de la organización como de las personas se trata de un registro vital en planes de continuidad, en cambio las operaciones con tipos de información relacionadas a servicios específicos se considera como base de datos donde se mantiene inventarios integrales.

SC: SG3 Desarrollar planes de continuidad de servicio.

Para gestionar las consecuencias de las interrupciones están los planes de continuidad del servicio que se basa en la gestión de riesgos con añadidura de lecciones aprendidas que soportan la resiliencia operacional.

El tiempo de respuesta será inmediato a la interrupción de modo que se mantenga y protege el funcionamiento del servicio sin obstaculizar el cumplimiento de los requisitos de resiliencia. Aunque este plan es muy eficiente y provechoso para la organización, su costo es elevado por lo que se debe evaluar y mantener equilibrado con los procesos de control.

SC: SG3.SP1 Identificar la elaboración de planes

Según mencionan (Caralli R. A., Allen, Curtis, White, & Young, Service Continuity (SC), 2010) algunos medios de identificar la continuidad del servicio, que incluyen cursos regulares de diseñar e implementar los requisitos de resiliencia, evaluaciones de riesgos, análisis de impacto de riesgos en la organización, auditorías legales, regulaciones y niveles de cumplimiento.

SC: SG3.SP2 Desarrollar y documentar planes de servicio continuo

La organización, propietarios del servicio, personal de TI son algunos encargados del desarrollo del plan de continuidad los cuales varían de acuerdo a la organización, al igual que el contenido del plan y los requisitos de documentación. Todo ello relacionado con las normas y directrices de continuidad.

¿Cuándo desarrollar un plan de continuidad? Se desarrollan estos planes cuando se detectan nuevos riesgos, cambios aunque generalmente van a la par con el desarrollo y ejecución de servicios.

SC: SG3.SP3 Asignar personal para planes de continuidad de servicio

El personal interno como externo que intervenga en la ejecución del plan debe contar con las capacidades necesarias para desarrollar las actividades encomendadas, y en caso de no contar con las capacidades suficientes, pues la organización tendrá que capacitarlos y evaluarlos al final de la misma para cerciorarse que ya son aptos para desempeñar sus actividades y cumplir con los objetivos del plan.

SC: SG3.SP4 Almacén y servicio seguro de planes de continuidad

La accesibilidad y viabilidad se tornan fundamentales puesto que la organización deberá otorgar el conocimiento de la ubicación de los planes de continuidad así como de sus últimas versiones, confidencialidad y evitar modificaciones por parte de terceros.

Además estos planes de continuidad pueden ser inventariados en una base de datos garantizando el acceso, control de versiones, planes de mantenimiento y control de cambios.

SC: SG3.SP5 Desarrollar servicios continuos de planes de capacitación

La organización deberá determinar las carencias de capacidades del personal que forma parte del plan de continuidad, para que pueda determinar en que está fallando y mejorarlo por medio de capacitaciones, de modo que se cumpla con los objetivos determinados en el plan.

SC: SG4 Validar planes de continuidad de servicios.

Se asegurará el cumplimiento de normas y directrices de la organización por medio de validaciones, que deben satisfacer las necesidades de capacidad de recuperación, evitando conflictos en los recursos.

SC: SG4.SP1 Validar planes para requisitos y estándares

Para cumplir los requisitos de capacidad de recuperación de activos y servicios se desarrollan los planes de continuidad, con niveles constantes de documentación y revisiones lógicas, con estas estrategias se corregirá incoherencias e imperfecciones del plan.

SC: SG4.SP2 Identificar y resolver conflictos del plan

Los planes de continuidad generalmente se ejecutan en una instalación abarcando todos los procesos, pero cuando se tiene más de un plan ejecutándose en la misma instalación este plan puede fallar al cumplir los requisitos de continuidad. Estos conflictos generan riesgos operacionales que pueden afectar a más de un plan así que deberán ser mitigados por cada plan.

SC: SG5 Ejercicio de planes de continuidad de servicio.

Una vez que se valida los planes de continuidad de servicios deberá ser probados, de modo que se compruebe que efectivamente funcionan ante interrupciones y se logre el cumplimiento de los objetivos de prueba.

SC: SG5.SP1 Desarrollar programas y estándares de prueba

¿Cómo comprobar si los planes lograrán cumplir los objetivos? Se podrá comprobar por medio de un programa de pruebas ejecutadas en ambientes controlados, sometidos a las normas de pruebas que establece la organización y con horarios de pruebas que se determinan en base a los factores de riesgo y posibles consecuencias para la organización.

SC: SG5.SP2 Desarrollar y documentar planes de prueba

Los planes de prueba de continuidad de servicio deberán ser documentados para asegurar que todos los involucrados en una prueba comprender los objetivos de la prueba, su papel en la prueba, y la manera en que se llevará a cabo la misma (Caralli R. A., Allen, Curtis, White, & Young, Service Continuity (SC), 2010).

Además, se establecen los objetivos de prueba y detalla la información específica sobre los participantes y entorno de la prueba.

SC: SG5.SP3 Planes de prueba

Los planes de prueba rigen los planes de continuidad para demostrar si se caracteriza o no como un plan eficaz. Estas pruebas establecerán la exactitud, precisión, viabilidad y calidad del plan.

Los interesados y participantes deberán conocer sus papeles dentro del plan a más de estar capacitados para ser parte de la prueba.

SC: SG5.SP4 Evaluar los resultados del plan de pruebas

Estos resultados se comparan con los objetivos del plan, de modo que sirven para conocer el nivel de exactitud del plan y se establecerá mejoras en el caso que las necesite.

SC: SG6 Ejecutar planes de continuidad de servicio.

Los planes de continuidad pueden aplicarse por varias razones como respuesta ante un incidente o razones menos prioritarias.

Cualquiera que sea el catalizador para la ejecución del plan, la organización debe ser capaz de determinar cuándo se debe ejecutar el plan y quién es responsable de iniciar la acción.

SC: SG6.SP1 Ejecutar planes

Las condiciones organizativas son las que solicitan la ejecución de los planes, los cuales entregarán documentados los resultados.

SC: SG6.SP2 Medir la efectividad del plan de operaciones

Se lo puede realizar aplicando la famosa técnica del interrogatorio, el cual es de suma importancia para detectar las fallas del plan, proponer y desarrollar mejoras. Además se podrá comparar la documentación resultante con las expectativas del plan.

SC: SG7 Mantener planes de continuidad del servicio.

Por los cambios en los planes de continuidad como de pruebas que pueden desarrollar en la organización, se deberá "establecer criterios de referencia para los cambios y gestionar los cambios en los planes a través de revisiones periódicas, actualización y control de versiones (Caralli R. A., Allen, Curtis, White, & Young, Service Continuity (SC), 2010)".

SC: SG7.SP1 Establecer criterios de cambios

La vida útil de los planes de continuidad se acortan por los cambios que sufren como: cambios en un servicio, actores del plan, líneas de negocio, obligaciones legales, y demás cambios significativos que afectan la organización.

SC: SG7.SP2 Mantener cambios en los planes

Por cada cambio en los planes se crea una versión de acuerdo a las normas de versionamiento de la organización, estos cambios serán informados a las partes interesadas, según como sea necesario.

Gestión de tecnología (TM)

El propósito de la gestión de tecnología es establecer y administrar un nivel adecuado de controles relacionados con la integridad y disponibilidad de los activos de la tecnología para apoyar la operación de resiliencia de los servicios de la organización (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

La tecnología se considera como activo de gran importancia en la organización. Esto es debido a que los activos tecnológicos apoyan directamente la automatización e incluso eficiencia de los servicios, además puesto que está estrechamente ligada a los activos de información, ya que proporciona las plataformas en las que se almacena la información,

transportada o procesada. Es por ello que para algunas organizaciones la tecnología es considerada como un elemento prominente de estrategia.

Desde una amplia perspectiva, la tecnología describe cualquier componente tecnológico o bien que los apoya o automatiza un servicio y facilita su capacidad para cumplir su misión. La tecnología tiene diferentes niveles que son específicos de un servicio (por ejemplo, un sistema de aplicación) y otros que son compartidos por la organización (por ejemplo, la infraestructura de red de toda la empresa) para apoyar a más de un servicio.

Las organizaciones deben describir los activos de tecnología suficientes como para facilitar el desarrollo y la satisfacción de los requisitos de la operación de resiliencia; por tanto se puede considerar que el área de proceso de la gestión de tecnología a más que referirse a los activos tecnológicos, también incluye su integridad y gestión de la disponibilidad, porque esta no solo se extiende hacia los límites internos de la organización, sino también hacia los externos.

Objetivos y prácticas específicas.

TM: SG1 Establecer y priorizar los activos de tecnología.

En este objetivo, la organización establece el subconjunto de los activos de tecnología (a partir de su inventario de activos de tecnología) en los que debe centrarse la actividad de resiliencia debido a su importancia para el funcionamiento sostenido de los servicios esenciales.

La priorización de los activos de tecnología es una actividad de gestión de riesgo, por lo que se establece los activos de tecnología de mayor valor e importancia para la organización y a su vez para su respectiva medida, protección y sostenimiento requeridos.

Los activos de tecnología son de alta prioridad para la organización y por tanto no considerarlos como tales puede ocasionar una inadecuada operación de resiliencia de altos valores, o a su vez un exceso, en los altos niveles de estos activos (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

TM: SG1.SP1 Priorizar los activos de tecnología

Los activos de tecnología se priorizan en relación con su importancia en el apoyo y soporte a la prestación de servicios de alto valor.

La priorización de los activos de tecnología debe realizarse con el fin de asegurar que la organización dirija adecuadamente su capacidad operacional de resiliencia de los recursos a los activos que afectan más directamente y contribuyan a los servicios en el soporte de la misión de la organización.

De esta forma se tiene que la priorización de los activos de tecnología está relacionada directamente a los servicios y sus correspondientes niveles de valores en las actividades de operación de resiliencia (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010), de manera similar que los activos de información.

TM: SG1.SP2 Establecimiento de los activos de tecnología centrados en la resiliencia

Los activos de tecnología que específicamente apoyan la ejecución de un servicio continuo y los planes de restauración de los mismos son identificados y categorizados.

Los planes de servicio continuo requieren altamente de los activos de tecnología para su exitosa ejecución; los cuales pueden ser los que están en producción u otros que han sido designados para propósitos de resiliencia.

Los activos de tecnología para la resiliencia pueden ser contratados o proporcionados por una entidad externa; por tanto estos activos deben ser incluidos en una lista de activos tecnológicos para propósitos de resiliencia y por tanto ser protegidos adecuadamente (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

TM: SG2 Protección de los activos de tecnología.

Los activos de tecnología son de vital importancia para la organización; ya que, ésta puede tener cientos o miles de servicios que son soportados o automatizados por dichos activos. Una principal complicación que se presenta a la organización es que muchos de estos activos pueden no ser propios de la organización y por tanto no tener el control y protección directos de los mismos.

Por tanto, mantener productivos los activos de tecnología, constituye un gran esfuerzo de la organización debido a que estos activos están directamente relacionados con el éxito de la misión de los servicios. He ahí que la integridad del activo es de suma importancia, por cuanto se garantiza fuertemente el cambio en procesos, configuración, controles y protección de los activos de tecnología de acceso indebido o no autorizado (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

TM: SG2. SP1 Asignar requisitos de resiliencia a los activos de tecnología

Los requisitos de resiliencia son la base de las acciones que la organización toma para proteger y mantener los activos de tecnología. Estos requisitos son establecidos de acuerdo con el valor de los activos para servicios a los que apoya; de esta manera se tiene que ellos tienen que ser asignados de acuerdo con los niveles apropiados para ser diseñados, implementados y monitoreados en concordancia con el cumplimiento de los mismos (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

Con los activos de tecnología puede existir instancias de conflicto en cuanto a estos requisitos porque muchos de ellos son activos compartidos por uno o más servicios y estos a su vez relacionados con los activos de información que contengan datos clasificados, categorizados o requisitos confidenciales. Por tanto, esta situación debe considerarse y analizarse en el momento de asignar los requisitos de resiliencia, con la intención de que los activos de tecnología asignados sean capaces de satisfacer dichos requisitos.

TM: SG2.SP2 Establecer e implementar controles

La organización debe implementar un sistema de control interno de tal forma que proteja y mantenga el funcionamiento esencial de los activos de tecnología de acuerdo con su rol en el apoyo y soporte a los servicios esenciales de la organización (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

Los controles son esencialmente los métodos, políticas y procedimientos que la organización utiliza para proteger y mantener el alto valor de los activos en un nivel aceptable. Existen por lo general tres categorías en los que generalmente fallan estos controles: administrativa, técnica y física.

Es notable considerar que la operación de resiliencia envuelve un amplio rango de controles, que no solo incluyen lógicos y físicos, sino también los controles de dirección, disponibilidad y operatividad de la tecnología, fuera y dentro de la organización.

TM: SG3 Gestionar el riesgo de los activos de tecnología.

La gestión de riesgo para los activos de tecnología es una aplicación específica de las herramientas de gestión de riesgo, de las técnicas y métodos de estos activos, por tanto, es menester considerar que debido a la naturaleza, complejidad y distintas formas en que

se pueden encontrar estos activos; existen muchas oportunidades de que estos se vean amenazados y por ende la organización.

Los riesgos para los activos de tecnología pueden traer consecuencias para la organización, como puede ser la ruptura del alto valor de servicios debido a la falta de utilización de tecnología y la disponibilidad. Además la gestión de los riesgos de los activos de tecnología debe determinar los lugares en los que estos activos "viven", esto es, donde se almacenan, transportan o son procesados.

TM: SG3.SP1 Identificar y evaluar la información de riesgo de los activos de tecnología

La identificación de los riesgos en un activo de tecnología constituye una línea base con la cual continuamente el proceso de gestión de riesgos puede ser establecido y gestionado.

Los riesgos operativos que pueden afectar a los activos de tecnología deben ser identificados y mitigado con el fin de gestionar activamente la resiliencia de estos activos y, más importante, la resiliencia de los servicios con los que estos activos estén asociados (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

TM: SG3.SP2 Mitigar el riesgo del activo de tecnología

Se desarrollarán e implementarán estrategias de mitigación de riesgos para los activos de tecnología.

La mitigación de riesgo del activo de tecnología también encierra el desarrollo de estrategias que permitan buscar minimizar los riesgos a un nivel aceptable, lo cual requiere un extensivo y significativo análisis debido a la importancia que supone la tecnología para la organización. Esto incluye el desarrollo de un plan de servicio continuo de los activos de tecnología, reduciendo su exposición a riesgos, el funcionamiento viable durante los tiempos de ruptura, la recuperación, restauración y control de la dirección debido a las consecuencias de los riesgos.

TM: SG4 Gestionar la integridad de los activos de tecnología.

La integridad de los activos de tecnología debe ser gestionada; esta es importante por cuanto asegura su utilidad y propósito, ya que al verse comprometida esta integridad, toda la información, datos almacenados, transportados, o procesados por los activos de información también se encontraría potencialmente en peligro.

La integridad del activo de tecnología debe ser considerado en contexto con el tipo de activo (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

TM: SG4.SP1 Controlar el acceso a los activo de tecnología

El acceso a los activos de tecnología debe ser controlado por parte del personal autorizado, lo que garantiza la continua integridad de estos activos, al limitar su autorización o modificación involuntaria.

El control de acceso para estos activos de tecnología puede ser de forma electrónica o física.

Para la eficacia de este control, la organización debe seleccionar cuidadosamente el personal y miembros que estén autorizados a acceder a los activos de tecnología, hacer modificaciones e implementar controles electrónicos y físicos para cumplir estos requisitos.

La gestión del acceso es un control complementario a otro que está centrado en el control de la integridad de los activos de tecnología, como la gestión de configuración, y gestión de cambio.

TM: SG4.SP2 Desarrollo de gestión de configuración

La gestión de configuración es una actividad fundamental de la resiliencia. Esto soporta la integridad de los activos de tecnología, asegurando que puedan ser restaurados a una forma aceptable cuando sea necesario, además provee un nivel de control sobre los cambios que potencialmente podrían interrumpir los servicios de la organización.

La gestión de configuración de los activos de tecnología es un control primario de resiliencia, esto es clave para la reconciliación de los atributos técnicos y físicos con sus requisitos de resiliencia todo el tiempo. Esta gestión de configuración está estrechamente relacionada con la gestión de control de cambio, porque el control de cambio y su gestión es una actividad especializada, en particular para los activos técnicos, lo que frecuentemente es considerada una función separada con sus propias prácticas, herramientas, técnicas y métodos.

La gestión de la configuración puede ser abordada a nivel empresarial o específicamente para cada activo de la tecnología. La organización debe decidir el enfoque más eficaz y debe tener en cuenta el hecho de que la gestión de configuración de los diferentes tipos

de activos de tecnología (es decir, basada en software activos frente a los activos basados en hardware) pueden diferir considerablemente y requieren procesos separados.

TM: SG4.SP3 Gestionar y realizar el control de cambios

Esto significa, gestión de los cambios a los activos de tecnología. Definir y comunicar los procedimientos de cambio, incluyendo cambios de rutina y de emergencia, asegura que los cambios en los activos de tecnología serán manejados de manera eficiente y de forma controlada, de acuerdo con la política de la organización, normas y directrices, con el mínimo impacto para la integridad, la disponibilidad y, finalmente, la capacidad de recuperación de los activos y los servicios que soporta.

El control de cambios y su gestión define un proceso organizativo que presenta la estructura y rigor a realizar cambios en los activos de tecnología y proporciona un medio para el seguimiento de estos cambios por lo que los problemas pueden ser detectados y corregidos.

TM: SG4.SP4 Realizar gestión de entrega

Realizar gestión de entrega está estrechamente vinculado a la gestión de configuración y control de cambios. Mientras que el control de cambios aborda el proceso del ciclo de vida de la gestión de una solicitud de cambio, el resultado es a menudo una nueva "entrega" (*release*) de un activo de tecnología. Por lo tanto, la gestión de entrega soluciona las sucesivas versiones de entrega de los activos de tecnología, dentro de una operación y el medio de producción.

La gestión de entrega requiere de un proceso de planificación, construcción, pruebas y activos de tecnología, de despliegue, su versión asociada de control y almacenamiento.

Una pobre gestión de entrega puede disminuir la operación de resiliencia y el despliegue de los activos de tecnología, junto a sus versiones de control y almacenamiento de estos.

TM: SG5 Gestionar la disponibilidad de activos de tecnología.

La disponibilidad de un activo de información es fundamental para apoyar y soportar los servicios de alto valor; ya que a pesar de que la información almacenada, transportada, procesada por un activo de información pueda ser precisa y completa, pero si no está disponible inmediatamente o en un tiempo oportuno, el servicio puede no ser capaz de cumplir con su misión.

Existe una diferencia entre el tiempo de inactividad planificado y el tiempo de inactividad no planificado. El primero es generalmente el resultado de un usuario o de gestión de evento iniciado por el que ha sido sujeto al proceso de gestión de cambio; mientras que el tiempo de inactividad no planificado normalmente surge de eventos o incidentes fuera del control de la organización, tales como cortes de energía, las brechas de seguridad y los desastres como inundaciones o huracanes. El tiempo de inactividad no planificado es el efecto de disminución de la operación de resiliencia.

Muchos activos de tecnología pueden ser replicados utilizando los activos de repuesto o de fácil adquisición, aunque el costo es una consideración de algunos activos. Para controlar eficazmente el entorno operativo de activos de tecnología, la organización debe realizar varias actividades. Ante todo, la organización debe planificar mantenimiento de los activos tecnológicos para asegurar la continuidad del funcionamiento de los servicios.

TM: SG5.SP1 Realizar un plan de sostenimiento de los activos de información

La disponibilidad y funcionalidad de los activos de tecnología de alto valor, es asegurado a través del desenvolvimiento de planes de mantenimiento de estos.

La planificación de sostenimiento de los activos de tecnología se puede integrar en el desarrollo de planes de continuidad del servicio, para los servicios o la instancia en los planes centrados específicamente en tecnologías de alto valor. Estos planes pueden ser desarrollados específicamente por el tipo de activos.

TM: SG5.SP2 Gestión del mantenimiento del activo de tecnología

En los activos de tecnología se realizará una gestión de mantenimiento operativo, esto es por cuanto el cumplimiento de los requisitos de disponibilidad de estos activos (en particular hardware) por lo general requiere la realización de un mantenimiento regular de actividades. Si bien estas actividades son típicamente de naturaleza física, algunos pueden ser virtuales o electrónicos. Los criterios utilizados para establecer pautas para el mantenimiento son realizados en relación con el valor de los servicios y su soporte relacionado.

En general los tipos de mantenimiento van de acuerdo con el tipo de activo de tecnología. A pesar de tener un regular mantenimiento de los activos de tecnología, lo cual asegura su disponibilidad, no obstante se debe prestar atención a riesgos adicionales, como errores inadvertidos o acciones deliberadas, por lo que es necesario que todo el

mantenimiento debe ser controlado, monitoreado y autorizado (Caralli R. A., Allen, Curtis, White, & Young, Technology Management (TM), 2010).

TM: SG5.SP3 Gestión de la capacidad de tecnología

La capacidad es un factor significativo en el cumplimiento de los requisitos de disponibilidad de los activos de tecnología y, a su vez de los servicios que dependen de estos activos. La capacidad operativa de los activos de tecnología debe ser gestionado acorde con las demandas operacionales de los servicios o de lo contrario estos pueden verse afectados en su operatividad.

La planificación y gestión de la capacidad consiste en la medición de la demanda, las pruebas para la demanda prevista y las tendencias de uso de recolección sobre el tiempo para ser capaz de predecir las necesidades de expansión. No obstante, es sustancial tener en cuenta que la demanda es muy variable y que la capacidad de los activos de tecnología puede ser necesaria para satisfacer una amplia gama de necesidades.

Por tanto, la planificación y gestión de la capacidad requiere una visión estratégica para asegurar la consideración de los objetivos estratégicos de la organización, así como satisfacción de requisitos de negocios y sistemas de servicio.

TM: SG5.SP4 Gestión de la interoperabilidad de tecnología.

Esto se refiere a la gestión de la interoperabilidad de los activos de tecnología, ya que estos raramente actúan aisladamente, sino que normalmente se dependen unos de otros de acuerdo con el servicio que soporten, de esta manera estos activos deben estar conectado y ser interoperables para cumplir con un objetivo compartido.

En realidad, la mayoría de las organizaciones tienen niveles significativos de tecnología en correspondencia con complejidad e interconexión entre sí, sobre todo en los activos, tales como la aplicación de sistemas.

El fracaso para identificar y abordar activamente los problemas relacionados con la interoperabilidad plantea un nivel adicional de riesgo operacional a la organización que puede resultar en la interrupción de los servicios de la organización. Desafortunadamente, los problemas relacionados con la interoperabilidad son a menudo desconocido hasta que sucede un resultado no deseado (por ejemplo, cuando el código de software falla o produce un resultado inesperado).

Por esto, la gestión de la interoperabilidad de los activos de tecnología requiere que la organización desarrolle y mantenga una estrategia para identificar, analizar y mitigar los riesgos operativos relacionados con la tecnología de la interoperabilidad de los activos (Caralli, Richard A.; Allen, Julia H.; Curtis, Pamela D.; White, David W.; Young, Lisa R., 2010).

B. **WBS**

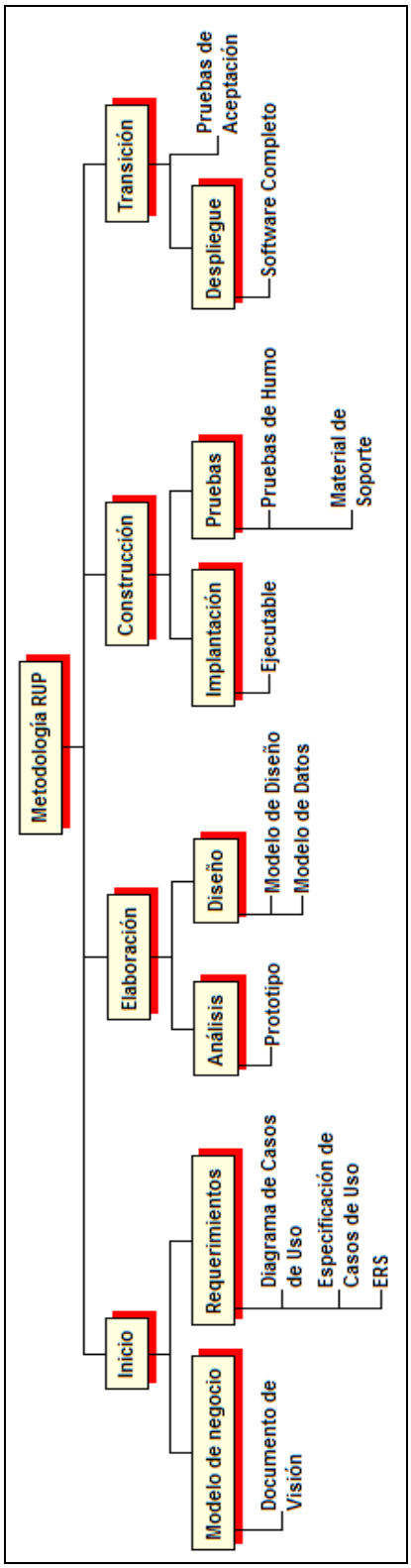


Figura 72. WBS SISGRES.

C. Cronograma

		Modo de	Nombre de tarea	Duración	Comienzo	Fin	% completado
1	✓		**Desarrollo de una Guía Metodológica de Elicitación de Requisitos sobre Sistemas de Información para el manejo de Resiliencia enfocado en los activos del modelo CERT-RMM.**	**210 días?**	**mié 26/06/13**	**mar 15/04/14**	**100%**
2	✓		Reunión inicial de proyecto	0,5 días	mié 26/06/1:	mié 26/06/1:	100%
3	✓		**Estado del arte sobre la Elicitación de Requerimientos y las áreas del Modelo Resiliencia CERT-RMM.**	**46 días**	**mié 26/06/13**	**jue 29/08/13**	**100%**
10	✓		**Desarrollo de la Guía Metodológica en base a las Áreas del modelo de resiliencia CERT-RMM.**	**83 días?**	**jue 29/08/13**	**lun 23/12/13**	**100%**
26	✓		**Implementación de la Guía a través de un Sistema de Información**	**47 días**	**mar 24/12/13**	**jue 27/02/14**	**100%**
33	✓		**Verificación de la Aplicabilidad de la Guía Metodológica**	**23 días**	**jue 27/02/14**	**mar 01/04/14**	**100%**
37	✓		**Entrega Final**	**10 días**	**mié 02/04/14**	**mar 15/04/14**	**100%**

Figura 73. Cronograma de actividades para el desarrollo de la guía.

D. Documento de visión

SISGRES - Sistema de Gestión de Resiliencia de Software
Documento de Visión

Historial de Revisiones

Fecha	Versión	Descripción	Autor
12-Octubre-2013	1.0	Creación del documento de Visión	Jackeline Palacios
22-Octubre-2013	1.0	Corrección del documento de Visión	Jackeline Palacios
14-Noviembre-2013	1.0	Corrección del documento de Visión	Jackeline Palacios
16-Noviembre-2013	1.0	Corrección del documento de Visión	Jackeline Palacios
20-Noviembre-2013	1.0	Corrección del documento de Visión	Jackeline Palacios

1. Introducción

1.1. Propósito.

El propósito de este documento es mejorar la captura de requerimientos de software resiliente a partir de plantillas diseñadas de acuerdo a la Metodología CERT-RMM, con el objetivo de evaluar el sistema de información (SI) de una organización para conocer su estado de resiliencia.

1.2. Alcance.

El SI tendrá apertura para dos tipos de usuarios: el usuario administrador que controlará los usuarios y cuestionarios, y el usuario cliente que resolverá los cuestionarios y al culminar obtendrá sugerencias para incluir la resiliencia en su SI.

1.3. Definiciones, Siglas y Abreviaturas

- **CERT:** Modelo de capacidad para la gestión de resiliencia operativa.
- **RMM**: Modelo de gestión de resiliencia.
- **SIGRES:** Sistema de Gestión de Resiliencia CERT-RMM.
- **RUP:** Metodología para la descripción del proceso de desarrollo de software.

2. Posicionamiento

2.1. Oportunidad de negocio.

El sistema SIGRES permitirá evaluar el SI y obtener criterios para alcanzar un estado de resiliencia, lo cual supondrá resultados eficientes que ayuden a mantener un SI confiable, continuo y seguro.

El sistema se desarrollará tipo web con interfaces gráficas de fácil percepción, agilidad en los procesos, respuesta inmediata e interacción directa entre el usuario y el sistema.

2.2. Definición del problema.

El problema de	Los analistas y desarrolladores que no conocen el estado de resiliencia del SI de la organización. No contar con información que permita a los directivos de la organización conocer el estado de su SI para enfrentar interrupciones o casos de estrés.
Que afecta a	Analistas, Desarrolladores, Usuarios empresariales.
El impacto de ello es	Un proceso largo de estudio de todas las áreas de la metodología CERT.
Una solución	Desarrollar e implementar un sistema web utilizando el Modelo

exitosa debería	de Gestión de Resiliencia CERT-RMM como base para evaluar el nivel de resiliencia de los SI del software y proponer sugerencias que ayuden a mejorar su funcionamiento.

3. Descripción de los interesados y usuarios

3.1. Resumen de los interesados.

Los interesados son todas aquellas personas directamente involucradas en la definición y alcance de este proyecto. A continuación se presenta la lista de los interesados*:*

Nombre	Descripción	Responsabilidad
Director del proyecto	Establece los lineamientos generales para el desarrollo del proyecto.	Otorgar dirección al proyecto. Evaluar el avance del proyecto.
Analista de sistemas	Responsable del proyecto que desarrolla los artefactos claves del proyecto de software.	Analizar y describir las necesidades que el sistema debe satisfacer.
Arquitecto de aplicaciones	Responsable del diseño que mantendrá el sistema.	Realizar el diseño del SI.
Programador	Encargado de la programación del código fuente del sistema.	Codificar el sistema de acuerdo a los requisitos.
Aseguramiento de Calidad	Evalúa el sistema garantizando que las normas de calidad se cumplen sobre el sistema y el manejo de los datos.	Realizar seguimiento a los procesos. Validar que el funcionamiento del sistema cumpla con estándares de calidad.
Directivo de la empresa	Cliente del proyecto.	Interactuar en el sistema.

3.2. Resumen de los usuarios.

Los usuarios son todas aquellas personas involucradas directamente en el uso del sistema SIGRES. A continuación se presenta una lista de los usuarios:

Nombre	Descripción	Responsabilidad
Administrador del sistema	Persona del que administra el sistema.	Administrar funcionalmente el sistema (gestionar usuarios y

Nombre	Descripción	Responsabilidad
		cuestionarios).
Directivo de la empresa	Persona que hará uso del sistema.	Responder los cuestionarios. Consultar los resultados de la evaluación.

3.3. Entorno de usuario.

Los usuarios ingresarán al sistema identificándose sobre un ordenador con cualquier sistema operativo puesto que se trata de una aplicación web y tras este paso entrarán a la parte de aplicación diseñada para cada uno según su papel en la empresa. Este sistema es de fácil percepción así que familiarizarse con el mismo será una tarea fácil.

Los resultados serán generados a partir de los datos proporcionados por los usuarios y almacenados en la base de datos.

3.4. Perfiles de los interesados

3.4.1. *Director del proyecto.*

Representante	Ing. Danilo Jaramillo
Descripción	Director del proyecto.
Tipo	Director
Responsabilidades	Establecer los lineamientos generales para el desarrollo del proyecto.
Criterio de éxito	Vigilar el cumplimiento del cronograma de trabajo.
Implicación	Jefe de proyecto (Project Manager)
Entregable	N/A
Comentarios	Mantener una relación constante con el desarrollo del proyecto. Brindar apoyo a nivel gerencial cuando sea necesario.

3.4.2. Analista del proyecto.

Representante	Analista
Descripción	Analista del proyecto.
Tipo	Desarrollo del proyecto.
Responsabilidades	Analizar y describir las necesidades que el sistema debe

	satisfacer.
Criterio de éxito	Plantear soluciones óptimas para cubrir las necesidades del sistema.
Implicación	Stakeholder
Entregable	Documento de Visión Casos de Uso Especificación de Requisitos
Comentarios	Mantener una idea clara de las necesidades del cliente.

3.4.3. Arquitecto del sistema.

Representante	Arquitecto de aplicaciones
Descripción	Arquitecto del proyecto.
Tipo	Desarrollo del proyecto.
Responsabilidades	Realizar el diseño del sistema.
Criterio de éxito	Desarrollo de una arquitectura flexible para el sistema.
Implicación	Stakeholder
Entregable	Modelo de Diseño Modelo de Datos Prototipo
Comentarios	Mantener una relación constante con los componentes del proyecto.

3.4.4. Desarrollador del proyecto.

Representante	Jackeline Palacios
Descripción	Desarrollador del proyecto.
Tipo	Desarrollador
Responsabilidades	Codificar el sistema en base a los requerimientos especificados.
Criterio de éxito	Cumplir con el cronograma determinado. Funcionamiento correcto del sistema.
Implicación	Stakeholder
Entregable	Ejecutable

	Manual de usuario. Capacitaciones.
Comentarios	Mantener una relación constante con el desarrollo del proyecto.

3.4.5. Aseguramiento de calidad del proyecto.

Representante	QA
Descripción	Evaluación del proyecto.
Tipo	Analista de calidad
Responsabilidades	Validar el cumplimiento y funcionamiento del sistema acorde con los requerimientos.
Criterios de éxito	Informe correcto de las inconsistencias del sistema.
Implicación	Stakeholder
Entregables	Casos de Pruebas Informe
Comentarios	Coordinar las pruebas de validación del nuevo sistema.

3.4.6. Directivo de la empresa contratante.

Representante	Directivo de la empresa contratante
Descripción	Cliente del proyecto.
Tipo	Directivo de la empresa.
Responsabilidades	Interactuar en el sistema.
Criterios de éxito	Informe correcto de las inconsistencias del sistema.
Implicación	Stakeholder
Entregables	Casos de Pruebas Informe
Comentarios	Coordinar las pruebas de validación del nuevo sistema.

3.5. Perfiles de usuario.

3.5.1. Administrador del sistema.

Representante	Jackeline Palacios
Descripción	Administrador del sistema SIGRES
Tipo	Usuario Experto.
Responsabilidades	Administrar funcionalmente el sistema: gestionar acceso a usuarios, dar mantenimiento al sistema frente a nuevos requerimientos.
Criterios de éxito	Mantener el sistema en buen funcionamiento y cumpliendo con los requerimientos solicitados.
Implicación	Desarrollar los artefactos e implementar el sistema.
Entregables	Ninguno
Comentarios	Mantener relación con todos los usuarios implicados.

3.5.2. Directivo de la *empresa.*

Representante	Cliente
Descripción	Personal que hará uso del SISGRES.
Tipo	Usuario casual.
Responsabilidades	Ejecutar los procedimientos del sistema. Realizar evaluación.
Criterios de éxito	Obtener un sistema amigable que cumpla con las necesidades presentadas.
Implicación	Ninguna
Entregables	Ninguno.
Comentarios	Ninguno.

3.6. Necesidades de los interesados y usuarios.

Necesidades	Prioridad	Inquietudes	Solución Actual	Solución propuesta
Control de acceso al sistema a través de claves de Usuario.	Alta	El control de acceso debe verificar que las claves correspondan	NO EXISTE	Desarrollar un control en base a roles de usuarios.

		a las credenciales de los usuarios.		
Manejar dos tipos de usuarios en el sistema.	Alta	Identificar y restringir las operaciones de los usuarios al gestionar de la información.	NO EXISTE	Gestionar dos roles, un rol de cliente que maneja el cliente con privilegios de lectura y escritura sobre los cuestionarios, y otro rol de administrador que cuente con todos los privilegios como son: lectura, escritura y ejecución sobre los usuarios y cuestionarios.
Levantar información acerca del estado de resiliencia del SI.	Alta	Las preguntas deben ser claras y concisas.	NO EXISTE	Elaborar preguntas para la elicitación en base a la metodología CERT, características de resiliencia y técnicas de elicitación.
Gestionar información de usuarios y cuestionarios.	Alta	Se debería registrar y actualizar información de usuarios y cuestionarios.	NO EXISTE	Desarrollar funciones de registro, eliminación y actualización de información, accesible a los usuarios permitidos.
Guardar información de usuarios y cuestionarios.	Alta	Guardar toda la información recolectada para estudios posteriores.	NO EXISTE	Manejar una base de datos MySQL para el almacenamiento de la información.
Conocer si el SI presenta algún nivel de resiliencia.	Alta	Se debe tomar los resultados de la elicitación para evaluar si el software es resiliente.	NO EXISTE	Comparar la información resultante con los lineamientos del CERT, para conocer si existe algún nivel de resiliencia en la empresa.

Implementar estrategias para proteger el software ante riesgos.	Alta	Los resultados deben aportar alguna ayuda para mejorar el SI.	NO EXISTE	En base a los resultados y tomando la metodología CERT, emitir sugerencias que puede incluir el SI.
El sistema debe de ser de fácil percepción para los usuarios.	Alta	Cumplir con todos los requisitos de los usuarios.	Desarrollo con la ayuda de los expertos en el tema.	Desarrollar la interfaz del sistema tomando en cuenta los requisitos del cliente, facilitar la interoperabilidad y tomar la resiliencia como herramienta de apoyo.

4. Vista General del Producto

4.1. Perspectiva del producto.

Este producto será un sistema web para evaluar el estado de resiliencia de una empresa, en el cual intervienen dos agentes fundamentales para el flujo de datos en el proceso que se describe a continuación:

Figura 74. Diagrama de Contexto SISGRES
Fuente: El autor.

4.2. Resumen de Capacidades.

Beneficios para el usuario	Características que lo soportan
Los clientes y administradores se pueden autenticar en el sistema.	El acceso al sistema a través de la Web permitirá a los usuarios un acceso inmediato desde cualquier punto geográfico.

Los clientes pueden resolver las preguntas de las áreas que crean convenientes.	Las preguntas son almacenadas en la base de datos y cargadas en el sistema.
El administrador puede controlar los usuarios que pueden interactuar en el SI.	El sistema provee el manejo de roles.
El administrador puede actualizar la información de usuarios y preguntas.	El sistema provee los formularios acordes a la interacción solicitada, con información actualizada y oportuna.
Los resultados pueden ser visualizados por los clientes luego de resolver los cuestionarios.	El sistema presentará las características de resiliencia en las que tenga aciertos y errores, así como las sugerencias por cada una de ellas.
Facilidades para el análisis de la información.	El sistema proveerá gran cantidad de información en base a la solución de los cuestionarios, que podrán ser utilizadas para análisis posteriores.
Verificación de información.	El sistema realiza la comparación de la información extraída con los lineamientos de la Metodología CERT-RMM. La verificación de datos permite evaluar el SI conforme a lineamientos de la resiliencia del software.

4.3. Características del producto.

Acceso al SI.

Los clientes y administradores deberán digitar una identificación válida para ingresar al sistema. A los clientes se les asignan su usuario y contraseña, por parte del administrador del sistema.

Consulta de información.

El administrador deberá visualizar una lista de todos los:

- Usuarios, incluidos clientes y administradores.
- Preguntas

El usuario cliente deberá visualizar:

- Preguntas
- Resultados

Registrar información.

El sistema permitirá el registro de usuarios y cuestionarios mediante formularios.

Actualizar información.

El sistema mostrará un formulario con la información de acuerdo a la opción seleccionada sea usuarios o cuestionarios.

Evaluación del SI.

El sistema presenta las preguntas, el cliente las resuelve de acuerdo a lo que crea conveniente.

Generar resultados.

En base a las respuestas de los cuestionarios, el sistema presentará: los aciertos y errores del SI con respecto a las características de resiliencia de software y sugerencias por cada característica para suplir los vacíos del SI.

Obtención inmediata de información.

Unos de los principales objetivos del SIGRES es presentar de manera oportuna la información concerniente al estado del SI, información que se utiliza para la toma de decisiones.

Facilidad de acceso y uso.

El SIGRES será de tipo web con interfaces bastante amigables lo cual facilitará el acceso e interacción del cliente en el SI.

Obtención de información detallada.

Las cargas de datos que realizará SIGRES, las hace de acuerdo a los accesos de los usuarios (cliente, administrador).

Acceso inmediato.

El sistema se encontrará disponible las 24 horas del día, los 365 días del año con lo que los usuarios podrán acceder a la información al momento que lo necesiten.

Gran cantidad de información.

Con la implementación web los accesos de usuarios aportarán varia información a la base para análisis posteriores.

Verificación de datos.

En base a la verificación de información se puede detectar oportunamente los errores encontrados en la evaluación de la empresa antes de emitir resultados erróneos.

5. Rangos de calidad

El desarrollo del Sistema SISGREC se ajustará a la Metodología de Desarrollo de Software RUP y a la Metodología de resiliencia CERT-RMM, contemplando los parámetros de calidad que las metodologías definan.

6. Precedencia y Prioridad

- Ingreso de datos.
- Verificación de datos.
- Realizar evaluación.
- Emisión de resultados.

7. Conclusiones y Recomendaciones

- La extracción de información se realiza con la ayuda de plantillas diseñadas en base a la metodología CERT-RMM.
- Las operaciones CRU son aplicables a usuarios y cuestionarios registrados en el sistema.
- Los informes resultantes se elaboran en base a la resolución de preguntas y lineamientos de la metodología.
- Toda la información de usuarios, preguntas y resultados son almacenadas en una base de datos relacional.

E. Especificación de requisitos de software

SISGRES - Sistema de Gestión de Resiliencia de Software
Especificación de Requisitos de Software

Historia de revisiones

Fecha	Versión	Descripción	Autor
16/03/2014	1.0	Creación del documento: Especificación de Requerimientos de Software.	Jackeline Palacios
18/03/2014	1.0	Corrección del documento: Especificación de Requerimientos de Software.	Jackeline Palacios
24/04/2014	1.0	Corrección del documento: Especificación de Requerimientos de Software.	Jackeline Palacios
05/05/2014	1.0	Corrección del documento: Especificación de Requerimientos de Software.	Jackeline Palacios

1. Introducción

Este documento detalla los requisitos de software para el Sistema de Gestión de Resiliencia de Software SIGRES, que describe los aspectos principales relacionados con los requisitos funcionales y suplementarios, así como el diagrama y narrativa de los casos de uso, toda esta información es fundamental para ofrecer un producto de calidad.

El documento consta de tres secciones, la primera detalla una descripción general del presente documento, la segunda presenta una descripción poco profunda de las funciones y datos asociados al sistema y la tercera define detalladamente los requisitos que debe satisfacer el SISGRES.

1.1. Propósito.

El propósito del documento es identificar, especificar y establecer lineamientos que deberán seguir los desarrolladores y analistas de software durante el desarrollo del SISGRES.

1.2. Alcance.

El alcance de esta especificación abarca los requisitos funcionales y no funcionales que se encuentran asociadas a la definición de casos de uso que permiten mantener una visión clara de los objetivos del sistema.

Las funciones principales incluyen el registro y gestión de información, ejecución de consultas y visualización de información resultante del análisis de resultados. Cada requisito amerita una prioridad durante esta fase inicial en la elaboración del desarrollo del sistema.

1.3. Definiciones, siglas y abreviaturas.

- SISGRES: Sistema de Gestión de Resiliencia de Software.
- CERT: Modelo de capacidad para la gestión de resiliencia operativa.
- RMM: Modelo de gestión de resiliencia.

1.4. Referencias

Documento Visión del Sistemas de gestión de Resiliencia de Software (SISGRES).

2. Descripción general

El sistema se desarrollará en un entorno web y automatizará la gestión de información de usuarios y la evaluación de software resiliente.

2.1. Perspectiva del producto.

2.1.1. Interfaces de usuario.

La interfaz de usuario contara de formularios, tablas, menús y botones, que construirá la aplicación y podrá visualizarse en los navegadores de web.

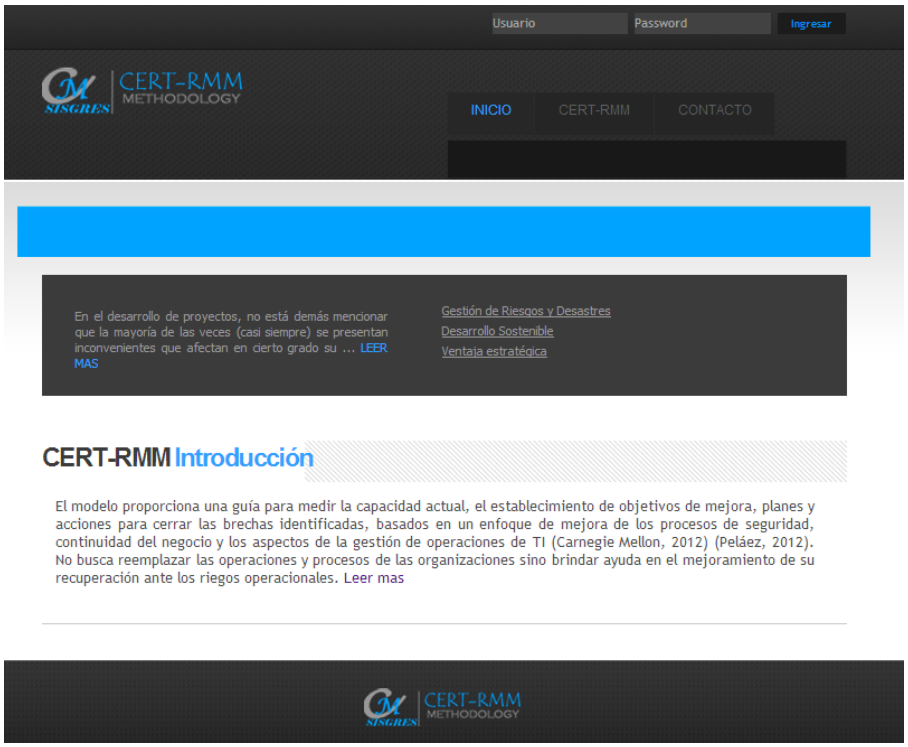


Figura 75. Interfaz del SISGRES.
Fuente: El autor.

2.1.2. Interfaces con hardware.

Los equipos en los que se utilizará el SISGRES deberán estar en buen estado y además constar de los componentes básicos como son: procesador, disco duro, memoria, mouse, teclado y adicionalmente un adaptador de red o wireless.

2.1.3. *Interfaces con software.*

El SISGRES se puede ejecutar en sistema operativos Windows XP o superior.

2.1.4. Interfaces de comunicación.

La comunicación del cliente, el sistema y el servidor será mediante los protocolos: FTP para la transferencia de datos y SSH que es un protocolo de red para distribuir la información del servidor.

2.2. Funciones del producto.

El producto que se desarrollará para evaluar la resiliencia de los SI tendrá las siguientes funciones:

- Administrar la información de usuarios por roles.
- Autenticar usuarios.
- Gestionar la información de los usuarios registrados en el sistema, lo cual incluye las operaciones de registro, actualización y eliminación.

- Gestionar las preguntas de acuerdo al área de proceso de la metodología CERT-RMM con las operaciones de registro, actualización y eliminación.
- Visualizar las preguntas de acuerdo al área de proceso de la metodología CERT-RMM definido en las plantillas de elicitación de requisitos de resiliencia.
- Controlar que se resuelvan los cuestionarios antes de mostrar los resultados.
- Generar resultados en base a las respuestas de los cuestionarios, que mostrará los aciertos y errores por cada característica de resiliencia de software.
- Mostrar sugerencias por cada característica de resiliencia de software.
- Guardar resultados.

2.3. Características de los usuarios.

Tipo de usuario	Administrador
Formación	Analista
Habilidades	Conocimiento en ingeniería del software e ingeniería de requisitos.
Actividades	Controlar todas las actividades del sistema.

Tipo de usuario	Cliente
Formación	Analista, Desarrollador, Jefe empresarial
Habilidades	Conocimiento del desarrollo del SI de la organización a la que pertenece.
Actividades	Resolver los cuestionarios que presenta el sistema y visualizar los resultados.

2.4. Restricciones de diseño.

- El servidor deberá responder a consultas simultáneas.
- El sistema constará de una estructura cliente/servidor.

2.5. Supuestos y dependencias.

- La aplicación mantiene dependencia al desarrollo de plantillas de elicitación de requisitos.
- Los requisitos que se describen son estables y deben cumplir su propósito.

3. Requisitos específicos

3.1. Requisitos Funcionales.

3.1.1. Autenticar Usuario.

Número del Requisito	RF01		
Nombre del Requisito	Autenticar Usuario		
Tipo de Requisito	(X) Requisito	( ) Restricción	
Característica del Requisito	Permitir la validación de los usuarios y acceso al sistema mediante el nombre de usuario y clave.		
Descripción del Requisito	La validación del usuario se efectúa al momento de ingresar al sistema, sin importar el tipo de actividad que se vaya a efectuar o el tipo de usuario que quiera ingresar, todos los usuarios deberán pasar por el proceso de validación mediante el uso de su identificación, que es el nombre de usuario y clave.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.2. Gestión de Usuarios.

Número del Requisito	RF02		
Nombre del Requisito	Gestión de Usuarios		
Tipo de Requisito	(X) Requisito	( ) Restricción	
Característica del Requisito	Administra la información de los usuarios registrados en el sistema.		
Descripción del Requisito	La gestión de usuarios comprende las tareas de registro, actualización y eliminación de la información personal de los usuarios tales como: nombre, apellido, correo, usuario, clave y rol. Cabe mencionar el nombre de usuario no puede ser editable. Sólo el usuario registrado como administrador puede realizar las operaciones antes mencionadas.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.3. Gestión de Cuestionarios.

Número del Requisito	RF03
Nombre del Requisito	Gestión de Cuestionarios

Tipo de Requisito	(X) Requisito	( ) Restricción	
Característica del Requisito	Administra la información de los cuestionarios con los que opera el sistema.		
Descripción del Requisito	La gestión de cuestionarios comprende las tareas de registro, actualización, eliminación y visualización de preguntas según el área de la Metología CERT_RMM a la que corresponda. Sólo el usuario registrado como administrador puede realizar las operaciones antes mencionadas.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.4. Visualizar Cuestionarios.

Número del Requisito	RF04		
Nombre del Requisito	Visualizar Cuestionarios		
Tipo de Requisito	(X) Requisito	( ) Restricción	
Característica del Requisito	Presenta los cuestionarios de acuerdo al área de proceso del CERT_RMM.		
Descripción del Requisito	De acuerdo a la información almacenada en la base de datos, el sistema presenta los cuestionarios de acuerdo al área de proceso del CERT_RMM a la que pertenecen. Esta información es presentada al usuario registrado como cliente al ingresar al sistema.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.5. Gestionar Respuestas.

Número del Requisito	RF05	
Nombre del Requisito	Resolver Cuestionarios	
Tipo de Requisito	(X) Requisito	( ) Restricción
Característica del Requisito	Guarda las respuestas de los cuestionarios en la base de datos.	
Descripción del Requisito	La gestión de respuestas comprende las tareas de registro, actualización, eliminación y visualización de respuestas de acuerdo a cada pregunta según corresponda. Sólo el usuario registrado como administrador puede realizar las operaciones antes	

	mencionadas.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.6. Gestionar Resultados.

Número del Requisito	RF06		
Nombre del Requisito	Gestionar Resultados Finales		
Tipo de Requisito	(X) Requisito	( ) Restricción	
Característica del Requisito	Analiza respuestas.		
Descripción del Requisito	El sistema toma las respuestas de los cuestionarios para contabilizar los aciertos y errores en cuanto al cumplimiento de las características de resiliencia de software y posteriormente presentarlos al usuario. Además el sistema se basa en las plantillas diseñadas para asignar las sugerencias correspondientes a cada característica de resiliencia de software. Las sugerencias ya se encuentran registradas en la base de datos. Si la característica de software no tiene cuestionarios erróneos pues no presenta sugerencias.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.7. Gestionar Sugerencias.

Número del Requisito	RF07		
Nombre del Requisito	Gestionar Sugerencias		
Tipo de Requisito	(X) Requisito	( ) Restricción	
Característica del Requisito	Asigna sugerencias a las características de resiliencia de software.		
Descripción del Requisito	El sistema se basa en los cuestionarios incorrectos por cada característica de resiliencia de software para buscar en la base de datos según las plantillas diseñadas las sugerencias correspondientes. Las sugerencias ya se encuentran registradas en la base de datos. Si la característica de software no tiene cuestionarios erróneos pues no presenta sugerencias.		
Prioridad del Requisito	(X) Alta/Esencial	( ) Media/Deseado	( ) Baja/ Opcional

3.1.8. Consultar Resultados.

Número del Requisito	RF06
Nombre del Requisito	Consultar Resultados
Tipo de Requisito	(X) Requisito ( ) Restricción
Característica del Requisito	Presenta resultados.
Descripción del Requisito	El sistema presenta el estado de resiliencia del SI evaluado presentando el número de preguntas correctas e incorrectas por cada característica de resiliencia de software y además presenta sugerencias por cada característica.
Prioridad del Requisito	(X) ( ) Media/Deseado ( ) Baja/ Opcional Alta/Esencial

3.2. Requisitos Suplementarios.

3.2.1. Requisitos de Rendimiento.

- La aplicación garantizará que los usuarios tengan una eficiencia (rapidez, ejecución) de un 95% al usar la aplicación.
- El tiempo de respuesta a los usuarios será de 1 a 2 segundos.

3.2.2. Seguridad.

- Se puede consultar y actualizar la información simultáneamente sin alterar el tiempo de respuesta.
- El método de encriptación MD5 se debe utilizar para cifrar las claves de los usuarios.
- Se maneja claves como método de protección para el sistema.

3.2.3. Fiabilidad.

El sistema debe presentar una interfaz sencilla de uso intuitivo para los usuarios.

3.2.4. Disponibilidad.

El sistema tendrá una disponibilidad correspondiente al 90%.

3.2.5. Mantenibilidad.

- El respaldo de la base de datos se realizará cada semestre.
- El mantenimiento de los computadores, servidor y red será semanal.
- El servidor que debe instalarse es Xamp 1.7.4 (MySQL, Apache).

3.2.6. Portabilidad

- El sistema será desarrollado en lenguaje web php (5.3.5) y se ejecuta en ambientes Windows pero podrá ser accedido desde varias plataformas.

F. Diagrama de casos de uso

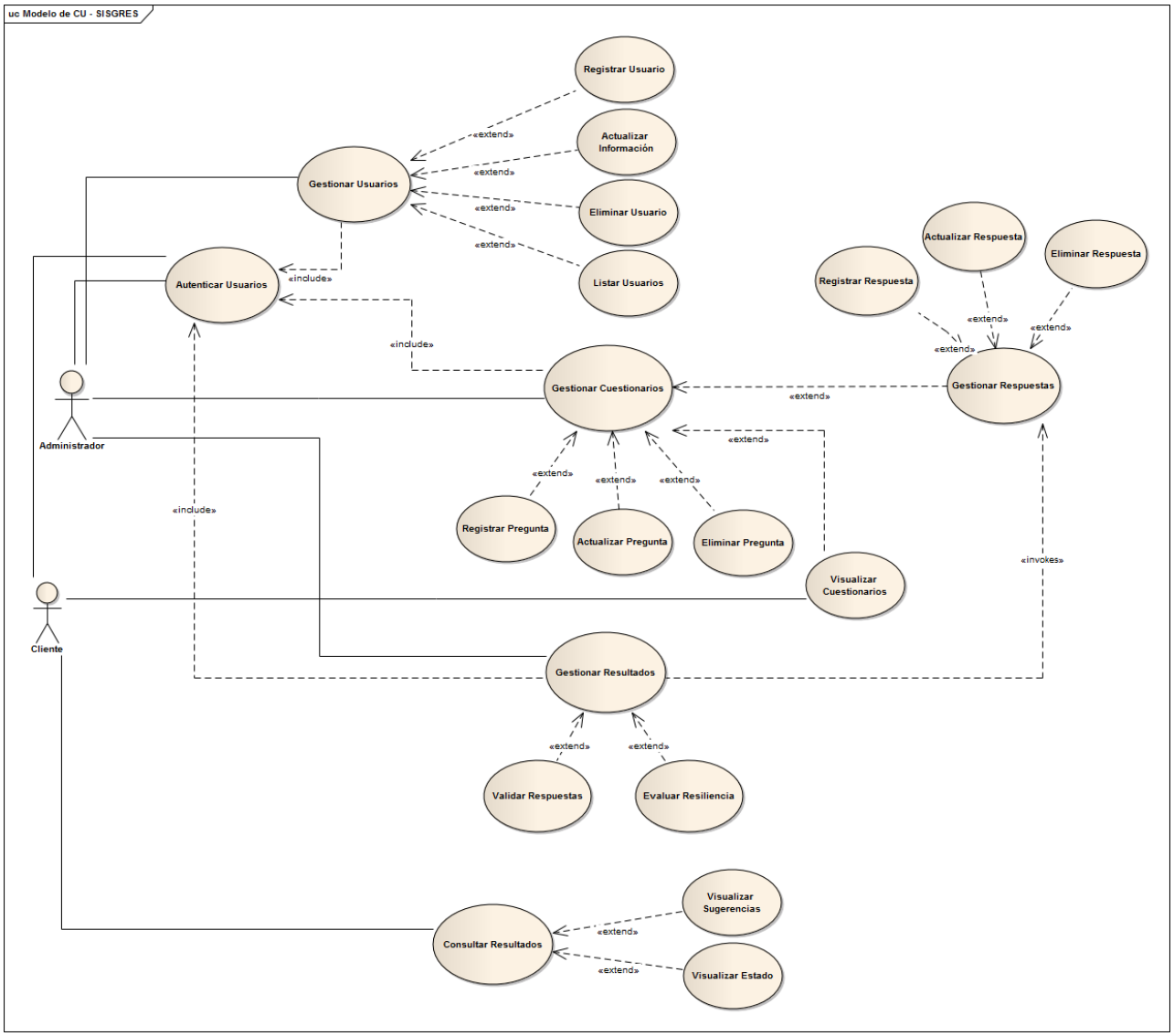


Figura 76. Diagrama de Caso de Uso SISGRES.
Fuente: El autor.

G. Especificación de casos de uso

Sistema de Gestión de Resiliencia de Software - SISGRES

Especificación de Caso de Uso 01: Autenticar Usuario

Versión 1.0

Historia de revisiones

Fecha	Versión	Descripción	Autor
05/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
08/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
11/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
20/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
23/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
01/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
14/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
21/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios

1. Descripción

Se verifica que el ingreso al sistema se dé únicamente a los usuarios registrados en sus dos perfiles (roles) sea administrador o cliente.

2. Flujo básico

1. Ingresar el nombre de usuario y clave.
2. Verificar que los datos estén completos. En el caso que existan datos incompletos se llama al flujo alterno 001.
3. Si los datos ingresados de usuario y clave corresponden a uno de los usuarios registrados, se autoriza el inicio de sesión, de lo contrario se llama al flujo alterno 002.

3. Flujo alternativo

3.1. Flujo alternativo 001.

Presentar una notificación de error y solicitar se llene los campos de usuario y clave.

3.2. Flujo alternativo 002.

Presentar una notificación de error y denegar el acceso al sistema.

4. Escenarios clave

4.1. Escenario de acceso al sistema.

El usuario ingresa al sistema e interactúa con la información presentada de acuerdo a su rol sea:

- Cliente con los permisos de lectura y ejecución o
- Administrador con todos los permisos (lectura, escritura y ejecución).

5. Precondiciones

1. El usuario debe constar en el registro del sistema.
2. El sistema debe restringir el acceso a los usuarios según su rol (cliente o administrador).

6. Postcondiciones

1. Se muestra la página principal según el rol.

7. Requerimientos especiales

7.1. Seguridad.

El sistema implementará estrategias de seguridad como el cifrado de las claves de acceso para delimitar el acceso a usuarios no autorizados.

7.2. Disponibilidad.

El producto presentará un porcentaje de disponibilidad del 90%, trabajando 24 horas los 365 días del año.

7.3. Accesibilidad.

El sistema podrá se accedido desde cualquier punto geográfico que mantenga conexión a internet.

8. Información adicional

8.1. Metodología CERT-RMM.

El Sistema se basa fundamentalmente en resiliencia tomando a la metodología CERT como medio de evaluación a las empresas a través de cuestionarios basados en sus activos, metas y prácticas.

8.2. Base de Datos MySQL.

Se utiliza una base de datos relacional para el almacenamiento de información de usuarios, empresas, cuestionarios e inclusive para los resultados obtenidos de cada evaluación que servirán para estudios posteriores.

Sistema de Gestión de Resiliencia de Software - SISGRES

Especificación de Caso de Uso 01: Gestionar Usuarios

Versión 1.0

Historia de revisiones

Fecha	Versión	Descripción	Autor
11/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
20/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
23/03/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
01/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
14/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
21/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios

1. Descripción

Se gestiona la información de las cuentas de los usuarios por medio de las operaciones de registrar, modificar, borrar y listar la información de usuarios en el sistema, además se administra permisos a los usuarios mediante la asignación de roles.

2. Flujo básico

1. Ingresar en el SI.
2. Seleccionar el menú Usuarios y la operación a realizar.
3. Presentar la información.
4. Interactuar con la información.
5. Guardar el resultado de la interacción.

3. Flujo alternativo

3.1. Flujo alternativo 001.

Presentar una notificación de error y mostrar la página inicial del administrador.

3.2. Flujo alternativo 002.

Presentar una notificación e indicar cuál es el error.

4. SubFlujos

4.1. Visualizar usuarios.

1. El usuario escoge la opción Listar usuarios.
2. El sistema busca si existen usuarios en la base de datos y los presenta. Si no existen usuarios el sistema muestra un mensaje que no existen usuarios registrados.

4.2. Registrar usuario.

1. El usuario escoge la opción Registrar usuario.
2. El sistema presenta el formulario.
3. El usuario ingresa los datos informativos del nuevo usuario como: nombres, apellidos, correo, usuario, contraseña y rol. Todos los campos deben estar completos para continuar.
4. El usuario selecciona la opción guardar y el sistema guarda los datos y regresa a la venta principal de Usuarios. En caso que el sistema falle al guardar los datos, se llama al Flujo alternativo 002.
5. El usuario selecciona la opción cancelar y el sistema regresa a la página principal de Usuarios.

4.3. Modificar usuario.

1. En la lista que presenta el sistema de usuarios registrados, el usuario selecciona el usuario a modificar.

2. El sistema busca al usuario en la base de datos.
3. El sistema muestra un formulario con sus datos.
4. El usuario realiza los cambios sobre el formulario.
5. El sistema verifica que el formulario esté completo y guarda la información actualizada del usuario.
6. En caso que el formulario no esté completo regresa al paso 3.
7. El sistema presenta la página principal de Usuarios.

4.4. Eliminar usuario.

1. En la lista que presenta el sistema de usuarios registrados el usuario selecciona el nombre de usuario a eliminar.
2. El sistema busca en la base de datos el usuario y muestra un mensaje de confirmación.
3. El usuario acepta el mensaje y el sistema elimina el usuario.
4. En caso que el usuario no acepte el mensaje se cancela la operación y el sistema presenta la página principal de Usuarios.

5. Escenarios clave

5.1. Escenario de gestionar usuarios.

El usuario registrado como administrador ingresa al sistema y gestiona la información de los usuarios.

6. Precondiciones

1. El sistema debe contar con usuarios registrados.
2. El sistema debe permitir el ingreso según el rol del usuario (los usuarios autenticados como administrador pueden ejecutar las operaciones).

7. Postcondiciones

1. Se muestra la página y el menú de opciones según el rol.

8. Requerimientos especiales

8.1. Seguridad.

El sistema implementará estrategias de seguridad como el cifrado de las claves de acceso para delimitar el acceso a usuarios no autorizados.

8.2. Disponibilidad.

El producto presentará un porcentaje de disponibilidad del 90%, trabajando 24 horas los 365 días del año.

8.3. Accesibilidad.

El sistema podrá se accedido desde cualquier punto geográfico que mantenga conexión a internet.

4. Información adicional

4.1. Metodología CERT-RMM.

El Sistema se basa fundamentalmente en resiliencia tomando a la metodología CERT como medio de evaluación a las empresas a través de cuestionarios basados en sus activos, metas y prácticas.

4.2. Base de Datos MySQL.

Se utiliza una base de datos relacional para el almacenamiento de información de usuarios, empresas, cuestionarios e inclusive para los resultados obtenidos de cada evaluación que servirán para estudios posteriores.

Sistema de Gestión de Resiliencia de Software - SISGRES

Especificación de Caso de Uso 01: Gestionar Cuestionarios

Versión 1.0

Historia de revisiones

Fecha	Versión	Descripción	Autor
11/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
20/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
23/03/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
01/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
14/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
21/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios

1. Descripción

Se administra de las preguntas en función de las áreas de proceso de la metodología CERT.

2. Flujo básico

1. El usuario se autentica en el SI.
2. El usuario escoge el menú Cuestionarios.
3. El sistema presenta la información.
4. El usuario selecciona una de las áreas de proceso del CERT-RMM.
5. El sistema lista las preguntas correspondientes a cada área y presenta las operaciones que se pueden ejecutar.
6. En el caso que no se listen las preguntas, se llama al flujo 001.
7. El usuario escoge la operación a realizar.
8. El sistema presenta la información.
9. El usuario interactúa con la información.
10. El sistema guarda el resultado de la interacción en la base de datos.

3. Flujo alternativo

3.1. Flujo alternativo 001.

Presentar una notificación de error y mostrar la página inicial de las operaciones.

3.2. Flujo alternativo 002.

Presentar una notificación e indicar cuál es el error.

4. SubFlujos

4.1. Registrar pregunta.

1. El usuario escoge la opción Registrar pregunta.
2. El sistema presenta el formulario de registro.
3. El usuario llena el formulario. Todos los campos deben estar completos para que pueda continuar.
4. El usuario selecciona la opción Guardar y el sistema guarda los datos en la base de datos.
5. En caso que el sistema falle al guardar los datos, se llama al Flujo alternativo 002.
6. El sistema presenta la página principal de Cuestionarios.

4.2. Visualizar preguntas.

1. El usuario selecciona una de las áreas de proceso del CERT_RMM.
2. Si el usuario registrado es de tipo administrador, el sistema sólo muestra la lista de preguntas registradas en la base de datos.

3. Si el usuario registrado es de tipo cliente el sistema muestra una lista de preguntas con sus respectivas respuestas y cada respuesta con un checkbox para que puedan ser resueltas por el usuario.
4. El usuario escoge por cada pregunta la o las respuestas que crea correctas.
5. El sistema guarda la información cuando el usuario seleccione el botón Finalizar y presenta la página donde se listan las áreas de proceso del CERT-RMM.
6. Si el usuario selecciona el botón Regresar, se pierde la información y se regresa a la página donde se listan las áreas de proceso del CERT-RMM.

4.3. Modificar pregunta.

1. El usuario selecciona la pregunta a modificar.
2. El sistema busca la pregunta en la base de datos.
3. El sistema muestra un formulario con sus datos.
4. El usuario realiza los cambios.
5. El sistema verifica que el formulario esté completo y guarda la información actualizada de la pregunta.
6. En caso que el formulario no esté completo regresa al paso 3.
7. El sistema presenta la página principal de Cuestionarios.

4.4. Eliminar pregunta.

1. El usuario selecciona la pregunta a eliminar.
2. El sistema busca en la base de datos la pregunta y muestra un mensaje de confirmación.
3. El usuario acepta el mensaje y el sistema elimina la pregunta. Al eliminarse la pregunta se eliminarán también las respuestas asociadas.
4. En caso que el usuario no acepte el mensaje se cancela la operación y el sistema presenta la página principal de Cuestionarios.

5. Escenarios clave

5.1. Escenario de administrar cuestionarios.

Las preguntas van en función a las áreas de proceso de la metodología CERT-RMM.

6. Precondiciones

1. El sistema debe contar con usuarios registrados.
2. El sistema debe permitir el ingreso según el rol del usuario (los usuarios marcados como administrador pueden ejecutar las operaciones).

7. Postcondiciones

1. El usuario de perfil cliente sólo puede ver y responder los cuestionarios.

2. El usuario de perfil administrador puede interactuar con los demás funcionalidades del sistema excepto las funcionalidades del cliente.

8. Requerimientos especiales

8.1. Seguridad.

El sistema implementará estrategias de seguridad como el cifrado de las claves de acceso para delimitar el acceso a usuarios no autorizados.

8.2. Disponibilidad.

El producto presentará un porcentaje de disponibilidad del 90%, trabajando 24 horas los 365 días del año.

8.3. Accesibilidad.

El sistema podrá se accedido desde cualquier punto geográfico que mantenga conexión a internet.

9. Información adicional

9.1. Metodología CERT-RMM.

El Sistema se basa fundamentalmente en resiliencia tomando a la metodología CERT como medio de evaluación a las empresas a través de cuestionarios basados en sus activos, metas y prácticas.

9.2. Base de Datos MySQL.

Se utiliza una base de datos relacional para el almacenamiento de información de usuarios, empresas, cuestionarios e inclusive para los resultados obtenidos de cada evaluación que servirán para estudios posteriores.

Sistema de Gestión de Resiliencia de Software - SISGRES

Especificación de Caso de Uso 01: Gestionar Respuestas

Versión 1.0

Historia de revisiones

Fecha	Versión	Descripción	Autor
11/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
20/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
23/03/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
01/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
14/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
21/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios

1. Descripción

Se administra las respuestas de acuerdo a la pregunta a la que pertenecen.

2. Flujo básico

1. El usuario escoge la opción a realizar.
2. El sistema presenta la información.
3. El usuario se ubica en la pregunta.
4. El sistema lista las respuestas.
5. En el caso que no se listen las preguntas, se llama al flujo 001.

3. Flujo alternativo

3.1. Flujo alternativo 001.

Presentar una notificación de error.

3.2. Flujo alternativo 002.

Presentar una notificación e indicar cuál es el error.

4. SubFlujos

4.1. Registrar respuesta.

1. El usuario solicita registrar una respuesta.
2. El sistema presenta el formulario de registro.
3. El usuario ingresa la respuesta en el campo de texto.
4. El sistema guarda los datos.
5. En caso que el sistema falle al guardar los datos, se llama al Flujo alternativo 002.

4.2. Visualizar respuestas.

1. El usuario solicita ver respuestas.
2. El sistema devuelve la lista de las respuestas registradas en la pregunta que se haya seleccionado con anterioridad.

4.3. Modificar respuesta.

1. El usuario selecciona la respuesta a modificar.
2. El sistema muestra los datos de la respuesta.
3. El usuario realiza los cambios.
4. El sistema actualiza la información de la respuesta.
5. En caso que el sistema no pueda actualizar la información de las respuestas, se llama al Flujo alternativo 002.

4.4. Eliminar respuesta.

1. El usuario selecciona la respuesta a eliminar.
2. El sistema muestra un mensaje de confirmación.

3. El usuario acepta el mensaje.
4. El sistema elimina la pregunta.
5. En caso que el sistema no pueda eliminar la respuesta, se llama al Flujo alternativo 001.

5. Escenarios clave

5.1. Escenario de visualizar cuestionario.

El usuario escoge en el menú la opción de visualizar respuestas y el sistema presenta una lista de ellas.

6. Precondiciones

1. El sistema debe estar cargado en la web.
2. El sistema debe contar con usuarios registrados.
3. El sistema debe constar con preguntas y respuestas registradas.
4. El sistema debe permitir el ingreso según el rol del usuario.

7. Requerimientos especiales

7.1. Seguridad.

El sistema implementará estrategias de seguridad como el cifrado de las claves de acceso para delimitar el acceso a usuarios no autorizados.

7.2. Disponibilidad.

El producto presentará un porcentaje de disponibilidad del 90%, trabajando 24 horas los 365 días del año.

7.3. Accesibilidad.

El sistema podrá se accedido desde cualquier punto geográfico que mantenga conexión a internet.

8. Información adicional

8.1. Metodología CERT-RMM.

El Sistema se basa fundamentalmente en resiliencia tomando a la metodología CERT como medio de evaluación a las empresas a través de cuestionarios basados en sus activos, metas y prácticas.

8.2. Base de Datos MySQL.

Se utiliza una base de datos relacional para el almacenamiento de información de usuarios, empresas, cuestionarios e inclusive para los resultados obtenidos de cada evaluación que servirán para estudios posteriores.

Sistema de Gestión de Resiliencia de Software - SISGRES

Especificación de Caso de Uso 01: Gestionar Resultados

Versión 1.0

Historia de revisiones

Fecha	Versión	Descripción	Autor
11/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
20/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
23/03/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
01/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
14/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
21/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios

1. Descripción

Se genera los resultados luego que el usuario haya resuelto las preguntas de los cuestionarios, esto por medio de comparaciones e implementando criterios de mejora (sugerencias).

2. Flujo básico

1. El usuario solicita generar resultados.
2. El sistema genera los resultados.
3. El sistema guarda el resultado de la interacción.

3. Flujo alternativo

3.1. Flujo alternativo 001.

El sistema presenta una notificación de error.

4. Subflujos

4.1. Validar respuestas.

1. El sistema verifica las respuestas digitadas por el usuarios
2. El sistema verifica si existe similitud ente las respuestas de los cuestionarios digitadas por el usuario con las repuestas almacenadas en la base de datos. Si existe similitud en la respuesta se le asigna a la pregunta un estado de correcto, caso contrario se le asigna un estado de incorrecto.
3. El sistema almacena los resultados.

4.2. Evaluar resiliencia.

1. El sistema verifica el estado de las preguntas resueltas por el usuario.
2. El sistema evalúa el nivel de resiliencia del SI en base a las características de resiliencia de software. En base al estado de las preguntas contabiliza las aquellas que son correctas e incorrectas para cada característica.
3. El sistema guarda en la base de datos por cada usuario el resultado de la evaluación.

5. Escenarios clave

5.1. Escenario de generar resultados.

El usuario ingresa al sistema, responde las preguntas y escoge la opción de generar resultados. El sistema procesa las respuestas y presenta los resultados.

6. Precondiciones

1. El sistema debe contar con usuarios registrados.
2. El sistema debe constar con preguntas registradas.
3. El sistema debe permitir el ingreso según el rol del usuario (los usuarios autenticados como administrador pueden ejecutar las operaciones).

7. Requerimientos especiales

7.1. Seguridad.

El sistema implementará estrategias de seguridad como el cifrado de las claves de acceso para delimitar el acceso a usuarios no autorizados.

7.2. Disponibilidad.

El producto presentará un porcentaje de disponibilidad del 90%, trabajando 24 horas los 365 días del año.

7.3. Accesibilidad.

El sistema podrá se accedido desde cualquier punto geográfico que mantenga conexión a internet.

8. Información adicional

8.1. Metodología CERT-RMM.

El Sistema se basa fundamentalmente en resiliencia tomando a la metodología CERT como medio de evaluación a las empresas a través de cuestionarios basados en sus activos, metas y prácticas.

8.2. Base de Datos MySQL.

Se utiliza una base de datos relacional para el almacenamiento de información de usuarios, empresas, cuestionarios e inclusive para los resultados obtenidos de cada evaluación que servirán para estudios posteriores.

Sistema de Gestión de Resiliencia de Software - SISGRES

Especificación de Caso de Uso 01: Consultar Resultados

Versión 1.0

Historia de revisiones

Fecha	Versión	Descripción	Autor
11/11/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
20/03/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
23/03/2013	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
01/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
14/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios
21/04/2014	1.0	Corrección del Documento de Especificación de Casos de Uso.	Jackeline Palacios

1. Descripción

Se verifica los resultados luego que el usuario haya respondido las preguntas de los cuestionarios.

2. Flujo básico

1. El usuario escoge generar resultados.
2. El sistema presenta los resultados.
3. El usuario selecciona la opción sugerencias.
4. El sistema lista las sugerencias.
5. En caso de no existir resultados se llama al Flujo alternativo 001.

3. Flujo alternativo

3.1. Flujo alternativo 001.

El sistema presenta una notificación de error.

4. Subflujos

4.1. Visualizar sugerencias.

1. El sistema presenta las características de resiliencia y el número de preguntas correctas e incorrectas.
2. El usuario escoge la opción sugerencias.
3. El sistema presenta las sugerencias de acuerdo a la característica de resiliencia de software.

4.2. Visualizar estado.

1. El usuario escoge la opción visualizar nivel de resiliencia.
2. El sistema presenta una tabla de resultados por cada área de la metodología CERT-RMM y el porcentaje del nivel de resiliencia de software alcanzado.

4.3. Visualizar reporte.

1. El usuario escoge la opción generar reporte.
2. El sistema presenta un resumen por cada una de las peguntas donde consta la respuesta elegida y el lineamiento correcto.

5. Escenarios clave

5.1. Escenario de visualizar resultados.

El usuario ingresa al sistema, responde las preguntas y visualiza los resultados de la evaluación del nivel de resiliencia de su SI.

6. Precondiciones

1. El sistema debe contar con usuarios registrados.
2. El sistema debe constar con preguntas registradas.

3. El sistema debe cargar los resultados de la evaluación en la base de datos.
4. El sistema debe permitir el ingreso según el rol del usuario (los usuarios autenticados como cliente pueden visualizar los resultados).

7. Requerimientos especiales

7.1. Seguridad.

El sistema implementará estrategias de seguridad como el cifrado de las claves de acceso para delimitar el acceso a usuarios no autorizados.

7.2. Disponibilidad.

El producto presentará un porcentaje de disponibilidad del 90%, trabajando 24 horas los 365 días del año.

7.3. Accesibilidad.

El sistema podrá se accedido desde cualquier punto geográfico que mantenga conexión a internet.

8. Información adicional

8.1. Metodología CERT-RMM.

El Sistema se basa fundamentalmente en resiliencia tomando a la metodología CERT como medio de evaluación a las empresas a través de cuestionarios basados en sus activos, metas y prácticas.

8.2. Base de Datos MySQL.

Se utiliza una base de datos relacional para el almacenamiento de información de usuarios, empresas, cuestionarios e inclusive para los resultados obtenidos de cada evaluación que servirán para estudios posteriores.

H. Diagrama de clases

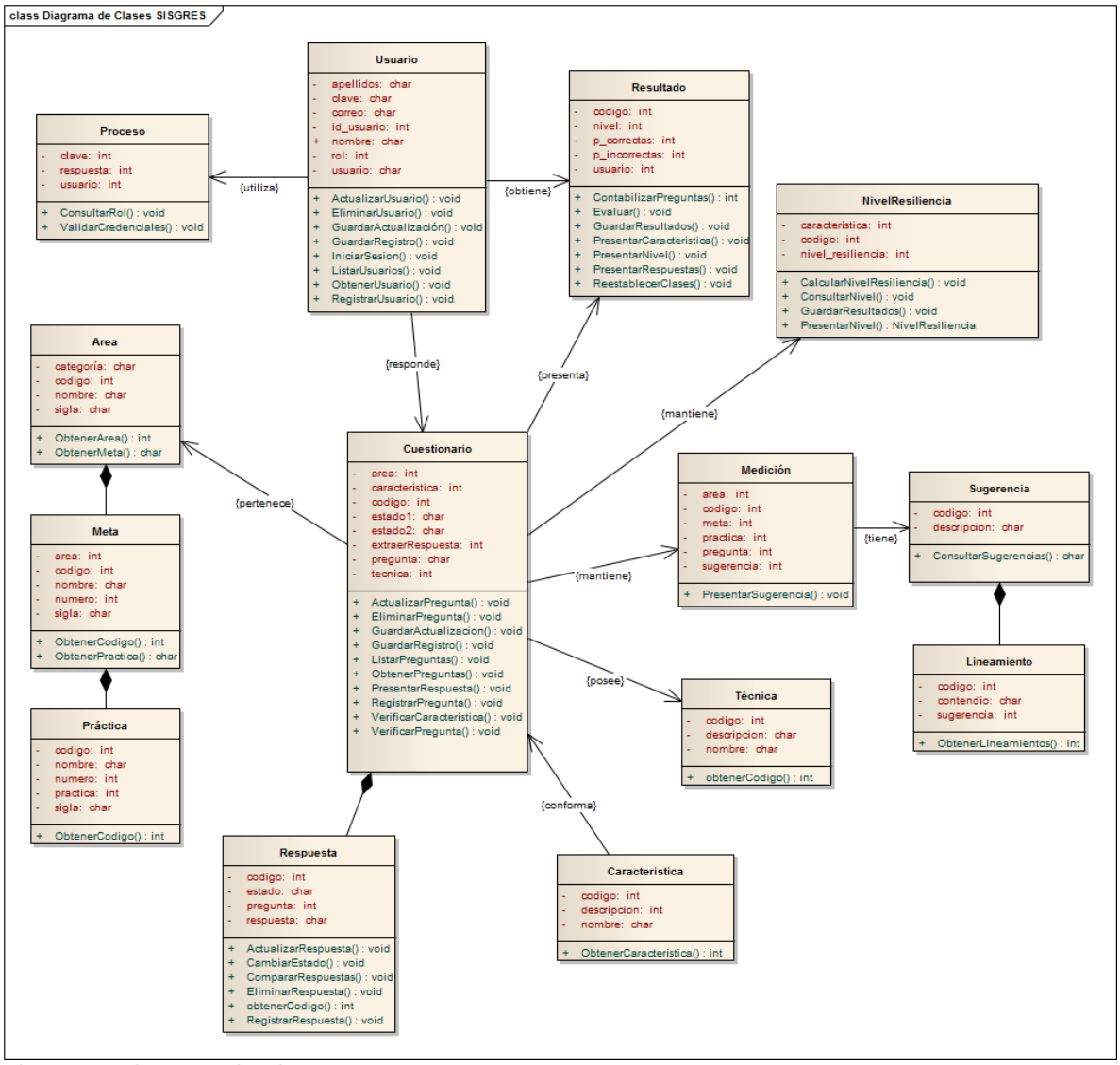


Figura 77. Diagrama de Clases SISGRES.
Fuente: El autor.

I. Diagrama de secuencia

Autenticar usuario

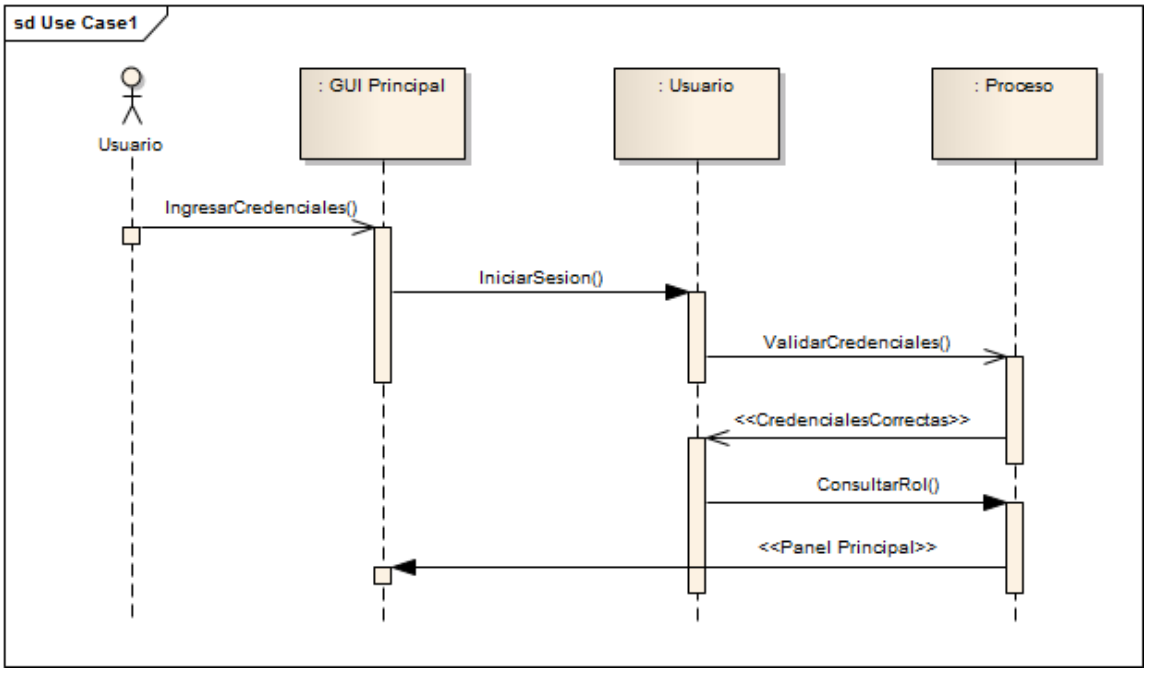


Figura 78. Diagrama de secuencia autenticar usuario.
Fuente: El autor.

Registrar usuario

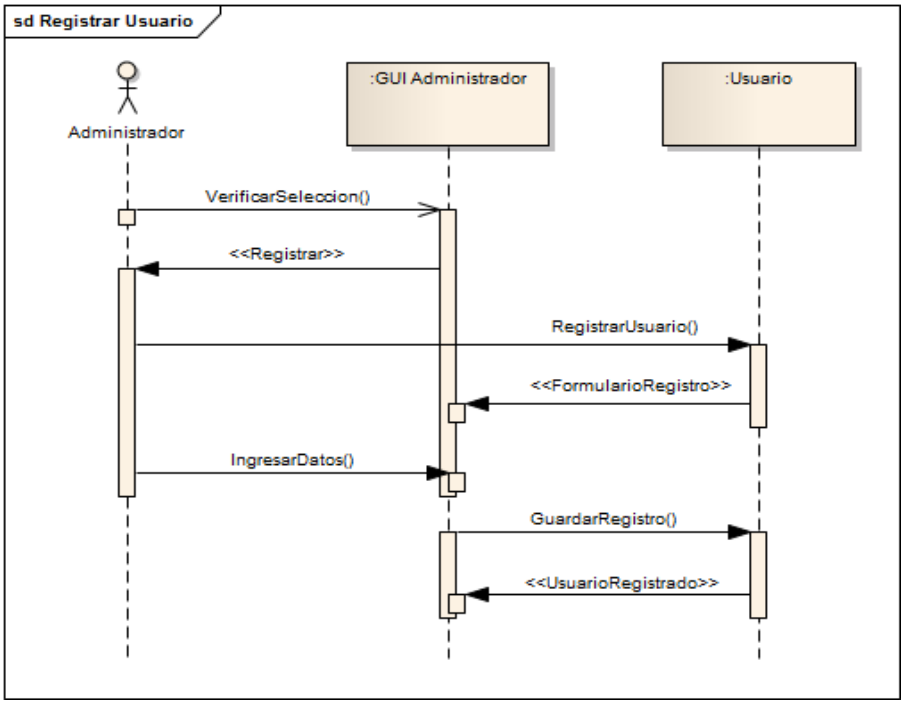


Figura 79. Diagrama de secuencia registrar usuario.
Fuente: El autor.

Actualizar información

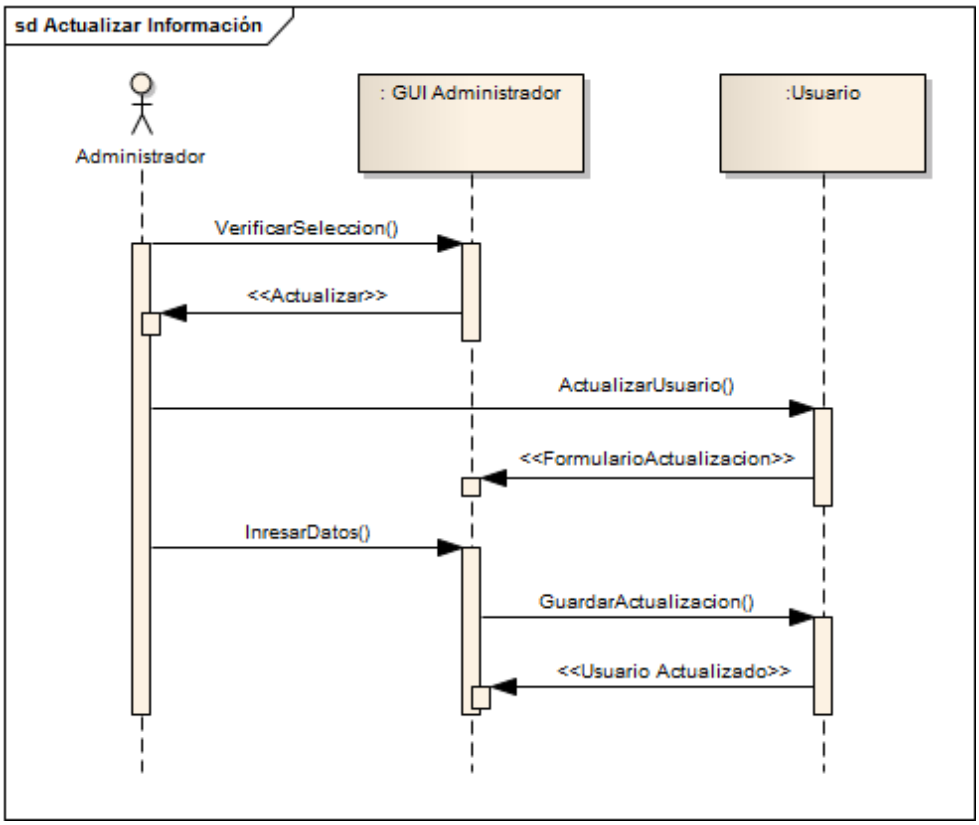


Figura 80. Diagrama de secuencia actualizar información.
Fuente: El autor.

Eliminar usuario

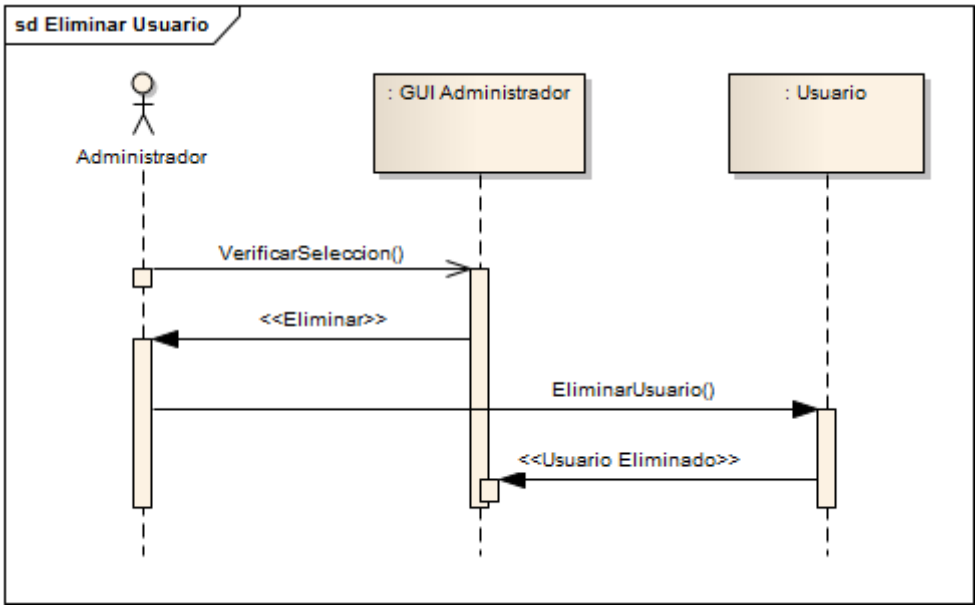


Figura 81. Diagrama de secuencia eliminar usuario.
Fuente: El autor.

Listar usuarios

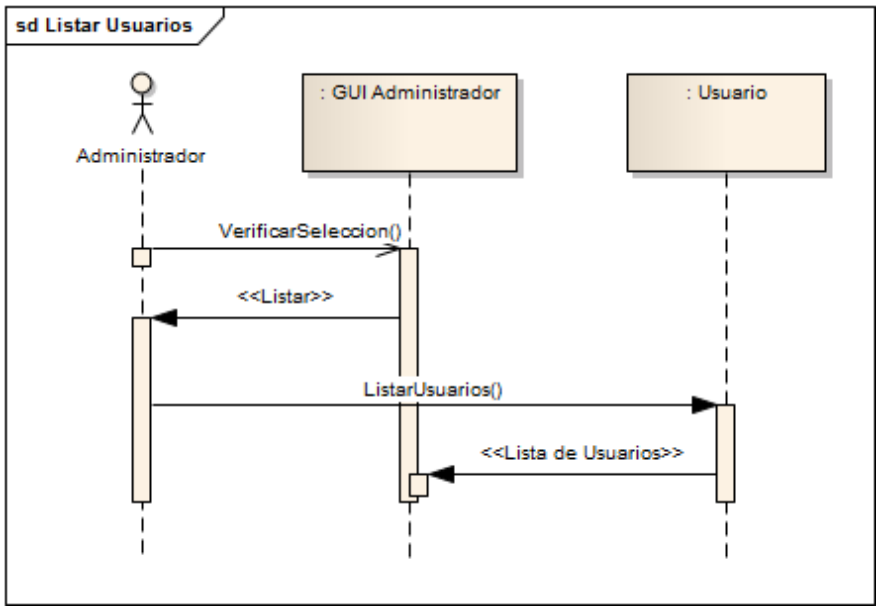


Figura 82. Diagrama de secuencia listar usuarios.
Fuente: El autor.

Registrar pregunta

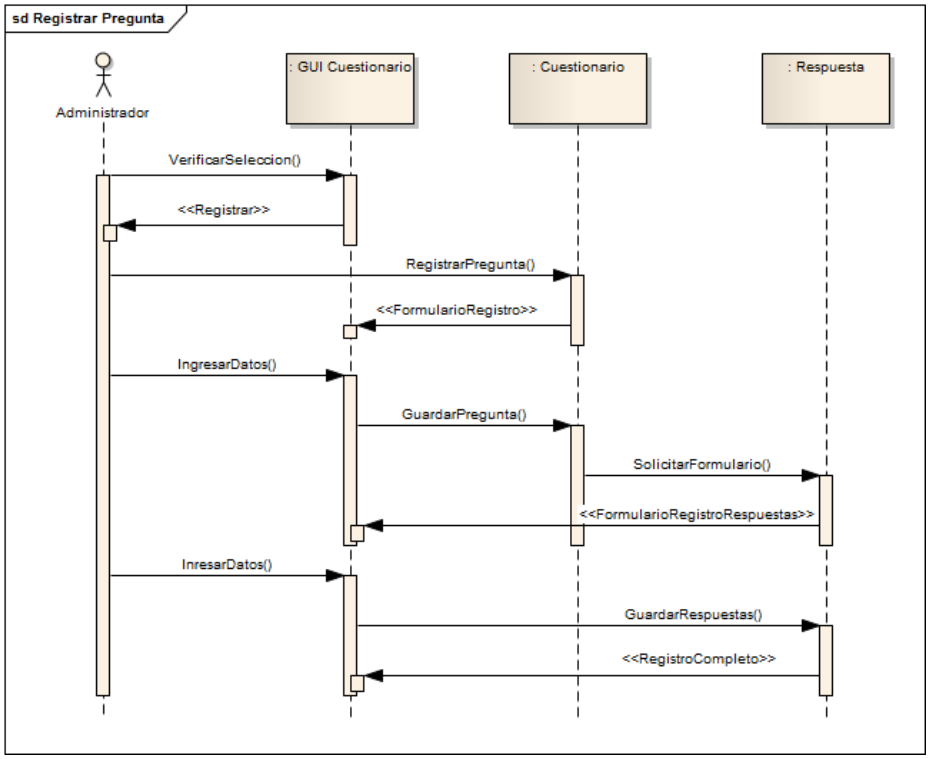


Figura 83. Diagrama de secuencia registrar pregunta.
Fuente: El autor.

Actualizar pregunta

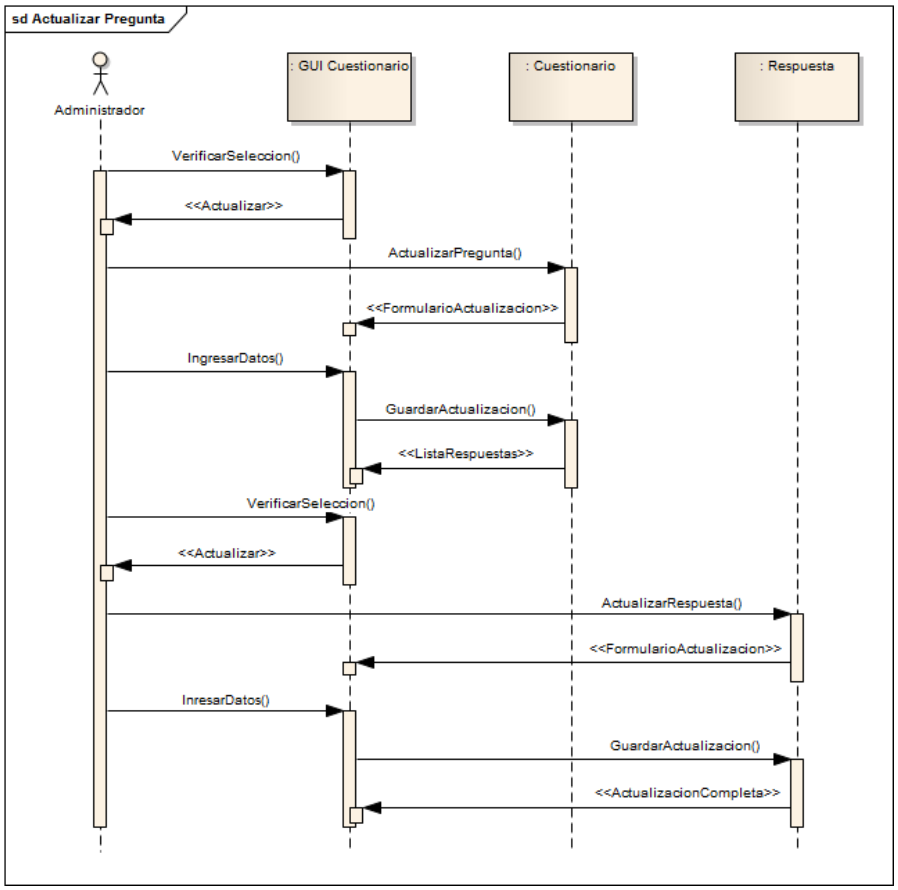


Figura 84. Diagrama de secuencia actualizar pregunta.
Fuente: El autor.

Eliminar pregunta

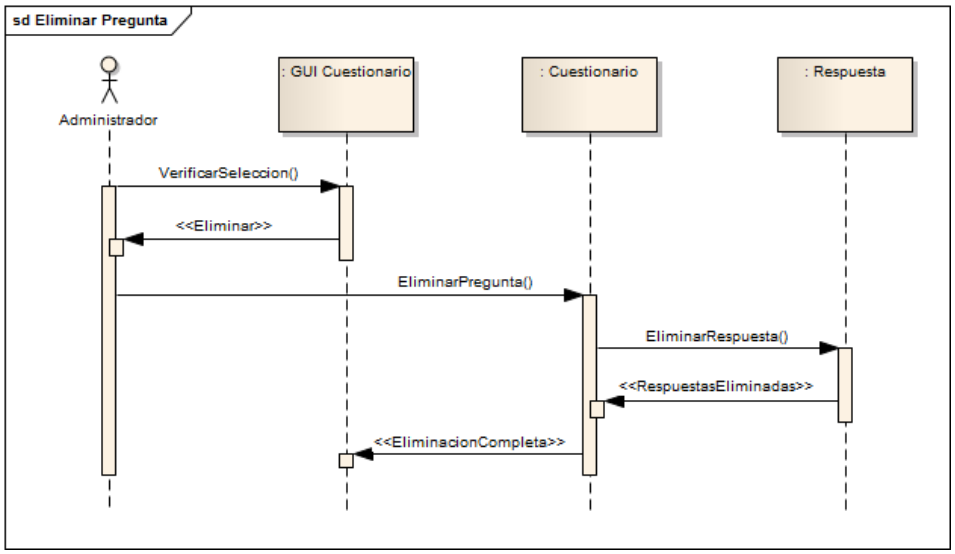


Figura 85. Diagrama de secuencia eliminar pregunta.
Fuente: El autor.

Validar respuestas

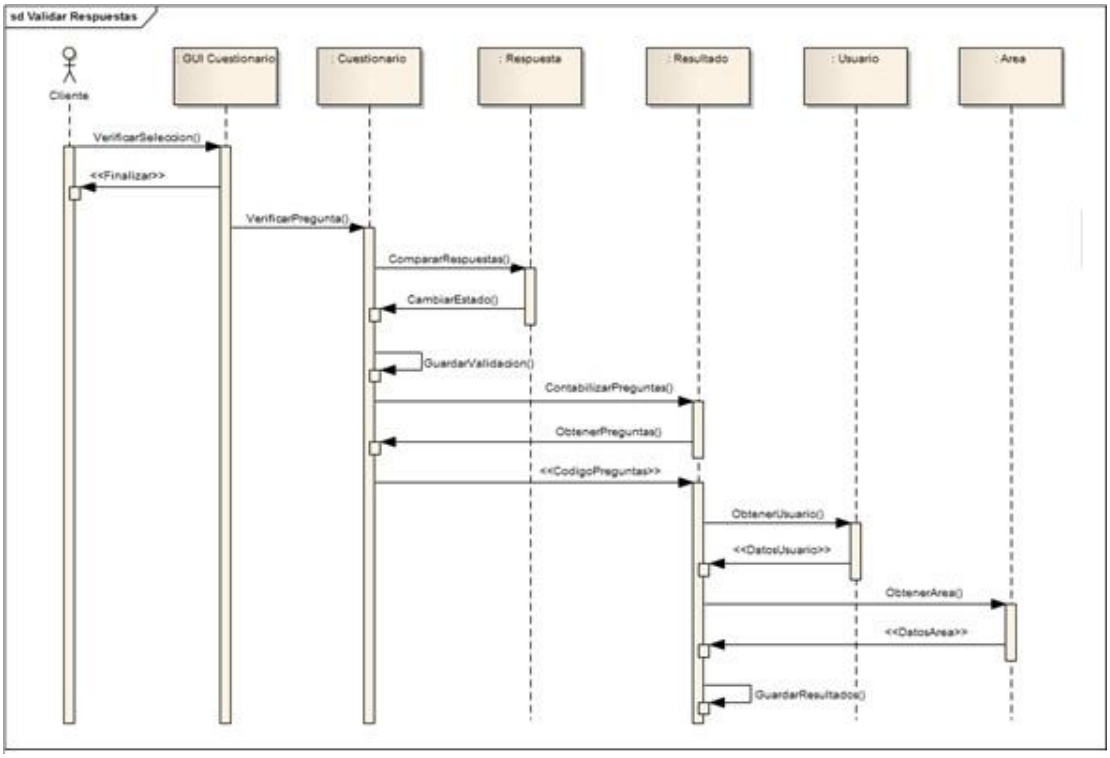


Figura 86. Diagrama de secuencia validar respuestas.
Fuente: El autor.

Evaluar resiliencia

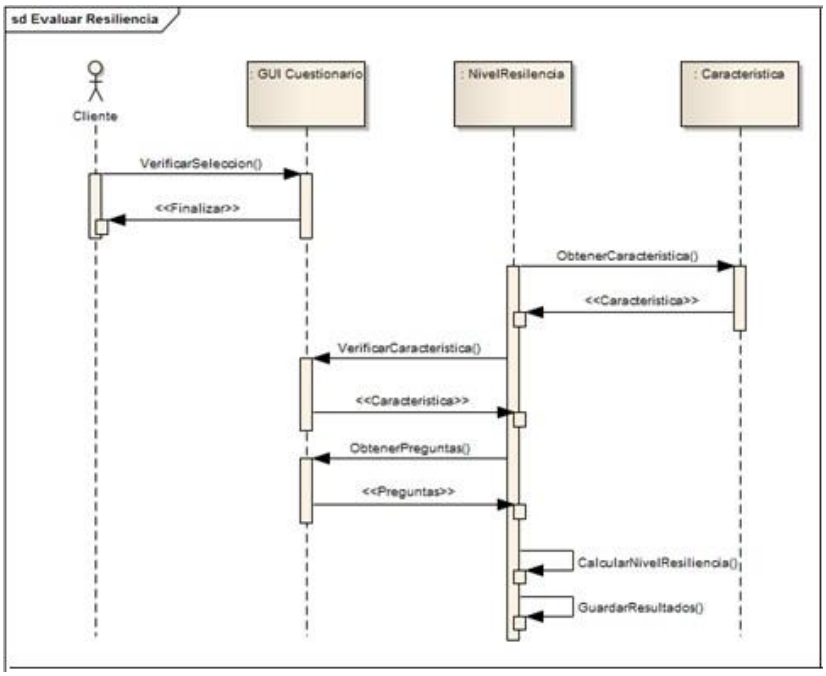


Figura 87. Diagrama de secuencia evaluar resiliencia.
Fuente: El autor.

Visualizar sugerencias

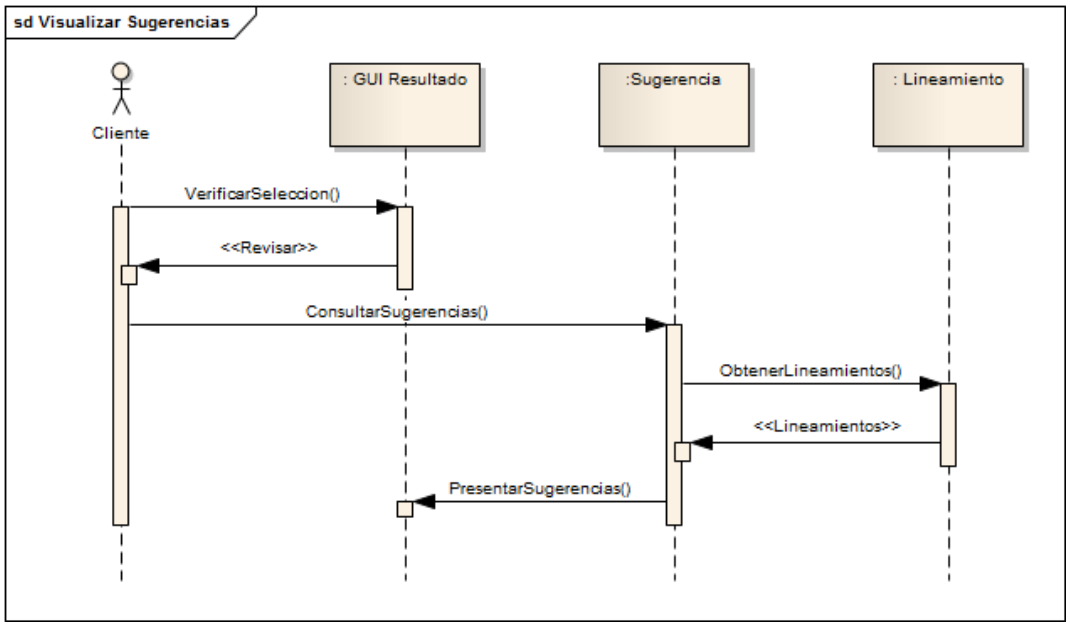


Figura 88. Diagrama de secuencia validar sugerencias.
Fuente: El autor.

Visualizar estado

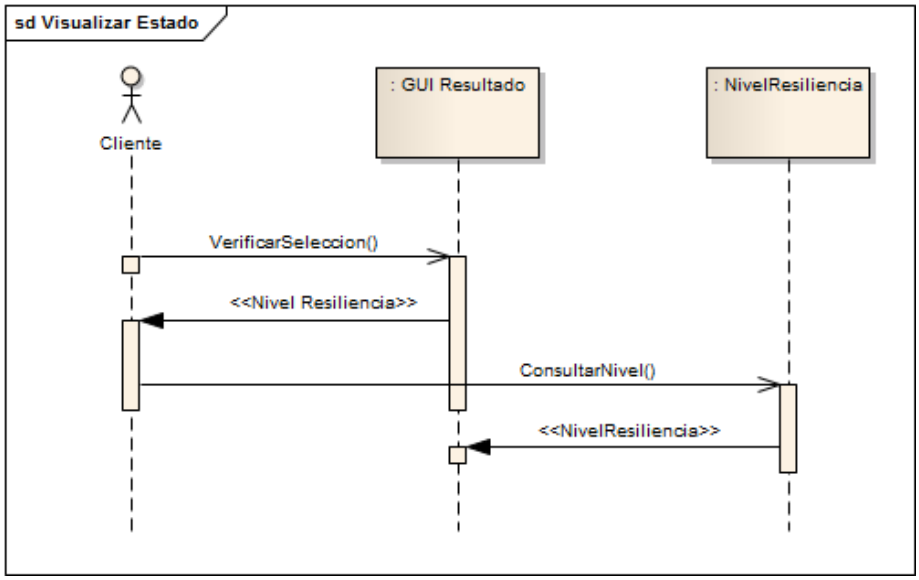


Figura 89. Diagrama de secuencia visualizar estado.
Fuente: El autor.

J. Diagrama de actividades

Autenticar usuario

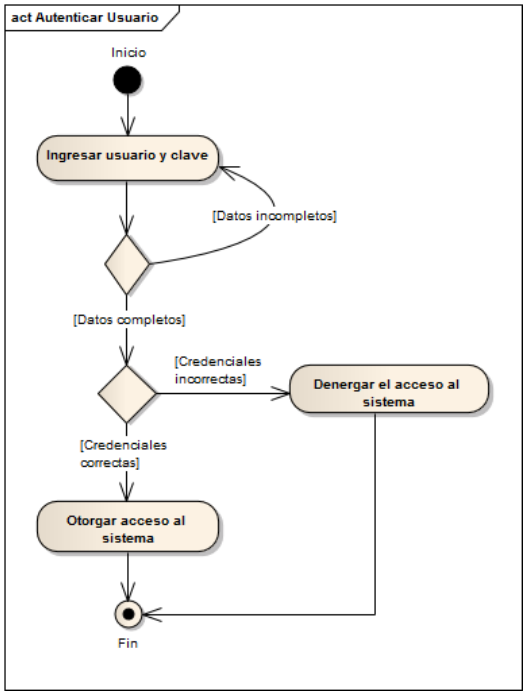


Figura 90. Diagrama de actividades autenticar usuario.
Fuente: El autor.

Actualizar información

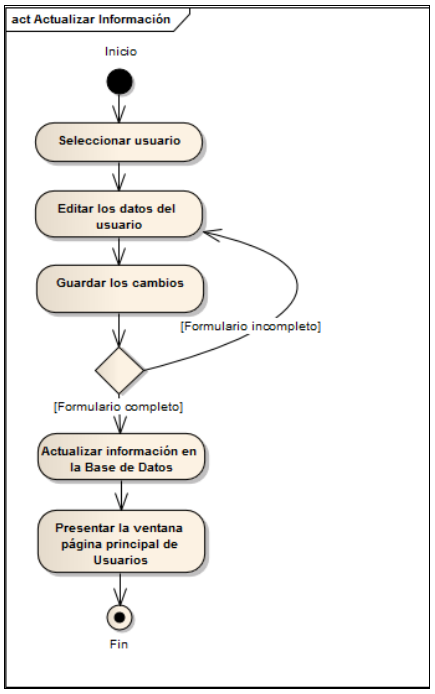


Figura 92. Diagrama de actividades actualizar información.
Fuente: El autor.

Registrar usuario

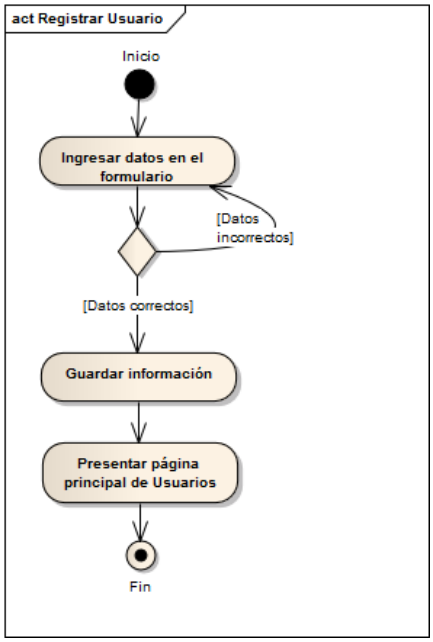


Figura 91. Diagrama de actividades registrar usuario.
Fuente: El autor.

Eliminar usuario

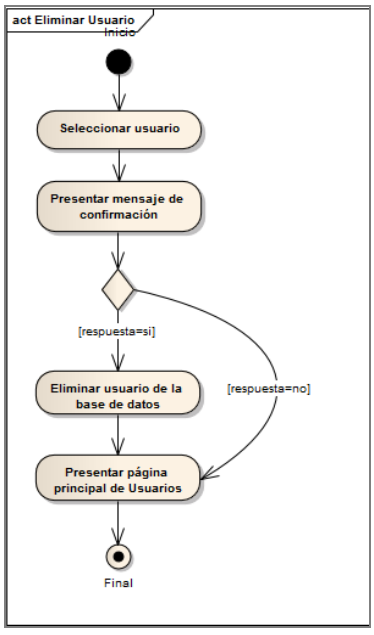


Figura 93. Diagrama de actividades eliminar usuario.
Fuente: El autor.

Listar usuarios

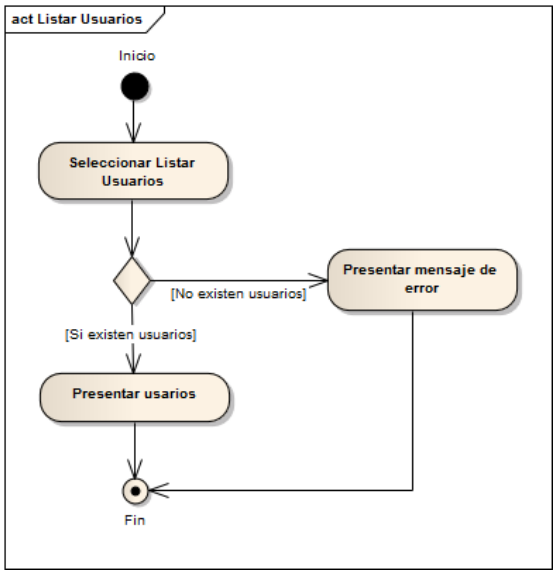


Figura 94. Diagrama de actividades listar usuarios.
Fuente: El autor.

Registrar pregunta

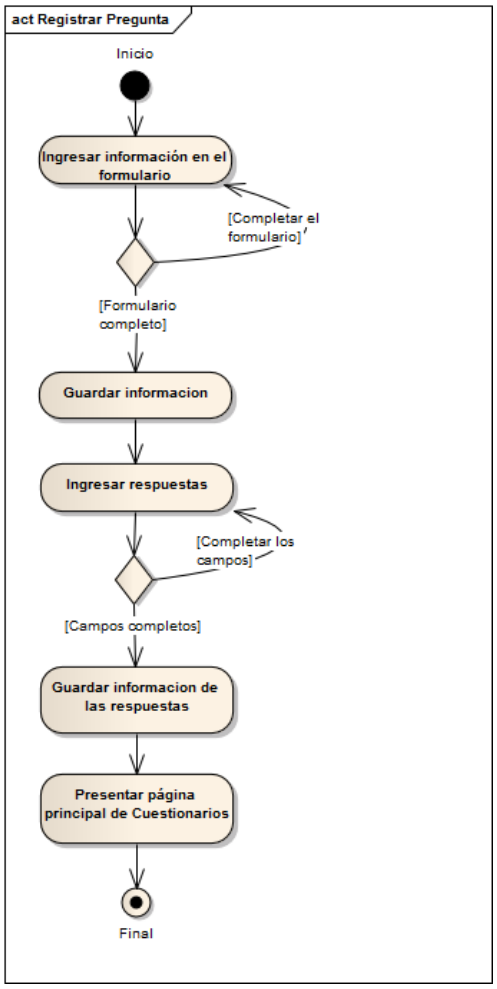


Figura 95. Diagrama de actividades registrar pregunta.
Fuente: El autor.

Actualizar pregunta

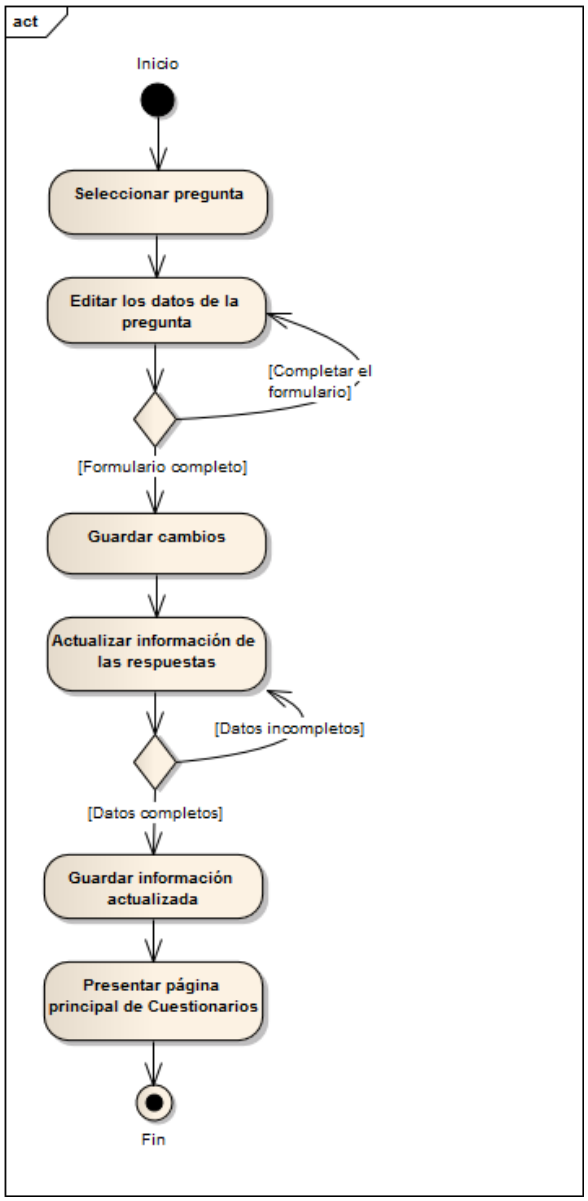


Figura 96. Diagrama de actividades actualizar pregunta.
Fuente: El autor.

Eliminar pregunta

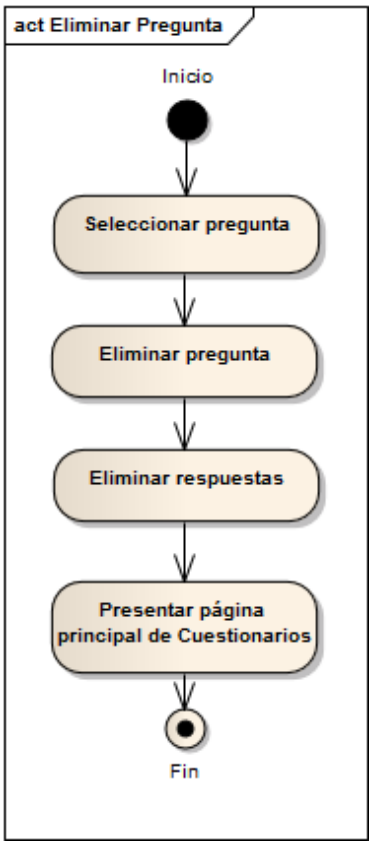


Figura 97. Diagrama de actividades eliminar pregunta.
Fuente: El autor.

Validar Respuestas

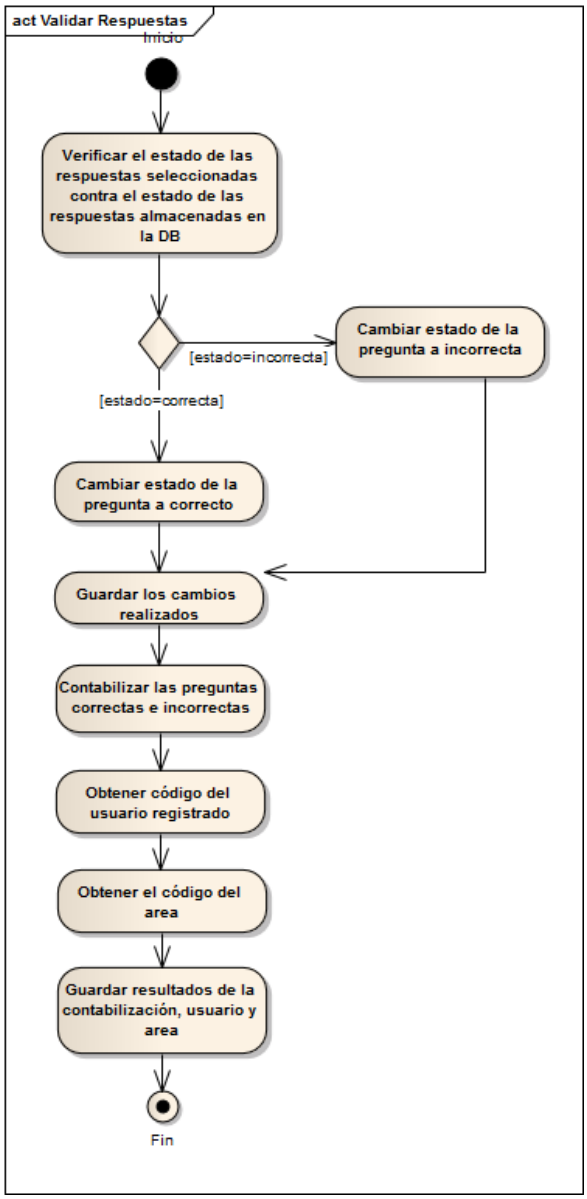


Figura 98. Diagrama de actividades validar respuestas.
Fuente: El autor.

Evaluar Resiliencia

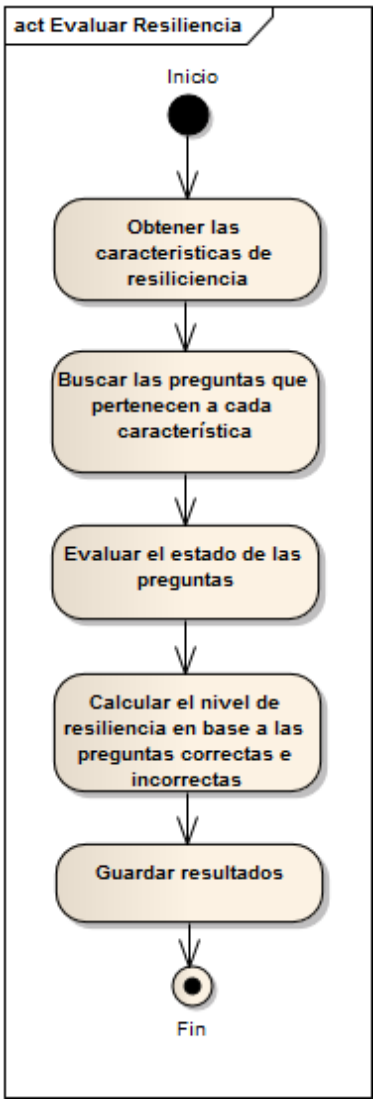


Figura 99. Diagrama de actividades evaluar resiliencia.
Fuente: El autor.

Visualizar sugerencias

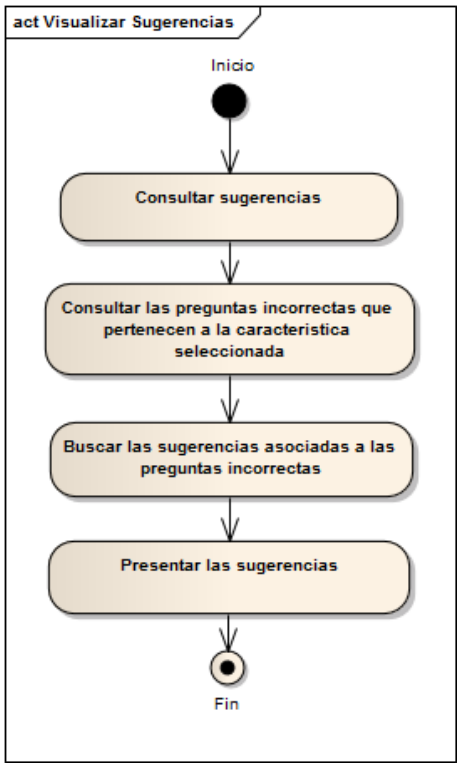


Figura 100. Diagrama de actividades visualizar sugerencias.
Fuente: El autor.

Visualizar estado

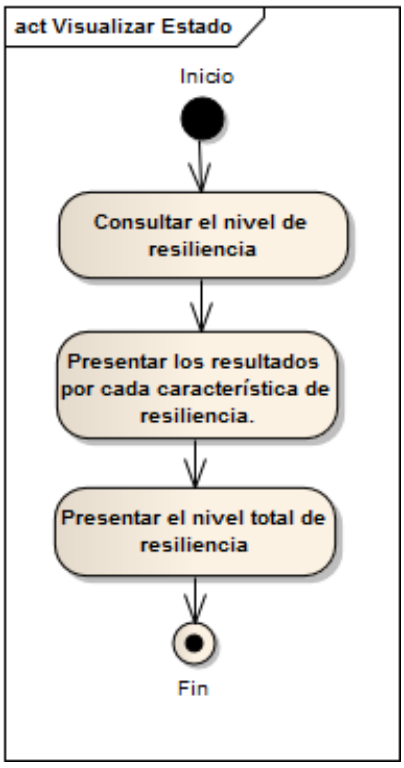


Figura 101. Diagrama de actividades visualizar estado.
Fuente: El autor.

K. Manual de usuario

1. Introducción

El sistema SISGRES se crea para evaluar la resiliencia en los sistemas de información sin importar el ámbito en el que se enfoquen; se maneja dos tipos de roles, un rol de tipo administrador dedicado a las operaciones básicas de inserción, actualización y eliminación de información tanto de los usuarios como de cuestionarios, y el otro rol de tipo cliente en cambio se encarga de responder los cuestionarios y el sistema presenta los resultados de la evaluación.

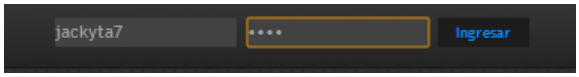
La página principal consta de las siguientes secciones:

1. En la parte superior de la página principal, se presenta la sección 1 correspondiente al logueo, donde se deberá ingresar el usuario y clave para acceder a las funcionalidades del sistema.
2. En la sección 2 está un menú de navegación que presenta información acerca de la metodología.
3. En la sección 3 se presenta un pequeño fragmento acerca de la resiliencia que podrá seguir leyendo si presiona clic en *LEER MÁS.*

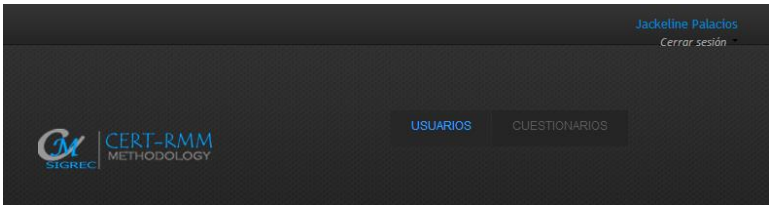
4. En la sección 4 están las áreas de resiliencia y al presionar clic sobre el nombre se podrá visualizar más información.
5. En la sección 5 se presenta un pequeño fragmento acerca de la metodología CERT-RMM que podrá seguir leyendo al presionar clic en *LEER MÁS.*

2. Funcionalidades del Usuario Administrador

Autenticarse en el sistema con el nombre usuario y clave.



Una vez dentro del sistema se procede a interactuar con las opciones que se presentan en el menú desplegable.



2.1. Usuarios.

En la gestión de usuarios se presenta una lista de los usuarios registrados en el sistema, con las opciones de actualizar y borrar, también está un submenú donde están las opciones de listar y registrar nuevo usuario.

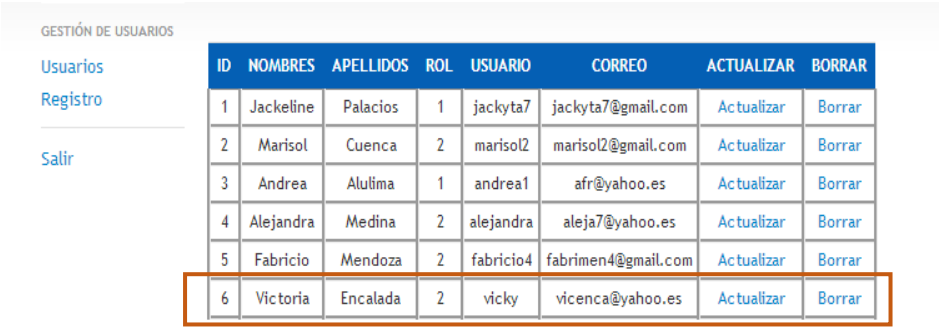
Registrar usuario.

Para registrar usuario se presiona clic en el submenú ***Registrar Usuario***.

Se presenta un formulario como el siguiente:

Debe completarse todos los campos del formulario y luego dar clic en el botón ***Registrarse*** para guardar la información. Cabe mencionar que todos los usuarios nuevos se registran con un rol de tipo cliente***.***

Luego se presentará el usuario registrado en la lista de usuarios.

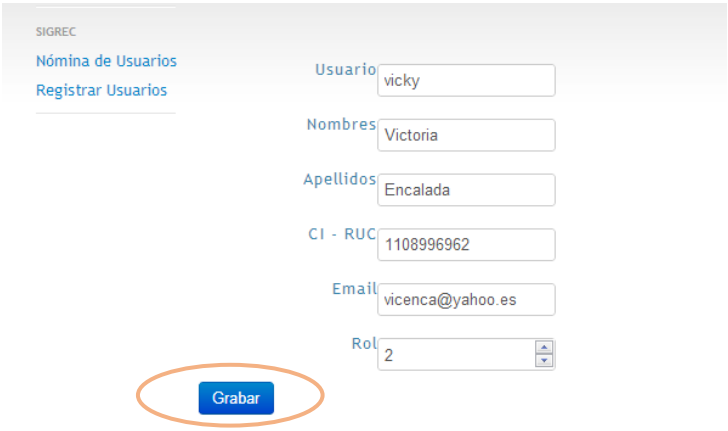


ID	NOMBRES	APELLIDOS	ROL	USUARIO	CORREO	ACTUALIZAR	BORRAR
1	Jackeline	Palacios	1	jackyta7	jackyta7@gmail.com	Actualizar	Borrar
2	Marisol	Cuenca	2	marisol2	marisol2@gmail.com	Actualizar	Borrar
3	Andrea	Alulima	1	andrea1	afr@yahoo.es	Actualizar	Borrar
4	Alejandra	Medina	2	alejandra	aleja7@yahoo.es	Actualizar	Borrar
5	Fabricio	Mendoza	2	fabricio4	fabrimen4@gmail.com	Actualizar	Borrar
6	Victoria	Encalada	2	vicky	vicenca@yahoo.es	Actualizar	Borrar

Actualizar usuario.

Para actualizar la información de los usuarios, se debe ubicar en el usuario a modificar y presionar clic en ***Actualizar.***

Luego se presenta un formulario con toda la información del usuario seleccionado y donde además se puede administrar el rol que desempeña (administrador, cliente). Para guardar los cambios se presiona el botón ***Grabar.***

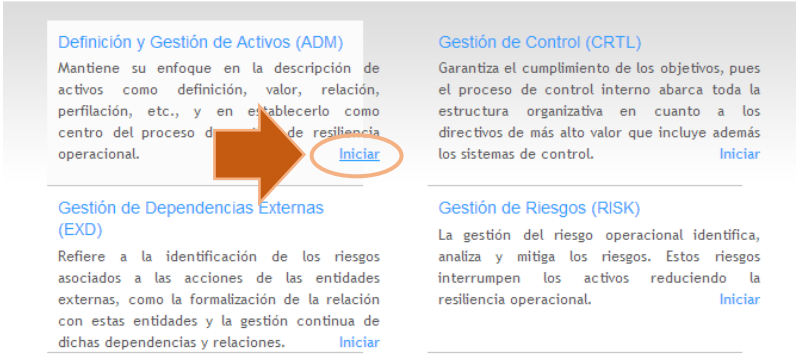


Eliminar usuario.

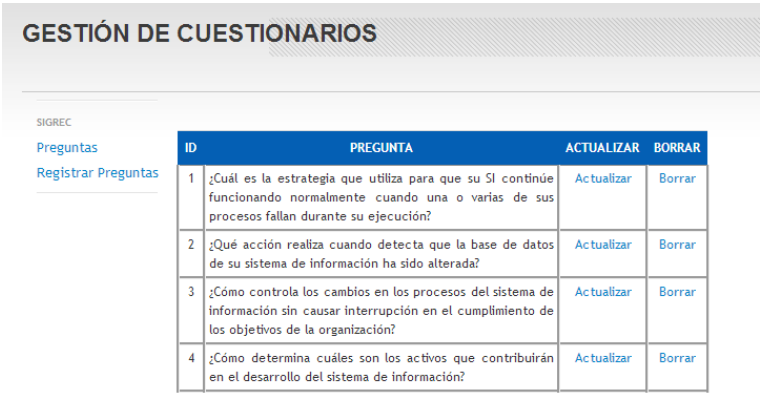
Para borrar la información de los usuarios, se debe ubicar en el usuario a modificar y presionar clic en ***Borrar.***

El usuario se eliminar en el instante.

2.2. Cuestionarios



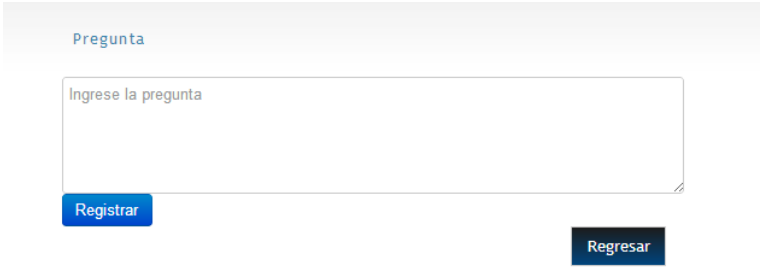
En la gestión de cuestionarios se presenta las áreas de la metodología y por cada área se presentarán un cuestionario. En este caso se analiza la primera área correspondiente a la ***Definición y Gestión de Activos (ADM)*** para mostrar los cuestionarios se da clic en ***Iniciar.***



Se presenta una lista de preguntas registradas en el sistema correspondiente al área seleccionada, con las opciones de actualizar y borrar, también está un submenú donde están las opciones para listar las preguntas y registrar preguntas nuevas.

Registrar pregunta

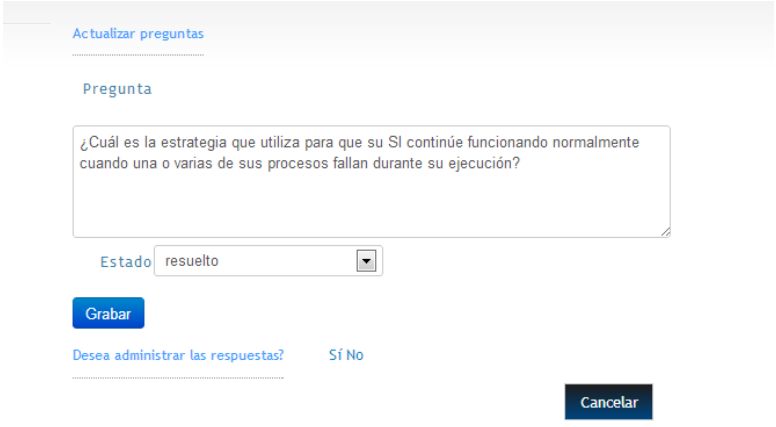
Para registrar una pregunta se presiona clic en el submenú ***Registrar Preguntas***.



Se presenta un recuadro en el cual se deberá ingresar el contenido de la pregunta. Para guardar se presiona clic en ***Registrar.***

Actualizar Pregunta

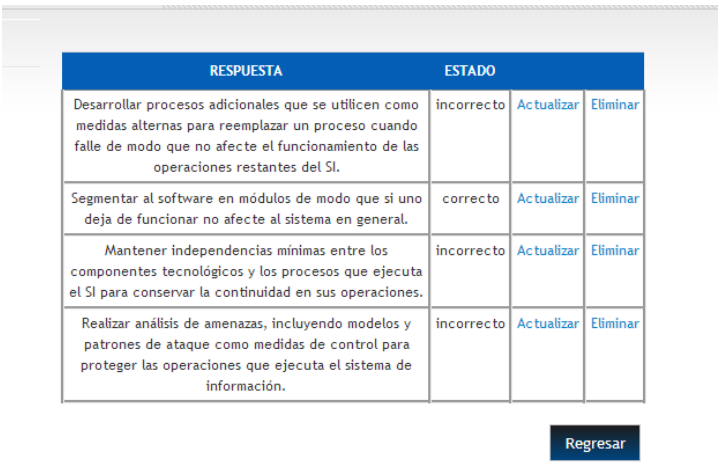
Para actualizar el contenido de las preguntas, se debe ubicar en la pregunta a modificar y presionar clic en ***Actualizar.*** Se presenta el contenido y estado de la pregunta.



Se puede editar el contenido de la pregunta y/o el estado (depende de las necesidades del usuario). Para guardar los cambios se presiona clic en el botón ***Grabar.***

Adicionalmente se muestra la opción de modificar el contenido de las respuestas pertenecientes a dicha pregunta.

En el caso de responder **Sí** a la modificación se lista las respuestas, con las opciones de Actualizar y Borrar.

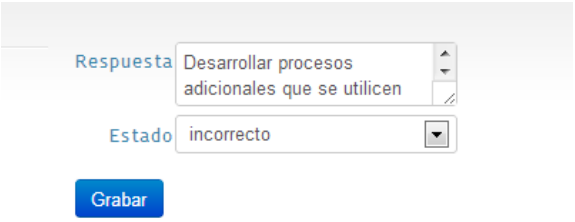


RESPUESTA	ESTADO		
Desarrollar procesos adicionales que se utilicen como medidas alternas para reemplazar un proceso cuando falle de modo que no afecte el funcionamiento de las operaciones restantes del SI.	incorrecto	Actualizar	Eliminar
Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.	correcto	Actualizar	Eliminar
Mantener independencias mínimas entre los componentes tecnológicos y los procesos que ejecuta el SI para conservar la continuidad en sus operaciones.	incorrecto	Actualizar	Eliminar
Realizar análisis de amenazas, incluyendo modelos y patrones de ataque como medidas de control para proteger las operaciones que ejecuta el sistema de información.	incorrecto	Actualizar	Eliminar

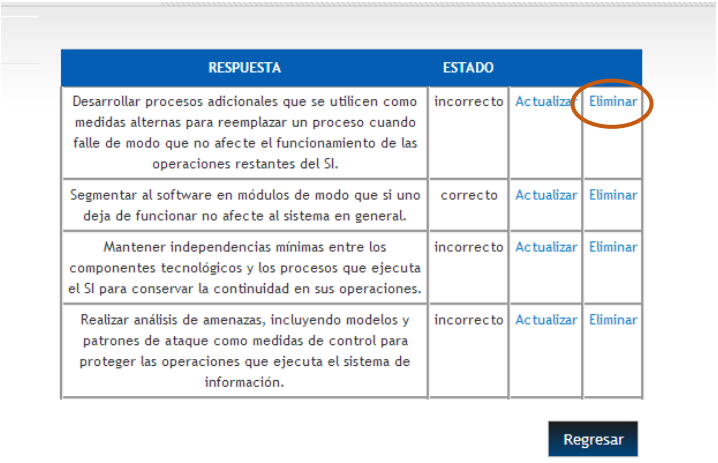
Regresar

Actualizar respuesta

Para actualizar el contenido de las respuestas, se debe ubicar en la pregunta a modificar y presionar clic en ***Actualizar.*** Se presenta el contenido y estado de la respuesta.



Se puede editar el contenido de la respuesta y/o el estado (depende de las necesidades del usuario). Para guardar los cambios se presiona clic en el botón ***Grabar.***



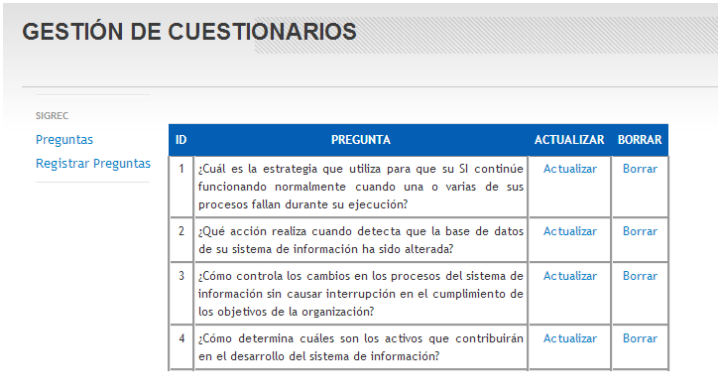
RESPUESTA	ESTADO		
Desarrollar procesos adicionales que se utilicen como medidas alternas para reemplazar un proceso cuando falle de modo que no afecte el funcionamiento de las operaciones restantes del SI.	incorrecto	Actualizar	Eliminar
Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.	correcto	Actualizar	Eliminar
Mantener independencias mínimas entre los componentes tecnológicos y los procesos que ejecuta el SI para conservar la continuidad en sus operaciones.	incorrecto	Actualizar	Eliminar
Realizar análisis de amenazas, incluyendo modelos y patrones de ataque como medidas de control para proteger las operaciones que ejecuta el sistema de información.	incorrecto	Actualizar	Eliminar

Regresar

Eliminar respuesta

Para eliminar las respuestas se debe ubicar en la repuesta a eliminar y presionar clic en ***Eliminar*** y la respuesta se elimina del registro del sistema.

Eliminar pregunta



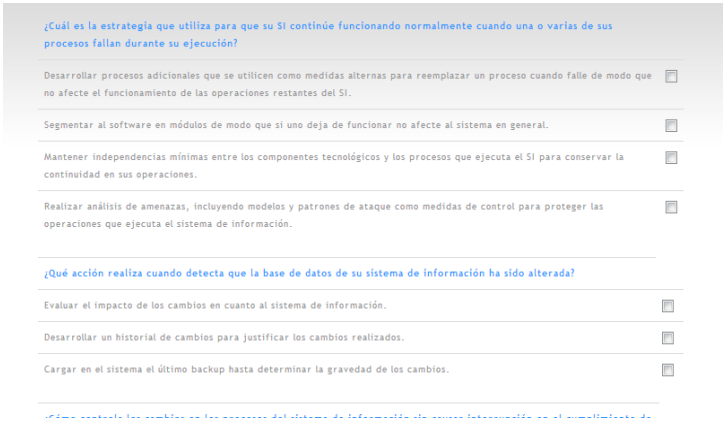
Para eliminar las preguntas del registro del sistema se debe ubicar en la pregunta a eliminar y se presiona clic en ***Borrar***.

3. Funcionalidades del usuario cliente

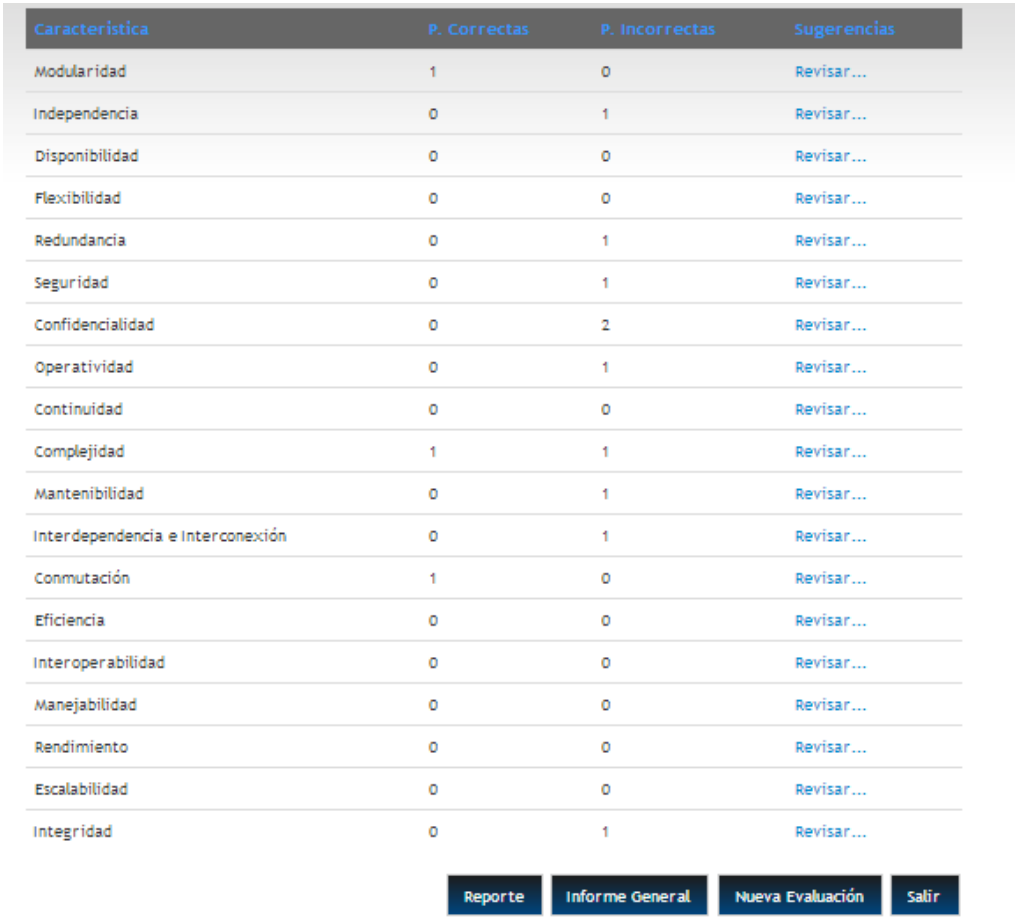
Para tener una idea clara de lo que se va realizar en esta funcionalidad, se presenta un mensaje donde el usuario debe aceptar o rechazar según su necesidad y conveniencia.

En el caso de aceptar el mensaje, se presenta las áreas de la metodología CERT-RMM donde cada una aloja un cuestionario que deberá resolverse.

Se toma la primera área correspondiente a la ***Definición y Gestión de Activos (ADM)*** y se da clic en Iniciar para que se listen las preguntas.



Una vez listadas las preguntas el usuario puede responderlas. De todas las respuestas listadas por cada pregunta se debe seleccionar la que crea correcta y al terminar se presiona un clic en el botón ***Terminar*** para guardar las respuestas.; una vez resueltos todos los cuestionarios de las áreas se procede a ***Generar los resultados.*** (Esta acción se realiza por cada área)



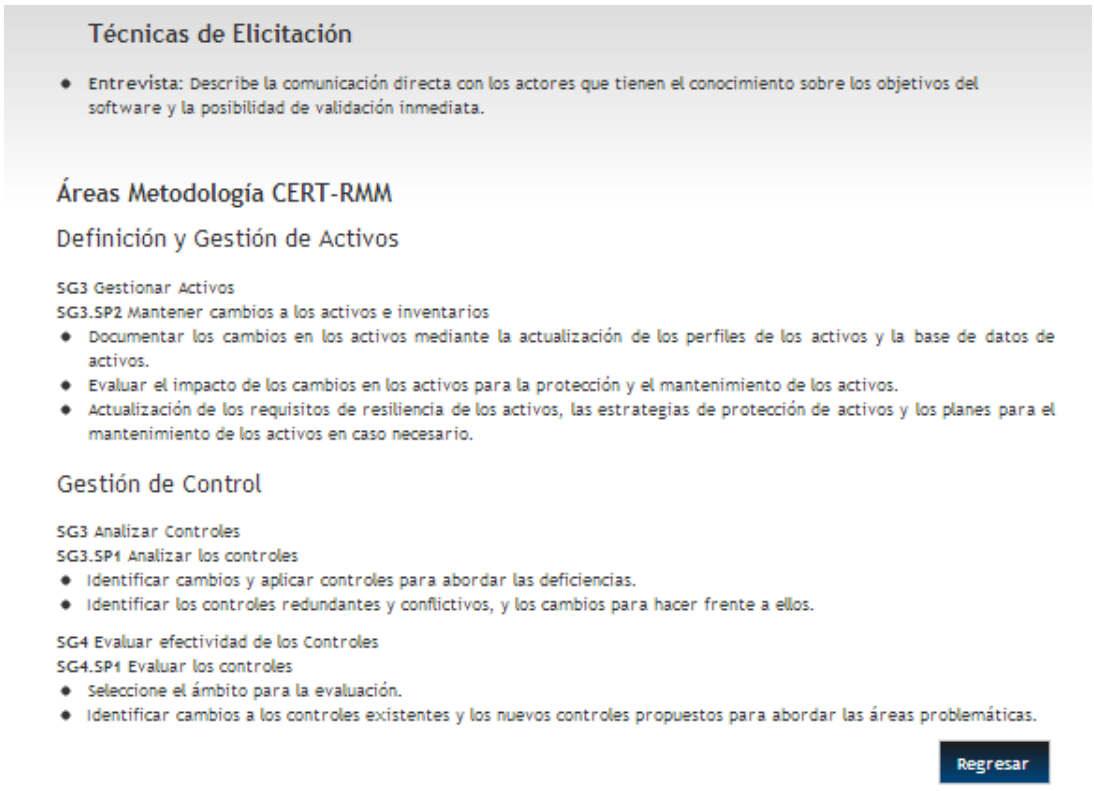
Característica	P. Correctas	P. Incorrectas	Sugerencias
Modularidad	1	0	Revisar...
Independencia	0	1	Revisar...
Disponibilidad	0	0	Revisar...
Flexibilidad	0	0	Revisar...
Redundancia	0	1	Revisar...
Seguridad	0	1	Revisar...
Confidencialidad	0	2	Revisar...
Operatividad	0	1	Revisar...
Continuidad	0	0	Revisar...
Complejidad	1	1	Revisar...
Mantenibilidad	0	1	Revisar...
Interdependencia e Interconexión	0	1	Revisar...
Conmutación	1	0	Revisar...
Eficiencia	0	0	Revisar...
Interoperabilidad	0	0	Revisar...
Manejabilidad	0	0	Revisar...
Rendimiento	0	0	Revisar...
Escalabilidad	0	0	Revisar...
Integridad	0	1	Revisar...

Reporte | Informe General | Nueva Evaluación | Salir

Es así que se presenta los resultados en base a las respuestas correctas e incorrectas enfocadas en cada una de las características del software resiliente. Por cada una de ellas se presentan sugerencias útiles para mejorar el sistema de información en el cual se haya basado el usuario para responder los cuestionarios. A las sugerencias se puede acceder presionando clic en la opción ***Revisar.***

Característica	P. Correctas	P. Incorrectas	Sugerencias
Modularidad	1	0	Revisar...
Independencia	0	1	Revisar...
Disponibilidad	0	0	Revisar...

Las sugerencias se otorgan de acuerdo a la metodología CERT-RMM para mejorar el nivel de cumplimiento por cada característica de resiliencia.



También se puede visualizar los resultados por área del CERT-RMM donde además presenta el nivel de resiliencia alcanzado por el sistema evaluado, dando clic en el botón ***Informe General.***

Areas	Total	L. Correctas	L. Incorrectas
Definición y Gestión de Activos	4	3	1
Gestión de Control	4	0	4
Gestión de Dependencias Externas	5	0	5
Gestión de Riesgos	0	0	0
Desarrollo de Requerimientos de Resiliencia	0	0	0
Gestión de Requerimientos de Resiliencia	0	0	0
Ingeniería de Soluciones Técnicas de Resiliencia	0	0	0
Continuidad del Servicio	0	0	0
Gestión Tecnológica	0	0	0
Respuestas	13	3	10

NIVEL DE RESILIENCIA: 0.39%

Regresar

Finalmente también se puede generar un reporte que consta del estado de las preguntas por área del CERT_RMM con resultados en el navegador o puede exportarlo en formato pdf.

Definición y Gestión de Activos

Pregunta	Lineamiento Sugerido	Lineamiento Marcado	Resultado
¿Cuál es la estrategia que utiliza para que su SI continúe funcionando normalmente cuando una o varias de sus procesos fallan durante su ejecución?	Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.	Segmentar al software en módulos de modo que si uno deja de funcionar no afecte al sistema en general.	correcto
¿Qué acción realiza cuando detecta que la base de datos de su sistema de información ha sido alterada?	Cargar en el sistema el último backup hasta determinar la gravedad de los cambios.	Cargar en el sistema el último backup hasta determinar la gravedad de los cambios.	correcto
¿Cómo controla los cambios en los procesos del sistema de información sin causar interrupción en el cumplimiento de los objetivos de la organización?	Mantener independencia entre los procesos de cada componente del sistema de información.	Desarrollar planes de control de cambios.	incorrecto
¿Cómo determina cuáles son los activos que contribuirán en el desarrollo del sistema de información?	Se realiza un inventario en base a los perfiles de los activos.	Se realiza un inventario en base a los perfiles de los activos.	correcto

Gestión de Control

Pregunta	Lineamiento Sugerido	Lineamiento Marcado	Resultado
¿Cuál es el tipo de control que utiliza para evitar actividades o interrupciones no deseadas en el software?	Controles técnicos que gestionan procesos automatizados y eficaces para la aplicación de necesidades de recuperación del software.	Se realiza un inventario en base a los perfiles de los activos.	incorrecto
¿Define estrategias de control jerárquico (por delegación de responsabilidades) como método de protección y mantenimiento de los activos del SI para asegurarse de que su exposición a vulnerabilidades y amenazas se gestiona?	Verdadero	Se realiza un inventario en base a los perfiles de los activos.	incorrecto
¿Cómo limita el acceso a los componentes del sistema de información?	Se maneja objetivos de control como políticas, normas, privilegios, etc.	Se realiza un inventario en base a los perfiles de los activos.	incorrecto