PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE UN MARCO DE TRABAJO PARA LA GESTIÓN DE INCIDENTES Y CRISIS DE CIBERSEGURIDAD BASADO EN LA NORMA ISO 22361

Tesis para obtener el título profesional de Ingeniero Informático

AUTOR:

Mauricio Gerardo Maldonado Alvarez

ASESORES:

Dr. Manuel Francisco Tupia Anticona

Dra. Mariuxi Alexandra Bruzza Moncayo (co-asesora)

Lima, Noviembre, 2024

INFORME DE SIMILITUD

Yo, MANUEL FRANCISCO TUPIA ANTICONA docente de la Facultad de CIENCIAS E INGENIERÍA de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado

DISEÑO DE UN MARCO DE TRABAJO PARA LA GESTIÓN DE INCIDENTES Y CRISIS DE CIBERSEGURIDAD BASADO EN LA NORMA ISO 22361

del/de la autor(a)/ de los(as) autores(as) MALDONADO ALVAREZ, MAURICIO GERARDO dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 27.%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el **13/11/2024**
- He revisado con detalle dicho reporte y confirmo que cada una de las coincidencias detectadas no constituyen plagio alguno, debido a que el porcentaje se debe a citas de imágenes y diagramas y porque el trabajo del alumno previamente fue subido durante los cursos de elaboración de tesis, por lo que hay similitud con sus propios avances.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 14 de noviembre de 2024

Apellidos y nombres del asesor / de la asesora: TUPIA ANTICONA MANUEL FRANCISCO	
DNI: 10279924	Firma
ORCID: 0000-0001-5260-2829	

Resumen

A partir de la revisión de la literatura, se ha podido identificar que los incidentes mal gestionados pueden desencadenar una crisis dentro de la organización con un mayor impacto al negocio. Adicionalmente, el no contar con un plan de respuesta definido para mitigar un incidente de ciberseguridad, produce el riesgo de que la organización experimente una recuperación más lenta, lo que intensifica cualquier daño causado generando en una crisis dentro de la organización. (Aljaryan et al., 2022).

Entonces, en relación a lo mencionado anteriormente, sin un correcto uso de procedimientos de gestión de crisis, la organización responde con una intervención inadecuada o incluso no brinda ninguna respuesta a la crisis en alguno de los tres puntos principales de la gestión de crisis definidos en (Weil & Murugesan, 2020): detección de la causa, estrategia de respuesta y comunicación durante la crisis. Este último punto resulta muy crítico para las organizaciones, porque sin una adecuada gestión de las comunicaciones durante las crisis se puede producir una afectación negativa en la reputación e imagen de la organización por falta de transparencia hacia las partes interesadas. Asimismo, una mala gestión de comunicaciones no permite identificar correctamente al equipo de respuesta y mucho menos permite la correcta distribución de responsabilidades, produciendo una respuesta nula o tardía a la crisis.

Por tales motivos, el presente proyecto de fin de carrera tiene como finalidad diseñar un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361. Este marco está conformado por tres dominios, los cuales agrupan procesos con sus respectivas descripciones, actividades, métricas, documentación relacionada, y lista de roles y responsabilidades. Asimismo, se incluye una guía de implementación del marco paso a paso. Finalmente, se realiza un análisis comparativo entre la gestión de crisis real seguida en un caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Capítulo 1. Generalidades

1.1 Problemática

En este capítulo se realiza la elaboración del árbol de problemas. Asimismo, se describe la problemática y se presenta el problema central del proyecto.

1.1.1 Árbol de Problemas

Tabla 1: Árbol de problemas

PROBLEMAS EFECTOS	Incidentes de ciberseguridad que derivan en crisis con un mayor impacto al negocio.	Inadecuada intervención del personal encargado de hacer frente a crisis generadas por incidentes de ciberseguridad.	Ineficiente distribución de responsabilidades en el personal de la organización, durante las crisis generadas por incidentes de ciberseguridad	Afectación negativa en la reputación e imagen de la organización por falta de transparencia hacia las partes interesadas (clientes, proveedores, entre otros).
PROBLEMA CENTRAL	**Inexistencia de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en buenas prácticas internacionales**			
PROBLEMAS CAUSAS	Los incidentes de ciberseguridad no son gestionados de una manera adecuada por la falta de seguimiento de buenas prácticas internacionalmente aceptadas.	Durante las crisis generadas por incidentes de ciberseguridad no se aplican apropiados procedimientos de gestión de crisis.	Durante las crisis generadas por incidentes de ciberseguridad no se gestiona adecuadamente las comunicaciones	

Fuente: Elaboración Propia

1.1.2 Descripción

En la actualidad y sobre todo a raíz de la pandemia de COVID-19, las organizaciones se han visto afectadas por un constante aumento de incidentes de ciberseguridad, esto

debido a distintas razones y circunstancias. En (Alawida et al., 2022) se menciona que los ciberdelincuentes han aprovechado algo tan generalizado y disruptivo como el COVID-19, para causar estragos en diferentes organizaciones y atacar sus datos más que nunca. Asimismo, en (Yerina et al., 2021) se comenta que año tras año, los delitos cibernéticos son cada vez más organizados, técnicamente avanzados y hasta psicológicamente elegantes, generando consecuencias cada vez más destructivas. De acuerdo con la Allianz Risk Barometer, las pérdidas globales por delitos cibernéticos alcanzan los 600,000 millones de USD por año, lo que es casi tres veces la pérdida anual promedio por desastres naturales (Allianz., 2019).

Es importante recalcar que como se menciona en (Sarabi et al., 2016) los ciberataques pueden tomar varias formas. Pueden abarcar la exposición accidental o la pérdida de datos, hasta los ataques de ransomware o la interrupción de los sistemas. Lo que significa que la prevención total vía la gestión de riesgos es casi imposible, ya que los ciberdelincuentes generalmente se encuentran por delante de la curva de seguridad. Por lo tanto, un enfoque puramente preventivo debe complementarse con medidas de mitigación y respuesta cuando la prevención es inalcanzable o demasiado costosa (Kuipers & Schonheit, 2022). Sin embargo, en muchas organizaciones no se tiene en cuenta este punto o de plano no se realiza gestión de riesgos, por lo que no existe o no se realiza una adecuada atención de este tipo de incidentes, lo que luego puede llevar a una crisis dentro de la organización como se menciona en (ISO, 2021).

Entonces a partir de la revisión de la literatura, se ha podido identificar que los incidentes mal gestionados pueden desencadenar una crisis dentro de la organización con un mayor impacto al negocio. Asimismo, sin una estrategia de respuesta clara para aliviar un incidente de ciberseguridad, se sufre el riesgo de que la organización tarde más en recuperarse y esto finalmente intensifica cualquier daño causado lo que se traduce en una crisis dentro de la organización sobre todo por la carencia de una adecuada comunicación durante las crisis y sus procesos de resolución (Aljaryan et al., 2022).

Es importante recalcar que aunque muchas crisis parecen ser únicas, a menudo tienen características consistentes que se presentan en (ISO, 2021):

- Baja predictibilidad: Las crisis suelen ser eventos o situaciones únicas y raras. Algunas crisis pueden anticiparse; sin embargo, el momento y el impacto por lo general no siempre son previsibles.
- Alto nivel de urgencia y presión: Una crisis siempre necesita atención urgente ya que el impacto puede ser muy alto. Por otro lado, dado el impacto potencial y el hecho de que una crisis tiene más visibilidad, es común que ejerza un alto nivel de presión sobre la organización.
- Alto impacto en la organización: Las crisis pueden trastornar o afectar a toda la organización, trascendiendo los límites organizativos, geográficos y sectoriales.
- Atraen la atención del público externo e interno: Es probable que las crisis generen un escrutinio e interés significativo entre las partes interesadas, incluidos miembros del público, usuarios de productos y servicios, grupos específicos (como reguladores, accionistas u organismos de la industria) y los medios de comunicación.
- Se requiere creatividad: Las crisis exigen una respuesta de liderazgo flexible, creativa, estratégica y sostenida que esté enraizada en los valores de la organización y en estructuras sólidas de gestión de crisis.

En general, es de suma importancia que se tome en cuenta cada una de estas características para manejar la crisis, porque de lo contrario esta terminará afectando de alguna u otra manera a la organización en su capacidad de funcionamiento, su reputación, marca, propiedad física, política, estructura organizativa, factores humanos, ambientales y económicos (ISO, 2021).

Por otro lado, se ha podido evidenciar que sin un correcto uso de procedimientos de gestión de crisis, la organización responde con una intervención inadecuada o incluso no brinda ninguna respuesta a la crisis en alguno de los tres puntos principales definidos en (Weil & Murugesan, 2020):

- Detección de la causa: La detección de la causa de una crisis producida por un incidente de ciberseguridad se refiere al proceso de identificar y comprender las causas subyacentes que han provocado la crisis en la organización, para poder abordarlas de manera efectiva y prevenir futuros incidentes similares. Asimismo, la detección de la causa de una crisis producida por un incidente de ciberseguridad puede implicar una revisión exhaustiva de los sistemas de seguridad y de la infraestructura tecnológica de la organización, la identificación de vulnerabilidades en el software o hardware, la revisión de los procesos de gestión de incidentes de seguridad y de la cultura de seguridad de la organización.
- Estrategia de respuesta: La estrategia de respuesta debe tener en cuenta diversos aspectos, como la evaluación de la magnitud del impacto, la definición de objetivos y prioridades, la coordinación de las acciones entre los diferentes equipos y partes interesadas, la asignación de responsabilidades y roles claros, la toma de decisiones rápidas y efectivas, la implementación de medidas para controlar y mitigar la crisis, y la comunicación clara y efectiva con los interesados.
- Comunicación durante la crisis: Abarca tanto la comunicación interna (equipo de respuesta a crisis) como la externa (clientes y público en general externo). Este subproceso requiere que la organización desarrolle una capacidad efectiva para comunicarse interna y externamente durante una crisis. Además, debe entregar un mensaje coherente que transmita la reacción de la organización ante una crisis, brindando información que se conozca en ese momento y de lo que se está haciendo para abordar los problemas.

Finalmente, una problemática que resulta muy habitual en las organizaciones durante las crisis generadas por incidentes de ciberseguridad es la inadecuada gestión de las comunicaciones, lo que en muchos casos produce una afectación negativa en la reputación e imagen de la organización por falta de transparencia hacia las partes interesadas (clientes, proveedores, entre otros). Esto se puede evidenciar en casos reales

donde muchas organizaciones perdieron confiabilidad y puntos de reputación por parte de sus clientes y los medios por una mala comunicación de la crisis (Kuipers & Schonheit, 2022). Asimismo, la mala gestión de las comunicaciones durante las crisis no permite identificar correctamente al equipo de respuesta y mucho menos permite la correcta distribución de responsabilidades, produciendo una respuesta nula o tardía a la crisis.

1.1.3 Problema seleccionado

Como se puede ver en la tabla 1, el problema seleccionado es la inexistencia de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en buenas prácticas internacionales. Resulta importante abordar este problema precisamente, porque en la actualidad es necesario contar con un conjunto de buenas prácticas que permita a las empresas responder de manera completa y adecuada a la crisis, lo que incluye la gestión de incidentes de ciberseguridad, de los equipos de respuesta, de la crisis producida y de las comunicaciones necesarias. Dicho esto, el presente proyecto de fin de carrera tiene como finalidad diseñar un un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un marco de trabajo que permita gestionar los incidentes y crisis de ciberseguridad siguiendo los principios de la norma ISO 22361.

1.2.2 Objetivos específicos

O 1. Definir la vista de componentes del marco a alto nivel.

O 2. Desarrollar los procesos que conforman los componentes.

O 3. Elaborar la guía de implementación del marco.

O 4. Aplicar la guía en un caso de estudio.

1.2.3 Resultados esperados

O 1. Definir la vista de componentes del marco a alto nivel.

R 1. Lista de procesos que conforman los componentes del marco.

O 2. Desarrollar los procesos que conforman los componentes.

R 2. Modelo de procesos, actividades y métricas de cada uno de los componentes.

R 3. Lista de roles y responsabilidades por proceso.

O 3. Elaborar la guía de implementación del marco.

R 4. Guía de implementación del marco.

O 4. Aplicar la guía a un caso de estudio.

R 5. Caso de estudio elegido.

R 6. Informe de aplicación del marco al caso de estudio.

1.2.4 Mapeo de objetivos, resultados y verificación

Tabla 2: Medio de verificación, indicadores y herramientas o métodos de los resultados esperados del primer objetivo específico

Objetivo 1: Definir la vista de componentes del marco a alto nivel.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramienta o Método**
R1: Lista de procesos que conforman los componentes del marco.	Informe con la hoja de ruta de creación de los componentes del marco a alto nivel.	Validación al 100% de la lista de componentes a alto nivel del marco por expertos en ciberseguridad o gestión de crisis.	1. NIST - Computer Security Incident Handling Guide 2. ITIL v4 3. ISO 22361 4. ENISA - How to setup CSIRT and SOC

Fuente: Elaboración Propia

Tabla 3: Medio de verificación, indicadores y herramientas o métodos de los resultados esperados del segundo objetivo específico

Objetivo 2: Desarrollar los procesos que conforman los componentes.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramienta o Método**
R2: Modelo de procesos, actividades y métricas de cada uno de los componentes.	Informe con la documentación completa del marco.	Validación al 100% del informe con la documentación completa por especialista en ciberseguridad o gestión de crisis.	1. NIST - Computer Security Incident Handling Guide 2. ITIL v4 3. ISO 22361 4. ENISA - How to setup CSIRT and SOC
R3: Lista de roles y responsabilidades por proceso.	Documento que contenga las matrices de roles y responsabilidades para cada proceso.	Validación al 100% de las matrices de roles y responsabilidades por experto en ciberseguridad, equipos de respuesta a incidentes o gestión de crisis.	1. NIST - Computer Security Incident Handling Guide 2. ITIL v4 3. ISO 22361 4. ENISA - How to setup CSIRT and SOC 5. Matriz RACI

Fuente: Elaboración Propia

Tabla 4: Medio de verificación, indicadores y herramientas o métodos de los resultados esperados del tercer objetivo específico

Objetivo 3: Elaborar la guía de implementación del marco.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramienta o Método**

R4: Guía de implementación del marco.	Documento con la guía de implementación del marco paso a paso.	Validación al 100% del documento con la guía de implementación del marco por especialista en seguridad, ciberseguridad o gestión de crisis.	1. Bizagi 2. Matriz RACI

Fuente: Elaboración Propia

Tabla 5: Medio de verificación, indicadores y herramientas o métodos de los resultados esperados del cuarto objetivo específico

Objetivo 4: Aplicar la guía a un caso de estudio.			
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**	**Herramienta o Método**
R5: Caso de estudio elegido.	Descripción detallada del caso de estudio que puede ser tomado de la realidad, que haya sido exitosamente o no resuelto.	Validación al 100% de la pertinencia del caso de estudio con el proyecto de tesis, realizado por un especialista en seguridad, ciberseguridad, gestión de continuidad o crisis.	1. Harvard Business Publishing Education 2. The Case Centre
R6: Informe de aplicación del marco al caso de estudio.	Análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado.	Validación al 100% del análisis comparativo por un especialista en seguridad, ciberseguridad, gestión de continuidad o crisis.	1. Análisis comparativo.

Fuente: Elaboración Propia

1.3 Métodos y Procedimientos

1.3.1 ISO 22361

Este estándar tiene como propósito ayudar en el diseño y desarrollo continuo de la capacidad de gestión de crisis de una organización. Establece los principios y prácticas necesarios para todas las organizaciones (ISO, 2021). Cabe decir que dentro de este estándar se detalla también cómo realizar la gestión de comunicaciones en crisis.

Esta ISO será usada para identificar los factores internos y externos que definen a las crisis generadas por incidentes de ciberseguridad. Además, se usará como referencia para definir cada una de las actividades del modelado de proceso de gestión de crisis cibernética y de comunicaciones en crisis.

1.3.2 NIST - Computer Security Handling Guide

Documento que proporciona pautas y mejores prácticas para la gestión de incidentes de ciberseguridad. Busca ayudar a las organizaciones a mitigar los riesgos de los incidentes de ciberseguridad proporcionando pautas prácticas para responder a los incidentes de manera eficaz y eficiente. Incluye lineamientos para establecer un programa efectivo de respuesta a incidentes; sin embargo, el enfoque principal del documento es detectar, analizar, priorizar y manejar incidentes (NIST, 2012).

Este documento se usará como referencia para elaborar la estructura de un equipo de respuesta a incidentes. Asimismo, será usado para definir los roles y responsabilidades de cada uno de los miembros del equipo de respuesta elaborado.

1.3.3 ITIL v4

Marco de buenas prácticas para garantizar un sistema flexible, coordinado e integrado para el gobierno y la gestión efectiva de los servicios habilitados de TI (ITIL, 2019). Dentro de este marco se proporcionan directrices sobre cómo establecer un proceso de gestión de incidentes eficiente. Lo que incluye la identificación, registro, clasificación,

priorización, investigación y resolución de incidentes. Además, dentro del marco se hace énfasis en los equipos de respuesta a incidentes de seguridad (CSIRT), proporcionando orientación sobre cómo establecer una colaboración efectiva, y detallando los roles y responsabilidades de cada miembro.

Este marco se usará como referencia para elaborar la estructura de un equipo de respuesta a incidentes. Asimismo, será usado para definir los roles y responsabilidades de cada uno de los miembros del equipo de respuesta elaborado.

1.3.4 ENISA

ENISA es una agencia de la Unión Europea dedicada a la ciberseguridad que tiene como objetivo principal mejorar la ciberseguridad en Europa. Entre sus principales actividades se incluyen el asesoramiento y recomendaciones en técnicas sobre ciberseguridad, análisis y evaluación de riesgos, capacitación y concientización, y cooperación internacional.

Dentro de sus publicaciones ENISA tiene un documento que se tomará como referencia para desarrollar algunos de los resultados planteados anteriormente:

- How to setup CSIRT and SOC

  Este documento se basa en un análisis de publicaciones actuales sobre el establecimiento del CSIRT. También, recoge las experiencias de diversos autores en el establecimiento y mejora del CSIRT como parte de numerosos proyectos llevados a cabo en Europa, Asia, África y América del Sur (ENISA, 2020).

  A lo largo de esta publicación se adopta un enfoque basado en los resultados para brindar orientación sobre las diferentes etapas involucradas en el establecimiento de una organización CSIRT o SOC, tomando en cuenta las siguientes fases: evaluación de la preparación, diseño, implementación, operaciones y mejora (ENISA, 2020).

Este documento se tomará como referencia para elaborar la estructura de un equipo de respuesta a incidentes. De igual manera, será usado para definir los roles y responsabilidades de cada uno de los miembros del equipo de respuesta elaborado.

1.3.5 Matriz RACI

La matriz RACI es una metodología de asignación de roles y responsabilidades utilizada en la gestión de proyectos y procesos. El acrónimo RACI proviene de las iniciales en inglés de los cuatros posible roles: Responsible (Responsable), Accountable (Responsable último), Consulted (Consultado), Informed (Informado).

Esta matriz tiene como objetivo ayudar en la definición clara de los roles y responsabilidades de los participantes en un proyecto o proceso, de manera que cada persona sepa exactamente qué se espera de ella y cómo se relaciona con los demás miembros del equipo.

Esta metodología se tomará como referencia para construir la estructura que permita definir la manera más adecuada de mostrar detalladamente la información de los roles y responsabilidades de cada miembro del equipo de respuesta a incidentes elaborado.

Un ejemplo del uso de la matriz RACI puede apreciarse en la Tabla 6, en donde un equipo de respuesta a incidentes tiene que realizar la detección y eliminación de un malware que afecta a la red de una empresa.

Tabla 6: Ejemplo de uso de la matriz RACI

Actividad / Recurso	Gestor de incidentes	Administrador de red	Oficial de seguridad	Experto en Ciberseguridad	Auditor de sistemas y TIC	Mesa de ayuda
Registro del incidente	A	I	C	C	I	R

Investigación de las causas raíz	R	C	A	C	-	I
Resolución del incidente de malware	C	C	A	R	-	I
Verificación de eliminación del malware	I	R	C	A	-	I
Medición de eficiencia y eficacia del equipo de respuesta a incidentes de ciberseguridad	I	I	A	I	R	I

Fuente: Elaboración Propia

1.3.6 Bizagi

Bizagi es una empresa de software que proporciona soluciones para la gestión de procesos de negocio (BPM, por sus siglas en inglés) y la transformación digital, ofreciendo herramientas que permiten a las organizaciones modelar, automatizar y mejorar sus procesos de negocio.

Específicamente, Bizagi Modeler es una herramienta popular utilizada para el modelado de procesos de negocio utilizando la notación BPMN (Business Process Model and Notation). Cabe decir que BPMN es un estándar gráfico ampliamente utilizado para representar visualmente los procesos de negocio.

Esta herramienta de software será utilizada para realizar el modelado de los procesos de gestión de crisis cibernética y comunicaciones utilizando la notación BPMN.

1.3.7 Análisis comparativo

Proceso de evaluar las similitudes y diferencias entre dos o más elementos, objetos, conceptos o entidades para comprender mejor sus características, rendimiento, ventajas o desventajas.

Para realizar un análisis comparativo se puede hacer uso de una matriz de comparación que enumera los diferentes aspectos o características que se desea comparar. Específicamente, en las columnas, se incluyen los elementos o entidades que se están comparando, y en las filas, se enumeran los criterios o características relevantes para la comparación. Además, dentro de la matriz se puede realizar un análisis de brechas para identificar si hay oportunidades de mejora o no.

Esta matriz de comparación será utilizada para realizar el análisis comparativo entre el caso de estudio elaborado y el protocolo propuesto de gestión de comunicaciones en crisis cibernética.

1.3.8 Harvard Business Publishing Education

Plataforma que se especializa en la creación y distribución de materiales de aprendizaje como casos de estudio, simulaciones, artículos, notas técnicas y otros recursos para apoyar la educación ejecutiva, la formación de líderes y el desarrollo profesional en el ámbito empresarial. Cabe resaltar que todos estos materiales de aprendizaje son recopilados de fuentes confiables, y por tanto su calidad está asegurada.

Esta plataforma será usada para seleccionar un caso de estudio que contenga un ejemplo de crisis cibernética. Luego, con el caso de estudio seleccionado se procederá a realizar el análisis comparativo entre este caso y el protocolo de comunicaciones en crisis cibernéticas desarrollado.

1.3.9 The Case Center

The Case Center es una organización sin fines de lucro que se dedica a la promoción y distribución de casos de estudio y materiales de enseñanza relacionados. Es una de las principales fuentes de casos de estudio utilizados en escuelas de negocios y programas de educación ejecutiva en todo el mundo.

The Case Centre será usada para seleccionar un caso de estudio que contenga un ejemplo de crisis cibernética. Posteriormente, con el caso de estudio seleccionado se procederá a realizar el análisis comparativo entre este caso y el protocolo de comunicaciones en crisis cibernéticas desarrollado.

Capítulo 2. Marco Legal/Regulatorio/Conceptual/otros

2.1 Introducción

El objetivo del marco conceptual es definir los principales conceptos que permitan contextualizar adecuadamente el problema que se va a resolver en el presente proyecto, haciendo énfasis en los conceptos relacionados a la gestión de crisis y el papel de las comunicaciones en la solución de incidentes de ciberseguridad que podrían convertirse en la categoría de crisis. Asimismo, cada concepto que se presente incluirá un ejemplo que permita comprender cómo estos se vinculan con el tema que se abordará acerca del diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361.

2.2 Desarrollo del marco conceptual

2.2.1 Ciberseguridad

Según el Instituto Nacional de Normas y Tecnologías (NIST, por sus siglas en inglés) se define ciberseguridad como “la prevención del daño, uso no autorizado, explotación y, en su caso, restauración de los sistemas electrónicos de información y comunicaciones, y la información que contienen, con el fin de fortalecer la confidencialidad, integridad y disponibilidad de estos sistemas” (NIST, 2015.). Los activos de la organización y del usuario incluyen dispositivos informáticos conectados, infraestructura, aplicaciones, sistemas de telecomunicaciones y la totalidad de información transmitida y/o almacenada en el entorno cibernético, en otras palabras, se pretende proteger los activos digitales.

Entonces, la ciberseguridad se esfuerza por garantizar el logro y el mantenimiento de las propiedades de seguridad de la organización y los activos del usuario frente a los riesgos de seguridad relevantes en el entorno cibernético. Es por ello que los objetivos generales de seguridad presentado en (ISO, 2013), enfocados en la ciberseguridad, comprenden lo siguiente:

- Disponibilidad: La información digital debe estar disponible en el tiempo que se requiera.
- Integridad: La información digital debe permanecer correcta y completa.
- Confidencialidad: La información digital solo debe ser accedida por personas autorizadas.

Relacionando este concepto con el tema que se abordara, se presenta a continuación los principales ataques informáticos usados para comprometer la seguridad de las organizaciones, según (Alawida et al., 2022) y (Aljaryan et al., 2022), y que por tanto afectan la disponibilidad, integridad o confidencialidad de la información:

- Hacking: Consiste en acceder o manipular las redes digitales como computadoras, laptops, tabletas y teléfonos. Robando así datos confidenciales como contraseñas, nombres de usuario, información bancaria y otros datos personales.
- Phishing: Método de explotación de ingeniería social que se utiliza con frecuencia para obtener información confidencial de los usuarios, como credenciales de inicio de sesión de banca en línea o credenciales de inicio de sesión de la empresa, todo ello mediante el envío de mensajes fraudulentos a su objetivo.
- Ransomware: Tipo de software malicioso que los delincuentes diseñan para evitar que los usuarios accedan a su información a menos que paguen dinero
- Botnet attack: Dispositivo como una computadora, servidor o teléfono infectado con un malware (programa malicioso) para realizar acciones destructivas sin el conocimiento del usuario.
- APT (Amenaza Persistente Avanzada): Un ataque o amenaza persistente avanzada conocido como APT ocurre cuando un usuario no autorizado utiliza formas avanzadas y sofisticadas para obtener acceso a un sistema o red.
- Malware: El malware es un software o código destinado a dañar las computadoras al cifrar archivos, dañar, deshabilitar, robar datos u obtener accesos no autorizados a diferentes sistemas.

- Business Email Compromise (BEC): Son un conjunto de estrategias de ingeniería social y correos electrónicos de phishing, utilizados para infiltrarse en las organizaciones, con el propósito de engañar a los empleados y ejecutivos desprevenidos para que realicen tareas que parecen provenir de un remitente confiable.
- Ataque DDoS: Es un tipo de ataque que los ciberdelincuentes implementan para hacer que los servicios en línea no estén disponibles para los usuarios al generar una gran cantidad de tráfico.
- Websites maliciosos: Representa un conjunto de aplicaciones web que pueden tomar diferentes formas, incluyendo páginas de phishing, páginas web infectadas con malware, páginas de descarga de software falso o páginas web fraudulentas que promueven esquemas fraudulentos.
- Spam: Son mensajes no solicitados o anónimos que se envían de forma masiva por correo electrónico, con el propósito de robar información de los usuarios.

2.2.2 Incidentes

Se define un incidente como una situación que puede ser (o podría conducir a) una interrupción, pérdida, emergencia o crisis (ISO, 2O18).

Sin embargo, en un contexto de ciberseguridad, según ITIL, se define un incidente como "cualquier interrupción no planificada en el servicio de TI o cualquier reducción en la calidad del mismo" (ITIL, 2019). Considerando que un incidente de TI puede variar en gravedad, desde un problema menor que afecta a un solo usuario hasta un problema crítico que afecta a múltiples usuarios o sistemas.

Ejemplo: Una crisis basada en un incidente de ciberseguridad se produjo en la organización de salud nacional de Irlanda (Flavin et al., 2022), siendo que el viernes 14 de mayo de 2021, se descubrió que la organización de salud nacional de Irlanda fue víctima de un ciberataque significativo en sus sistemas de tecnología de la información (TI), a través de un Ransomware. Como resultado, más del 80 % de la infraestructura de

TI se vio afectada, con la pérdida generalizada de información y diagnóstico de los pacientes. Esto resultó en graves efectos en el servicio nacional de salud y la prestación de atención, incluida la oncología. También se perdieron los sistemas nacionales de comunicación, incluidas las redes telefónicas.

2.2.3 Gestión de Incidentes

Según ITIL se define la gestión de incidentes como "el proceso de gestión de eventos no planificados o interrupciones no previstas que afectan a los servicios de TI y la capacidad del negocio para operar" (ITIL, 2019). En otras palabras, la gestión de incidentes en ITIL se maneja como un proceso reactivo que se enfoca en restaurar los servicios de TI lo más rápido posible, de tal forma que se minimice el impacto del incidente en el negocio.

El ciclo de vida de la gestión de incidentes, según ITIL, se muestra en la figura 1 presentada a continuación:

Figura 1: Ciclo de vida de gestión de incidentes. Tomado de ITIL v4 (2019)

Un ejemplo de una gestión de incidentes inicial se muestra a continuación, a través del caso de estudio presentado en (Ribaux & Souvignet, 2020):

El 6 de agosto de 2019, el Director de la Escuela de Justicia Penal, se vio afectado por un intento de suplantación de identidad, a través de correos electrónicos, con el fin de tomar su posición para exigir un servicio que implicaba un robo monetario a los miembros de la Escuela de Justicia Penal.

En primer lugar, cuando el director se dio cuenta de este intento de suplantación, informó al departamento de TI de la Escuela sobre la situación actual. Enseguida, el departamento de TI comenzó con la creación de un número de ticket para el incidente detectado. Al principio se priorizo el incidente como medio, debido a que se pensaba que era un pequeño intento de suplantación. Sin embargo, debido a la insistencia del director y al hecho de que un miembro de la Escuela ya se había visto comprometido por esta suplantación, se procedió a escalar el incidente a una priorización de alto impacto, esto generó que el departamento de TI de una respuesta rápida al incidente. Esta respuesta consistió en la elaboración de un script para interceptar cualquier correo enviado a la dirección "falsa", con ello se buscaba evitar que más miembros de la Escuela se comunicaran con esta dirección falsa de correo (persona que intentaba suplantar al Director). Finalmente, con esta respuesta se logró contener el intento de suplantación y se dio por concluido el incidente.

2.2.4 Crisis

Se define crisis como un evento o situación anormal que amenaza a una organización o comunidad y requiere una respuesta estratégica, adaptativa y oportuna para preservar su viabilidad e integridad (ISO, 2021). Asimismo, cuando se habla de crisis se deben considerar los siguientes puntos:

- El evento o situación puede incluir un alto grado de complejidad, inestabilidad e incertidumbre. Asimismo, puede exceder la capacidad de respuesta de la organización.

- Dada la naturaleza de una crisis, se necesita un enfoque flexible y dinámico, además de los planes y procedimientos ensayados.
- Las crisis pueden afectar la capacidad de funcionamiento de la organización, su reputación, marca, propiedad física, política, estructura organizativa, factores humanos, ambientales y económicos.

Es importante mencionar, que a menudo una crisis es precipitada por un incidente. En la figura 2 se muestra la relación entre un incidente y una crisis.

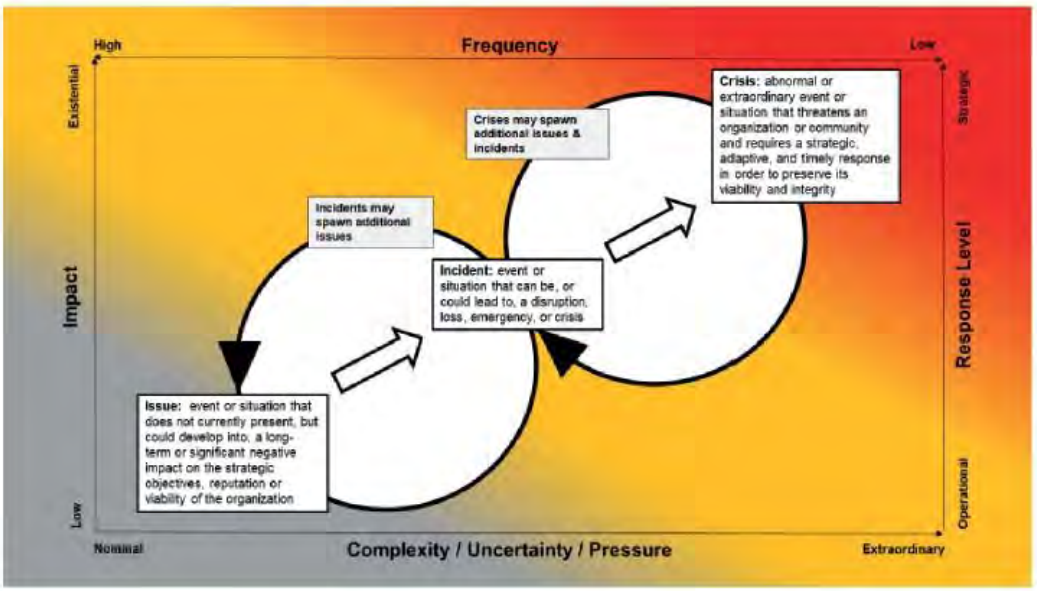


Figura 2: Relación entre un incidente y una crisis. Tomado de ISO 22361: Crisis management (2021)

Un ejemplo claro de cómo un incidente se puede convertir en la categoría de crisis se muestra a continuación con el caso producido en el Centro Médico de la Universidad de Vermont (Stowman et al., 2022):

A medida que los sistemas hospitalarios se vuelven más grandes, más complejos y cada vez más interdependientes, las organizaciones son mucho más vulnerables a los ataques de malware y ransomware. Además, aunque los hospitales y laboratorios han realizado grandes inversiones en sistemas médicos, muchos no han adoptado medidas de seguridad adecuados para combatir posibles ataques y carecen de la infraestructura de

tecnología de la información (TI) necesaria para negociar un ataque, sobrevivir al tiempo de inactividad, y poner en marcha un plan de recuperación. Entonces cuando el centro médico fue atacado ciberneticamente, tanto su sistema médico “EHR”, como los sistemas de farmacia, programación, radiología, facturación, y nómina, fueron completamente bloqueados. Asimismo, todos los sistemas informáticos asociados al hospital se desconectaron, incluidos los de 5 hospitales de la red en todo Vermont y Nueva York. El cierre finalmente duró más de 25 días, con algunas interrupciones del subsistema que duraron más de 40 días.

En este caso se puede observar como un incidente de ciberseguridad, se convierte en la categoría de crisis, debido a su gran escala e intensidad que sobrepasa los planes de respuesta que se puedan tener dentro de la gestión de incidentes.

2.2.5 Gestión de Crisis

Se define gestión de crisis como un conjunto de actividades coordinadas para liderar, dirigir y controlar una organización con respecto a la crisis (ISO, 2021). Asimismo se menciona que una gestión exitosa de crisis requiere flexibilidad y creatividad. Esto puede implicar salirse de las reglas normales de la organización o de su entorno empresarial y estar preparado para defender o justificar sus acciones. Es importante mencionar que en el presente trabajo, la gestión de crisis se acotará a solo crisis de ciberseguridad, es decir, aquellas que son producidas por incidentes de ciberseguridad

Los principios base para la gestión de crisis, según (ISO, 2021) se mencionan a continuación:

- Gobernanza: La gestión de crisis depende de una gobernanza eficaz en todos los niveles de la organización, comenzando con la alta dirección.
- Estrategia: La gestión de crisis es una capacidad estratégica.
- Riesgo: La capacidad de gestión de crisis es dinámica y se basa en la gestión eficaz del riesgo.

- Toma de decisiones: La toma de decisiones eficaz depende de una buena gestión de la información, la conciencia situacional y la compresión de los intereses de las partes interesadas.
- Comunicación: La gestión de crisis requiere de una comunicación efectiva.

Como se mencionó en la sección 2.2.4, una inadecuada gestión de crisis o una falta de gestión de crisis, puede generar daños profundos en la organización con respecto a su reputación, funcionamiento, entre otros aspectos. Entonces, a continuación se plantea un ejemplo extraído de (Kuipers & Schonheit, 2022) que permite evidenciar como una mala o ausente gestión de crisis generada por un incidente de ciberseguridad puede producir que se tome cualquier acción incorrecta que produce daños en la organización:

El caso de la empresa Equifax implicó la filtración de 143 millones de datos PII (Información Personal de Identificación) de consumidores de los sistemas de la agencia de informes crediticios. Esto se produjo debido al software defectuoso de la empresa y la falta de parches de vulnerabilidades conocidas durante más de un año. Asimismo, se menciona que debido a una inadecuada gestión de respuesta a la crisis, Equifax redirigió a sus clientes a una nueva página web de la empresa, sin saber que los piratas informáticos también ya habían instalado un malware en esa página. Lo mencionado anteriormente, junto al hecho de que la empresa negaba cualquier tipo de ineficiencia en su gestión de respuesta a la crisis, produjo una negativa aceptación por parte de sus clientes y los medios de comunicación, lo que afectó notablemente a su reputación.

2.2.6 Gestión de las comunicaciones en crisis

La gestión de las comunicaciones en crisis, según la norma ISO 22361 se define como "comunicaciones tanto internas como externas para proporcionar información, actualizaciones e instrucciones a las partes interesadas internas y externas" (ISO, 2021). Asimismo, menciona que una comunicación de crisis adecuada tiene como objetivo proteger la reputación y la marca de la organización.

Adicionalmente, se recalca una serie de aspectos que las organizaciones deben tener en cuenta para la gestión de comunicaciones en crisis:

- Desarrollar una capacidad efectiva para establecer una comunicación interna y externa durante una crisis.
- Desarrollar y entregar un mensaje coherente que transmita la reacción de la organización ante una crisis.
- Proporcionar información que se conoce en ese momento y lo que se está haciendo para abordar los problemas y sus respuestas tanto a nivel humano como organizacional.

A continuación, se presenta un flujo práctico de comunicación en crisis que muestra los aspectos más importantes de la misma:

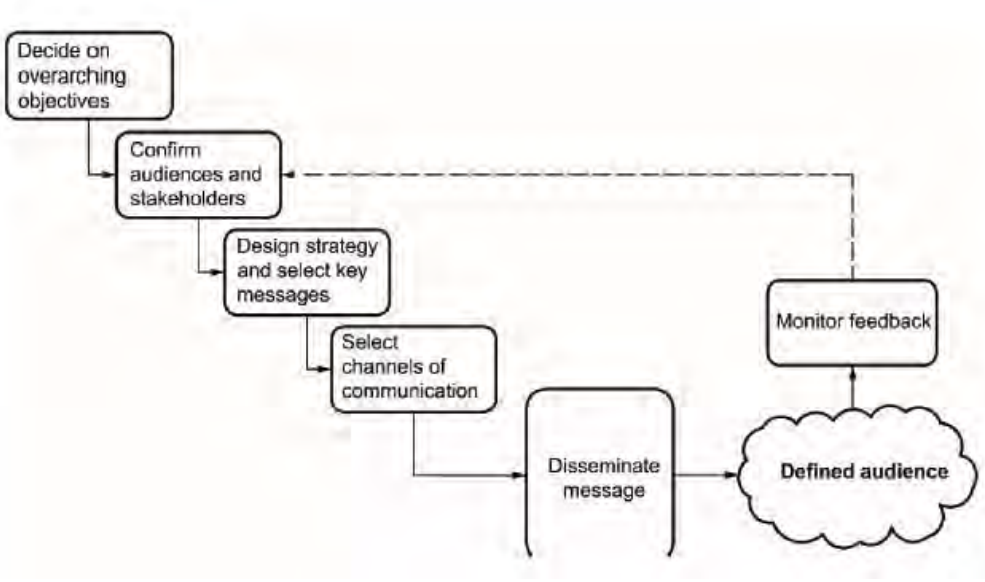


Figura 3: Flujo de comunicación en crisis. Tomado de ISO 22361: Crisis management (2021)

Es importante mencionar que este concepto es parte de los principios de la gestión de crisis, y por tanto su correcto manejo resulta relevante para responder a una crisis. En el siguiente ejemplo, recogido de (Kuipers & Schonheit, 2022), se recalca la importancia

de una correcta gestión de comunicaciones en crisis para así evitar que esta dañe por completo la reputación y confianza hacia organización:

La aseguradora de salud privada Anthem reveló su violación de datos el 4 de febrero de 2015. La violación incluyó 80 millones de filtraciones de información de identificación personal que contenía números de seguro social. Podría decirse que la autorrevelación colocó a la organización en una posición ventajosa. La mayoría de los artículos de los medios elogiaron la notificación oportuna y proactiva de Anthem sobre

la infracción. Los expertos en seguridad cibernética y los funcionarios del FBI respaldaron la respuesta de Anthem en comparación con el modus operandi habitual: "las organizaciones no por lo general, proporcionan una notificación tan pronto". Además, los medios de comunicación describieron el ataque como altamente sofisticado y culparon a los grupos criminales chinos, mientras informaban a la audiencia sobre el compromiso de Anthem con la seguridad cibernética mediante la actualización de los estándares de cifrado en su base de datos.

2.2.7 Gestión de la continuidad del negocio

Según la norma ISO 22301, se define la gestión de la continuidad del negocio como "el conjunto de procesos y medidas que se llevan a cabo para garantizar que una organización pueda continuar operando en caso de incidentes disruptivos y recuperarse de ellos, y de esa manera minimizar su impacto en el negocio, sus empleados y otras partes interesadas" (ISO, 2019).

Adicionalmente, la ISO establece que la gestión de continuidad del negocio implica los siguientes puntos:

- Identificación de los riesgos potenciales que puedan interrumpir la continuidad del negocio y la evaluación de su impacto.
- Implementación de planes y medidas de mitigación para minimizar los riesgos.

- Elaboración de planes de recuperación ante desastres para garantizar la continuidad de los servicios críticos en caso de un evento disruptivo.

Este concepto resulta relevante, ya que la gestión de la continuidad del negocio es un aspecto importante en la preparación para la gestión de crisis. En particular, los planes de continuidad del negocio son utilizados para garantizar que los servicios críticos puedan continuar funcionando durante y después de una crisis, lo que significa que los planes de continuidad son parte fundamental de la respuesta a una crisis.

Un ejemplo de cómo la gestión de la continuidad resulta importante para la gestión de crisis se muestra a continuación:

Retomando el ejemplo de (Flavin et al., 2022), se puede apreciar que se sufrió un ciberataque significativo en sus sistemas de tecnología de la información (TI), debido a un ataque de Ransomware. Como resultado, más del 80% de su infraestructura de TI se vio afectada. Esto resultó en graves efectos en el servicio nacional de salud y la prestación de atención. Entonces una vez que la organización detecta esta interrupción en su infraestructura de TI, procede a utilizar de inmediato su plan de continuidad, asegurando primero la asistencia del servicio de policía de la Oficina Nacional de Delitos Cibernéticos, la Organización Internacional de Policía Criminal (Interpol) y el Centro Nacional de Seguridad Cibernética. Asimismo, forma un equipo de respuesta, comunica a las partes interesadas sobre el ataque y toma medidas de contingencia. Todo lo mencionado, aseguró que se gestione de la mejor manera la crisis y se reduzca su impacto en la organización.

2.2.8 Recuperación ante desastres

La norma ISO 22301 define la recuperación ante desastres como “la capacidad de una organización para recuperarse de un incidente disruptivo y continuar las operaciones críticas del negocio en un nivel predefinido dentro de un plazo de tiempo aceptable, luego de una interrupción no planificada” (ISO, 2019). Teniendo como objetivo los siguientes puntos:

- Minimizar el impacto de una interrupción no planificada del negocio.
- Reducir el tiempo de inactividad.
- Garantizar la continuidad del negocio en el futuro.

Del caso anterior presentado en la sección 2.2.7, se menciona que se tomaron medidas de contingencia, dentro de estas medidas se tiene el plan de recuperación ante desastres que consistió en el restablecimiento de registros en papel, redistribución de personal para comunicarse eficazmente con los pacientes y realizar tareas administrativas, y finalmente la transferencia de información de pacientes a hospitales privados.

2.2.9 Equipo de respuesta a crisis

Según la norma ISO 22361, se define al equipo de respuesta a crisis como el "grupo de individuos funcionalmente responsables de liderar la respuesta de gestión de crisis de la organización" (ISO, 2021).

Este equipo generalmente debe incluir a la alta dirección porque ésta proporciona una visión estratégica y la autoridad necesaria para tomar decisiones en situaciones de crisis. Asimismo, el equipo debe contar con el apoyo de equipos operativos y tácticos que permitan realizar una correcta planificación e implementación activa. En rasgos generales, se menciona que el tamaño del equipo varía según el tamaño de una organización y la naturaleza de la crisis, pero generalmente el equipo se conforma de tomadores de decisiones estratégicas y representantes de áreas comerciales claves (ISO, 2021).

Por otro lado, en la ISO se menciona los aspectos que el equipo debe tener en cuenta para responder a una crisis:

- Conciencia situacional
- Evaluación de posibles consecuencias
- Definir metas y objetivos
- Planificación y priorización

- Implementación
- Evaluación

Cabe mencionar que dentro de este equipo de respuesta se deben considerar los siguientes tipos de equipos de respuesta a incidentes de ciberseguridad, ya que estos son los encargados específicamente de resolver el ataque informático que generó la crisis:

- CERT (Computer Emergency Response Team): Equipo de respuesta a incidentes de seguridad informática que se encarga de prevenir, detectar y responder a incidentes de seguridad en una organización o en una comunidad.
- CSIRT (Computer Security Incident Response Team): Equipo de respuesta a incidentes de seguridad informática que se enfoca en responder a los incidentes de seguridad que afectan a una organización específica.
- SOC (Security Operations Center): Centro de operaciones de seguridad que monitorea y administra la seguridad de la información de una organización. Se enfoca en la prevención, detección, análisis y respuesta a incidentes de seguridad informática en tiempo real.

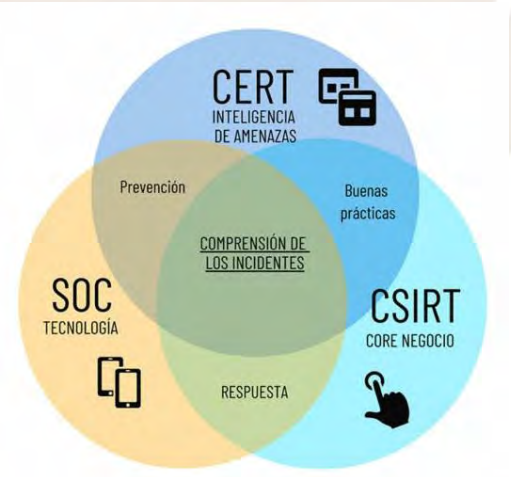


Figura 4: Complementariedad de los equipos de respuesta. Tomado de FIRST Annual Threat Intelligence Report (2020)

Un ejemplo de la importancia de la formación de equipos de respuesta a crisis se evidencia en el caso presentado anteriormente en (Flavin et al., 2022) donde una organización pública de salud en Irlanda fue víctima de un ciberataque significativo en sus sistemas de tecnología de la información (TI), debido a una infección de malware.

En este caso, el primer paso que se tomó para una correcta gestión de crisis, luego de la identificación de los riesgos, fue la formación de un equipo de respuesta que se reunió diariamente hasta que se restablecieron los servicios de radioterapia en todos los centros. La principales prioridades de este equipo era brindar tratamiento de emergencias de radioterapia, restablecer los servicios de salud en todos los centros y realizar una comunicación activa a las partes interesadas (pacientes y público en general).

2.2.9.1 Roles y Responsabilidades

Se refieren a las funciones y tareas específicas asignadas a una persona o a un grupo. Estas funciones definen las áreas de autoridad, deberes y tareas que se espera que desempeñen los responsables asignados para lograr un propósito planteado. Para este caso en específico, se buscará la solución de las actividades que desempeñan los equipos de respuesta a crisis.

Para explicar con más detalle qué son los roles y responsabilidades se tiene lo siguiente:

- Roles: Son posiciones dentro de una organización. Cada rol tiene un conjunto de responsabilidades y autoridad asociada. Por ejemplo, un rol dentro del equipo de respuesta a crisis generadas por incidentes de ciberseguridad es el de Oficial de Seguridad. Cabe decir que cada uno de estos roles tiene diferentes responsabilidades y niveles de autoridad.
- Responsabilidades: Son las tareas y deberes específicos que se asignan a un rol. Por ejemplo, una responsabilidad del Oficial de seguridad es el de investigar las causas raíz de un incidente de ciberseguridad.

Capítulo 3. Estado del Arte

3.1 Introducción

En este capítulo se realiza la revisión sistemática (Kitchenham, 2004) del Estado del Arte en relación a la gestión de crisis ante ciberataques en las organizaciones, haciendo énfasis en la gestión de comunicaciones.

3.2 Objetivos de revisión

En primer lugar, se realizará una revisión sistemática exploratoria, ya que es importante identificar estudios que proporcionen metodologías, normas y modelos útiles relacionados a la gestión de crisis cibernéticas. Además, se realizará una revisión empírica porque se va a buscar casos de estudio reales acerca de cómo se hace frente a estas crisis.

Siguiendo la etapa de planeamiento de la revisión propuesta por (Kitchenham, 2004), primero se debe identificar cuales son las necesidades de esta revisión, por lo cual se plantean los siguientes objetivos:

- Conocer cuándo un incidente de ciberseguridad adquiere la categoría de crisis.
- Identificar metodologías, normas y casos de estudios que permitan conocer cómo se gestionan las crisis generadas por ciber incidentes en diversas organizaciones a nivel mundial.
- Conocer qué papel juega la gestión de las comunicaciones en las crisis generadas por ciber incidentes en diversas organizaciones a nivel mundial.

3.3 Preguntas de revisión

Para realizar la formulación de las preguntas de revisión, se elaboró la Tabla 7 con las palabras identificadas para cada criterio según el método PICOC.

Tabla 7: Criterios de PICOC

Criterio	Descripción
Población	Continuidad del negocio, Resolución de crisis
Intervención	Gestión de incidentes, crisis, comunicaciones
Comparación	No aplica
Salidas	Metodologías, normas, casos de estudio para la identificación de incidentes que pueden convertirse en crisis, gestión de crisis, gestión de comunicaciones en crisis
Contexto	Ataques informáticos a las organizaciones que generan crisis

Fuente: Elaboración Propia

Una vez identificadas las palabras claves para cada criterio, se procedió a plantear las preguntas de revisión, teniendo en cuenta que cada una de las siguientes preguntas debe cubrir detalladamente cada uno de los objetivos planteados en la sección 3.2.

- P1: ¿De qué manera los incidentes de ciberseguridad se convierten en la categoría de crisis al interior de las empresas?
- P2: ¿De qué manera son resueltas las crisis en la empresas generadas por incidentes de ciberseguridad?
- P3: ¿Cómo se gestionan las comunicaciones a nivel estratégico y operativo para la gestión de crisis en las empresas generadas por incidentes de ciberseguridad?

3.4 Estrategia de búsqueda

3.4.1 Motores de búsqueda a usar

Los motores de búsqueda seleccionados para realizar la revisión son los siguientes:

- Scopus

- IEEE
- Springer

Estos fueron elegidos, debido a que son fuentes confiables y reconocidas a nivel mundial para obtener información de índole académico.

3.4.2 Cadenas de búsqueda a usar

Para construir las cadenas de búsqueda se utilizó las palabras claves identificadas en la Tabla 8, y los conectores lógicos AND y OR. Además, es importante mencionar que las palabras utilizadas se colocaron en inglés, debido a que la mayoría de información, en los motores de búsqueda seleccionados, se encuentra en ese idioma.

Tabla 8: Cadenas de búsqueda por pregunta de revisión

Nro. de Pregunta	Cadena de búsqueda
P1	(incident OR “incident management” OR “incident level”) AND (cybersecurity OR cyberattack OR “cyber threat”) AND (“crisis management” OR crisis)
P2	(crisis OR “crisis management”) AND (cybersecurity OR cyberattack OR “cyber threat”) AND (methodology OR standard OR model OR framework OR “case study” OR solution OR response OR study) AND (company OR organization OR business OR enterprise)
P3	(crisis OR “crisis management”) AND (cybersecurity OR cyberattack OR “cyber threat”) AND (communications OR “communications management”) AND (company OR organization OR business OR enterprise)

Fuente: Elaboración Propia

A continuación, se presenta la siguiente Tabla 9 que contiene las cadenas base formuladas en la Tabla 8, pero adaptadas al formato de búsqueda para cada motor escogido en la sección 3.4.1.

Tabla 9: Cadenas de búsqueda por motor de búsqueda

Nro. de pregunta	Motor de búsqueda	Cadena de Búsqueda
P1	Scopus	TITLE-ABS-KEY(("incident*" OR "incident management" OR "incident level") AND ("cybersecurity" OR "cyberattack*" OR "cyber threat*") AND ("crisis management" OR "crisis"))
	IEEE	("All Metadata":incident* OR "All Metadata":"incident management" OR "All Metadata":"incident level") AND ("All Metadata":cybersecurity OR "All Metadata":cyberattack* OR "All Metadata":"cyber threat*") AND ("All Metadata":"crisis management" OR "All Metadata":crisis)
	Springer	((incident* OR "incident management" OR "incident level") AND ft(cybersecurity OR cyberattack* OR "cyber threat*") AND ft("crisis management" OR crisis))
P2	Scopus	TITLE-ABS-KEY(("crisis" OR "crisis management") AND ("cybersecurity" OR "cyberattack*" OR "cyber threat*") AND ("methodology" OR "standard" OR "model" OR "framework" OR "case study" OR "solution" OR "response" OR "stud*") AND ("company" OR "organization" OR "business" OR "enterprise"))
	IEEE	("All Metadata":crisis OR "All Metadata":"crisis management") AND ("All Metadata":cybersecurity OR "All Metadata":cyberattack* OR "All Metadata":"cyber threat*") AND ("All Metadata":methodology OR "All Metadata":standard OR "All Metadata":model OR "All Metadata":framework OR "All Metadata":"case study" OR "All Metadata":solution OR "All Metadata":response OR "All Metadata":stud*) AND ("All Metadata":company OR "All Metadata":organization OR "All Metadata":business OR "All Metadata":enterprise)
	Springer	((crisis OR "crisis management") AND ft(cybersecurity OR cyberattack* OR "cyber threat*") AND ft(methodology OR standard OR model OR framework OR "case study" OR solution OR response OR stud*) AND ft(company OR organization OR business OR enterprise))
P3	Scopus	TITLE-ABS-KEY(("crisis" OR "crisis management") AND ("cybersecurity" OR "cyberattack*" OR "cyber threat*") AND ("communication*" OR "communications management") AND ("company" OR "organization" OR "business" OR "enterprise"))
	IEEE	("All Metadata":crisis OR "All Metadata":"crisis management") AND ("All Metadata":cybersecurity OR "All

		Metadata":cyberattack* OR "All Metadata":"cyber threat*") AND ("All Metadata":communication* OR "All Metadata":"communications management") AND ("All Metadata":company OR "All Metadata":organization OR "All Metadata":business OR "All Metadata":enterprise)
	Springer	((crisis OR "crisis management") AND ft(cybersecurity OR cyberattack* OR "cyber threat*") AND ft(communication* OR "communications management") AND ft(company OR organization OR business OR enterprise))

Fuente: Elaboración Propia

3.4.3 Documentos encontrados

Tabla 10: Documentos encontrados por pregunta de revisión sin filtros aplicados

Nro. de Pregunta	Motor de búsqueda	Resultados de la búsqueda	Total
P1	Scopus	41	113
	IEEE	8	
	Springer	64	
P2	Scopus	77	180
	IEEE	20	
	Springer	83	
P3	Scopus	20	107
	IEEE	6	
	Springer	81	

Fuente: Elaboración Propia

3.4.4 Criterios de inclusión/exclusión

A continuación, se presentan los criterios de inclusión y exclusión utilizados para limitar la cantidad de documentos encontrados en los motores de búsqueda empleados.

Criterios de inclusión:

- El título y el resumen del documento deben dar indicios de que este sirve para responder a una o más preguntas de revisión planteadas anteriormente.

  Justificación: Los documentos que se seleccionan deben tener una relación directa con alguna de las preguntas de revisión a responder.

- El documento brinda información detallada de cómo resolver crisis informáticas producidas por incidentes de ciberseguridad, mediante el uso de una propuesta, marco de trabajo, metodología o caso de estudio.

  Justificación: Es necesario encontrar documentos que desarrollen o muestren la forma de gestión empleada para resolver la crisis.

- El documento detalla las características y circunstancias que producen que el incidente se convierta en categoría de crisis.

  Justificación: Para definir cuando un incidente se convierte en categoría de crisis, es necesario encontrar documentos que muestren específicamente el contexto necesario para ello.

- El documento presenta información detallada sobre la gestión de comunicaciones en crisis.

  Justificación: Es necesario encontrar documentos que muestren el proceso detallado de gestión de comunicaciones que se realiza en una crisis de ciberseguridad.

Criterios de exclusión:

- El documento fue publicado hace más de 10 años.

  Justificación: Los documentos con una antigüedad mayor a 10 años pueden contener información obsoleta y desfasada.

- El documento no se encuentra elaborado en español o inglés.

Justificación: Los documentos elaborados en un idioma diferente al inglés o español, pueden generar errores de interpretación y dificultades en el entendimiento del mismo.

- El documento no está referido a crisis producidas por ataques cibernéticos.

  Justificación: El tema del trabajo a desarrollar se centra en la gestión de crisis producidas por ataques informáticos, es por ello que las crisis producidas por cualquier otro factor, ya sea por desastres naturales o errores humanos no se toman en cuenta.

- El documento es repetido de otra base de datos.

  Justificación: Los documentos se pueden repetir en más de una base de datos, por tanto solo se debe considerar uno de todos los repetidos.

3.5 Formulario de extracción de datos

A continuación, se presenta la Tabla 11 elaborada para la extracción de datos, en la cual se muestran los campos definidos para extraer los datos más relevantes de los documentos encontrados, además se presenta un breve descripción y observaciones de los campos.

Tabla 11: Formulario de extracción de datos

Campos	Descripción	Observaciones
ID	Sirve para identificar y poder hacer referencia a un documento	Generales
Título	Título del documento encontrado	
Autor(es)	Autor(es) del documento encontrado	
Año de Publicación	Año de publicación del documento encontrado	
Tipo de referencia	Tipo de documento encontrado: Revista, conferencia, paper, etc	

Nro. de citas	Cantidad de veces que el documento ha sido citado	
País	País de publicación del documento	
¿Cuáles son las circunstancias que producen que un incidente de seguridad se convierta en categoría de crisis?	Cuál es el contexto o aspectos que producen una crisis al interior de la organización.	P1
¿Qué metodologías, framework o caso de estudio se mencionan para resolver la crisis al interior de la organización?	Qué métodos se utilizan para gestionar la crisis al interior de la organización.	P2
¿Qué metodología, framework o caso de estudio se menciona para la gestión de comunicaciones en crisis?	Qué herramientas se utilizan para gestionar las comunicaciones en crisis.	P3

Fuente: Elaboración Propia

Se adjunta el formulario de extracción de datos completo en el **Anexo A**.

3.6 Resultados de la revisión

Una vez realizada la búsqueda correspondiente en cada motor seleccionado, se obtuvieron los resultados presentados en la Tabla 12. Cabe decir que para realizar estas búsquedas y escoger los documentos más relevantes, se aplicaron los criterios de exclusión e inclusión elaborados en la sección 3.4.4.

Tabla 12: Documentos encontrados por motor de búsqueda con filtros aplicados

Motor de Búsqueda	Nro. de Pregunta	Cantidad de resultados	Documentos relevantes
Scopus	P1	41	5
	P2	77	3
	P3	20	3
IEEE	P1	8	1
	P2	20	3
	P3	6	1
Springer	P1	64	1
	P2	83	0
	P3	81	0
Total	-	387	12*

Fuente: Elaboración Propia

*Para calcular el total, solo se consideró una vez los documentos repetidos.

Aplicados los criterios de exclusión e inclusión se obtuvieron en total 12 documentos relevantes. A continuación se presenta la Tabla 13 que muestra la lista de los estudios primarios seleccionados usando el estándar de referencia bibliográfica APA.

Tabla 13: Lista de estudios primarios

ID	Referencia del Estudio
A1	Schauer, S., Kalogeraki, E.-M., Papastergiou, S., & Douligeris, C. (2019). Detecting Sophisticated Attacks in Maritime Environments using Hybrid Situational Awareness. 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 1–7. https://doi.org/10.1109/ICT-DM47966.2019.9032900
A2	Aljaryan, L. K., Alfalahi, W. H., & Khamis, T. S. Al. (2022). Cyberattacks and Solutions for Future Factories. 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), 1–7. https://doi.org/10.1109/CICN56167.2022.10008258

A3	B. S. Dykstra, J. A., & Orr, S. R. (2016). Acting in the unknown: the cynefin framework for managing cybersecurity risk in dynamic decision making. 2016 International Conference on Cyber Conflict (CyCon U.S.), 1–6. https://doi.org/10.1109/CYCONUS.2016.7836616
A4	Kuipers, S., & Schonheit, M. (2022). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. Corporate Reputation Review, 25(3), 176–197. https://doi.org/10.1057/s41299-021-00121-9
A5	Weil, T., & Murugesan, S. (2020). IT Risk and Resilience—Cybersecurity Response to COVID-19. IT Professional, 22(3), 4–10. https://doi.org/10.1109/MITP.2020.2988330
A6	Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security, 105, 102239. https://doi.org/10.1016/j.cose.2021.102239
A7	Flavin, A., O'Toole, E., Murphy, L., Ryan, R., McClean, B., Faul, C., McGibney, C., Coyne, S., O'Boyle, G., Small, C., Sims, C., Kearney, M., Coffey, M., & O'Donovan, A. (2022). A National Cyberattack Affecting Radiation Therapy: The Irish Experience. Advances in Radiation Oncology, 7(5), 100914. https://doi.org/10.1016/j.adro.2022.100914
A8	Zdzikot, T. (2022). Cyberspace and Cybersecurity. In Cybersecurity in Poland (pp. 9–21). Springer International Publishing. https://doi.org/10.1007/978-3-030-78551-2_2
A9	Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
A10	Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99, 102036. https://doi.org/10.1016/j.cose.2020.102036
A11	Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. Science and Innovation, 17(3), 3–13. https://doi.org/10.15407/scine17.03.003
A12	Stowman, A. M., Frisch, N., Gibson, P. C., John, T. S., Cacciatore, L. S., Cortright, V., Schwartz, M., Anderson, S. R., & Kalof, A. N. (2022). Anatomy of a Cyberattack: Part 1: Managing an Anatomic Pathology Laboratory During 25 Days of Downtime. American Journal of Clinical Pathology, 157(4), 510–517. https://doi.org/10.1093/ajcp/aqab145

Fuente: Elaboración Propia

3.6.1 Respuesta a la pregunta "¿De qué manera los incidentes de ciberseguridad se convierten en la categoría de crisis al interior de las empresas?"

En la actualidad las organizaciones, tanto privadas como públicas, se han visto afectadas por un constante aumento de incidentes de ciberseguridad, esto debido a distintas razones y circunstancias, pero principalmente a lo sucedido por la pandemia del COVID-19. En (Alawida et al., 2022) se menciona que los ciberdelincuentes han aprovechado algo tan generalizado y disruptivo como el COVID-19, para causar estragos en diferentes organizaciones y sus datos más que nunca. Recalcando que en el año 2020 (inicio de la pandemia) los ataques cibernéticos han tenido un gran impacto en las organizaciones, generando múltiples crisis dentro de ellas.

Entonces, en primer lugar, para brindar un mejor contexto a la respuesta de la pregunta, se elaboró la Tabla 14 con el objetivo de resumir los ataques informáticos más usados, según (Alawida et al., 2022) y (Aljaryan et al., 2022), para atacar a las organizaciones:

Tabla 14: Ataques informáticos más usados para atacar a las organizaciones

Ataques informáticos	Descripción
Hacking	Consiste en acceder o manipular las redes digitales como computadoras, laptops, tabletas y teléfonos. Robando así datos confidenciales como contraseñas, nombres de usuario, información bancaria y otros datos personales.
Phishing	Método de explotación de ingeniería social que se utiliza con frecuencia para obtener información confidencial de los usuarios, como credenciales de inicio de sesión de banca en línea o credenciales de inicio de sesión de la empresa, todo ello mediante el envío de mensajes fraudulentos a su objetivo.
Ransomware	El ransomware es un tipo de software malicioso que los delincuentes diseñan para evitar que los usuarios accedan a su información a menos que paguen dinero.
Botnet attack	Dispositivo como una computadora, servidor o teléfono infectado con un malware (programa malicioso) para realizar acciones destructivas sin el conocimiento del usuario.
APT (Amenaza Persistente Avanzada)	Un ataque o amenaza persistente avanzada conocido como APT ocurre cuando un usuario no autorizado utiliza formas

	avanzadas y sofisticadas para obtener acceso a un sistema o red. Este ataque generalmente implementa técnicas como ransomware, phishing, malware y violaciones de datos para lanzar ataques a sus objetivos.
Malware	El malware es un software o código destinado a dañar las computadoras al cifrar archivos, dañar, deshabilitar, robar datos u obtener accesos no autorizados a diferentes sistemas.
Business Email Compromise (BEC)	Son un conjunto de estrategias de ingeniería social y correos electrónicos de phishing, utilizados para infiltrarse en las organizaciones, con el propósito de engañar a los empleados y ejecutivos desprevenidos para que realicen tareas que parecen provenir de un remitente confiable.
Ataque DDoS	Es un tipo de ataque que los ciberdelincuentes implementan para hacer que los servicios en línea no estén disponibles para los usuarios al generar una gran cantidad de tráfico.
Websites maliciosos	Representa un conjunto de aplicaciones web que pueden tomar diferentes formas, incluyendo páginas de phishing, páginas web infectadas con malware, páginas de descarga de software falso o páginas web fraudulentas que promueven esquemas fraudulentos.
Spam (Correos electrónicos no deseados)	Son mensajes no solicitados o anónimos que se envían de forma masiva por correo electrónico, con el propósito de robar información de los usuarios.

Fuente: Elaboración Propia

Teniendo en claro, cuales son los ataques informáticos más recurrentes y considerando que año tras año, los delitos cibernéticos son cada vez más organizados, técnicamente avanzados y psicológicamente elegantes, y las consecuencias del uso del ciberespacio para fines ilegales son cada vez más generalizadas y destructivas (Yerina et al., 2021). Además de que cualquier perturbación grave en el funcionamiento del ciberespacio afectará la sensación de seguridad de los ciudadanos, la seguridad de las transacciones comerciales, la eficiencia de las instituciones del sector público y, en consecuencia, la seguridad en general (Zdzikot, 2022). Se presenta la siguiente lista de empresas de talla mundial, que sufrieron un incidente de ciberseguridad, generado por uno o más ataques informáticos detallados en la Tabla 8, que finalmente produjeron una crisis al interior de la organización. Es importante mencionar que estos casos son presentados para

ejemplificar cómo es que un incidente de ciberseguridad se convierte en una crisis. Asimismo, mencionar que estos casos se extrajeron de (Kuipers & Schonheit, 2022) y (Stowman et al., 2022).

- **Caso de TJX:**

Divulgación masiva de datos personales de sus clientes, debido a la aplicación inadecuada de los requisitos reglamentarios de protección de datos y seguridad cibernética.

- **Caso de SONY:**

La violación de datos que comprometio 77 millones de registros y una interrupcion de la red de Play Station por más de 20 días. Esto debido a que la empresa no encriptó los datos de sus usuarios, ni estableció los cortafuegos adecuados para manejar una contingencia de intrusión en sus servidores. Asimismo, no proporcionó advertencias rápidas y adecuadas de las violaciones de seguridad, ya que no contaba con un protocolo de actuación establecido ante emergencias.

- **Caso de Target:**

Piratas informáticos extrajeron 110 millones de registros y penetraron en los servidores de Target aprovechando las credenciales de proveedores de terceros. Esto se produjo debido a la insuficiente preparación en seguridad cibernética demostrada antes y durante el evento, igualmente, no se contaba con un protocolo de actuación definido para este tipo de eventos de ciberseguridad.

- **Caso de Global Payments:**

Hackeo a los servidores de Global Payments que comprometió 10 millones de cuentas de tarjetas de pago. Esto sucedió producto de múltiples vulnerabilidades dentro de su sistema de pagos, y por la falta de medidas necesarias para contener fugas de información.

- **Caso de The Home Depot:**

Ataque de malware personalizado que comprometió los datos personales de sus clientes. Aquí se menciona que los ejecutivos de la organización estaban muy conscientes de las vulnerabilidades existentes en su sistema, y que igualmente descartaron las preocupaciones por lo equipos internos de TI de mejorar sus defensas de seguridad.

- **Caso de Equifax:**

Este caso implicó la filtración de 143 millones de datos PII (Información Personal de Identificación) de consumidores de los sistemas de la agencia de informes crediticios. Esto se produjo debido al software defectuoso de la empresa y la falta de parches de vulnerabilidades conocidas durante más de un año. Asimismo, se menciona que debido a una falta de gestión de respuesta a la crisis, Equifax redirigió a sus clientes a una nueva página web de la empresa donde los piratas informáticos también habían instalado un malware.

- **Caso del Centro Médico de la Universidad de Vermont (UVMMC):**

A medida que los sistemas hospitalarios se vuelven más grandes, más complejos y cada vez más interdependientes, las organizaciones son mucho más vulnerables a los ataques de malware y ransomware. Además, aunque los hospitales y laboratorios han realizado grandes inversiones en sistemas médicos, muchas de estos sistemas no han adoptado medidas de seguridad adecuados para combatir posibles ataques y carecen de la infraestructura de tecnología de la información (TI) necesaria para negociar un ataque, sobrevivir al tiempo de inactividad, y poner en marcha un plan de recuperación. Entonces cuando el centro médico fue atacado ciberneticamente, tanto su sistema médico “EHR”, como los sistemas de farmacia, programación, radiología, facturación, y nómina, fueron completamente bloqueados. Asimismo, todos los sistemas informáticos asociados al hospital se desconectaron, incluidos los de 5 hospitales de la red en todo Vermont y Nueva York. El cierre finalmente duró más de 25 días, con algunas interrupciones del subsistema que duraron más de 40 días.

A partir de los ejemplos detallados anteriormente, se puede evidenciar aspectos importantes que producen que los incidentes de ciberseguridad se conviertan en la categoría de crisis: La falta de políticas de ciberseguridad de retención y manejo de datos correctamente establecidas (falta de backups, auditorias, controles de acceso, entre otros), el mal uso interno de los datos y las vulnerabilidades propias de los sistemas son las causas más comunes que producen que un incidente de ciberseguridad se convierta en categoría de crisis. Sin embargo, es de suma importancia mencionar que la prevención total de estos ciberataques es casi imposible, ya que los ciberdelincuentes generalmente se encuentran por delante de la curva de seguridad. Por lo tanto, la falta de un protocolo de actuación que permita resolver oportunamente el incidente es otra causa muy común de las crisis dentro de las organizaciones (Kuipers & Schonheit, 2022).

En conclusión, sin una estrategia de respuesta clara para aliviar un incidente de ciberseguridad, se sufre el riesgo de que la organización tarde más en recuperarse y esto finalmente intensifica cualquier daño causado lo que se traduce en una crisis dentro de la organización (Aljaryan et al., 2022).

3.6.2 Respuesta a la pregunta "¿De qué manera son resueltas las crisis en la empresas generadas por incidentes de ciberseguridad?"

En la actualidad, muchas organizaciones se ven afectadas por crisis generadas por incidentes de ciberseguridad, lo que genera que cada una establezca o utilicen diferentes metodologías, normas y modelos que les permitan gestionar y responder adecuadamente a la crisis, de tal forma que se reduzca su impacto negativo en la organización. Entonces a partir de la investigación realizada se identificaron tres maneras de hacer frente a las crisis, siendo éstas las siguientes:

- **Conciencia de la situación cibernética:**

La Conciencia de la Situación Cibernética (CSA) brinda la capacidad de obtener información relevante del dominio cibernético, darle sentido a esa información recolectada y prever algunas de sus implicaciones para el futuro (Schauer et al., 2019). Asimismo, para este modelo se hace uso de una Imagen Corporativa Común (COP), que en otras palabras, puede verse como un artefacto que almacena y distribuye información útil necesaria para obtener el CSA, por ejemplo, guarda información con respecto a las respuestas más comunes en casos de crisis.

A partir de lo mencionado, se puede decir que el Conciencia de la Situación Cibernética (CSA) y la Imagen Corporativa Común (COP) son dos artefactos importantes que se requieren cuando varias partes interesadas deben cooperar para manejar grandes crisis (Varga et al., 2021). Entonces los pasos para lograr y aplicar correctamente el CSA son los siguientes:

1. Conocimiento de la situación actual.
2. Conocimiento del impacto del ataque.
3. Conciencia de cómo están evolucionando las situaciones (el contexto de la organización durante la crisis).
4. Conocimiento del comportamiento del atacante.
5. Conciencia de por qué y cómo se produjo la situación actual de la organización.

6. Conocimiento de la calidad y confiabilidad de la información que se tiene de la situación actual.
7. Evaluación de futuros plausibles de la situación actual.

El cumplimiento de cada uno de los pasos, permitirá a la organización obtener el conocimiento necesario para tomar decisiones de acción rápidas y efectivas que reduzcan el impacto de la crisis.

En general, este modelo se enfoca más en la capacidad de la organización para obtener información relevante de su contexto actual en situación de crisis, de tal forma que pueda comprenderla y proyectar una respuesta inmediata.

- **Cynefin Framework:**

Cynefin Framework es una herramienta que se utiliza para ayudar a comprender y tomar decisiones en entornos complejos y en constante cambio. Contiene cinco dominios que describen problemas o situaciones, y que guían la acción para la gestión de crisis (B. S. Dykstra & Orr, 2016):

- Dominio del desorden: El dominio del desorden describe el estado de no conocer la relación entre causa y efecto en un problema o situación dada, y por tanto se debe contextualizar la situación para después tomar las medidas necesarias.
- Dominio obvio: En el dominio obvio, la relación entre causa y efecto se entiende claramente, los hechos de la situación se evalúan, clasifican y luego se ejecuta una respuesta basada en las prácticas establecidas.
- Dominio complicado: En el dominio complicado, la relación entre causa y efecto no necesariamente se entiende bien y requiere la ayuda de un análisis experto.
- Dominio complejo: La relación entre causa y efecto no puede entenderse de inmediato y, a menudo, solo en retrospectiva revela las interrelaciones entre causa y efecto.

- Dominio caótico: No existe una relación perceptible entre causa y efecto. Las decisiones urgentes ad-hoc para estabilizar la situación son la primera prioridad, después de lo cual se puede determinar el siguiente paso para comprender y responder a las causas fundamentales del caos. En el dominio caótico, la práctica novedosa gobierna la acción.

En este caso, el framework presentado se enfoca en estructurar lo desconocido para revelar el contexto que permite una correcta toma de decisiones y ejercicio de acciones durante la crisis para contrarrestar su impacto.

- **Teoria de comunicación en crisis situacional:**

El marco de Teoría de comunicación en crisis situacional (SCCT) distingue entre tipos de crisis y factores de intensificación para evaluar el grado de responsabilidad de la crisis que las partes interesadas atribuyen a la organización después de un incidente (Kuipers & Schonheit, 2022). Primero, la tipología de las crisis se basa en la responsabilidad organizacional inicial: crisis de víctimas (situaciones que se cree que están totalmente fuera del control de la organización), crisis accidental (están vinculadas al curso de acción de la organización, pero carecen de intencionalidad o control sobre el evento) y crisis prevenible (la organización es directamente responsable del desarrollo de la crisis porque intencionalmente causó la crisis o podría haber evitado que ocurriera pero no lo hizo). Considerar que cada tipo de crisis se vincula a un grupo predeterminado de estrategia de respuesta de comunicación.

Asimismo, este marco introduce dos factores intensificadores que pueden influir directamente en cómo la crisis es percibida por las partes interesadas: la gravedad de la crisis y el historial de desempeño de la organización en la gestión de crisis pasadas.

A continuación, se muestra un caso de estudio (Flavin et al., 2022) que permite observar cómo una organización de salud en Irlanda gestionó una crisis abarcando los tres puntos principales de respuesta a la crisis: detección de la causa, estrategia de respuesta y comunicación en crisis (Weil & Murugesan, 2020).

El viernes 14 de mayo de 2021, se descubrió que una organización pública de salud en Irlanda fue víctima de un ciberataque significativo en sus sistemas de tecnología de la información (TI), debido a una infección de malware. Como resultado, más del 80% de su infraestructura de TI se vio afectada. Esto resultó en graves efectos en el servicio nacional de salud y la prestación de atención. Entonces la medidas que tomó la organización fueran las siguientes:

1. Identificación de los riesgos experimentados: se identificaron diversos riesgos como la falta de acceso a la información del paciente y los sistemas de salud, la falta de infraestructura de comunicación, etc.
2. Formación de un equipo de respuesta: este equipo se reunió diariamente hasta que se restablecieron los servicios de salud en todos los centros.
3. Comunicación a las partes interesadas: se estableció como prioridad la comunicación con los pacientes y el público. Los medios de comunicación nacionales y el sitio web de la organización se utilizaron para alertar a los pacientes sobre la necesidad de comunicarse con su departamento de radioterapia mediante líneas telefónicas dedicadas recientemente establecidas.
4. Acciones de respuesta: la organización tomó diversas acciones de respuesta para contrarrestar el impacto de la crisis como el restablecimiento de registros en papel.
5. Etapa post crisis: después de que el equipo de respuesta logrará resolver el incidente de seguridad, los sistemas volvieron a funcionar. Sin embargo, es importante mencionar que todo el proceso de recuperación total duró exactamente 5 meses.

En conclusión, cada una de las tres maneras de gestionar las crisis presentadas, muestran las diferentes formas que utilizan las organizaciones para gestionar las crisis. Sin embargo, en rasgos generales se puede mencionar que la aplicación en conjunto de estas permiten una gestión de crisis completa, porque con su aplicación conjunta se abarca los tres puntos principales de respuesta a la crisis: detección de la causa, estrategia de respuesta y comunicación en crisis (Weil & Murugesan, 2020).

3.6.3 Respuesta a la pregunta "¿Cómo se gestionan las comunicaciones a nivel estratégico y operativo para la gestión de crisis en las empresas generadas por incidentes de ciberseguridad?"

Como se mencionó anteriormente, el marco SCCT distingue entre tipos de crisis y factores de intensificación para evaluar el grado de responsabilidad de la crisis que las partes interesadas atribuyen a la organización después de un incidente. Teniendo eso en cuenta, este marco implementa los siguientes dos pasos de comunicación (Kuipers & Schonheit, 2022):

1. Los esfuerzos de respuesta a la crisis siempre deben empezar con "respuestas bases", es decir, se debe instruir y ajustar la información dirigida directamente a moldear la percepción pública del evento. Por un lado instruir la información, sirve para proteger a las partes interesadas del daño adicional provocado por la crisis. Por otro lado, ajustar la información comunica lo que la empresa está haciendo para evitar que la crisis vuelva a ocurrir, dando a la audiencia información sobre los esfuerzos de reparación.
2. Posteriormente, las organizaciones deben seleccionar una estrategia de comunicación en función al tipo de crisis que están afrontando:
    - Denegar: Las crisis de las víctimas podrían manejarse con medidas de negación como la negación o el chivo expiatorio.
    - Disminuir: Las crisis accidentales requieren que la comunicación se actualice hacia estrategias de disminución, como la justificación (minimizar el impacto) o la negación de la voluntad (alegando falta de control sobre el evento).
    - Reconstruir: Las crisis prevenibles deben incluir estrategias de reconstrucción, que van desde las disculpas hasta la rectificación (demostrando pleno compromiso con la prevención futura).
    - Reforzar: Esta estrategia representa medidas complementarias, a las estrategias presentadas anteriormente, principalmente se enfoca en

congeniar con las partes interesadas y recordar casos exitosos de gestión de crisis pasadas (en caso se tenga).

Adicionalmente este marco SCCT, se puede complementar con otro marco definido en (Knight & Nurse, 2020) que abarca, de igual manera una estructura de comunicación a nivel estratégico. Este marco consta de los siguientes pasos:

1. Decidir si revelar: Responde a la pregunta si es necesario divulgar información del incidente que produjo la crisis al interior de la empresa.
2. Establecer que revelar: Aquí se puede aplicar el marco de SCCT.
3. Elegir cuándo revelar: Se debe decidir si es mejor o no notificar al público externo lo más rápido posible, además se debe considerar el equilibrio entre precisión y tiempo, ya que una notificación temprana implica que no se tenga información completa de la crisis.
4. Seleccionar como revelar: Se debe seleccionar entre métodos directos como envío de correos electrónicos, sitios web o llamadas telefónicas. Por otro lado, también se tiene métodos indirectos como medios de comunicación social (Facebook, Twitter, etc) o medios de comunicación tradicionales (Televisión, radio, etc). Es importante mencionar que la elección de la forma de divulgación dependerá del alcance que se quiera tener y de los medios establecidos que posee la organización.

Por otro lado, a partir de los casos de estudios analizados en (Schauer et al., 2019) y (Flavin et al., 2022), una correcta gestión de comunicaciones dentro de la organización también implica las siguientes consideraciones:

1. Identificar el equipo de respuesta: Es importante que la organización tenga un equipo de respuesta a incidentes de ciberseguridad establecido de antemano. Asimismo, se recomienda que el equipo de respuesta esté conformado por expertos de ciberseguridad, representantes de la alta dirección y otros miembros claves de la organización, por ejemplo, personal que conoce a profundidad los procesos que se han visto afectados por el ataque informático.

2. Definir los criterios de alerta: La organización debe establecer criterios claros para alertar al equipo de respuesta en el momento indicado, por ejemplo, la violación de datos sensibles en la organizacion podría ser un detonante.
3. Establecer un proceso de alerta: Una vez que se hayan definido los criterios de alerta, la organización debe establecer un proceso claro para notificar al equipo de respuesta. Esto puede incluir la designación de un punto de contacto de emergencia (medio por el cual se dará las comunicaciones) y la creación de un protocolo de comunicación para garantizar que se pueda tomar medidas rápidas y efectivas.
4. Probar el proceso de alerta: Dentro de (Flavin et al., 2022) se recalca la necesidad de probar las medidas de comunicación establecidas para asegurarse de que sean efectivas.

3.7 Conclusiones

En primer lugar, con respecto a la primera pregunta se concluye que sin una estrategia de respuesta clara para aliviar un incidente de ciberseguridad, se sufre el riesgo de que la organización tarde más en recuperarse y esto finalmente intensifica cualquier daño causado lo que se traduce en una crisis dentro de la organización (Aljaryan et al., 2022).

Por otro lado, con respecto a la segunda pregunta de revisión se puede concluir que cada una de las tres maneras de gestionar las crisis presentadas, muestran las diferentes formas que utilizan las organizaciones para gestionar las crisis. Sin embargo, en rasgos generales se puede mencionar que la aplicación en conjunto de las formas mencionadas permite una gestión de crisis completa, porque con su aplicación conjunta se abarca completamente tres puntos principales de respuesta a la crisis: detección de la causa, estrategia de respuesta y comunicación en crisis (Weil & Murugesan, 2020).

Finalmente, en relación con la tercera pregunta de revisión se presentan dos marcos que se complementan entre sí y que permiten una gestión de las comunicaciones en crisis con las partes interesadas. Asimismo, se mencionan una serie de consideraciones que resultan relevantes para establecer una correcta comunicación con el equipo de respuesta.

Capítulo 4. Definición de los componentes del marco a alto nivel

4.1 Introducción

El presente capítulo desarrolla el Objetivo Específico 1 (OE1). Dentro de este capítulo se definen los componentes necesarios para la elaboración de un marco de trabajo que permita gestionar incidentes y crisis de ciberseguridad. Estos componentes han sido definidos siguiendo los principios de la norma ISO 22361 para la gestión efectiva de las crisis. Asimismo, se utilizó un conjunto de buenas prácticas, estándares internacionales y los resultados obtenidos del estado del arte que involucran la detección de la causa, estrategia de respuesta y comunicación en crisis. Es importante mencionar que toda la investigación realizada se enfocó en crisis producidas por incidentes de ciberseguridad.

4.2 Resultados Alcanzados (RE1)

El resultado alcanzado es la lista de componentes que se han definido para la elaboración del marco de trabajo.

Para la construcción de los componentes del marco se siguió un enfoque basado en dominios, esto con la finalidad de mantener una estructura organizada para abordar los diferentes aspectos claves del marco. Entonces, cada dominio se enfoca en un conjunto particular de procesos necesarios para hacer frente a las crisis generadas por incidentes de ciberseguridad. Es importante mencionar que los componentes del marco de trabajo se han desarrollado en un informe de hoja de ruta en el **Anexo C.** Asimismo**,** en el **Anexo D** se muestra el acta de validación del resultado esperado RE1.

A continuación, se muestra la estructura completa del marco:

Tabla 15: Estructura de los componentes del marco

Marco de trabajo para la gestión de incidentes y crisis de ciberseguridad			
Componentes	**Dominios**	**Procesos**	**Estándares o buenas prácticas**
	Organizacional (ORG)	1. Gestión de recursos financieros y tecnológicos 2. Gestión de riesgos de ciberseguridad 3. Gestión de la continuidad de TI	- ITIL v4 - ISO 27005 - NIST Cybersecurity Framework 2.0 - COBIT 5 for Risk - ISO 22301 - NIST 800-34
	Operacional (OPE)	4. Gestión de incidentes de ciberseguridad 5. Gestión de problemas 6. Gestión del conocimiento	- NIST 800-61 - ITIL v4 - ISO 20000-1
	Respuesta a Crisis (RAC)	7. Gestión de crisis 8. Gestión de la comunicación en crisis 9. Gestión de equipos de respuesta	- ISO 22361 - ENISA - How to setup CSIRT and SOC.

Fuente: Elaboración Propia

Componentes del marco

- Dominio Organizacional (ORG): Este dominio se centra en los procesos que se necesitan para estar preparados a dar respuesta a una crisis producida por incidentes de ciberseguridad, de tal forma que se asegure que la empresa pueda seguir operando ante una crisis.
    - Gestión de recursos financieros y tecnológicos: Proceso para gestionar aquellos recursos tecnológicos y financieros con los que cuenta la empresa y que van a ser utilizados para gestionar la crisis producida.
    - Gestión de riesgos de ciberseguridad: Necesario para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información. Este proceso es fundamental para prevenir la ocurrencia de incidentes de ciberseguridad que puedan producir una crisis.

- Gestión de la continuidad de TI: Ante una crisis resulta importante que la empresa pueda seguir operando. Por ello es esencial contar con este proceso para garantizar que la infraestructura de TI y los servicios digitales sigan funcionando de manera efectiva, incluso en situaciones adversas, minimizando así el impacto de interrupciones en el negocio.

- Dominio Operacional (OPE): Este dominio abarca los procesos necesarios para resolver de manera efectiva y oportuna los incidentes de ciberseguridad que produjeron la crisis dentro de la organización.
  - Gestión de incidentes de ciberseguridad: Es un proceso esencial para responder y resolver de manera rápida y eficaz a los incidentes que produjeron la crisis dentro de la empresa.
  - Gestión de problemas: Es un proceso que permite reducir el impacto de los incidentes, mediante la identificación de su causa raíz. Por ello, dentro de este proceso se busca tener mapeado las causas de los incidentes y soluciones temporales que puedan ser usadas.
  - Gestión del conocimiento: Proceso fundamental para capturar, almacenar, organizar y distribuir el conocimiento y la información relevante dentro de la organización. Mediante este proceso se busca mejorar la eficiencia en la toma de decisiones al aprovechar el conocimiento acumulado. Cabe decir que este proceso resulta importante para tener documentada la información de las causas raíz y soluciones de los incidentes de ciberseguridad.

- Dominio de Respuesta a crisis (RAC): Este dominio se concentra en detallar las actividades necesarias para responder de manera efectiva, oportuna y completa a una crisis, abarcando los procesos necesarios para su gestión.
  - Gestión de crisis: Componente principal del marco, donde se detallan las actividades necesarias para gestionar una crisis de manera rápida y eficiente, de tal forma que se manejen los incidentes de forma oportuna,

se proteja la reputación de la empresa y se minimicen los impactos negativos sobre ella.

- Gestión de la comunicación en crisis: Este proceso resulta crucial para proporcionar información precisa, oportuna y transparente sobre las acciones que se están tomando para gestionar la crisis a todas las partes interesadas (internas y externas).
- Gestión de equipos de respuesta: Proceso para definir, monitorear y supervisar los roles y responsabilidades asignados al personal para hacer frente a las crisis generadas por incidentes de ciberseguridad.

4.3 Discusión

En esta sección se presentó un conjunto de componentes que conforman el marco de trabajo para la gestión de incidentes y crisis de ciberseguridad. Cabe decir que estos componentes se encuentran divididos en dominios con la finalidad de mantener una estructura organizada para abordar los diferentes aspectos claves del marco.

Finalmente, resulta importante mencionar que toda la investigación realizada se enfocó solo en la gestión de crisis producidas por incidentes de ciberseguridad; sin embargo, se podría generalizar el uso de los componentes para gestionar cualquier tipo de crisis dentro de una organización

Capítulo 5. Desarrollar los procesos que conforman los componentes

5.1 Introducción

El presente capítulo abarca la elaboración del Objetivo Específico 2 (OE2). Dentro de este capítulo se desarrollan cada uno de los procesos que conforman los componentes del marco. Para ello se estableció una tabla donde se detalla la siguiente información para cada proceso: Descripción, Propósito, Actividades, Documentación relacionada y Métricas e indicadores. Asimismo, como parte del objetivo también se definen los roles y responsabilidades para cada proceso mediante una matriz RACI.

5.2 Resultados Alcanzados (RE2 y RE3)

A continuación, se presentan los componentes del marco dividido en tres dominios: Organizacional, Operacional y Respuesta a Crisis.

En el **Anexo E** y **Anexo F** se muestran las actas de validación de los resultados esperados RE2 y RE3 respectivamente.

5.2.1 Dominio Organizacional (ORG)

- **Gestión de recursos financieros y tecnológicos (ORG01)**

Tabla 16: ORG01 - Gestión de recursos financieros y tecnológicos

Dominio ORGANIZACIONAL **ORG01 - Gestión de recursos financieros y tecnológicos**	
Descripción	
Gestionar los recursos tecnológicos y financieros con los que cuenta la organización, y que van a ser utilizados para asegurar la continuidad de los servicios de TI y para gestionar las crisis cibernéticas.	
Objetivo	
Gestionar los recursos de la organización para garantizar la continuidad del negocio dentro de marcos de tiempo y costos aceptables	
Actividades del proceso	
1. Gestionar los recursos tecnológicos necesarios para las funciones de continuidad de los servicios de TI.	
2. Gestionar los recursos financieros necesarios para las funciones de continuidad de los servicios de TI y de gestión de crisis.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ITIL v4 - 2019	Modelo de buenas prácticas del sistema de valor del servicio
ISO 22301:2019	Cláusula 7.1
Actividades de implementación	**Actividad de proceso**
Realizar un inventario de los recursos tecnológicos con los que se cuenta para las funciones de continuidad de los servicios de TI.	1

Clasificar los activos en diferentes categorías según su tipo y función.	1
Realizar actividades de mantenimiento de los recursos tecnológicos para garantizar su funcionamiento óptimo. Para esta actividad se pueden establecer políticas para llevar a cabo dichas actividades de manera planificada.	1
Establecer un presupuesto para el desarrollo de las actividades de continuidad de servicios de TI y de gestión de la crisis.	2
Asignar recursos financieros para el desarrollo de dichas actividades según el presupuesto elaborado.	2
Generar informes que muestren el uso de los recursos financieros asignados y garantizar que se mantengan dentro de los límites presupuestarios establecidos.	2
Métricas e indicadores	**Unidad de medida**
Número de actualizaciones anuales del inventario de recursos tecnológicos.	Numérico sin unidades.
Porcentaje utilizado del presupuesto destinado a la gestión de continuidad de servicios de TI y de gestión de la crisis.	Numérico sin unidades.

Fuente: Elaboración Propia

Tabla 17: Matriz de roles y responsabilidades del proceso ORG01

Rol / Responsabilidad	Gerente de TI	Gerente de Logística	Administrador de Recursos y Servicios de TI	Gerente de Finanzas
Gestionar los recursos tecnológicos necesarios para las funciones de continuidad de los servicios de TI	A	C	R	-
Gestionar los recursos financieros necesarios para las funciones de continuidad de los servicios de TI y de gestión de crisis	AR	-	-	R

Fuente: Elaboración Propia

- **Gestión de riesgos de ciberseguridad (ORG02)**

Tabla 18: ORG02 - Gestión de riesgos de ciberseguridad

Dominio ORGANIZACIONAL **ORG02 - Gestión de riesgos de ciberseguridad**	
Descripción	
Identificar, evaluar y tratar los riesgos relacionados a la ciberseguridad que puedan generar una crisis dentro de la organización.	
Objetivo	
Gestionar los riesgos de ciberseguridad que puedan afectar a la organización, de tal manera que se garantice la continuidad del negocio.	
Actividades del proceso	
1. Establecer escenarios de crisis provenientes de riesgos cibernéticos.	
2. Realizar el inventario y valorización de los activos de TI.	
3. Identificar los riesgos de ciberseguridad.	
4. Analizar y evaluar los riesgos identificados.	
5. Tratar los riesgos y establecer los controles respectivos.	
6. Monitorear y revisar los riesgos.	
7. Comunicar los resultados a las partes interesadas involucradas.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 27005:2022	Cláusulas 5, 6, 7 y 8
NIST Cybersecurity Framework 2.0 - 2024	Capítulo 5

COBIT 5 for Risk - 2013	Capítulo 3
Actividades de implementación	**Actividad de proceso**
Desarrollar escenarios de crisis que pueda sufrir la organización a causa de riesgos de ciberseguridad.	1
Localizar e identificar los activos de TI que se considerarán dentro de la gestión de riesgos (Inventariado).	2
Identificar los procesos de negocio a los que brindan soporte.	2
Valorizar los activos de TI identificados en base a niveles de sensibilidad y criticidad.	2
Priorizar los activos en base a su valorización.	2
Identificar las vulnerabilidades de los activos de TI.	3
Identificar las amenazas que puedan aprovechar las vulnerabilidades y conocer las condiciones en las que pueden manifestarse dichos eventos amenazantes.	3
Identificar los riesgos asociados a los activos de TI.	3
Evaluar el impacto y la probabilidad de ocurrencia de los riesgos identificados.	4
Valorizar los riesgos en base a su probabilidad de ocurrencia e impacto.	4
Evaluar y definir el tipo de tratamiento más adecuado para los riesgos (Eliminar, transferir, mitigar o aceptar el riesgo).	5
Desarrollar e implementar el tipo de tratamiento seleccionado. En caso se seleccione la opción de mitigar se debe diseñar e implementar controles para abordar los riesgos.	5
Establecer mecanismos para monitorear y revisar continuamente los riesgos de ciberseguridad, y la efectividad de las medidas de tratamiento.	6
Establecer una comunicación efectiva con todas las partes interesadas relevantes, incluyendo a la alta dirección, personal de seguridad y áreas afectadas.	7
Métricas e indicadores	**Unidad de medida**

Número de incidentes de ciberseguridad producidos mensualmente.	Numérico sin unidades.
Número de veces que se revisa y actualiza el contexto de la organización anualmente.	Numérico sin unidades.
Número de veces que se revisa y actualiza el inventariado de activos de TI anualmente.	Numérico sin unidades.
Número de veces que se identifican y monitorean los riesgos de ciberseguridad anualmente.	Numérico sin unidades.
Número de evaluaciones anuales de la efectividad de las medidas de tratamiento.	Numérico sin unidades.

Fuente: Elaboración Propia

Tabla 19: Matriz de roles y responsabilidades del proceso ORG02

Rol / Responsabilidad	Oficial de Seguridad	Analistas de Riesgos	Especialista en Ciberseguridad	Auditor de Sistemas y TIC	Alta Dirección
Establecer escenarios de crisis provenientes de riesgos cibernéticos	A	R	C	-	-
Realizar el inventario y valorización de los activos de TI	A	R	-	-	-
Identificar los riesgos de ciberseguridad	A	R	C	-	-
Analizar y evaluar los riesgo identificados	A	R	C	-	-

Tratar los riesgos y establecer los controles respectivos	A	R	C	-	I
Monitorear y revisar los riesgos	A	R	-	I	I
Comunicar los resultados a las partes interesadas involucradas	AR	-	-	I	I

Fuente: Elaboración Propia

- **Gestión de la continuidad de TI (ORG03)**

Tabla 20: ORG03 - Gestión de la continuidad de TI

Dominio ORGANIZACIONAL **ORG03 - Gestión de la continuidad de TI**	
Descripción	
Definir e implementar estrategias y procedimientos de continuidad de TI que permitan a la organización responder y recuperarse rápidamente de eventos que puedan afectar la continuidad de los servicios de TI.	
Objetivo	
Garantizar la continuidad de los servicios de TI en tiempos y costos aceptados por la organización, de tal forma que se minimicen las interrupciones en el negocio.	
Actividades del proceso	
1. Definir las estrategias del plan.	
2. Establecer los recursos necesarios para llevar a cabo las estrategias.	
3. Desarrollar el plan de continuidad de TI.	
4. Definir las pruebas y el mantenimiento que recibirá el plan de continuidad .	
5. Comunicar y concientizar sobre el uso del plan de continuidad de TI.	
6. Ejecutar el plan cuando se requiera.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301:2019	Cláusula 8
NIST 800-34 - 2010	Capítulo 3

Actividades de implementación	Actividad de proceso
Definir los objetivos y alcance del plan de continuidad de TI.	1
Realizar un análisis de impacto en el negocio para identificar los procesos críticos, activos de TI y sus interdependencias.	1
Establecer estrategias de continuidad de los servicios de TI.	1
Definir los límites de tiempo para la recuperación de procesos y activos de TI (MTD, RTO y RPO).	1
Establecer procedimientos para llevar a cabo cada estrategia.	1
Definir los recursos, personal y capacidades necesarias para llevar a cabo las estrategias.	2
Asignar responsables de las tareas del plan.	2
Documentar el plan de continuidad de TI.	3
Definir pruebas y ejercicios para garantizar que el plan de continuidad funcione como se espera.	4
Establecer un cronograma de revisión y actualización del plan de continuidad de TI para reflejar cambios en los procesos y activos de TI.	4
Comunicar el plan de continuidad de TI a todas las partes interesadas relevantes.	5
Concientizar y capacitar al equipo de continuidad en sus roles y responsabilidades.	5
Ejecutar el plan cuando se requiera.	6
Analizar la efectividad del plan ejecutado.	6
Métricas e indicadores	**Unidad de medida**
Número de veces anuales que se revisa el plan de continuidad de TI.	Numérico sin unidades.
Número de pruebas y ejercicios anuales que se realizan para garantizar que el plan de continuidad funcione como se espera.	Numérico sin unidades.

Número de horas anuales de capacitaciones al equipo de continuidad de TI.	Horas
Número de planes de continuidad ejecutados de forma exitosa anualmente.	Numérico sin unidades.

Fuente: Elaboración Propia

Tabla 21: Matriz de roles y responsabilidades del proceso ORG03

Rol / Responsabilidad	Gerente de TI	Gerente de Operaciones	Gerente de Continuidad	Equipo de Recursos Humanos	Alta Dirección
Definir las estrategias del plan	R	I	R	-	A
Establecer los recursos necesarios para llevar a cabo las estrategias	R	I	R	-	A
Desarrollar el plan de continuidad de TI	R	I	R	-	A
Definir las pruebas y el mantenimiento que recibirá el plan de continuidad	R	I	R	-	A
Comunicar y concientizar sobre el uso del plan de continuidad de TI	R	I	R	R	A

Ejecutar el plan cuando se requiera	AR	I	R	-	I

Fuente: Elaboración Propia

5.2.2 Dominio Operacional (OPE)

- **Gestión de incidentes de ciberseguridad (OPE01)**

Tabla 22: OPE01 - Gestión de incidentes de ciberseguridad

Dominio OPERACIONAL **OPE01 - Gestión de incidentes de ciberseguridad**	
Descripción	
Detectar, analizar y responder a los incidentes de ciberseguridad que generaron la crisis dentro de la organización	
Objetivo	
Minimizar el impacto negativo de las incidencias. Con la finalidad de garantizar la continuidad de los servicios de TI en tiempos y costos aceptados por la organización.	
Actividades del proceso	
1. Establecer el plan de manejo de incidentes.	
2. Registrar y clasificar el incidente.	
3. Activar la gestión de problemas para que identifique la causa-raíz del incidente.	
4. Contener y resolver el incidente.	
5. Restaurar los servicios de TI afectados por el incidente.	
6. Monitorear el incidente y comunicar los resultados a las partes interesadas.	
7. Documentar el incidente y registrar las lecciones aprendidas.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**

NIST 800-61 - 2012	Capítulo 3
ITIL v4 - 2019	Modelo de buenas prácticas del sistema de valor del servicio
Actividades de implementación	**Actividad de proceso**
Establecer las políticas y procedimientos (comunicación con terceros, notificación de los incidentes, entre otros) necesarios para el manejo de incidentes de ciberseguridad.	1
Establecer un equipo de respuesta a incidentes (CSIRT), y asignar los roles y responsabilidades definidos.	1
Identificar a través de herramientas de monitoreo, alertas o reportes de usuarios la existencia de un incidente y analizar si verdaderamente se trata de uno.	2
Registrar el incidente en un repositorio, herramienta o sistema de seguimiento.	2
Priorizar el manejo del incidente en función de su gravedad e impacto en el negocio.	2
Informar el incidente al personal encargado de la gestión de problemas	3
Realizar un análisis en profundidad del incidente para entender su naturaleza, alcance y causa raíz. Para esta actividad se puede utilizar una base de datos de conocimientos.	3
Ejecutar acciones para detener la propagación del incidente y minimizar su impacto en los sistemas y datos de la organización.	4
Identificar y mitigar todas las vulnerabilidades que fueron explotadas. Además, eliminar malware, materiales inapropiados u otros componentes usados para el ataque.	4
Restaurar los servicios de TI afectados a su correcto estado operativo.	5
Restaurar los procesos de negocio que se hayan visto afectados por el incidente	5
Realizar un seguimiento continuo para garantizar que el incidente esté completamente resuelto.	6

Notificar continuamente a las partes interesadas internas o externas el estado del incidente.	6
Registro detallado de todas las acciones e información recolectada durante el manejo del incidente. Para esta actividad se puede utilizar una base de datos de conocimientos.	7
Generar un informe de lecciones aprendidas con todas las partes que participaron en la resolución del incidente.	7
Métricas e indicadores	**Unidad de medida**
Tiempo promedio de detección del incidente mensualmente.	Horas
Tiempo promedio de respuesta al incidente mensualmente.	Horas
Tiempo promedio de recuperación de los servicios de TI mensualmente.	Horas
Tiempo promedio de recuperación de los procesos de negocios mensualmente.	Horas
Número de horas anuales de capacitaciones al equipo de respuesta a incidentes.	Horas
Número de incidentes recurrentes mensualmente.	Numérico sin unidades
Número total de incidentes mensualmente.	Numérico sin unidades

Fuente: Elaboración Propia

Tabla 23: Matriz de roles y responsabilidades del proceso OPE01

Rol / Responsabilidad	Gestor de Incidentes	Oficial de Seguridad	Gerente de TI	Especialista en Ciberseguridad	Analistas de Redes y SO	Analistas de Sistemas	Auditor de Sistemas y TIC	Equipo de Soporte Técnico	Gestor de Problemas	Alta Dirección
Establecer el plan de manejo de incidentes	R	R	C	R	C	C	I	I	C	A
Registrar y clasificar al incidente	AR	I	I	I	R	R	-	R	-	-
Activar a la gestión de problemas para que identifique la causa-raíz del incidente	A	I	-	C	C	C	-	I	R	-
Contener y resolver el incidente	R	A	-	R	R	R	-	I	-	I
Restaurar los servicios de TI afectados por el incidente	R	R	A	R	R	R	I	I	-	I
Monitorear el incidente y comunicar los resultados a las partes interesadas	R	A	I	R	C	C	I	I	-	I

Documentar el incidente y registrar las lecciones aprendidas	R	A	I	R	-	-	I	I	I	I

Fuente: Elaboración Propia

- **Gestión de problemas (OPE02)**

Tabla 24: OPE02 - Gestión de problemas

Dominio OPERACIONAL **OPE02 - Gestión de problemas**	
Descripción	
Identificar las causas raíz que provocaron los incidentes e investigar tanto soluciones temporales como definitivas para evitar recurrencia.	
Objetivo	
Reducir el impacto de los incidentes de ciberseguridad y brindar una respuesta oportuna, mediante la identificación de sus causas reales y potenciales.	
Actividades del proceso	
1. Identificar y registrar los problemas.	
2. Investigar y diagnosticar los problemas.	
3. Implementar soluciones.	
4. Registrar los errores conocidos.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ITIL v4 - 2019	Modelo de buenas prácticas del sistema de valor del servicio
ISO 20000-1:2018	Cláusula 8.6.3
Actividades de implementación	**Actividad de proceso**
Realizar análisis de tendencias y patrones en incidentes para determinar problemas subyacentes.	1

Registrar el problema en un sistema o repositorio de seguimiento.	1
Clasificar los problemas según su gravedad y prioridad.	1
Realizar un análisis exhaustivo de los problemas para determinar su causa raíz. Para esta actividad se puede utilizar técnicas como la de análisis de causa raíz (RCA).	2
Desarrollar y probar soluciones para resolver los problemas (soluciones temporales o permanentes).	3
Mantener y actualizar la documentación sobre soluciones y errores conocidos. Para esta actividad se puede utilizar un sistema o repositorio de gestión del conocimiento.	4
Métricas e indicadores	**Unidad de medida**
Tiempo promedio para determinar causas raíz por incidente mensualmente.	Horas
Número de incidentes con causas raíz determinadas mensualmente.	Numérico sin unidades
Número de incidentes resueltos usando el registro de errores conocidos mensualmente.	Numérico sin unidades

Fuente: Elaboración Propia

Tabla 25: Matriz de roles y responsabilidades del proceso OPE02

Rol / Responsabilidad	Gestor de Problemas	Analistas de Sistemas	Analistas de Redes y SO	Especialista en Ciberseguridad
Identificar y registrar los problemas	AR	-	-	-
Investigar y diagnosticar los problemas	AR	R	R	C
Implementar soluciones	AR	R	R	C
Registrar los errores conocidos	AR	-	-	-

Fuente: Elaboración Propia

- **Gestión del conocimiento (OPE03)**

Tabla 26: OPE03 - Gestión del conocimiento

Dominio OPERACIONAL **OPE03 - Gestión del conocimiento**	
Descripción	
Definir, estructurar, reutilizar y compartir información, habilidades, buenas prácticas, soluciones temporales, causas raíz, procedimientos de respuesta manejados por la organización durante la gestión de crisis producidas por incidentes de ciberseguridad	
Objetivo	
Mantener y mejorar el uso efectivo, eficiente y conveniente del conocimiento generado al interior de la organización, de tal manera que partes interesadas que sean responsables dentro de la gestión de crisis cibernéticas, obtengan la información correcta, en el formato adecuado y en el momento correcto, de acuerdo a su nivel de acceso	
Actividades del proceso	
1. Identificar y captar el conocimiento.	
2. Organizar y estructurar el conocimiento.	
3. Almacenar de manera diligente y segura el conocimiento.	
4. Disponibilizar y mantener el conocimiento.	
5. Capacitar y sensibilizar el uso y generación de conocimientos al interior de la organización	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ITIL v4 - 2019	Modelo de buenas prácticas del sistema de valor del servicio
Actividades de implementación	**Actividad de proceso**

Identificar situaciones, problemas resueltos, mejores prácticas y lecciones aprendidas que generen conocimiento valioso.	1
Capturar y documentar el conocimiento identificado en bases de datos, repositorios o en un sistema de gestión del conocimiento.	1
Categorizar el conocimiento capturado para facilitar su búsqueda. Para esta actividad se puede establecer sistemas de etiquetados para categorizarlo en diferentes áreas.	2
Clasificar el conocimiento según niveles de acceso, de tal manera que se asegure la seguridad de información crítica para la organización.	2
Asegurar que el conocimiento esté disponible para las partes interesadas que lo necesiten, de acuerdo a su nivel de acceso. Para esta actividad se puede utilizar herramientas de colaboración, intranets o sistemas internos.	3
Revisar y actualizar regularmente el conocimiento almacenado para mantenerlo relevante y preciso.	4
Eliminar información obsoleta o incorrecta para evitar confusiones.	4
Proporcionar capacitación a los miembros de la organización (equipos de respuesta a incidentes, crisis, continuidad de TI, entre otros) sobre cómo acceder y utilizar eficazmente el conocimiento compartido.	5
Sensibilizar a los equipos sobre la importancia de compartir y aplicar el conocimiento.	5
Métricas e indicadores	**Unidad de medida**
Promedio de calificación trimestral de calidad del conocimiento por parte de los miembros de la organización.	Numérico sin unidades.
Número de miembros de la organización que acceden a los repositorios o sistemas donde se encuentra el conocimiento mensualmente.	Numérico sin unidades.
Número de revisiones y actualizaciones anuales del conocimiento.	Numérico sin unidades.

Fuente: Elaboración Propia

Tabla 27: Matriz de roles y responsabilidades del proceso OPE03

Rol / Responsabilidad	Gestor de Conocimiento	Administrador del conocimiento	Equipo de Recursos Humanos
Identificar y captar el conocimiento	AR	R	-
Organizar y estructurar el conocimiento	A	R	-
Almacenar de manera diligente y segura el conocimiento	A	R	-
Disponibilizar y mantener el conocimiento	A	R	-
Capacitar y sensibilizar el uso y generación de conocimientos al interior de la organización	A	C	R

Fuente: Elaboración Propia

5.2.3 Dominio Respuesta a Crisis (RAC)

- **Gestión de Crisis (RAC01)**

Tabla 28: RAC01 - Gestión de Crisis

Dominio RESPUESTA A CRISIS **RAC01 - Gestión de Crisis**	
Descripción	
Prevenir, responder y recuperarse de eventos críticos producidos por incidentes de ciberseguridad y que ponen en riesgo la continuidad operativa del negocio y la reputación de la organización.	
Objetivo	
Minimizar los impactos negativos de los eventos de crisis o situaciones inesperadas y garantizar que la organización pueda continuar operando de manera efectiva, durante dichos eventos.	
Actividades del proceso	
1. Definir una estrategia de gestión de crisis.	
2. Identificar la crisis	
3. Responder a la crisis	
4. Implementar acciones de recuperación después de las crisis.	
5. Monitorear y evaluar el desenvolvimiento durante las crisis.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22361:2022	Cláusula 5 y 9
Actividades de implementación	**Actividad de proceso**

Designar un equipo de gestión de crisis (CMT) con roles y responsabilidades claros.	1
Definir los procedimientos de comunicación interna y externa durante la crisis.	1
Definir los procedimientos para establecer una conciencia situacional compartida durante la crisis.	1
Desarrollar el plan de gestión de crisis (CMP).	1
Reconocer y detectar señales tempranas de una crisis potencial o en desarrollo producida por un incidente de ciberseguridad.	2
Activar el equipo de gestión de crisis (CMT) y los mecanismos de comunicación definidos.	2
Evaluar la situación en tiempo real y tomar decisiones rápidas y efectivas.	3
Coordinar las acciones de respuesta de acuerdo con los planes establecidos (activando plan de gestión de crisis, de continuidad de TI, de gestión de incidentes de ciberseguridad).	3
Informar sobre la situación actual de la crisis a las partes interesadas internas y externas (Gestión de comunicaciones en crisis).	3
Evaluar los daños y pérdidas ocasionados por la crisis.	4
Implementar las acciones de recuperación detalladas en los planes para restablecer las operaciones normales del negocio.	4
Analizar e identificar las lecciones aprendidas de la crisis y las oportunidades de mejoras.	5
Realizar revisiones periódicas de los planes para la gestión de crisis e implementar cambios y actualizaciones según sea necesario.	5
Realizar ejercicios para probar la estrategia de gestión de crisis.	5
Métricas e indicadores	**Unidad de medida**
Número de revisiones gerenciales que se hacen al plan de gestión de crisis anualmente.	Numérico sin unidades.
Número de ejercicios de simulación de escenarios que se realizan para probar el plan de gestión de crisis anualmente.	Numérico sin unidades.

Número de horas que se capacita al equipo de gestión de crisis anualmente.	Horas
Número de lecciones aprendidas identificadas post-crisis.	Numérico sin unidades.

Fuente: Elaboración Propia

Tabla 29: Matriz de roles y responsabilidades del proceso RAC01

Rol / Responsabilidad	Líder de Crisis	Gerente de Operaciones	Gerente de Finanzas	Gerente de Continuidad	Gerente de TI	Oficial de Seguridad	Equipo Legal	Líder de Comunicación	Equipo de Soporte Técnico	Equipo de Recursos Humanos	Alta Dirección
Definir una estrategia de gestión de crisis	I	I	I	R	R	R	I	I	I	I	AR
Identificar la crisis	I	I	I	AR	R	R	I	I	I	I	I
Responder a la crisis	R	I	I	AR	R	R	R	R	R	R	I
Recuperarse de las crisis	R	I	I	AR	R	R	R	R	R	R	I
Monitorear y evaluar el desenvolvimiento durante las crisis	I	-	-	AR	R	R	-	-	-	-	I

Fuente: Elaboración Propia

- **Gestión de la Comunicación en crisis (RAC02)**

Tabla 30: RAC02 - Gestión de la Comunicación en crisis

Dominio RESPUESTA A CRISIS **RAC02 - Gestión de la Comunicación en crisis**	
Descripción	
Proporcionar información precisa, oportuna y transparente sobre las acciones que se están tomando para gestionar la crisis a todas las partes interesadas (internas y externas).	
Objetivo	
Asegurar una comunicación rápida y efectiva, tanto a las partes interesadas internas como externas, de las acciones tomadas e información relevante para gestionar la crisis.	
Actividades del proceso	
1. Establecer la estrategia y plan de comunicación.	
2. Establecer una comunicación activa durante la crisis.	
3. Capacitar y preparar al equipo de comunicación.	
4. Evaluar las lecciones aprendidas.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22361:2022	Cláusula 8
Actividades de implementación	**Actividad de proceso**
Identificar a todas las partes interesadas que puedan verse afectadas por la crisis.	1
Segmentar a la audiencia según sus necesidades, intereses y nivel de influencia.	1

Definir la estructura y composición del equipo de comunicaciones.	1
Designar los roles y responsabilidades a miembros capacitados y autorizados para hablar en nombre de la organización.	1
Definir los canales de comunicación que usarán para llegar a la audiencia.	1
Definir pautas y directrices para la comunicación a través de los diferentes canales.	1
Planificar entrevistas, conferencias de prensa y otras interacciones con los medios de comunicación.	1
Documentar el plan de comunicación en crisis.	1
Comunicar a las partes interesadas internas los procedimientos a seguir y las medidas tomadas.	2
Comunicar a las partes interesadas externas información relevante y actualizada de lo que se está haciendo para gestionar la crisis.	2
Monitorear las redes sociales y los medios de comunicación para detectar y abordar rápidamente rumores, información incorrecta o dudas.	2
Proporcionar actualizaciones regulares a todas las partes interesadas a medida que se desarrolla la crisis y se obtiene nueva información.	2
Asegurar que las actualizaciones sean coherentes en todos los canales de comunicación.	2
Capacitar y preparar al equipo en técnicas de comunicación efectiva.	3
Realizar simulacros de comunicación en crisis y proporcionar retroalimentación.	3
Mantener un registro detallado de todas las comunicaciones relacionadas con la crisis.	4
Identificar y evaluar lecciones aprendidas, éxitos y áreas de mejoras.	4
Métricas e indicadores	**Unidad de medida**
Número de horas de capacitaciones al equipo de comunicación anuales.	Horas
Promedio de calificación del nivel de satisfacción de las partes interesadas externas sobre la gestión de crisis.	Numérico sin unidades.

Fuente: Elaboración Propia

Tabla 31: Matriz de roles y responsabilidades del proceso RAC02

Rol / Responsabilidad	Líder de Comunicación	Portavoces / Responsables de prensa	Escritor	Encargado de relaciones con los medios sociales	Encargado de comunicaciones internas	Encargado de comunicaciones externas	Equipo de Recursos Humanos	Alta Dirección
Establecer la estrategia y plan de comunicación	R	I	I	I	I	I	-	AR
Establecer una comunicación activa durante la crisis	AR	R	R	R	R	R	-	I
Capacitar y preparar al equipo de comunicación	AR	I	I	I	I	I	R	I
Evaluar las lecciones aprendidas	AR	I	I	I	I	I	-	I

Fuente: Elaboración Propia

- **Gestión de Equipos de Respuesta (RAC03)**

Tabla 32: RAC03 - Gestión de Equipos de Respuesta

Dominio RESPUESTA A CRISIS **RAC03 - Gestión de Equipos de Respuesta**	
Descripción	
Definir, monitorear y supervisar los roles y responsabilidades específicamente asignados a los miembros de la organización, como parte de los equipos de respuesta, para hacer frente a las crisis generadas por incidentes de ciberseguridad.	
Objetivo	
Asegurar que se asignen las responsabilidades y los encargados para cada rol definido. Asimismo, garantizar el correcto cumplimiento de sus actividades.	
Actividades del proceso	
1. Identificar los roles y responsabilidades para cada proceso.	
2. Asignar los roles al personal calificado.	
3. Capacitar al personal del equipo de respuesta	
4. Supervisar el desempeño del equipo de respuesta	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22361:2022	Cláusulas 8.4 y 5.3.4
ENISA - How to setup CSIRT and SOC - 2020	Capítulo 2
Actividades de implementación	**Actividad de proceso**

Documentar las descripciones de los roles requeridos que incluyan las responsabilidades claves, los objetivos del rol, las habilidades necesarias y criterios de evaluación de desempeño.	1
Definir las habilidades, experiencia y capacidades necesarias para cada rol.	1
Identificar y asignar los roles al personal que cumpla con los perfiles deseados.	2
Comunicar claramente los roles y responsabilidades al personal identificado, de tal forma que comprendan sus roles y cómo estos contribuyen al éxito de la organización.	2
Capacitar al personal de acuerdo a su rol asignado.	3
Realizar evaluaciones de desempeño para garantizar el cumplimiento de los objetivos de los roles	4
Generar informes de desempeño y comunicarlos a todas las partes interesadas (Alta dirección, responsables de los roles, entre otros).	4
Métricas e indicadores	**Unidad de medida**
Número de actualizaciones anuales que se realiza al documento de roles y responsabilidades.	Numérico sin unidades
Número de evaluaciones anuales de desempeño.	Numérico sin unidades
Número de horas de capacitaciones anuales al personal de acuerdo a rol asignado.	Horas

Fuente: Elaboración Propia

Tabla 33: Matriz de roles y responsabilidades del proceso RAC03

Rol / Responsabilidad	Gerente de TI	Gerente de Continuidad	Oficial de Seguridad	Equipo de Recursos Humanos	Alta Dirección
Identificar los roles y responsabilidades para cada proceso	R	R	R	I	A
Asignar los roles al personal calificado	R	R	R	R	A
Capacitar al personal del equipo de respuesta	R	R	R	R	A
Supervisar el desempeño del equipo de respuesta	R	R	R	R	A

Fuente: Elaboración Propia

5.3 Discusión

En esta sección se presentó el desarrollo de cada uno de los procesos que conforman el marco de trabajo para la gestión de incidentes y crisis de ciberseguridad. Para cada proceso se especificó la siguiente información: Descripción, Propósito, Actividades, Documentación relacionada y Métricas e indicadores. Además se definieron los roles y responsabilidades necesarios para gestionar correctamente los procesos, para lo cual se utilizó el modelo de una matriz RACI.

Capítulo 6. Elaborar la guía de implementación del marco

6.1 Introducción

El presente capítulo abarca la elaboración del Objetivo Específico 3 (OE3). Dentro de este capítulo se detalla la guía de implementación del marco para hacer frente a las crisis producidas por incidentes de ciberseguridad. Cabe decir que dentro de la guía se establecen cuales son las actividades necesarias para implementar cada uno de los componentes del marco. Asimismo, se detalla cuales son los roles y responsabilidades por proceso mediante una matriz RACI.

6.2 Resultados Alcanzados (RE4)

A continuación, se presenta la guía de implementación del marco dividida en tres partes: introducción, descripción de cada uno de los roles utilizados dentro de la guía y finalmente las actividades de implementación para cada componente del marco. Es importante mencionar que se colocó la descripción de cada uno de los roles utilizados con la finalidad de mantener un estándar en su definición. Por otro lado, las actividades de implementación se detallan por cada uno de los componentes del marco, los cuales están agrupados en tres dominios: Organizacional, Operacional y Respuesta a Crisis.

En el **Anexo G** se muestra el acta de validación del resultado esperado.

Guía de Aplicación del Marco

1. Introducción

En este documento se presentarán los pasos para poder realizar la implementación de cada uno de los procesos que conforman el marco de trabajo para hacer frente a crisis producidas por incidentes de ciberseguridad.

2. Descripción de Roles

2.1. Gerente de TI

Encargado de liderar la estrategia y la gestión de todos los aspectos relacionados con la tecnología de la información dentro de una organización.

2.2. Gerente de Logística

Encargado de supervisar y gestionar las actividades relacionadas con la cadena de suministro y la distribución de productos o servicios en una organización.

2.3. Administrador de Recursos y Servicios de TI

Encargado de gestionar y supervisar los recursos y servicios relacionados con la infraestructura de TI en una organización.

2.4. Gerente de Finanzas

Tiene la responsabilidad principal de supervisar y gestionar todas las actividades relacionadas con las finanzas y la gestión financiera de la empresa

2.5. Oficial de Seguridad

Encargado de gestionar y supervisar las actividades relacionadas con la seguridad, tanto física como digital, con el objetivo de proteger los activos, la información y la integridad de la organización.

2.6. Analistas de Riesgos

Encargado de identificar, evaluar y gestionar los riesgos que enfrenta una organización.

2.7. Especialista en Ciberseguridad

Tiene la responsabilidad de proteger los sistemas de información, las redes y los activos digitales de una organización contra amenazas cibernéticas y ataques informáticos.

2.8. Auditor de Sistemas y TIC

Encargado de evaluar y verificar la seguridad y eficiencia de los sistemas informáticos y las tecnologías de la información en una organización.

2.9. Alta Dirección

Nivel más alto de liderazgo dentro de una organización. Está compuesta por los ejecutivos y directivos de mayor rango en la jerarquía organizacional y tiene la responsabilidad de tomar decisiones estratégicas clave que afectan a toda la organización.

2.10. Gerente de Operaciones

Supervisa y coordina las actividades diarias de una organización para garantizar que sus operaciones sean eficientes, efectivas y estén alineadas con los objetivos estratégicos.

2.11. Gerente de Continuidad

Encargado de planificar, desarrollar y mantener estrategias y medidas que aseguren la continuidad de las operaciones de una organización en situaciones de crisis, desastres o interrupciones significativas.

2.12. Equipo de Recursos Humanos

Su función principal es administrar y desarrollar el capital humano de la organización, lo que incluye a los empleados, contratistas y personal temporal.

2.13. Gestor de Incidentes

Encargado de coordinar y supervisar la respuesta a incidentes dentro de una organización, especialmente en el ámbito de la tecnología de la información (TI) y la ciberseguridad

2.14. Analistas de Redes y SO

Encargado de la gestión, mantenimiento y optimización de las redes informáticas y los sistemas operativos de una organización.

2.15. Analistas de Sistemas

Encargado de analizar, diseñar, desarrollar e implementar sistemas de software y soluciones tecnológicas para satisfacer las necesidades y objetivos de una organización.

2.16. Equipo de Soporte Técnico

Grupo de profesionales de tecnología de la información (TI) que se encargan de proporcionar asistencia y resolver problemas relacionados con hardware, software y sistemas de tecnología en una organización.

2.17. Gestor de Problemas

Encargado de coordinar y supervisar la gestión de problemas dentro de una organización.

2.18. Gestor de Conocimiento

Responsable de recopilar, organizar, gestionar y compartir el conocimiento y la información crítica de la organización.

2.19. Administrador del conocimiento

Encargado de gestionar y facilitar la creación, organización, almacenamiento y distribución del conocimiento crítico para la organización.

2.20. Líder de Crisis

Tiene la responsabilidad de dirigir y coordinar la respuesta de una organización ante situaciones de crisis o emergencia.

2.21. Equipo Legal

Grupo de profesionales legales que trabajan en conjunto para proporcionar asesoramiento jurídico y representación legal a la organización.

2.22. Líder de Comunicación

Encargado de la planificación, gestión y ejecución de estrategias de comunicación efectivas en una organización.

2.23. Portavoces / Responsables de prensa

Encargados de representar a una organización o entidad en interacciones con los medios de comunicación y el público en general.

2.24. Escritor

Encargado de redactar y producir los mensajes y comunicados relacionados con una crisis o situación de emergencia que afecta a una organización.

2.25. Encargado de relaciones con los medios sociales

Encargado de la gestión de la presencia de la organización en plataformas de medios sociales durante una crisis o situación de emergencia.

2.26. Encargado de comunicaciones internas

Encargado de planificar, coordinar y ejecutar la comunicación interna durante situaciones de crisis o emergencias.

2.27. Encargado de comunicaciones externas

Encargado de planificar, coordinar y ejecutar la comunicación externa durante situaciones de crisis o emergencias.

3. Dominios

3.1. Dominio Organizacional (ORG)

3.1.1. Gestión de recursos financieros y tecnológicos (ORG01)

- **Descripción**

Gestionar los recursos tecnológicos y financieros con los que cuenta la organización, y que van a ser utilizados para asegurar la continuidad de los servicios de TI y para gestionar la crisis cibernéticas.

- **Actividades de proceso**

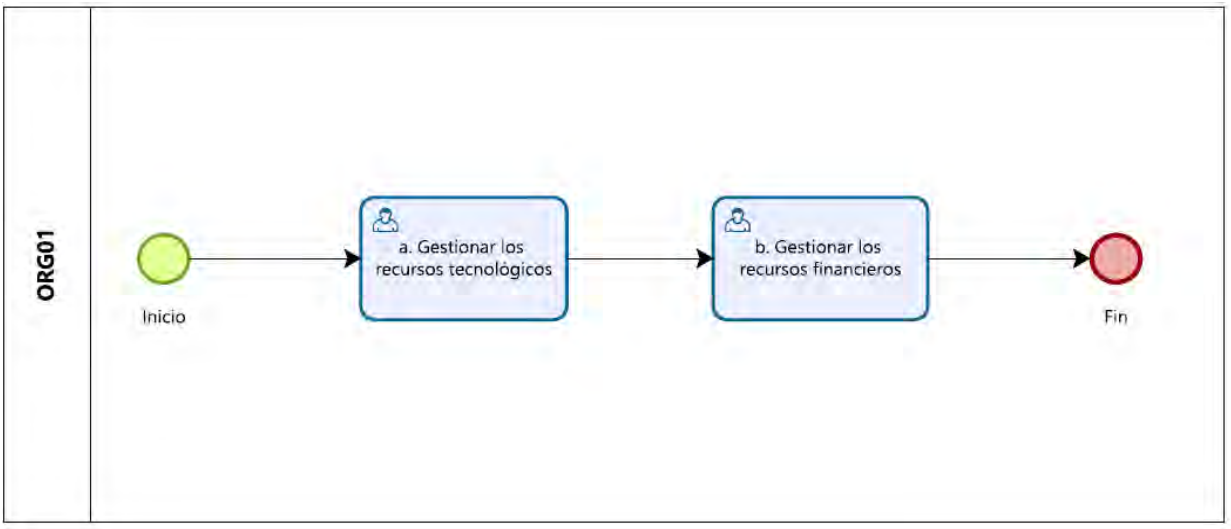


Figura 5: Flujo del proceso ORG01. Fuente: Elaboración Propia

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 5.

a. Gestionar los recursos tecnológicos

i. Realizar un inventario de los recursos tecnológicos con los que se cuenta para las funciones de continuidad de los servicios de TI.

ii. Clasificar los activos en diferentes categorías según su tipo y función. Las categorías por tipo pueden ser Hardware, Software, Redes y Datos. Por otro lado las categorías por función pueden ser Infraestructura de TI, Estaciones de trabajo, Aplicaciones de Negocio, Seguridad de la Información, Datos y Almacenamiento.

iii. Realizar actividades de mantenimiento de los recursos tecnológicos para garantizar su funcionamiento óptimo. Para esta actividad se pueden establecer políticas para llevar a cabo dichas actividades de manera planificada.

b. Gestionar los recursos financieros

i. Establecer un presupuesto para el desarrollo de las actividades de continuidad de servicios de TI y de gestión de la crisis.

ii. Asignar recursos financieros para el desarrollo de dichas actividades según el presupuesto elaborado.

iii. Generar informes que muestren el uso de los recursos financieros asignados y garantizar que se mantengan dentro de los límites presupuestarios establecidos.

- **Roles y Responsabilidades**

Tabla 34: Matriz de roles y responsabilidades del proceso ORG01

Rol / Responsabilidad	Gerente de TI	Gerente de Logística	Administrador de Recursos y Servicios de TI	Gerente de Finanzas
Gestionar los recursos tecnológicos necesarios para las funciones de continuidad de los servicios de TI	A	C	R	-
Gestionar los recursos financieros necesarios para las funciones de continuidad de los servicios de TI y de gestión de crisis	AR	-	-	R

Fuente: Elaboración Propia

3.1.2. Gestión de riesgos de ciberseguridad (ORG02)

- **Descripción**

Identificar, evaluar y tratar los riesgos relacionados a la ciberseguridad que puedan generar una crisis dentro de la organización.

- **Actividades de proceso**

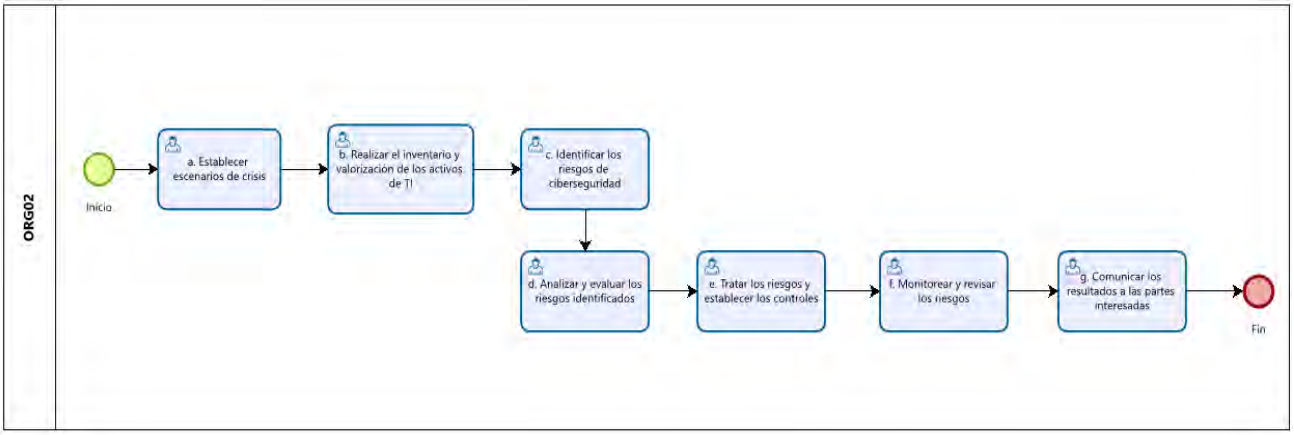


Figura 6: Flujo del proceso ORG02. Fuente: Elaboración Propia

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 6.

a. Establecer escenarios de crisis

i. Desarrollar escenarios de crisis que pueda sufrir la organización a causa de riesgos de ciberseguridad. Para la elaboración de los escenarios de riesgos se puede hacer uso de la plantilla mostrada en la tabla 35.

Tabla 35: Plantilla para la elaboración de escenarios de riesgo

Título del escenario de riesgo	Título corto del escenario de riesgo
Categoría del escenario de riesgo	Seleccionar una categoría: Establecimiento y mantenimiento de la cartera, Gestión del ciclo de vida del programa/proyecto, Toma de decisiones sobre inversiones en TI, Experiencia y habilidades en TI, Operaciones del personal, Información, Arquitectura, Infraestructura, Software, Propiedad empresarial de TI, Proveedores, Cumplimiento normativo, Geopolítica, Robo o destrucción de infraestructura, Malware, Ataques lógicos, Acción industrial, Medio ambiente, Actos de la naturaleza o Innovación.
Referencia del escenario de riesgo	Código del escenario de riesgo
Escenario de riesgo	

Descripción detallada del escenario de riesgo. Tener en cuenta que un escenario de riesgo es una descripción de un evento posible que, cuando ocurra, tendrá un impacto incierto en el logro de los objetivos de la empresa. El impacto puede ser positivo o negativo.		
Componentes del escenario de riesgo		
Tipo de Amenaza ¿Es maliciosa? Si no es así, ¿es accidental o es una falla de un proceso bien definido? ¿Es un evento natural?		
Agente ¿Quién genera la amenaza que explota una vulnerabilidad? Los agentes pueden ser internos o externos y pueden ser humanos o no humanos: - Los agentes internos están dentro de la empresa (personal o contratistas). - Entre los agentes externos incluyen las personas ajenas a la empresa (competidores, reguladores y mercado).		
Evento ¿Es la divulgación de información confidencial, la interrupción de un sistema o de un proyecto, robo o destrucción?. La acción también incluye el diseño ineficaz de sistemas y procesos, o la ejecución ineficaz de procesos (procedimientos de gestión de cambios, procedimientos de adquisición, procesos de priorización de proyectos, entre otros).		
Activo/Recurso (causa) Activo o recurso que conduce al impacto en el negocio. Por ejemplo para un escenario de riesgo de infección de virus el activo/recurso son las personas, específicamente los hackers que atacan a los sistemas con un virus.		
Activo/Recurso (efecto) Activo o recursos que se son afectados por el evento. Para el caso del escenario de riesgo de una infección de virus el activo/recurso son los diferentes procesos de negocio que son interrumpidos.		
Tiempo Dimensión, donde se podría describir lo siguiente, si es relevante para el escenario: - La duración del evento. - El momento (¿El evento ocurre en un momento crítico?). - Detección (¿La detección es inmediata o no?). - Tiempo transcurrido entre el evento y la consecuencia (¿Existe una consecuencia inmediata?).		
Tipo de riesgo (Una "P" indica el grado más alto, una "S" indica un grado inferior, N/A indica que no es relevante)		
Habilitación del beneficio/valor de TI		Asociado con oportunidades (perdidas) de usar la tecnología para mejorar la eficiencia o la efectividad de los procesos de negocio, o como un habilitador para nuevas iniciativas de negocios. Ejemplo: Falta de habilidades y experiencia para usar la tecnología para nuevas iniciativas del negocio.
Entrega del proyecto y programa		Asociado con la aportación de TI a soluciones

de TI		empresariales nuevas o mejoradas, usualmente en forma de proyectos y programas. Ejemplo: No hay avance en los proyectos.
Entrega del servicio y operaciones de TI		Asociado con la estabilidad operativa, la disponibilidad, la protección y la recuperación de los servicios de TI, que pueden causar destrucción o reducción de valor a la empresa. Ejemplo: Problemas de seguridad, cuestiones de cumplimiento, etc.
Posibles respuestas al riesgo		
- Evasión del riesgo - Aceptación del riesgo - Compartir/transferir el riesgo - Mitigación del riesgo		

Fuente: Tomado de COBIT 5 for Risk (2013)

b. Realizar el inventario y valorización de los activos de TI

i. Localizar e identificar los activos de TI que se considerarán dentro de la gestión de riesgos (Inventariado).
ii. Identificar los procesos de negocio a los que brindan soporte.
iii. Valorizar los activos de TI identificados en base a niveles de sensibilidad y criticidad.
iv. Priorizar los activos en base a su valorización.

c. Identificar los riesgos de ciberseguridad

i. Identificar las vulnerabilidades de los activos de TI.
ii. Identificar las amenazas que puedan aprovechar las vulnerabilidades y conocer las condiciones en las que pueden manifestarse dichos eventos amenazantes.
iii. Identificar los riesgos asociados a los activos de TI.

Para esta actividad se recomienda elaborar un cuadro con las siguientes columnas: Activo, Vulnerabilidad, Amenaza y Riesgos.

d. Analizar y evaluar los riesgos identificados

i. Evaluar el impacto y la probabilidad de ocurrencia de los riesgos identificados.
Para evaluar el impacto se puede utilizar la tabla 36:

Tabla 36: Categorías de impacto

Impacto	Descripción	Valor
GRAVE	Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la organización.	20
MODERADO	Si el hecho llegara a presentarse, tendría medio impacto o efecto sobre la organización.	10
LEVE	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	5

Fuente: Elaboración Propia

Por otro lado, para evaluar la probabilidad se puede utilizar la tabla 37:

Tabla 37: Categorías de probabilidad

Probabilidad	Descripción	Valor
ALTA	Es muy factible que el hecho se presente.	3
MEDIA	Es factible que el hecho se presente.	2
BAJA	Es muy poco factible que el hecho se presente.	1

Fuente: Elaboración Propia

ii. Valorizar los riesgos en base a su probabilidad de ocurrencia e impacto. Para ello se puede utilizar la siguiente fórmula:

Riesgo = Impacto x Probabilidad

Luego, agrupar los riesgos según su valorización:

- Alto Riesgo: aquellos riesgos cuyo valor está en el rango [30, 60]
- Medio Riesgo: aquellos riesgos cuyo valor está en el rango [15, 30[
- Bajo Riesgo: aquellos riesgos cuyo valor está en el rango [5, 15[

e. Tratar los riesgos y establecer los controles

i. Evaluar y definir el tipo de tratamiento más adecuado para los riesgos:

- Eliminar: Se elimina la actividad, proceso o activo de información que está generando el riesgo.
- Transferir: Se transfiere el riesgo a un tercero. Por ejemplo, un seguro sobre un activo.
- Mitigar: Se implementan controles propios.
- Aceptar el riesgo: Se acepta o tolera el riesgo por la organización.

ii. Desarrollar e implementar el tipo de tratamiento seleccionado. En caso se seleccione la opción de mitigar se debe diseñar e implementar controles para abordar los riesgos.
Para la elaboración de los controles se puede utilizar la plantilla mostrada en la tabla 38.

Tabla 38: Plantilla para la elaboración del control

Título del control	Nombre del control
Riesgo asociado	Que riesgo mitiga el control
Identificador del control	Código del control
Descripción De qué trata el control.	
Propósito Cual es el objetivo del control.	
Tipo de Control Preventivo, detectivo o correctivo.	
Responsable Responsables del control.	
Guía de implementación De qué forma se debe implementar el control.	
Métricas e indicadores Cómo se medirá el desempeño del control.	
Información relacionada Referencia a otros documentos.	

Fuente: Elaboración Propia

f. Monitorear y revisar los riesgos

i. Establecer mecanismos para monitorear y revisar continuamente los riesgos de ciberseguridad, y la efectividad de las medidas de tratamiento.

g. Comunicar los resultados a las partes interesadas

i. Establecer una comunicación efectiva con todas las partes interesadas relevantes, incluyendo a la alta dirección, personal de seguridad y áreas afectadas.

- **Roles y responsabilidades**

Tabla 39: Matriz de roles y responsabilidades del proceso ORG02

Rol / Responsabilidad	Oficial de Seguridad	Analistas de Riesgos	Especialista en Ciberseguridad	Auditor de Sistemas y TIC	Alta Dirección
Establecer escenarios de crisis provenientes de riesgos cibernéticos	A	R	C	-	-
Realizar el inventario y valorización de los activos de TI	A	R	-	-	-
Identificar los riesgos de ciberseguridad	A	R	C	-	-
Analizar y evaluar los riesgo identificados	A	R	C	-	-
Tratar los riesgos y establecer los controles respectivos	A	R	C	-	I
Monitorear y revisar los riesgos	A	R	-	I	I
Comunicar los resultados a las partes interesadas involucradas	AR	-	-	I	I

Fuente: Elaboración Propia

3.1.3. Gestión de la continuidad de TI (ORG03)

- **Descripción**

Definir e implementar estrategias y procedimientos de continuidad de TI que permitan a la organización responder y recuperarse rápidamente de eventos que puedan afectar la continuidad de los servicios de TI.

- **Actividades de proceso**

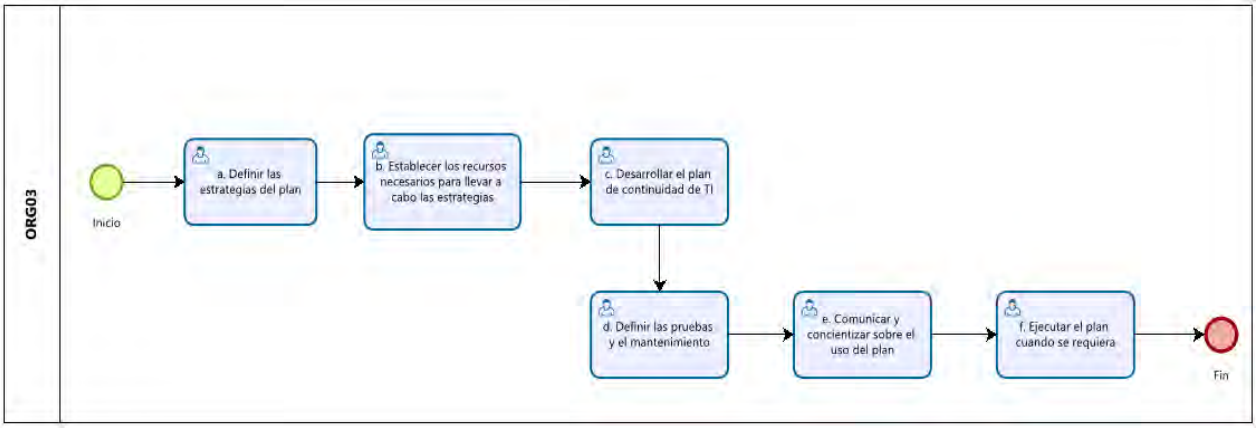


Figura 7: Flujo del proceso ORG03. Fuente: Elaboración Propia

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 7.

a. Definir las estrategias del plan

i. Definir los objetivos y alcance del plan de continuidad de TI.

ii. Realizar un análisis de impacto en el negocio para identificar los procesos críticos, activos de TI y sus interdependencias. Un ejemplo del análisis BIA se puede observar en la figura 8.

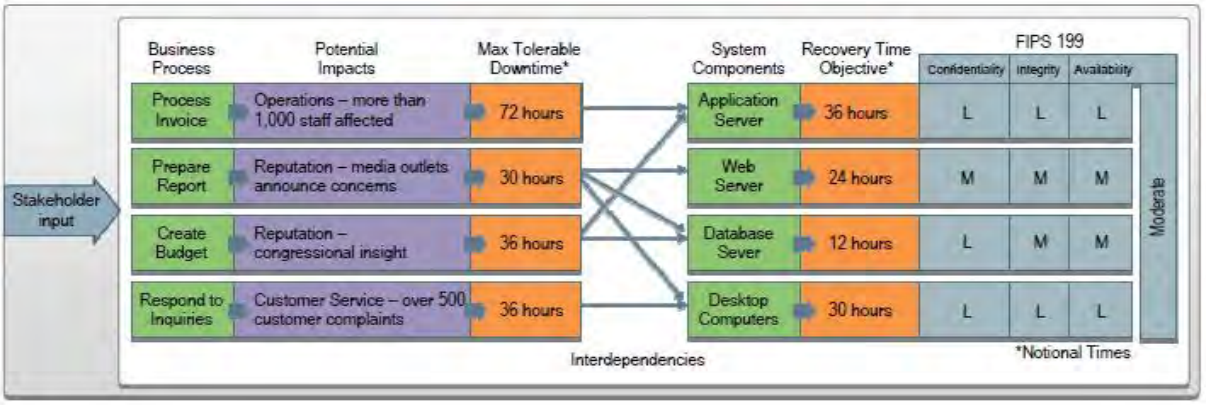


Figura 8: Proceso de Análisis de Impacto Empresarial. Tomado del NIST 800-34

iii. Establecer estrategias de continuidad de los servicios de TI.

iv. Definir los límites de tiempo para la recuperación de procesos y activos de TI (MTD, RTO y RPO).

v. Establecer procedimientos para llevar a cabo cada estrategia.

b. Establecer los recursos necesarios para llevar a cabo las estrategias

i. Definir los recursos, personal y capacidades necesarias para llevar a cabo las estrategias.

ii. Asignar responsables de las tareas del plan.

c. Desarrollar el plan de continuidad de TI

i. Documentar el plan de continuidad de TI.

d. Definir las pruebas y el mantenimiento

i. Definir pruebas y ejercicios para garantizar que el plan de continuidad funcione como se espera.

ii. Establecer un cronograma de revisión y actualización del plan de continuidad de TI para reflejar cambios en los procesos y activos de TI.

e. Comunicar y concientizar sobre el uso del plan

i. Comunicar el plan de continuidad de TI a todas las partes interesadas relevantes.

ii. Concientizar y capacitar al equipo de continuidad en sus roles y responsabilidades.

f. Ejecutar el plan cuando se requiera

i. Ejecutar el plan cuando se requiera.

ii. Analizar la efectividad del plan ejecutado.

- **Roles y responsabilidades**

Tabla 40: Matriz de roles y responsabilidades del proceso ORG03

Rol / Responsabilidad	Gerente de TI	Gerente de Operaciones	Gerente de Continuidad	Equipo de Recursos Humanos	Alta Dirección
Definir las estrategias del plan	R	I	R	-	A
Establecer los recursos necesarios para llevar a cabo las estrategias	R	I	R	-	A
Desarrollar el plan de continuidad de TI	R	I	R	-	A
Definir las pruebas y el mantenimiento que recibirá el plan de continuidad	R	I	R	-	A

Comunicar y concientizar sobre el uso del plan de continuidad de TI	R	I	R	R	A
Ejecutar el plan cuando se requiera	AR	I	R	-	I

Fuente: Elaboración Propia

3.2. Dominio Operacional (OPE)

3.2.1. Gestión de incidentes de ciberseguridad (OPE01)

- **Descripción**

Detectar, analizar y responder a los incidentes de ciberseguridad que generaron la crisis dentro de la organización.

- **Actividades de proceso**

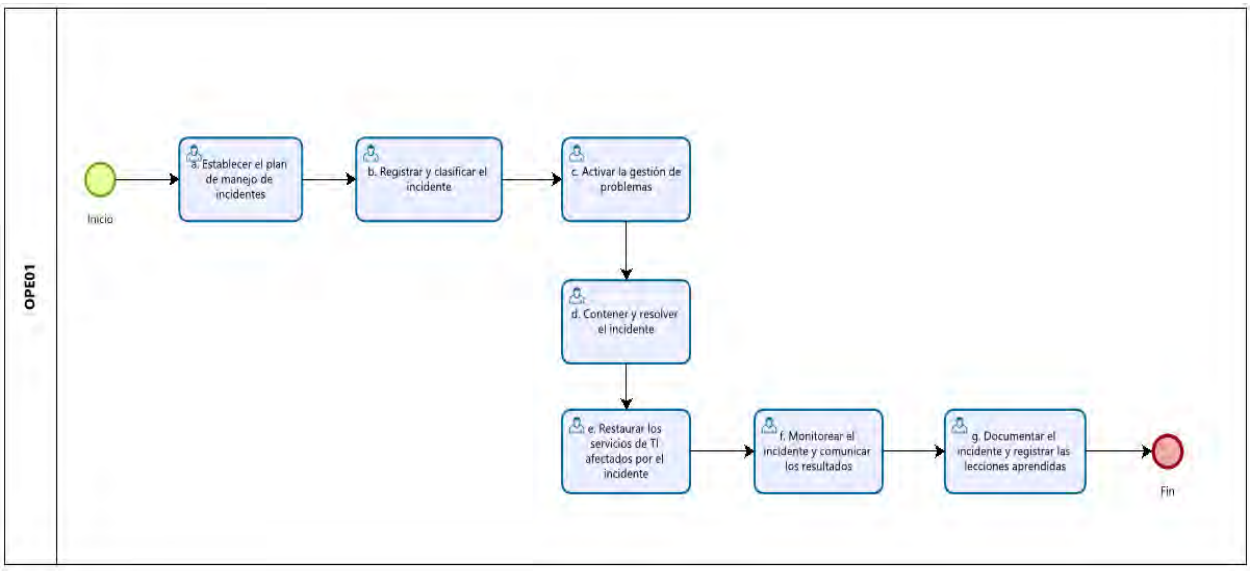


Figura 9: Flujo del proceso OPE01. Fuente: Elaboración Propia

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 9.

a. Establecer el plan de manejo de incidentes

i. Establecer las políticas y procedimientos (comunicación con terceros, notificación de los incidentes, entre otros) necesarios para el manejo de incidentes de ciberseguridad.
   Las políticas pueden tener la siguiente estructura:
   - Número de Política: Es el identificador universal de la política.
   - Versión: Son numeradas consecutivamente, 1.0, 2.0, etc.
   - Título: Indicar de forma clara y concisa el título en no más de un número limitado de caracteres.
   - Propósito: Debe dar una idea del tema que la política va a dictar.
   - Objetivo: Que se busca con la política.
   - Área de Impacto: Listar las áreas afectadas por esta política.
   - Aprobaciones: Indicar nombre y rol de quienes la han aprobado, señalando la fecha de aprobación en formato standard.

- Fecha de implementación: Fecha en que la política entrará en vigencia, en formato estándar.
- Excepciones: Indicar qué o quiénes están exentos de seguir esta política.

ii. Establecer un equipo de respuesta a incidentes (CSIRT), y asignar los roles y responsabilidades definidos.

b. Registrar y clasificar el incidente

i. Identificar a través de herramientas de monitoreo, alertas o reportes de usuarios la existencia de un incidente y analizar si verdaderamente se trata de uno.

ii. Registrar el incidente en un repositorio, herramienta o sistema de seguimiento.

iii. Priorizar el manejo del incidente en función de su gravedad (Nivel de esfuerzo para la recuperación) e impacto (Funcional o de Información) en el negocio.

Para evaluar el nivel de esfuerzo para la recuperación se puede utilizar la tabla 41:

Tabla 41: Categorías de Esfuerzos de Recuperación

Categoría	Definición
Regular	El tiempo de recuperación es previsible con los recursos existentes.
Complementado	El tiempo de recuperación es previsible con recursos adicionales
Extendido	El tiempo de recuperación es imprevisible. Se necesitan recursos adicionales y ayuda externa.
No recuperable	No es posible recuperarse del incidente (por ejemplo, datos confidenciales filtrados y publicados públicamente). Se debe iniciar una investigación profunda.

Fuente: Tomado de NIST 800-61 - Computer Security Incident Handling Guide (2012)

Para evaluar el impacto Funcional se puede utilizar la tabla 42:

Tabla 42: Categorías de impacto Funcional

Categoría	Definición
No aplica	Ningún efecto sobre la capacidad de la organización para proporcionar todos los servicios a todos sus usuarios.

Bajo	Efecto mínimo. La organización aún puede proporcionar todos los servicios críticos a todos los usuarios, pero ha perdido eficiencia.
Medio	La organización ha perdido la capacidad de proporcionar un servicio crítico a un subconjunto de usuarios.
Alto	La organización ya no puede proporcionar algunos servicios críticos a ningún usuario.

Fuente: Tomado de NIST 800-61 - Computer Security Incident Handling Guide (2012)

Para evaluar el impacto en la Información se puede utilizar la tabla 43:

Tabla 43: Categorías de impacto en la Información

Categoría	Definición
No aplica	Ninguna información fue filtrada, cambiada, eliminada o comprometida.
Violación de privacidad	Se accedió o se filtró información confidencial de identificación personal (PII) de contribuyentes, empleados, beneficiarios, etc.
Violación de propiedad	Se accedió o se filtró información de propiedad no clasificada, como información de infraestructura crítica protegida (PCII).
Pérdida de integridad	Se cambió o eliminó información confidencial o de propiedad exclusiva.

Fuente: Tomado de NIST 800-61 - Computer Security Incident Handling Guide (2012)

c. Activar la gestión de problemas

i. Informar el incidente al personal encargado de la gestión de problemas.

ii. Realizar un análisis en profundidad del incidente para entender su naturaleza, alcance y causa raíz. Para esta actividad se puede utilizar una base de datos de conocimientos.

d. Contener y resolver el incidente

i. Ejecutar acciones para detener la propagación del incidente y minimizar su impacto en los sistemas y datos de la organización.

ii. Identificar y mitigar todas las vulnerabilidades que fueron explotadas. Además, eliminar malware, materiales inapropiados u otros componentes usados para el ataque.

e. Restaurar los servicios de TI afectados por el incidente

i. Restaurar los servicios de TI afectados a su correcto estado operativo.

ii. Restaurar los procesos de negocio que se hayan visto afectados por el incidente

f. Monitorear el incidente y comunicar los resultados

i. Realizar un seguimiento continuo para garantizar que el incidente esté completamente resuelto.

ii. Notificar continuamente a las partes interesadas internas o externas el estado del incidente.

g. Documentar el incidente y registrar las lecciones aprendidas

i. Registro detallado de todas las acciones e información recolectada durante el manejo del incidente. Para esta actividad se puede utilizar una base de datos de conocimientos.

ii. Generar un informe de lecciones aprendidas con todas las partes que participaron en la resolución del incidente.

- **Roles y responsabilidades**

Tabla 44: Matriz de roles y responsabilidades del proceso OPE01

Rol / Responsabilidad	Gestor de Incidentes	Oficial de Seguridad	Gerente de TI	Especialista en Ciberseguridad	Analistas de Redes y SO	Analistas de Sistemas	Auditor de Sistemas y TIC	Equipo de Soporte Técnico	Gestor de Problemas	Alta Dirección
Establecer el plan de manejo de incidentes	R	R	C	R	C	C	I	I	C	A
Registrar y clasificar al incidente	AR	I	I	I	R	R	-	R	-	-
Activar a la gestión de problemas para que identifique la causa-raíz del incidente	A	I	-	C	C	C	-	I	R	-
Contener y resolver el incidente	R	A	-	R	R	R	-	I	-	I

Restaurar los servicios de TI afectados por el incidente	R	R	A	R	R	R	I	I	-	I
Monitorear el incidente y comunicar los resultados a las partes interesadas	R	A	I	R	C	C	I	I	-	I
Documentar el incidente y registrar las lecciones aprendidas	R	A	I	R	-	-	I	I	I	I

Fuente: Elaboración propia.

3.2.2. Gestión de problemas (OPE02)

- **Descripción**

Identificar las causas raíz que provocaron los incidentes e investigar tanto soluciones temporales como definitivas para evitar recurrencia.

- **Actividades de proceso**

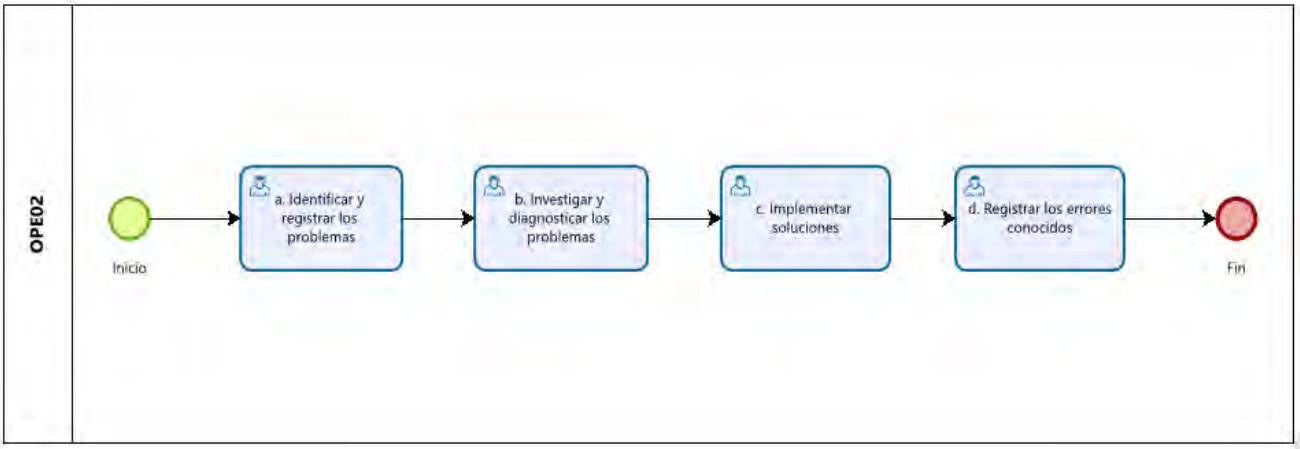


Figura 10: Flujo del proceso OPE02. Fuente: Elaboración propia.

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 10.

a. Identificar y registrar los problemas

i. Realizar análisis de tendencias y patrones en incidentes para determinar problemas subyacentes.

ii. Registrar el problema en un sistema o repositorio de seguimiento.
iii. Clasificar los problemas según su gravedad y prioridad.

Para clasificar los problemas según su gravedad se puede utilizar la tabla 45:

Tabla 45: Categorías de Gravedad

Categoría	Definición
Baja	Problemas menores que tienen un impacto limitado en los servicios o el negocio. No son urgentes pero aún deben resolverse.
Media	Problemas importantes pero no críticos que afectan los servicios de TI o el negocio. Tienen un impacto moderado y requieren atención oportuna.
Alta	Problemas críticos que tienen un impacto significativo en los servicios de TI o en el negocio. Pueden causar una interrupción importante o pérdida financiera.

Fuente: Elaboración propia.

Para clasificar los problemas según su prioridad se puede utilizar la tabla 46:

Tabla 46: Categorías de Prioridad

Categoría	Definición
Baja	Problemas que pueden esperar y resolverse en un momento conveniente. Tienen un impacto limitado en la operación y pueden programarse para resolverse más tarde.
Media	Problemas importantes que deben resolverse en un plazo razonable. No son tan urgentes como los de alta prioridad, pero aún requieren atención pronta.
Alta	Problemas que deben resolverse de inmediato, generalmente debido a su impacto crítico en los servicios o el negocio. Pueden afectar la disponibilidad o la seguridad.

Fuente: Elaboración propia

b. Investigar y diagnosticar los problemas

i. Realizar un análisis exhaustivo de los problemas para determinar su causa raíz. Para esta actividad se puede utilizar técnicas como la de análisis de causa raíz (RCA).

c. Implementar soluciones

i. Desarrollar y probar soluciones para resolver los problemas (soluciones temporales o permanentes).

d. Registrar los errores conocidos

i. Mantener y actualizar la documentación sobre soluciones y errores conocidos. Para esta actividad se puede utilizar un sistema o repositorio de gestión del conocimiento.

- **Roles y responsabilidades**

Tabla 47: Matriz de roles y responsabilidades del proceso OPE02

Rol / Responsabilidad	Gestor de Problemas	Analistas de Sistemas	Analistas de Redes y SO	Especialista en Ciberseguridad
Identificar y registrar los problemas	AR	-	-	-
Investigar y diagnosticar los problemas	AR	R	R	C
Implementar soluciones	AR	R	R	C
Registrar los errores conocidos	AR	-	-	-

Fuente: Elaboración propia.

3.2.3. Gestión del conocimiento (OPE03)

- **Descripción**

Definir, estructurar, reutilizar y compartir información, habilidades, buenas prácticas, soluciones temporales, causas raíz, procedimientos de respuesta manejados por la organización durante la gestión de crisis producidas por incidentes de ciberseguridad.

- **Actividades de proceso**

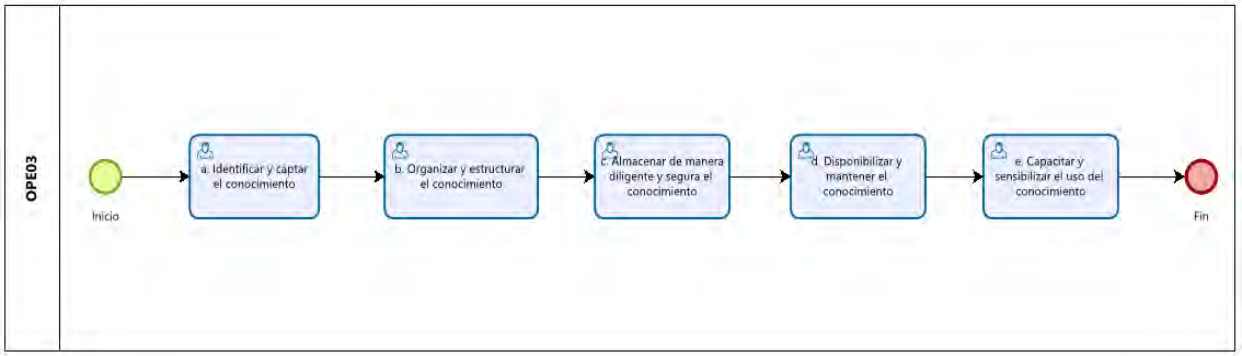


Figura 11: Flujo del proceso OPE03. Fuente: Elaboración Propia

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 11.

a. Identificar y captar el conocimiento

i. Identificar situaciones, problemas resueltos, mejores prácticas y lecciones aprendidas que generen conocimiento valioso.

ii. Capturar y documentar el conocimiento identificado en bases de datos, repositorios o en un sistema de gestión del conocimiento.

b. Organizar y estructurar el conocimiento

i. Categorizar el conocimiento capturado para facilitar su búsqueda. Para esta actividad se puede establecer sistemas de etiquetados para categorizarlo en diferentes áreas.

ii. Clasificar el conocimiento según niveles de acceso, de tal manera que se asegure la seguridad de información crítica para la organización.
Para clasificar el conocimiento según niveles de acceso se puede utilizar la tabla 48:

Tabla 48: Categorías de Nivel de acceso

Categoría	Definición
Acceso Público	El conocimiento está disponible públicamente para todos los empleados de la organización y para partes externas.
Acceso Interno	El conocimiento está disponible solo para los empleados de la organización y se utiliza para fines internos.
Acceso Restringido	El conocimiento está disponible solo para un grupo selecto de empleados que tienen permiso específico para acceder a él.
Acceso Confidencial	El conocimiento está altamente restringido y solo está disponible para un número muy limitado de personas con un nivel extremadamente alto de autorización.

Fuente: Elaboración propia.

c. Almacenar de manera diligente y segura el conocimiento

i. Asegurar que el conocimiento esté disponible para las partes interesadas que lo necesiten, de acuerdo a su nivel de acceso. Para esta actividad se puede utilizar herramientas de colaboración, intranets o sistemas internos.

d. Disponibilizar y mantener el conocimiento

i. Revisar y actualizar regularmente el conocimiento almacenado para mantenerlo relevante y preciso.

ii. Eliminar información obsoleta o incorrecta para evitar confusiones.

e. Capacitar y sensibilizar el uso del conocimiento

i. Proporcionar capacitación a los miembros de la organización (equipos de respuesta a incidentes, crisis, continuidad de TI, entre otros) sobre cómo acceder y utilizar eficazmente el conocimiento compartido.
ii. Sensibilizar a los equipos sobre la importancia de compartir y aplicar el conocimiento.

- **Roles y responsabilidades**

Tabla 49: Matriz de roles y responsabilidades del proceso OPE03

Rol / Responsabilidad	Gestor de Conocimiento	Administrador del conocimiento	Equipo de Recursos Humanos
Identificar y captar el conocimiento	AR	R	-
Organizar y estructurar el conocimiento	A	R	-
Almacenar de manera diligente y segura el conocimiento	A	R	-
Disponibilizar y mantener el conocimiento	A	R	-
Capacitar y sensibilizar el uso y generación de conocimientos al interior de la organización	A	C	R

Fuente: Elaboración propia.

3.3. Domino Respuesta a Crisis (RAC)

3.3.1. Gestión de Crisis (RAC01)

- **Descripción**

Prevenir, responder y recuperarse de eventos críticos producidos por incidentes de ciberseguridad y que ponen en riesgo la continuidad operativa del negocio y la reputación de la organización.

- **Actividades de proceso**

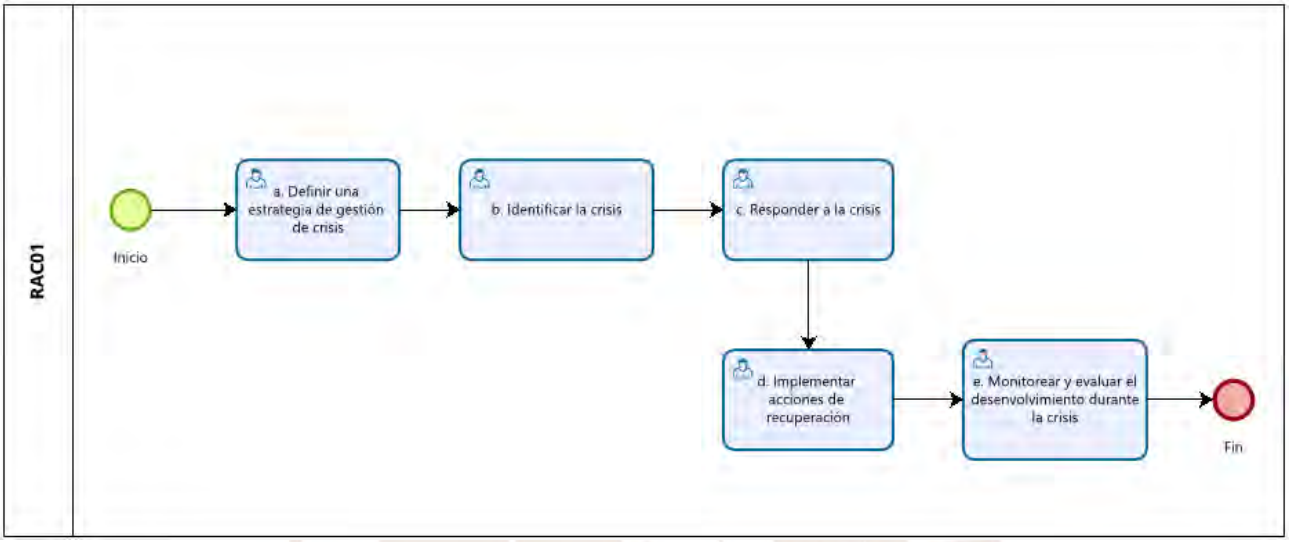


Figura 12: Flujo del proceso RAC01. Fuente: Elaboración propia.

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 12.

a. Definir una estrategia de gestión de crisis

i. Designar un equipo de gestión de crisis (CMT) con roles y responsabilidades claras.
ii. Definir los procedimientos de comunicación interna y externa durante la crisis.
iii. Definir los procedimientos para establecer una conciencia situacional compartida durante la crisis.
iv. Desarrollar el plan de gestión de crisis (CMP).

b. Identificar la crisis

i. Reconocer y detectar señales tempranas de una crisis potencial o en desarrollo producida por un incidente de ciberseguridad.
ii. Activar el equipo de gestión de crisis (CMT) y los mecanismos de comunicación definidos.

c. Responder a la crisis

i. Evaluar la situación en tiempo real y tomar decisiones rápidas y efectivas.

ii. Coordinar las acciones de respuesta de acuerdo con los planes establecidos. Activando el plan de gestión de crisis, de continuidad de TI y de gestión de incidentes de ciberseguridad.
iii. Informar sobre la situación actual de la crisis a las partes interesadas internas y externas (Gestión de comunicaciones en crisis).

d. Implementar acciones de recuperación

i. Evaluar los daños y pérdidas ocasionados por la crisis.
ii. Implementar las acciones de recuperación detalladas en los planes para restablecer las operaciones normales del negocio.

e. Monitorear y evaluar el desenvolvimiento durante las crisis

i. Analizar e identificar las lecciones aprendidas de la crisis y las oportunidades de mejoras.
ii. Realizar revisiones periódicas de los planes para la gestión de crisis e implementar cambios y actualizaciones según sea necesario.
iii. Realizar ejercicios para probar la estrategia de gestión de crisis.

- **Roles y responsabilidades**

Tabla 50: Matriz de roles y responsabilidades del proceso RAC01

Rol / Responsabilidad	Líder de Crisis	Gerente de Operaciones	Gerente de Finanzas	Gerente de Continuidad	Gerente de TI	Oficial de Seguridad	Equipo Legal	Líder de Comunicación	Equipo de Soporte Técnico	Equipo de Recursos Humanos	Alta Dirección
Definir una estrategia de gestión de crisis	I	I	I	R	R	R	I	I	I	I	AR
Identificar la crisis	I	I	I	AR	R	R	I	I	I	I	I
Responder a la crisis	R	I	I	AR	R	R	R	R	R	R	I
Recuperarse de las crisis	R	I	I	AR	R	R	R	R	R	R	I

Monitorear y evaluar el desenvolvimiento durante las crisis	I	-	-	AR	R	R	-	-	-	-	I

Fuente: Elaboración propia.

3.3.2. Gestión de la Comunicación en crisis (RAC02)

- **Descripción**

Proporcionar información precisa, oportuna y transparente sobre las acciones que se están tomando para gestionar la crisis a todas las partes interesadas (internas y externas).

- **Actividades de proceso**

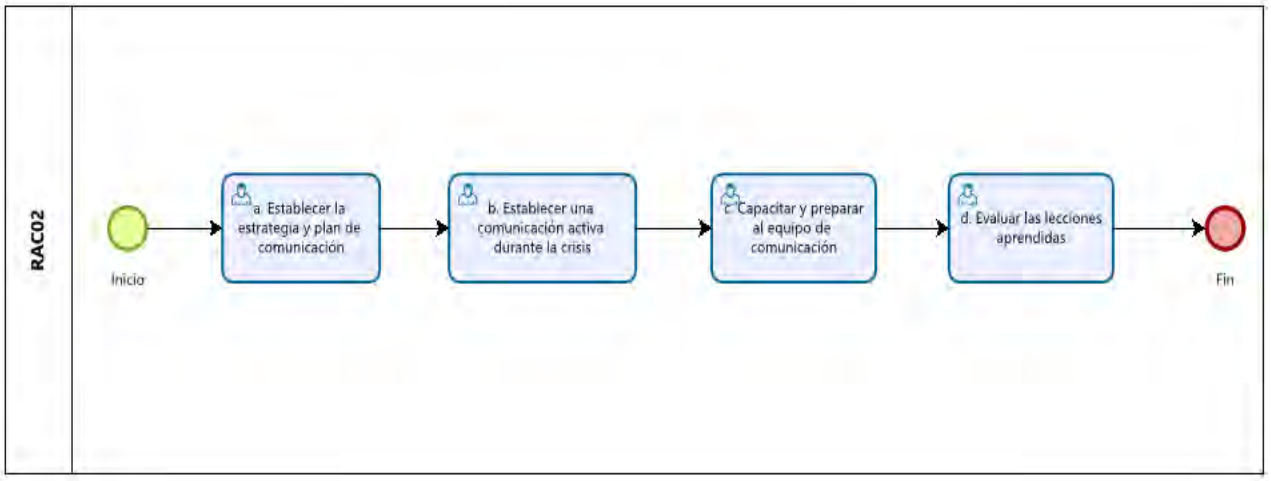


Figura 13: Flujo del proceso RAC02. Fuente: Elaboración propia.

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 13.

a. Establecer la estrategia y plan de comunicación

i. Identificar a todas las partes interesadas que puedan verse afectadas por la crisis.
ii. Segmentar a la audiencia según sus necesidades, intereses y nivel de influencia.
iii. Definir la estructura y composición del equipo de comunicaciones.
iv. Designar los roles y responsabilidades a miembros capacitados y autorizados para hablar en nombre de la organización.

v. Definir los canales de comunicación que usarán para llegar a la audiencia.
vi. Definir pautas y directrices para la comunicación a través de los diferentes canales.
vii. Planificar entrevistas, conferencias de prensa y otras interacciones con los medios de comunicación.
viii. Documentar el plan de comunicación en crisis.

b. Establecer una comunicación activa durante la crisis

i. Comunicar a las partes interesadas internas los procedimientos a seguir y las medidas tomadas.
ii. Comunicar a las partes interesadas externas información relevante y actualizada de lo que se está haciendo para gestionar la crisis.
iii. Monitorear las redes sociales y los medios de comunicación para detectar y abordar rápidamente rumores, información incorrecta o dudas.
iv. Proporcionar actualizaciones regulares a todas las partes interesadas a medida que se desarrolla la crisis y se obtiene nueva información.
v. Asegurar que las actualizaciones sean coherentes en todos los canales de comunicación.

c. Capacitar y preparar al equipo de comunicación

i. Capacitar y preparar al equipo en técnicas de comunicación efectiva.
ii. Realizar simulacros de comunicación en crisis y proporcionar retroalimentación.

d. Evaluar las lecciones aprendidas

i. Mantener un registro detallado de todas las comunicaciones relacionadas con la crisis.
ii. Identificar y evaluar lecciones aprendidas, éxitos y áreas de mejoras.

- **Roles y responsabilidades**

Tabla 51: Matriz de roles y responsabilidades del proceso RAC02

Rol / Responsabilidad	Líder de Comunicación	Portavoces / Responsables de prensa	Escritor	Encargado de relaciones con los medios sociales	Encargado de comunicaciones internas	Encargado de comunicaciones externas	Equipo de Recursos Humanos	Alta Dirección
Establecer la estrategia y plan de comunicación	R	I	I	I	I	I	-	AR
Establecer una comunicación activa durante la crisis	AR	R	R	R	R	R	-	I
Capacitar y preparar al equipo de comunicación	AR	I	I	I	I	I	R	I
Evaluar las lecciones aprendidas	AR	I	I	I	I	I	-	I

Fuente: Elaboración propia.

3.3.3. Gestión de Equipos de Respuesta (RAC03)

- **Descripción**

Definir, monitorear y supervisar los roles y responsabilidades específicamente asignados a los miembros de la organización, como parte de los equipos de respuesta, para hacer frente a las crisis generadas por incidentes de ciberseguridad.

- **Actividades de proceso**

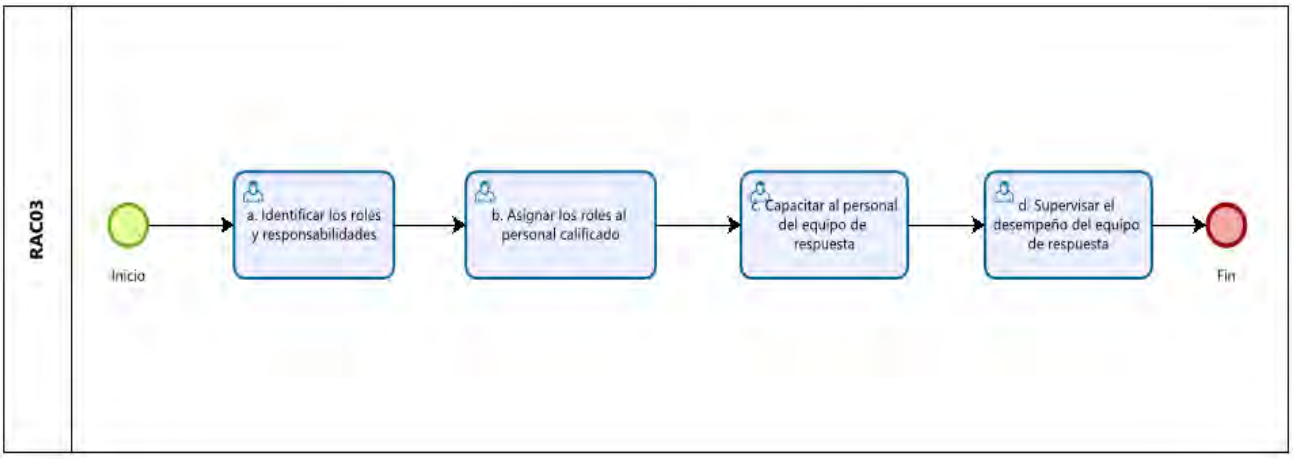


Figura 14: Flujo del proceso RAC03. Fuente: Elaboración propia.

A continuación, se indica de qué manera se debe llevar a cabo cada una de las las actividades mostradas en la Figura 14.

a. Identificar los roles y responsabilidades

i. Documentar las descripciones de los roles requeridos que incluyan las responsabilidades claves, los objetivos del rol, las habilidades necesarias y criterios de evaluación de desempeño.

ii. Definir las habilidades, experiencia y capacidades necesarias para cada rol.

b. Asignar los roles al personal calificado

i. Identificar y asignar los roles al personal que cumpla con los perfiles deseados.

ii. Comunicar claramente los roles y responsabilidades al personal identificado, de tal forma que comprendan sus roles y cómo estos contribuyen al éxito de la organización.

c. Capacitar al personal del equipo de respuesta

i. Capacitar al personal de acuerdo a su rol asignado.

d. Supervisar el desempeño del equipo de respuesta

i. Realizar evaluaciones de desempeño para garantizar el cumplimiento de los objetivos de los roles

ii. Generar informes de desempeño y comunicarlos a todas las partes interesadas (Alta dirección, responsables de los roles, entre otros).

- **Roles y responsabilidades**

Tabla 52: Matriz de roles y responsabilidades del proceso RAC03

Rol / Responsabilidad	Gerente de TI	Gerente de Continuidad	Oficial de Seguridad	Equipo de Recursos Humanos	Alta Dirección
Identificar los roles y responsabilidades para cada proceso	R	R	R	I	A
Asignar los roles al personal calificado	R	R	R	R	A
Capacitar al personal del equipo de respuesta	R	R	R	R	A
Supervisar el desempeño del equipo de respuesta	R	R	R	R	A

Fuente: Elaboración propia.

6.3 Discusión

En esta sección se presentó la guía de implementación del marco dividida en tres partes: introducción, descripción de cada uno de los roles utilizados y las actividades de implementación para cada uno de los componentes del marco. Asimismo, la guía no solo incluye las actividades de implementación del marco, sino también los roles y responsabilidades para cada proceso y plantillas de referencia en caso se necesiten para una actividad de implementación en particular. Es importante mencionar, que tanto las actividades de implementación como los roles y responsabilidades detallados en la guía pueden ser adaptados según la estructura y tamaño de la organización.

Capítulo 7. Aplicar la guía a un caso de estudio

7.1 Introducción

El presente capítulo abarca la elaboración del Objetivo Específico 4 (OE4). Dentro de este capítulo se realiza la selección de un caso de estudio acerca de una crisis real producida por un incidente de ciberseguridad. Posteriormente, se realiza un informe con la descripción detallada del caso. Asimismo, como parte del objetivo también se elabora un informe de aplicación del marco al caso de estudio elegido.

7.2 Resultados alcanzados (RE5 y RE6)

A continuación, se presenta el informe con la descripción detallada del caso de estudio elegido y el análisis comparativo entre la gestión de crisis real seguida en el caso versus la gestión de crisis aplicando el marco de trabajo elaborado. Es importante mencionar que para realizar el análisis comparativo se utilizaron siete aspectos relevantes de comparación (Estrategia, Riesgos, Respuesta y toma de decisiones, Coordinación de equipos de respuesta, Recuperación, Comunicación y Aprendizaje), los cuales se encuentran detallados en el informe del resultado obtenido.

En el **Anexo H** y **Anexo I** se muestran las actas de validación de los resultados esperados R5 y R6 respectivamente.

Descripción detallada del caso de estudio elegido

1. Introducción

El caso de estudio seleccionado se extrajo de la plataforma Harvard Business Publishing Education que se especializa en la creación y distribución de materiales de aprendizaje como casos de estudio, simulaciones, artículos y notas técnicas.

Es importante mencionar que este caso fue elegido en base a los siguientes criterios:

- Tema del caso: Dado que una crisis puede ser producida por diferentes causas. El caso elegido debe ser de una crisis real producida exclusivamente por un incidente de ciberseguridad. Cabe decir que no se considera un sector en específico, debido a que el marco elaborado puede ser aplicado a cualquier tipo de organización.
- Detalles proporcionados: El caso debe ofrecer detalles suficientes sobre el contexto de la organización en el momento de la crisis, la naturaleza del incidente y las medidas tomadas por la organización para gestionar la crisis.
- Fuente confiable: El caso debe estar basado en fuentes fiables, y bien documentadas para garantizar la precisión y credibilidad de la información presentada.

Título del caso: “The Phoenix Project: Remediation of a Cybersecurity Crisis at the University of Virginia”

Fecha de Publicación: 27 de septiembre de 2017

2. Contexto Inicial

El documento empieza con Virgina Evans, la Directora de Información (CIO) de la Universidad de Virginia (UVA), asistiendo a una reunión de la Junta de Visitantes (BOV). Durante esta reunión, recibe un mensaje urgente por parte de las autoridades federales que le informan sobre el descubrimiento de que posibles actores estatales tenían acceso a los sistemas de la UVA y sólo podían adivinar las intenciones de los ciberatacantes. Ante esta situación, durante una reunión a puerta cerrada el viernes 15 de junio de 2015, Evans informó a la BOV que los sistemas

de información de la UVA habian experimentado una “gran violación de seguridad”.

Para la época en que se desarrolló la crisis cibernética, las universidades se estaban convirtiendo rápidamente en el objetivo favorito de los ciberdelincuentes y actores estatales peligrosos, en gran parte debido a su apertura y naturaleza descentralizada. Es importante recalcar que las universidades podrían ser un objetivo principal porque a menudo tenían una importante propiedad intelectual de investigación y grandes reservas de Información de Identificación Personal (por sus siglas en inglés PII) e información financiera, incluida información de pago de estudiantes e información fiscal de empleados.

En el momento del ciberataque a la UVA, los tres métodos más comunes de ataques eran pear phishing, unpatched systems y zero-day exploits. Con respecto al método de ataque unpatched systems, había que recalcar que la oficina de Servicios de Tecnología de Información de la UVA (por sus siglas en inglés ITS) gestionaba varios cientos de servidores para una variedad de grupos de trabajo que ejecutaban una gran cantidad de aplicaciones y servicios. Además, había cientos de computadoras utilizadas por los empleados universitarios y cientos más de laboratorios de computación de estudiantes que necesitaban parches constantemente. Esto producía que el ITS tenga muy poco control sobre cómo y cuándo se actualizaban estos dispositivos con los últimos parches de seguridad. Entonces, la forma más común de mitigar estos tres ataques fue mediante un modelo de seguridad de TI llamado “defensa en profundidad”. En el caso de la UVA, se utilizó una conceptualización similar, donde la información más sensible era identificada y protegida por muchas capas de sistemas. A continuación se muestra las principales capas de defensa que estaban colocadas en la UVA en el momento del ataque:

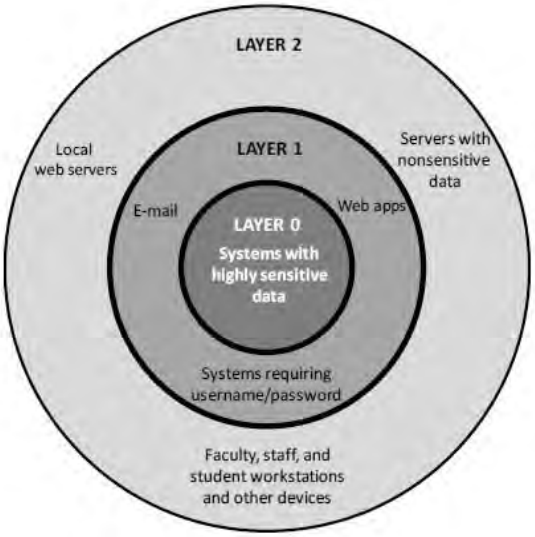


Figura 15: Capas de defensa de la UVA. Tomado de The Phoenix Project: Remediation of a Cybersecurity Crisis at the University of Virginia (2017)

El objetivo final del modelo de defensa en profundidad era reforzar el perímetro de la red manteniendo al mismo tiempo un núcleo seguro, que permitiera detectar el acceso no autorizado a los recursos y reaccionar a los incidentes de seguridad a medida que ocurrían. Sin embargo, en el caso de la UVA, el ciberataque había sido detectado por una agencia del gobierno federal que notificó de inmediato al director de seguridad de la información de la UVA, quien, a su vez, se puso en contacto con su jefe, Evans.

3. Respuesta a la crisis

3.1. Primeras acciones ante la crisis

La primera respuesta que tomó Evans a la crisis detectada, fue comunicarse con representantes de Mandiant, una firma de ciberseguridad reconocida internacionalmente. Para luego, firmar un contrato de remediación con ellos, que fue aprobado por la Oficina de Adquisiciones de la UVA en un tiempo récord. Los representantes de Mandiant llegaron con sus propios dispositivos de ciberseguridad que conectaron a los servidores de red de la UVA para monitorear la actividad y realizar el trabajo forense necesario. Mandiant descubrió rápidamente que dos atacantes no autorizados de China habían estado accediendo a los sistemas de la UVA, probablemente a través de dos sistemas sin parches. Además de Mandiant, se

aprovechó los servicios de Microsoft para centrarse en componentes de infraestructura específicos que debían monitorearse y remediarse rápidamente.

En segundo lugar, sobre la base de esta evaluación inicial, estaba claro que sería necesario un equipo de gestión de alto nivel para controlar la situación, especialmente teniendo en cuenta que las redes de la UVA incluían el Centro Médico de la UVA, una empresa de gestión de inversiones que gestionaba la dotación de 5.3 billones de dólares de la UVA, y una base de patentes. Con la ayuda de Pat Hogan (Vicepresidente ejecutivo y director de operaciones), Evans formó el equipo de respuesta llamado "Omaha", compuesto por dos miembros del BOV, un representante senior de comunicaciones, un asesor general de gestión de riesgos empresariales, el jefe de seguridad de la información (CISO), un asesor legal externo y la misma Evans (CIO). El equipo Omaha fue responsable de brindar supervisión ejecutiva para el esfuerzo de remediación de principio a fin.

Entonces bajo la dirección del equipo Omaha, de Mandiant y de Microsoft Services pasaron tres semanas evaluando el impacto de la infiltración para determinar el alcance del requisito de remediación. Descubrieron que 62 servidores habían sido comprometidos, algunos de los cuales contenían cantidades masivas de datos. En ese momento, Evans supo que el esfuerzo de remediación sería enorme y requeriría la atención de alguien con amplia experiencia en la gestión de grandes proyectos de TI.

3.2. Creación del plan de respuesta y remediación Phoenix

Ante el descubrimiento del alcance del ciberataque, se inició un proyecto encubierto llamado Phoenix con Dan German como directora principal del proyecto. Este se centraría en lo siguientes objetivos de alto nivel:

- Determinar el alcance de la intrusión. Aunque Mandiant había realizado una investigación preliminar de la intrusión durante las últimas semanas, era necesaria una evaluación más profunda para garantizar que todos tuvieran información completa.
- Desarrollar un plan de remediación. En los próximos días será necesario desarrollar un plan detallado para abordar las deficiencias del sistema, y

dado que la actividad final de remediación implicaría desactivar todos los sistemas UVA para permitir la implementación de un nuevo sistema de seguridad, una de las primeras decisiones sería programar una "fase de oscurecimiento".

- Ejecutar el plan de remediación. La ejecución implicó realizar todas las actividades necesarias hasta la fase de oscurecimiento, que incluyen:
    - Rastrear las actividades de los atacantes extranjeros y responder según sea necesario.
    - Desarrollar métodos de procedimiento para reconstruir y proteger aplicaciones y datos críticos en los sistemas comprometidos.
    - Identificar todas las estaciones de trabajo afectadas por la intrusión.
    - Evaluar el sistema de gestión de contraseñas de la UVA.
    - Prepararse para apoyar a los usuarios finales durante y después de la fase de oscurecimiento, y comunicarse con todos los grupos de interés internos y externos.
- Endurecer las defensas de la UVA, con la finalidad de bloquear nuevas actividades maliciosas.
- Restaurar servicios. Todos los sistemas tendrían que restaurarse y probarse hacia el final de la fase de oscuridad.

Es importante recalcar que para lograr estos objetivos, sería necesario un gran número de personal diverso. Entonces, los desafíos que implicaba identificar las habilidades necesarias, "tomar prestado" al personal de sus asignaciones y luego organizarlo en un equipo de alto funcionamiento eran casi demasiado para comprender.

3.3. Conformación de los equipos de respuesta necesarios para el plan Phoenix

Además del equipo de nivel ejecutivo Omaha; Evans y German iniciaron nueve equipos de soporte en la UVA y dos equipos de consultoría externos: uno de Microsoft Services y otro de Mandiant. Adicionalmente, la agencia que

originalmente detectó el ataque continuó involucrada en calidad de asesor. A continuación se muestra un organigrama de los equipos conformados:

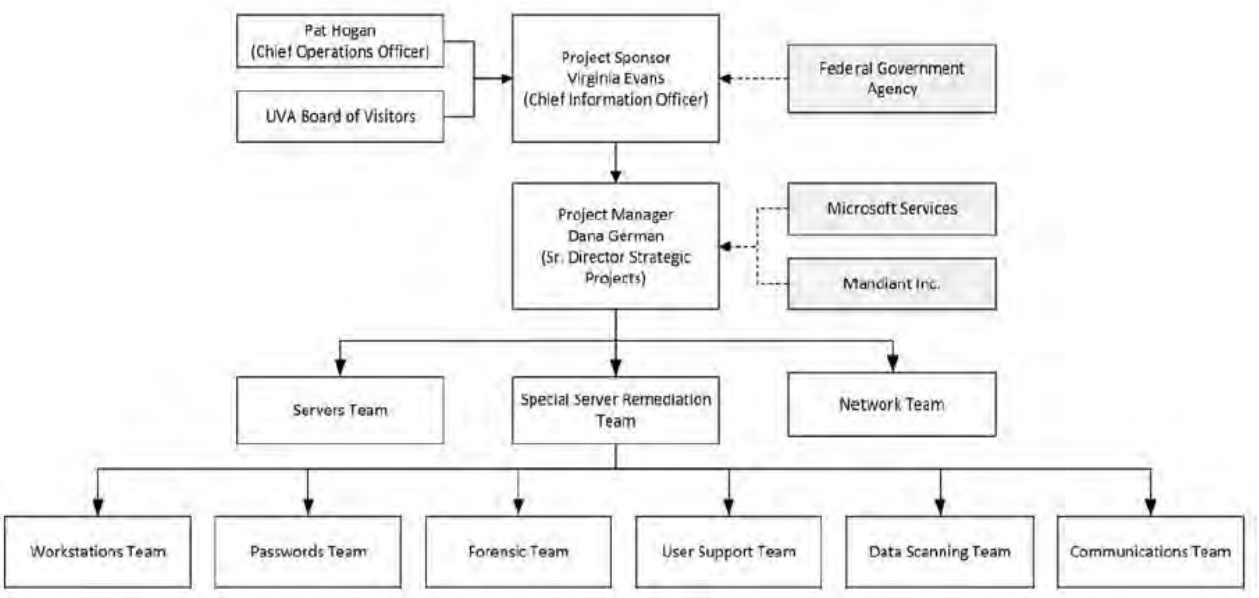


Figura 16: Organigrama de los equipos de respuesta. Tomado de The Phoenix Project: Remediation of a Cybersecurity Crisis at the University of Virginia (2017)

- Equipo de servidores: Responsable de confirmar qué servidores habían sido infiltrados por atacantes extranjeros e identificar todas las aplicaciones y datos críticos en los sistemas comprometidos.
- Equipo de Remediación de servidores especializados: Se centró en evaluar el efecto del ciberataque en los sistemas de correo electrónico de los profesores y personal de la UVA. Los miembros debían garantizar que los servidores comprometidos fueran identificados y reparados adecuadamente.
- Equipo de Red: Se encargó de analizar los segmentos de red en busca de posibles infracciones. Tenían que ayudar a monitorear la actividad de los atacantes, configurar entornos de red separados que pudieran usarse durante la remediación y garantizar que estuviera claro qué se apagaba o se mantenía durante el fin de semana de remediación.
- Equipo de Estaciones de Trabajo: Tuvo la tarea de ayudar con la investigación y reparación de las estaciones de trabajo afectadas por la

intrusión e implementar dispositivos de monitoreo en un subconjunto de estaciones de trabajo.

- Equipo de Contraseñas: Responsable de la gestión de contraseñas como parte de las actividades de remediación. El equipo necesitaba diseñar un plan para cambiar las contraseñas de las cuentas y hacerlas más seguras.
- Equipo Forense: Se centró en identificar intrusiones y rastrearlas hasta su origen. Tuvieron que evaluar a qué intentaban acceder las entidades extranjeras. Aprovechando los servicios de Mandiant, este equipo necesitaría monitorear la red continuamente durante todo el proyecto.
- Equipo de Soporte a Usuario: Se centró en brindar soporte a los usuarios finales después de que se implementaron cambios significativos en el frente de seguridad, por ejemplo, nuevos requisitos de contraseña. Se estimó que entre 40,000 y 50,000 personas necesitarían realizar los cambios necesarios inmediatamente después de su primer intento de inicio de sesión.
- Equipo de Escaneo de Datos: Era una combinación de personal de Mandiant y personal de ITS de UVA. El equipo era responsable de examinar cada servidor y estación de trabajo que habían sido comprometidos o potencialmente comprometidos para determinar qué datos había en la máquina y comprender si algún dato confidencial había sido expuesto.
- Equipo de Comunicaciones: Fue responsable de gestionar las comunicaciones del proyecto desde una perspectiva interna y externa. En el aspecto interno, el equipo necesitaba garantizar que se desarrollara y siguiera un plan de comunicaciones claro para dirigirse a todas las partes interesadas. Esto incluyó comunicaciones a los niveles más altos de la UVA (BOV, vicepresidentes y decanos), a todos los profesores, personal, estudiantes, jubilados y exalumnos. Las partes interesadas externas incluyeron al fiscal general, la oficina del gobernador, el público en general y la prensa (por ejemplo, el periódico local y las estaciones de televisión).
- Equipos externos: Se tuvieron dos equipos de consultoría externos.

    - El equipo de Servicios de Microsoft se centró en componentes de infraestructura específicos que debían monitorearse y reforzarse rápidamente.
    - El equipo de Mandiant brindó apoyo al equipo forense y al mismo tiempo ayudó a Evans y German a formular un plan de remediación.
- Agencia de Gobierno Federal: Tenía una función de asesoramiento para Evans.

Dada la gran cantidad de personas involucradas (176 personas en total), fue particularmente difícil mantener tanto la agilidad como el secreto. Cada nuevo miembro del equipo tenía que prestar juramento de guardar secreto antes de ser informado sobre el proyecto. Además, para evitar que otros atacantes supieran que se había detectado una infracción, toda la comunicación se realizó fuera de los sistemas de UVA, utilizando Google Gmail y Google Docs. Cabe decir que aunque todos los líderes del equipo tenían un alto nivel de experiencia y estaban dispuestos a cooperar, pronto se hizo evidente que había distintos grados de compromiso y cooperación. En esos casos especiales, Evans actuó rápidamente para realizar los ajustes de personal necesarios.

Adicionalmente a lo anterior, se recalcó la necesidad de que los líderes de equipo tendrían que operar a partir de un plan y un cronograma bien orquestados, pero con la agilidad necesaria para responder rápidamente a medida que surgiera nueva información.

3.4. Ejecución del plan Phoenix

Como parte del proceso de remediación, todos los involucrados consideraron necesario que la UVA tuviera que apagar su conexión a Internet (“fase de oscuridad”), durante potencialmente varios días para permitir que los servidores reconstruidos se pusieran en línea, eliminar cualquier cuenta comprometida, evitar que los atacantes se trasladen a otros sistemas y reforzar cada una de las capas de la red para evitar daños mayores. Todo lo mencionado anteriormente, tendría un impacto significativo en muchas partes interesadas.

Finalmente, Evans y German establecieron la fase de oscuridad para el fin de semana del 14 al 16 de agosto. Es importante recalcar que los esfuerzos de remediación debían concluir antes del inicio del semestre de otoño, dado que la alternativa de esperar hasta después del inicio del semestre significaba aumentar la probabilidad de que los atacantes o la duración de la remediación cuando la escuela estaba en pleno funcionamiento, dañaran a la UVA. Entonces, durante ese fin de semana, todos los sistemas serían desactivados, reconstruidos, reactivados y probados. Dependiendo de cómo fuera ese proceso, la comunicación adecuada se enviaría a todas las partes interesadas internas y externas.

Análisis comparativo

1. Introducción

El documento presenta el análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado.

2. Análisis comparativo

Para desarrollar el análisis comparativo se utilizó un cuadro de doble entrada, donde se colocaron una serie de aspectos a evaluar. Cabe decir que estos aspectos se definieron en base a los principios de gestión de crisis establecidos en la norma ISO 22361. La descripción de cada uno de los aspectos a evaluar se detalla a continuación:

- Estrategia: Enfoque general y el plan de acción que se utiliza para abordar la crisis, en otras palabras, se trata de cómo la organización se organiza y establece su dirección en respuesta a una crisis.
- Riesgos: Se trata de identificar, evaluar y tratar los riesgos de ciberseguridad potenciales que pueden desencadenar una crisis.
- Respuesta y toma de decisiones: Acciones tomadas por la organización en respuesta a una crisis. Esto incluye cómo se abordan los problemas, la velocidad de respuesta y de qué manera se toman las decisiones durante la crisis.
- Coordinación de equipos de respuesta: Se refiere a la gestión que realiza la organización para definir, monitorear y supervisar los roles y responsabilidades asignados a los miembros de la organización.
- Recuperación: Acciones tomadas para restaurar la normalidad. Esto incluye la restauración de los servicios de TI y la implementación de medidas para prevenir futuras crisis similares.
- Comunicación: Se refiere a la comunicación interna y externa durante la crisis. Incluye la difusión de información rápida y efectiva, tanto a las partes interesadas internas como externas, de las acciones tomadas e información relevante para gestionar la crisis.
- Aprendizaje: Se refiere a la capacidad de una organización para analizar la gestión de crisis pasadas, identificar lecciones aprendidas y aplicar ese conocimiento para mejorar la preparación y respuesta a futuras crisis. Esto incluye tener debidamente capacitados y entrenados a todos los miembros encargados de hacer frente a la crisis en base a los conocimientos adquiridos.

A continuación se muestra el análisis comparativo realizado en la Tabla 53:

Tabla 53: Análisis comparativo usando el caso de estudio elegido

Aspecto	Gestión de crisis real	Aplicando el marco de trabajo	Conclusión
Estrategia	La UVA no contaba con una planificación previa que le hubiera permitido responder rápidamente a la crisis. La planificación del plan de respuesta y remediación se elaboró durante la misma crisis, después de descubrir el alcance de la intrusión y de realizar coordinaciones para formar un equipo de gestión de crisis y establecer los objetivos del plan.	El marco de trabajo propone dentro de sus componentes la elaboración de tres planes principales que permitan a la organización estar preparada para responder y recuperarse lo más rápido posible ante una crisis producida por un incidente de ciberseguridad. Entonces, aplicando el marco de trabajo, la UVA contaría con un plan de gestión de incidentes de ciberseguridad que le hubiera permitido minimizar el impacto negativo de las incidencias, atacando de manera rápida y estructurada el incidente. Por otro lado, tendría elaborado un plan de continuidad de TI que le hubiera garantizado la continuidad de los servicios de TI en tiempos y costos aceptados por la organización, de tal forma que hubiera minimizado los tiempos de interrupción. Finalmente, con el plan de gestión de crisis ya elaborado, la UVA podría haber respondido rápidamente a la crisis sin necesidad de haber esperado a realizar coordinaciones para la creación del plan de respuesta y remediación a la crisis.	En general si se hubiera aplicado el marco de trabajo la UVA podría haber respondido a la crisis en una menor cantidad de tiempo, pues ya contaría con planes elaborados que detallen qué acciones se deben tomar.

Riesgos	La UVA contaba con un modelo de seguridad de TI llamado “defensa en profundidad”, donde la información más sensible era identificada y protegida por muchas capas de sistemas. Esto con la finalidad de tratar los riesgos de los tres ciberataques más comunes de la época, los cuales eran “pear phishing”, “unpatched systems” y “zero-day exploits”. Asimismo, es importante mencionar que en el caso de la UVA, el ciberataque fue detectado por una agencia del gobierno federal.	Aplicando el marco la UVA hubiera podido gestionar los riesgos tanto de los ataques más comunes de la época como otros riesgos relacionados a la ciberseguridad. Para ello, la UVA hubiera tenido que seguir una serie de actividades que propone el marco para implementar la gestión de riesgos que van desde la identificación y evaluación de los riesgos hasta el tratamiento de los mismos estableciendo los controles respectivos.	En general si se hubiera aplicado el marco de trabajo la UVA podría haber gestionado los riesgos de los tres ciberataques más comunes de la época, así como también otros riesgos que pudieron haber afectado a la organización.
Respuesta y toma de decisiones	La primera acción que tomó la UVA fue comunicarse con una empresa de ciberseguridad externa para firmar un contrato de remediación con ellos. Esta colaboración externa que recibió la UVA sirvió para identificar rápidamente quiénes y cómo produjeron el incidente de ciberseguridad. Posteriormente a ello, se estableció un equipo de gestión de crisis llamado “Omaha”, cuya finalidad era la de brindar supervisión ejecutiva para el esfuerzo de remediación de principio a fin. Finalmente, luego de descubrir el alcance de la instrusión (donde se identificaron que 62 servidores habían sido comprometidos), se inició un proyecto encubierto llamado Phoenix. Este se centraría en los siguientes objetivos de alto nivel: Determinar el alcance de la intrusión, Desarrollar un plan de remediación, Ejecutar el plan de remediación, Endurecer las defensas de la UVA y Restaurar los servicios.	Con el uso del marco de trabajo se tendría un componente exclusivo de gestión a crisis, mediante el cual, el UVA hubiera podido gestionar la crisis de manera completa, rápida y estructurada; pues ya se contaría de antemano con una serie de planes de respuesta y recuperación. Entonces, con el uso del componente de respuesta a crisis la UVA hubiera podido evaluar la situación en tiempo real y a la vez tomar decisiones rápidas. Asimismo, hubiera sido más efectiva la coordinación de las acciones de respuesta a la crisis, porque estas se realizarían de acuerdo con los planes ya establecidos (plan de gestión de crisis, de continuidad de TI, de incidentes de ciberseguridad y de comunicaciones). Es importante mencionar que para cada plan establecido se tendría un equipo de respuesta ya conformado con sus respectivos roles y responsabilidades.	En general, como se mencionó anteriormente con el uso del marco, ya se hubiera tenido una estrategia de respuesta previa que hubiera permitido a la UVA responder rápidamente a la crisis según los planes de respuesta ya establecidos, con los cuales se hubiera gestionado el incidente que produjo la crisis y garantizado la continuidad de los servicios de TI en tiempos y costos aceptados por la organización.

Coordinación de equipos de respuesta	Además del equipo de gestión de crisis llamado "Omaha", se conformaron nueve equipos de soporte en la UVA y dos equipos de consultoría externos. Cabe mencionar que los equipos de soporte estaban más enfocados en la resolución del incidente de ciberseguridad y en la remediación de los daños causados a los servicios de TI. Es importante mencionar que dada la gran cantidad de personas involucradas (176 personas en total), para la UVA fue particularmente difícil identificar las habilidades necesarias, "tomar prestado" al personal de sus asignaciones y luego organizarlos en equipos. Esto también produjo que fuera muy difícil mantener tanto la agilidad como el secreto.	Dentro del marco se propone un componente de gestión de equipos de respuesta que permite definir, monitorear y supervisar los roles y responsabilidades específicamente asignados a los miembros de la organización. Entonces, aplicando el marco de trabajo, la UVA contaría con un proceso ya establecido que le hubiera permitido gestionar de una forma mucho más efectiva a los equipos de respuesta, garantizando el correcto funcionamiento de sus responsabilidades, pues este componente hace énfasis en las actividades que permiten identificar, y asignar los roles y responsabilidades al personal debidamente capacitado a cada proceso (de gestión de incidentes de ciberseguridad, de continuidad de TI, de gestión de crisis y de comunicaciones).	En general, con el uso del marco se hubiera gestionado de una forma más rápida y efectiva a los equipos de respuesta necesarios para enfrentar la crisis, evitando así los impactos negativos y dificultades de conformar desde cero a los equipos de respuesta en plena crisis.
Recuperación	Como parte del proceso de recuperación, todos los involucrados en el proyecto Phoenix, consideraron necesario que la UVA tuviera que apagar su conexión a internet ("fase de oscuridad"), durante potencialmente varios días para permitir que los servidores reconstruidos se pusieran en línea, eliminar cualquier cuenta comprometida, evitar que los atacantes se trasladen a otros sistemas y reforzar cada una de las capas de la red para evitar daños mayores. Todo lo mencionado anteriormente, tendría un impacto significativo en muchas partes interesadas de la UVA.	Dentro del marco se propone un componente de gestión de la continuidad de TI que abarca la definición e implementación de estrategias y procedimientos de continuidad que permitan a la organización responder y recuperarse rápidamente de eventos que puedan afectar a los servicios de TI. Entonces, aplicando el marco de trabajo, la UVA contaría de antemano con un plan de continuidad de TI, que le hubiera garantizado la continuidad de los servicios de TI en tiempos y costos aceptados por la organización, de tal manera que se hubieran minimizado las interrupciones en la UVA, y por tanto se hubiera reducido el impacto negativo en las partes interesadas. Es importante mencionar que dentro del plan, la UVA hubiera tenido una serie de estrategias de contingencia para cada uno de los sistemas afectados debido al ciberataque.	En general con la aplicación del marco, la UVA hubiera podido establecer un proceso de recuperación alineado a los tiempos y costos aceptados por la organización, evitando de esa manera generar un impacto negativo en muchas partes interesadas de la universidad.

Comunicación	Dentro del plan de remediación a crisis se conformó un equipo de comunicaciones, el cual fue responsable de gestionar las comunicaciones del proyecto Phoenix (proyecto de remediación de la crisis) desde una perspectiva interna y externa. En el aspecto interno, el equipo necesitaba garantizar que se desarrollara y siguiera un plan de comunicaciones claro para dirigirse a todas las partes interesadas. Esto incluyó comunicaciones a los niveles más altos de la UVA (BOV, vicepresidentes y decanos), a todos los profesores, personal, estudiantes, jubilados y exalumnos. Las partes interesadas externas incluyeron al fiscal general, la oficina del gobernador, el público en general y la prensa.	Aplicando el marco la UVA hubiera podido asegurar una comunicación rápida y efectiva, tanto a las partes interesadas internas como externas, de las acciones tomadas e información relevante para gestionar la crisis. Para ello, la UVA hubiera tenido que seguir una serie de actividades que le hubieran permitido implementar el componente de gestión de comunicaciones en crisis. Estas actividades van desde el establecimiento de un plan de comunicaciones hasta el establecimiento de una comunicación activa durante la crisis.	En general con la aplicación del marco, la UVA hubiera podido establecer una comunicación activa a todas las partes interesadas. Específicamente, se hubiera comunicado a las partes internas los procedimientos a seguir y las medidas tomadas. Y por otro lado, a las partes externas se hubiera comunicado la información relevante y actualizada de lo que se está haciendo para gestionar la crisis.
Aprendizaje	Durante la gestión de crisis no se realizaron actividades de capacitación ni se aseguró que el personal que conformó los equipos de respuesta estuvieran totalmente calificados para el rol asignado. Es por ello, que en algunos casos había que realizar ajustes de personal. Por otro lado, se recalcó la necesidad de que los líderes de equipo tendrían que operar a partir de un plan y un cronograma bien orquestados, pero con la agilidad necesaria para responder rápidamente a medida que surgieran nuevos conocimientos.	Dentro del marco de trabajo se cuenta con dos componentes que permiten gestionar a los equipos de respuesta y el conocimiento. Entonces, aplicando el marco de trabajo la UVA hubiera podido mantener a su personal capacitado de acuerdo a su rol asignado y supervisar el desempeño de los mismos, de tal forma que se hubiera evitado casos de reajustes de personal. Todo ello como parte de la implementación que hubiera realizado del componente de gestión de equipos de respuesta. Por otro lado, contaría con un proceso de manejo del conocimiento que le hubiera permitido mantener el uso efectivo, eficiente y conveniente del conocimiento generado al interior de la universidad, de tal manera que las partes interesadas responsables de la gestión de la crisis, hubieran obtenido la información correcta, en el formato adecuado y en el momento correcto, de acuerdo a su nivel de acceso.	En general con la aplicación del marco, la UVA hubiera podido asegurar que el personal que conformaba a los equipos de respuesta hubiera estado debidamente capacitado para cumplir con sus responsabilidades de acuerdo a su rol. Por otra parte, todo el conocimiento que hubieran adquirido durante la gestión de la crisis hubiera estado correctamente organizado y almacenado para que esté disponible a todas las partes interesadas que lo necesiten, en el formato y tiempo adecuado.

Fuente: Elaboración Propia

7.3 Discusión

En esta sección se presentó la descripción detallada del caso de estudio seleccionado sobre una crisis real producida por un incidente de ciberseguridad. Asimismo, se realizó el análisis comparativo entre la gestión de crisis real seguida en el caso versus la gestión de crisis aplicando el marco de trabajo elaborado. Es importante mencionar que los resultados obtenidos del análisis resultan muy importantes, ya que sirven como un medio para comprobar la efectividad del marco frente a una crisis real. Cabe decir que para cada uno de los aspectos evaluados se obtuvo una conclusión donde se evidenció, en general, que si la organización hubiera seguido el marco de trabajo, habría podido responder de forma más rápida y efectiva a la crisis.

Capítulo 8. Conclusiones y trabajos futuros

8.1 Introducción

En este capítulo se presentarán las conclusiones obtenidas para cada uno de los objetivos específicos del proyecto de fin de carrera. Asimismo, se detallarán los trabajos futuros que se pueden realizar sobre el proyecto elaborado.

8.2 Conclusiones

En primer lugar, con respecto al objetivo específico 1, se puede concluir que no existen marcos de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en buenas prácticas internacionales. Lo cual resulta importante abordar, porque en la actualidad sin una estrategia de respuesta clara para aliviar una crisis producida por un incidente de ciberseguridad, se sufre el riesgo de que la organización tarde más en recuperarse y esto finalmente intensifica cualquier daño causado. Es por ello, que el marco elaborado reúne un conjunto de buenas prácticas que permita a las empresas responder de manera completa y oportuna a las crisis producidas por incidentes de ciberseguridad, lo que incluye la gestión de los incidentes de ciberseguridad, de los equipos de respuesta, de la continuidad de TI y de la crisis producida.

En segundo lugar, con respecto al objetivo específico 2, se puede concluir que ha sido posible identificar 3 dominios que permiten gestionar las crisis e incidentes de ciberseguridad de manera completa y efectiva. Cada dominio abarca un conjunto de procesos, los cuales tienen un propósito en particular y han sido desarrollados a partir de requisitos de cumplimiento, marcos y estándares internacionalmente aceptados.

Por otro lado, con respecto al objetivo específico 3, se puede concluir que la guía de implementación elaborada cubre las actividades de implementación del marco, así como los roles y responsabilidades para cada proceso. Cabe decir que tanto las actividades de implementación como los roles y responsabilidades detallados en la guía pueden ser adaptados según la estructura y tamaño de la organización.

Finalmente, con respecto al objetivo específico 4, se puede concluir a partir del análisis comparativo, entre la gestión de crisis real seguida en el caso de estudio versus la gestión

aplicando el marco elaborado, que el marco resulta efectivo para hacer frente a una crisis real producida por un incidente de ciberseguridad. Asimismo, es importante mencionar que para cada uno de los aspectos evaluados se obtuvo como conclusión, en general, que si la organización hubiera seguido el marco de trabajo, habría podido responder de forma más rápida y efectiva a la crisis de ciberseguridad.

8.3 Trabajos futuros

Como parte de trabajos futuros a realizarse para este marco de trabajo, se tiene lo siguiente:

- Probar el marco de trabajo en una organización real, con la finalidad de verificar completamente su efectividad y encontrar oportunidades de mejoras que pudieran incluirse dentro del marco.
- Implementar una herramienta o software que permita gestionar de manera conjunta los componentes del marco.
- Profundizar en algún componente en particular del marco, como es la gestión de la continuidad de los servicios de TI, o la gestión de incidentes en general, de tal forma que el marco ofrezca un mayor alcance.

Referencias

Guirao Goris, Silamani J. Adolf. (2015). Utilidad y tipos de revisión de literatura. Ene, 9(2) https://dx.doi.org/10.4321/S1988-348X2015000200002

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele University,UK and National ICT Australia.

Elsevier B.V. (n.d.). Scopus. https://www.scopus.com/

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). IEEE Xplore Digital Library. https://ieeexplore.ieee.org/

Springer Nature. (n.d.). Home - Springer. https://www.springer.com/

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Aljaryan, L. K., Alfalahi, W. H., & Khamis, T. S. Al. (2022). Cyberattacks and Solutions for Future Factories. *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, 1–7. https://doi.org/10.1109/CICN56167.2022.10008258

B. S. Dykstra, J. A., & Orr, S. R. (2016). Acting in the unknown: the cynefin framework for managing cybersecurity risk in dynamic decision making. *2016 International Conference on Cyber Conflict (CyCon U.S.)*, 1–6. https://doi.org/10.1109/CYCONUS.2016.7836616

Flavin, A., O'Toole, E., Murphy, L., Ryan, R., McClean, B., Faul, C., McGibney, C., Coyne, S., O'Boyle, G., Small, C., Sims, C., Kearney, M., Coffey, M., & O'Donovan, A. (2022). A National Cyberattack Affecting Radiation Therapy: The Irish Experience. *Advances in Radiation Oncology*, *7*(5), 100914. https://doi.org/10.1016/j.adro.2022.100914

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036

Kuipers, S., & Schonheit, M. (2022). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. *Corporate Reputation Review*, *25*(3), 176–197. https://doi.org/10.1057/s41299-021-00121-9

Schauer, S., Kalogeraki, E.-M., Papastergiou, S., & Douligeris, C. (2019). Detecting Sophisticated Attacks in Maritime Environments using Hybrid Situational Awareness. *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 1–7. https://doi.org/10.1109/ICT-DM47966.2019.9032900

Stowman, A. M., Frisch, N., Gibson, P. C., John, T. S., Cacciatore, L. S., Cortright, V., Schwartz, M., Anderson, S. R., & Kalof, A. N. (2022). Anatomy of a Cyberattack: Part 1: Managing an Anatomic Pathology Laboratory During 25 Days of Downtime. *American Journal of Clinical Pathology*, *157*(4), 510–517. https://doi.org/10.1093/ajcp/aqab145

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience—Cybersecurity Response to COVID-19. *IT Professional*, *22*(3), 4–10. https://doi.org/10.1109/MITP.2020.2988330

Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation*, *17*(3), 3–13. https://doi.org/10.15407/scine17.03.003

Zdzikot, T. (2022). Cyberspace and Cybersecurity. In *Cybersecurity in Poland* (pp. 9–21). Springer International Publishing. https://doi.org/10.1007/978-3-030-78551-2_2

Ribaux, O., & Souvignet, T. R. (2020). "Hello are you available?" Dealing with online frauds and the role of forensic science. *Forensic Science International: Digital Investigation*, *33*, 300978. https://doi.org/10.1016/j.fsidi.2020.300978

AXELOS Limited. (2019). ITIL 4: Managing Professional. The Stationery Office.

International Organization for Standardization. (2019). Societal security - Business continuity management systems - Requirements (ISO 22301:2019). ISO.

International Organization for Standardization. (2021). Security and resilience - Crisis management - Guidelines for a strategic capability (ISO 22361:2021). ISO.

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. Journal of Cybersecurity, 2, 15-28.

National Institute of Standards and Technology. (2015). Framework for improving critical infrastructure cybersecurity (NISTIR 8074). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

Allianz. (2019). Allianz Risk Barometer Top Business Risks For 2019. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf

FIRST. (2020). FIRST Annual Threat Intelligence Report 2020. https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf

National Institute of Standards and Technology (NIST). (2012). Computer Security Handling Guide.

ENISA. (2020). How to Setup CSIRT and SOC.

Hevner, A. R., & Chatterjee, S. (2010). Metodología de ciencia del diseño.

Nelson, R., & Wright, R. (2017). The Phoenix Project: Remediation of a Cybersecurity Crisis at the University of Virginia. University of Virginia McIntire School of Commerce Foundation.

International Organization for Standardization. (2022). ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO/IEC.

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0. U.S. Department of Commerce.

ISACA. (2013). COBIT 5 for Risk. ISACA.

National Institute of Standards and Technology. (2010). NIST 800-34 - Contingency Planning Guide for Federal Information Systems. U.S. Department of Commerce.

National Institute of Standards and Technology. (2012). NIST 800-61 - Computer Security Incident Handling Guide. U.S. Department of Commerce.

International Organization for Standardization. (2018). ISO/IEC 20000-1:2018 - Information technology - Service management - Part 1: Service management system requirements. ISO/IEC.

Anexos

Anexo A: Formulario de extracción

El formulario de extracción de datos completo se encuentra en el siguiente archivo excel llamado “Formulario de Extracción.xlsx”. Enlace:

https://docs.google.com/spreadsheets/d/1NNVR2h7IcsUapB7rk3IOFAzHYEPb2yNj/edit?usp=sharing&ouid=106208104366554105467&rtpof=true&sd=true

Anexo B: Plan de Proyecto

- **Justificación**

Como se ha podido observar en el Capítulo 1, relacionado a la problemática descrita para este proyecto, en la actualidad y sobre todo a raíz de la pandemia de COVID-19, las organizaciones se han visto afectadas por un constante aumento de incidentes de ciberseguridad. En (Yerina et al, 2021) se menciona que año tras año, los delitos cibernéticos son cada vez más organizados, técnicamente avanzados y hasta psicológicamente elegantes, generando consecuencias cada vez más destructivas en las empresas. De acuerdo con la Allianz Risk Barometer, las pérdidas globales por delitos cibernéticos alcanzan los 600,000 millones de USD por año, lo que es casi tres veces la pérdida anual promedio por desastres naturales (Allianz., 2019).

A partir de la revisión de la literatura, se ha podido identificar que los incidentes mal gestionados pueden desencadenar una crisis dentro de la organización con un mayor impacto al negocio. Adicionalmente, el no contar con un plan de respuesta definido para mitigar un incidente de ciberseguridad, produce el riesgo de que la organización experimente una recuperación más lenta, lo que intensifica cualquier daño causado generando en una crisis dentro de la organización. (Aljaryan et al., 2022).

Entonces, en relación a lo mencionado anteriormente, sin un correcto uso de procedimientos de gestión de crisis, la organización responde con una intervención inadecuada o incluso no brinda ninguna respuesta a la crisis en alguno de los tres puntos principales de la gestión de crisis definidos en (Weil & Murugesan, 2020): detección de la causa, estrategia de respuesta y comunicación durante la crisis. Este último punto resulta muy crítico para las organizaciones, porque sin una adecuada gestión de las comunicaciones durante las crisis se puede producir una afectación negativa en la reputación e imagen de la organización por falta de transparencia hacia las partes interesadas (clientes, proveedores, entre otros). Asimismo, una mala gestión de comunicaciones no permite identificar correctamente al equipo de respuesta y mucho

menos permite la correcta distribución de responsabilidades, produciendo una respuesta nula o tardía a la crisis.

Por tales motivos, el presente proyecto de fin de carrera tiene como finalidad diseñar un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361.

- **Viabilidad**

Viabilidad Temporal

El presente trabajo de fin de carrera tendrá una extensión equivalente a 8 meses, a partir de finales de marzo del 2023 hasta principios de noviembre del mismo año. Lo que se puede observar en el Cronograma del Proyecto donde se evidencia que es factible culminar y a su vez verificar el proyecto (mediante una prueba de papel o teórica) cumpliendo los plazos establecidos.

Viabilidad Técnica

Para la realización del presente proyecto, se cuenta con acceso y conocimiento a todas las herramientas y buenas prácticas seleccionadas:

- ISO 22361
- NIST - Computer Security Handling Guide
- ITIL v4
- ENISA
- Matriz RACI
- Bizagi
- Análisis comparativo
- Harvard Business Publishing Education
- The Case Center

Asimismo, las herramientas mencionadas son de aprendizaje rápido y de poca complejidad. Cabe decir que tanto el asesor como la co-asesora de este proyecto de tesis

son expertos en el área de gestión de incidentes y crisis. Por lo tanto, este proyecto es técnicamente viable.

Viabilidad Económica

En el presente proyecto no se han identificado costos significativos. Sin embargo, si se requiere usar un caso de estudio del repositorio de Harvard Business Publishing Education o The Case Centre (que no sea gratuito) se tendrá que realizar un pago de un costo poco significativo. Entonces, en base a lo mencionado anteriormente se concluye que el proyecto es viable económicamente.

- **Alcance**

El presente proyecto de fin de carrera va a seguir una serie de procesos que permitirán diseñar un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad. Este marco abarcará los siguientes dominios: organizacional, operacional y de recuperación a crisis.

Entonces, el presente proyecto que pertenece al área de Tecnologías de Información tiene como objetivo el diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361, el cual constará de los siguientes resultados:

En primer lugar, se definirá la vista de componentes del marco a alto nivel. Posteriormente, se realizará la validación del resultado obtenido con un experto en ciberseguridad o gestión de crisis.

En segundo lugar, se realizará el desarrollo de los procesos que conforman los componentes del marco. Este desarrollo implica la elaboración de los modelos de procesos, actividades y métricas de cada uno de los componentes, así como la lista de roles y responsabilidades por proceso. Para ambos casos, se realizará una validación completa por un experto en ciberseguridad, equipos de respuesta a incidentes o gestión de crisis.

En tercer lugar, se realizará la guía de implementación del marco, para este caso la validación del resultado la realizará un experto en seguridad, ciberseguridad o gestión de crisis.

Finalmente, se realizará la selección de un caso de estudio (extraído de la literatura) que contenga un ejemplo de crisis cibernética. Este caso de estudio será usado posteriormente para realizar el informe de aplicación del marco al caso de estudio. Para ello, se efectuará un análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado. Es importante mencionar que la validación del caso de estudio elegido y del análisis desarrollado será realizada por un especialista en seguridad, ciberseguridad, gestión de continuidad o crisis.

- **Limitaciones**

El presente proyecto se encuentra limitado en los siguientes dos aspectos:

- No se va a definir un nuevo procedimiento de gestión de incidentes ni de gestión de crisis, sino que se realizará una adaptación de las normas y buenas prácticas internacionales ya existentes, usando principalmente la norma ISO 22361.
- Este proyecto de fin de carrera no incluirá el desarrollo de algún tipo de herramienta de software que permita gestionar alguno de los componentes establecidos en el marco.

- **Identificación de los riesgos del proyecto**

En la siguiente tabla 54, se muestran los riesgos identificados del proyecto. Asimismo, se coloca su descripción, probabilidad de ocurrencia (P), impacto que pueda ocasionar en caso ocurriese (I), severidad (S), controles de mitigación y medidas de contingencias para cada uno de ellos.

Tabla 54: Riesgos del proyecto

Riesgo	Descripción del riesgo	Síntomas	P	I	S	Mitigación	Contingencia
Problemas de salud personal o familiar.	Dificultad para avanzar con el desarrollo del proyecto y cumplir con las actividades según lo planteado en el cronograma.	El tesista o un familiar cercano se enferma.	3	4	12	Tomar las medidas de salud necesarias para reducir el riesgo de contraer enfermedades.	Reprogramar las actividades afectadas. En caso de ser muy grave, posponer el desarrollo del proyecto y solicitar el retiro del curso.
Deterioro de los equipos de trabajo	Mal funcionamiento de los equipos de trabajo utilizados para desarrollar el proyecto.	El equipo de trabajo presenta cualquier tipo de falla.	2	3	6	Contar con equipos de respaldo.	Usar el equipo de respaldo o usar los de la universidad.
Pérdida de los avances desarrollados	Pérdida o daño de los avances realizados del proyecto.	Errores de guardado o sobreescritura de archivos.	2	4	8	Contar con respaldo de los avances en la nube	Usar los respaldos guardados en la nube para restaurar los avances.
Los expertos que se comprometieron a contribuir en la validación de los resultados no cuentan con disponibilidad.	Los expertos no realizan la validación de los resultados dentro de los tiempos establecidos.	El experto comunica al tesista que no podrá tener lista la validación de los resultados en el tiempo previsto.	4	4	16	Coordinar de manera anticipada la disponibilidad de los expertos.	Solicitar al experto su mayor disponibilidad posible o cambiar de experto. Adicionalmente, solicitar mayor tiempo para el cumplimiento de la entrega de las validaciones requeridas.
No se cuenta con disponibilidad de un caso de estudio para realizar	No se logra obtener un caso de estudio adecuado que permita realizar la validación del	No se logra obtener un caso de estudio válido dentro del plazo	3	4	12	Realizar una búsqueda de casos adecuados con una considerable	Solicitar mayor tiempo para el cumplimiento de la entrega del resultado. Asimismo,

la validación del protocolo desarrollado	protocolo de comunicación en crisis cibernética desarrollado. Es importante recalcar que el protocolo no se puede probar en una empresa que esté sufriendo una crisis en tiempo real, porque ninguna probaría un protocolo recién desarrollado durante una crisis real.	establecido.				anticipación.	solicitar ayuda al asesor para la búsqueda del caso.
Actualización de las herramientas utilizadas (normas, buenas prácticas, modelos)	Algunas de las herramientas utilizadas pueden sufrir cambios durante el desarrollo del proyecto.	Lanzamiento de alguna nueva versión o actualización de una herramienta utilizada.	1	3	3	Estar alertas de cuando se podrían dar actualizaciones de las herramientas a utilizar.	Reprogramar las actividades afectadas para realizar los cambios de acuerdo a la nueva versión de la herramienta.

Fuente: Elaboración Propia

Donde:

- **P: Probabilidad, la cual tiene la siguiente escala:**

  1: Muy improbable

  2: Improbable

  3: Moderado

  4: Probable

  5: Muy Probable

- **I: Impacto, la cual tiene la siguiente escala:**

  1: Muy poco crítico

2: Poco crítico

3: Moderadamente critico

4: Crítico

5: Muy crítico

- **S: Severidad, la cual se calcula con la siguiente fórmula: S = P*I**

- **Estructura de descomposición del trabajo (EDT)**

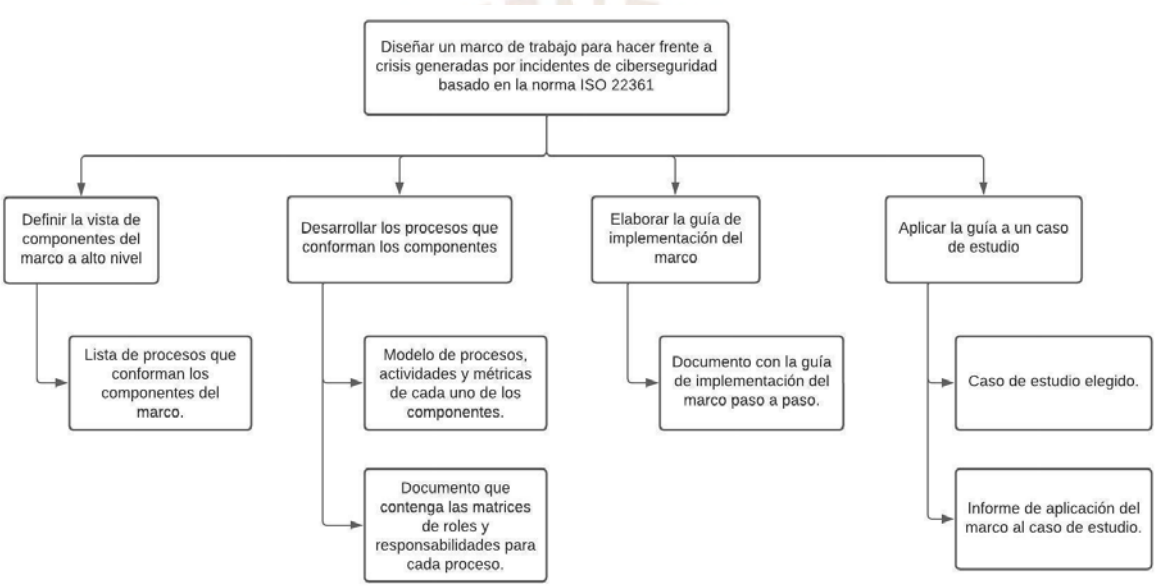


Figura 17: Estructura de Descomposición de Trabajo. Fuente: Elaboración Propia

- **Lista de tareas**

Tabla 55: Lista de tareas

Tarea	Duración Estimada (días)	Esfuerzo Asociado (horas-persona)	Costo estimado
Entregable 1.1			
Elaboración de Ficha de registro de idea de tesis y asesor.	1	5	200
Reunión con asesores.	1	1	40
Revisión de los asesores.	1	1	0
Entregable 1.2			
Elaboración del protocolo de revisión y diseño de formulario de extracción.	5	15	600
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	1	40
Revisión de los asesores.	1	1	0
Entregable 1.3			
Elaboración del reporte de ejecución de la revisión.	5	25	1000
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0
Entregable 1.4			
Elaboración del reporte de ejecución de la revisión y formulario de extracción completo.	6	30	1200
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0

Entregable 1.5			
Elaboración del marco conceptual.	5	15	600
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0
Entregable 1			
Definición de la problemática.	5	15	600
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0
Entregable 2.1			
Elaboración del árbol de objetivos.	4	8	320
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0
Entregable 2			
Definición de métodos y procedimientos.	4	15	600
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0
Entregable 3			
Definición parcial del Plan del Proyecto	3	12	480
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0

Entregable 4			
Definición del Plan del Proyecto completa.	3	12	480
Reunión con asesores.	1	1	40
Realizar correcciones del entregable anterior.	1	2	80
Revisión de los asesores.	1	1	0
Objetivo 1: Definir la vista de componentes del marco a alto nivel.			
R1. Lista de procesos que conforman los componentes del marco.			
Elaboración del informe con la hoja de ruta de creación de los componentes del marco a alto nivel.	5	18	720
Reunión con los asesores.	1	1	40
Validación al 100% de la lista de componentes a alto nivel del marco por experto en ciberseguridad o gestión de crisis.	1	2	600
Objetivo 2: Desarrollar los procesos que conforman los componentes.			
R2. Modelo de procesos, actividades y métricas de cada uno de los componentes.			
Elaboración del modelo de procesos, actividades y métricas de cada uno de los componentes.	5	18	720
Reunión con los asesores.	1	1	40
Validación al 100% del informe con la documentación completa por especialista en ciberseguridad o gestión de crisis.	1	2	600
R3. Lista de roles y responsabilidades por proceso			
Elaboración del documento que contenga las matrices de roles y responsabilidades para cada proceso.	5	18	720
Reunión con los asesores.	1	1	40

Validación al 100% de las matrices de roles y responsabilidades por experto en ciberseguridad, equipos de respuesta a incidentes o gestión de crisis.	1	2	600
Objetivo 3: Elaborar la guía de implementación del marco.			
R4. Guía de implementación del marco.			
Elaboración del documento con la guía de implementación del marco paso a paso.	5	25	1000
Reunión con los asesores.	1	1	40
Validación al 100% del documento con la guía de implementación del marco por especialista en seguridad, ciberseguridad o gestión de crisis.	1	2	600
Objetivo 4: Aplicar la guía a un caso de estudio.			
R5. Caso de estudio elegido.			
Selección (compra) de un caso de estudio que contenga un ejemplo de crisis cibernética.	1	2	80
Reunión con los asesores.	1	1	40
Validación al 100% de la pertinencia del caso de estudio con el proyecto de tesis, realizado por un especialista en seguridad, ciberseguridad, gestión de continuidad o crisis.	1	2	600
R6. Informe de aplicación del marco al caso de estudio.			
Análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado.	5	43	1720
Reunión con los asesores.	1	1	40
Validación al 100% del análisis comparativo por un especialista en seguridad,	1	2	600

ciberseguridad, gestión de continuidad o crisis.			

Fuente: Elaboración Propia

Donde:

- Costo por hora de esfuerzo del tesista: 40 soles.
- Costo por hora de esfuerzo del asesor: 0 soles.
- Costo por hora de esfuerzo del especialista: 300 soles.

- **Cronograma de actividades del proyecto**

Tabla 56: Cronograma de actividades de tesis 1

TESIS 1		
Semana	**Entregable**	**Actividad**
1	**1.1**	Elaboración de Ficha de registro de idea de tesis y asesor.
		Reunión con asesores.
		Revisión de los asesores.
2	**1.2**	Elaboración del protocolo de revisión y diseño de formulario de extracción.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
3	**1.3**	Elaboración del reporte de ejecución de la revisión.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.

4	**1.4**	Elaboración del reporte de ejecución de la revisión y formulario de extracción completo.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
5	**1.5**	Elaboración del marco conceptual.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
6	**1**	Definición de la problemática.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
7	**2.1**	Elaboración del árbol de objetivos.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
8 - 10	**2**	Definición de métodos y procedimientos.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
		Definición parcial del Plan del Proyecto
		Reunión con asesores.

11 - 12	**3**	Realizar correcciones del entregable anterior.
		Revisión de los asesores.
13	**4**	Definición del Plan del Proyecto completa.
		Reunión con asesores.
		Realizar correcciones del entregable anterior.
		Revisión de los asesores.
14 - 15	**Exposiciones finales**	

Fuente: Elaboración Propia

Tabla 57: Cronograma de actividades de tesis 2

Semana	**Avances a presentar**		
	Resultado	**Tipo de avance**	**Porcentaje**
1	**Objetivo 1: Definir la vista de componentes del marco a alto nivel.**		
	R1: Lista de procesos que conforman los componentes del marco.	Investigación de los componentes necesarios para el marco.	50%
2	**Objetivo 1: Definir la vista de componentes del marco a alto nivel.**		
	R1: Lista de procesos que conforman los componentes del marco.	Informe con la hoja de ruta de creación de los componentes del marco a alto nivel.	100%
3	**Objetivo 1: Definir la vista de componentes del marco a alto nivel.**		
	R1: Lista de procesos que conforman los componentes del marco.	IOV: Validación al 100% de la lista de componentes a alto nivel del marco por experto en ciberseguridad o gestión de crisis.	100%
	Objetivo 2: Desarrollar los procesos que conforman los componentes.		
	R2: Modelo de procesos, actividades y métricas de cada uno de los componentes.	Avance del informe con la documentación del marco.	30%
4	**Objetivo 2: Desarrollar los procesos que conforman los componentes.**		
	R2: Modelo de procesos, actividades y métricas de cada uno de los componentes.	Avance del informe con la documentación del marco.	50%

5	**Objetivo 2: Desarrollar los procesos que conforman los componentes.**		
	R2: Modelo de procesos, actividades y métricas de cada uno de los componentes.	Avance del informe con la documentación del marco.	70%
6	**Objetivo 2: Desarrollar los procesos que conforman los componentes.**		
	R2: Modelo de procesos, actividades y métricas de cada uno de los componentes.	Informe con la documentación completa del marco.	100%
	R3: Lista de roles y responsabilidades por proceso.	Avance del documento que contenga las matrices de roles y responsabilidades.	40%
7	**Objetivo 2: Desarrollar los procesos que conforman los componentes.**		
	R2: Modelo de procesos, actividades y métricas de cada uno de los componentes.	IOV: Validación al 100% del informe con la documentación completa por especialista en ciberseguridad o gestión de crisis.	100%
	R3: Lista de roles y responsabilidades por proceso.	Documento que contenga las matrices de roles y responsabilidades.	100%
8	**Exposición y entregable parcial**		
	Objetivo 2: Desarrollar los procesos que conforman los componentes.		
	R3: Lista de roles y responsabilidades por proceso.	IOV: Validación al 100% de las matrices de roles y responsabilidades por experto en ciberseguridad, equipos de respuesta a incidentes o gestión de crisis.	100%
	Objetivo 3: Elaborar la guía de implementación del marco.		
	R4: Guía de implementación del marco.	Documento con la guía de implementación del marco paso a paso.	100%
9	**Objetivo 3: Elaborar la guía de implementación del marco.**		
	R4: Guía de implementación del marco.	IOV: Validación al 100% del documento con la guía de implementación del marco por especialista en seguridad, ciberseguridad o gestión de crisis.	100%
	Objetivo 4: Aplicar la guía a un caso de estudio.		
	R5: Caso de estudio elegido.	Descripción detallada del caso de estudio que puede ser tomado de la realidad, que haya sido	100%

		exitosamente o no resuelto.	
10	**Objetivo 4: Aplicar la guía a un caso de estudio.**		
	R5: Caso de estudio elegido.	IOV: Validación al 100% de la pertinencia del caso de estudio con el proyecto de tesis, realizado por un especialista en seguridad, ciberseguridad, gestión de continuidad o crisis	100%
	R6: Informe de aplicación del marco al caso de estudio.	Avance del análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado.	50%
11	**Objetivo 4: Aplicar la guía a un caso de estudio.**		
	R6: Informe de aplicación del marco al caso de estudio.	Análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado.	100%
		IOV: Validación al 100% del análisis comparativo por un especialista en seguridad, ciberseguridad, gestión de continuidad o crisis.	100%
12	**Entregable final (Se presentará el desarrollo al 100% y las observaciones de la exposición 5)**		
13	**Revisión de parte del jurado**		
14	**Revisión de parte del jurado**		
15	**Levantamiento de observaciones del entregable final**		
16	**Exposición final**		
17	**Exposición final**		

Fuente: Elaboración Propia

- **Lista de Recursos**

A continuación, se describe la lista de recursos necesarios para el desarrollo del presente proyecto de fin de carrera.

- **Personas involucradas y necesidades de capacitación**

Tabla 58: Personas involucradas y necesidades de capacitación

Persona involucrada	Rol	Necesidades de capacitación
Mauricio Maldonado	Tesista	Investigación relacionada a gestión de crisis e incidentes.
Dr. Manuel Tupia	Asesor	No
Dra. Mariuxi Alexandra Bruzza Moncayo	Coasesor	No
-	Especialista en ciberseguridad	No
-	Especialista en seguridad	No
-	Especialista en crisis	No
-	Especialista en equipos de respuesta a incidentes.	No

Fuente: Elaboración Propia

- **Materiales requeridos para el proyecto**

Tabla 59: Materiales requeridos para el proyecto

Materiales requeridas	Importancia
Internet	Resulta de suma importancia para poder realizar los trabajos de investigación, así como también las reuniones con los asesores y especialistas.
Plan de datos	Respaldo a utilizar en caso falle el servicio de internet.
Caso de estudio	Resulta de suma importancia para poder realizar el análisis comparativo entre la gestión de comunicaciones real seguida en el caso de estudio versus la gestión de las comunicaciones aplicando el protocolo propuesto al mismo caso

Fuente: Elaboración Propia

- **Estándares o Buenas Prácticas utilizadas en el proyecto**

Tabla 60: Estándares o Buenas Prácticas utilizados en el proyecto

Estándar o Buena Práctica	Importancia
ISO 22361	Estándar necesario para identificar los factores internos y externos que definen a las crisis generadas por incidentes de ciberseguridad. Además, se usará como referencia para definir cada una de las actividades del modelado de proceso de gestión de crisis cibernética y de comunicaciones en crisis.
ENISA - How to setup CSIRT and SOC	Documento que se tomará como referencia para elaborar la estructura de un equipo de respuesta a incidentes. De igual manera, será usado para definir los roles y responsabilidades de cada uno de los miembros del equipo de respuesta elaborado.
NIST - Computer Security Incident Handling Guide	Documento de buenas prácticas que se usará como referencia para elaborar la estructura de un equipo de respuesta a incidentes. Asimismo, será usado para definir los roles y responsabilidades de cada uno de los miembros del equipo de respuesta elaborado.
ITIL v4	Marco de buenas prácticas que se emplerará como referencia para elaborar la estructura de un equipo de respuesta a incidentes. Asimismo, será usado para definir los roles y responsabilidades de cada uno de los miembros del equipo de respuesta elaborado.

Fuente: Elaboración Propia

- **Equipamiento requerido**

Tabla 61: Equipamiento requerido

Equipamiento	Importancia
Computadora	Equipo electrónico necesario para elaborar los entregables del proyecto de fin de carrera, así como realizar las entrevistas, reuniones, entre otras tareas.

Fuente: Elaboración Propia

- **Herramientas requeridas**

Tabla 62: Herramientas requeridas

Herramientas	Importancia
Bizagi	Esta herramienta de software será utilizada para realizar el modelado de los procesos del marco de trabajo elaborado.
Matriz RACI	Se usará para construir la estructura que permita mostrar detalladamente la información de los roles y responsabilidades de cada miembro de los equipos de respuesta.
Harvard Business Publishing Education y/o The Case Centre	Se usará uno de estos dos repositorios de casos de estudio para adquirir un caso que contenga un ejemplo de crisis cibernética.

Fuente: Elaboración Propia

- **Costeo del Proyecto**

Tabla 63: Costeo del proyecto

Item	Descripción	Unidad	Cantidad	Valor Unidad (S/.)	Monto Parcial (S/.)	Monto Total (S/.)
0	**Costo total del proyecto**	**---**	**---**	**---**	**---**	**20,200.00**
1	**Estudiante o tesistas**	**---**	**---**	**---**	**---**	**12,360.00**
1.1	Mauricio Maldonado	Horas	309	40	12360	
2	**Otros participantes**	**---**	**---**	**---**	**---**	**3,600.00**
2.1	Dr. Manuel Tupia	Horas	10	0	0	
2.2	Dra. Mariuxi Alexandra Bruzza Moncayo	Horas	10	0	0	
2.3	Especialista en ciberseguridad	Horas	4	300	1200	

2.4	Especialista en seguridad	Horas	4	300	1200	
2.5	Especialista en crisis	Horas	2	300	600	
2.6	Especialista en equipos de respuesta a incidentes.	Horas	2	300	600	
3	**Materiales e insumos**	**---**	**---**	**---**	**---**	**740.00**
3.1	Internet	mes	9	50	450	
3.2	Plan de datos	mes	9	25	225	
3.3	Caso de estudio	unidad	1	65	65	
4	**Bienes y equipos**	**---**	**---**	**---**	**---**	**3,500.00**
4.1	Computadora	unidad	1	3500	3500	

Fuente: Elaboración Propia

Anexo C: Informe de Hoja de Ruta

Informe de hoja de ruta del Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad.

Segun Hevner y Chatterjee (2010), se pueden identificar las siguientes fases de la metodología de Ciencia del Diseño:

1. Conciencia del problema
2. Propuesta de solución
3. Desarrollo del artefacto
4. Evaluación del artefacto
5. Conclusiones

A continuación se presenta cada uno de ellos aplicados al proyecto de tesis:

1. **Conciencia del problema**

   Según la problemática desarrollada se pudo identificar un problema principal: **Inexistencia de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en buenas prácticas internacionales.** Resulta importante abordar este problema precisamente, porque en la actualidad es necesario contar con un conjunto de buenas prácticas que permita a la empresas responder de manera completa y oportuna a la crisis, lo que incluye la gestión de incidentes de ciberseguridad, de los equipos de respuesta, de la crisis producida y de las comunicaciones necesarias. Dicho esto, surge la necesidad de contar con un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad.

2. **Propuesta de solución**

   En esta fase, se pretende construir el marco siguiendo un enfoque basado en dominios, esto con la finalidad de mantener una estructura organizada para abordar los diferentes aspectos claves del marco. Entonces, cada dominio se enfoca en un conjunto particular de procesos necesarios para hacer frente a las crisis generadas por incidentes de ciberseguridad.

Es importante mencionar que los dominios del marco y sus componentes se establecieron siguiendo los principios de la norma ISO 22361 para la gestión efectiva de las crisis. Asimismo, se utilizó un conjunto de buenas prácticas, estándares internacionales y los resultados obtenidos del estado del arte que involucran la detección de la causa, estrategia de respuesta y comunicación en crisis.

3. Desarrollo del artefacto

En esta fase, se procede con la definición del marco a alto nivel. Utilizando las buenas prácticas y normas que se mencionaron anteriormente. Entonces la estructura del modelo será la siguiente:

Tabla 64: Componentes del Marco de Trabajo

Marco de trabajo para la gestión de incidentes y crisis de ciberseguridad			
Componentes	**Dominios**	**Procesos**	**Estándares o buenas prácticas**
	Organizacional (ORG)	1. Gestión de recursos financieros y tecnológicos 2. Gestión de riesgos de ciberseguridad 3. Gestión de la continuidad de TI	- ITIL v4 - ISO 27005 - NIST Cybersecurity Framework 2.0 - COBIT 5 for Risk - ISO 22301 - NIST 800-34
	Operacional (OPE)	4. Gestión de incidentes de ciberseguridad 5. Gestión de problemas 6. Gestión del conocimiento	- NIST 800-61 - ITIL v4 - ISO 20000-1
	Respuesta a Crisis (RAC)	7. Gestión de crisis 8. Gestión de la comunicación en crisis 9. Gestión de equipos de respuesta	- ISO 22361 - ENISA - How to setup CSIRT and SOC.

Fuente: Elaboración Propia

Componentes del marco

- Dominio Organizacional (ORG): Este dominio se centra en los procesos que se necesitan para estar preparados a dar respuesta a una crisis producida por incidentes de ciberseguridad, de tal forma que se asegure que la empresa pueda seguir operando ante una crisis.
    - Gestión de recursos financieros y tecnológicos: Proceso para gestionar aquellos recursos tecnológicos y financieros con los que cuenta la empresa y que van a ser utilizados para gestionar la crisis producida.
    - Gestión de riesgos de ciberseguridad: Necesario para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información. Este proceso es fundamental para prevenir la ocurrencia de incidentes de ciberseguridad que puedan producir una crisis.
    - Gestión de la continuidad de TI: Ante una crisis resulta importante que la empresa pueda seguir operando. Por ello es esencial contar con este proceso para garantizar que la infraestructura de TI y los servicios digitales sigan funcionando de manera efectiva, incluso en situaciones adversas, minimizando así el impacto de interrupciones en el negocio.

- Dominio Operacional (OPE): Este dominio abarca los procesos necesarios para resolver de manera efectiva y oportuna los incidentes de ciberseguridad que produjeron la crisis dentro de la organización.
    - Gestión de incidentes de ciberseguridad: Es un proceso esencial para responder y resolver de manera rápida y eficaz a los incidentes que produjeron la crisis dentro de la empresa.
    - Gestión de problemas: Es un proceso que permite reducir el impacto de los incidentes, mediante la identificación de su causa raíz. Por ello, dentro de este proceso se busca tener mapeado las causas de los incidentes y soluciones temporales que puedan ser usadas.
    - Gestión del conocimiento: Proceso fundamental para capturar,

almacenar, organizar y distribuir el conocimiento y la información relevante dentro de la organización. Mediante este proceso se busca mejorar la eficiencia en la toma de decisiones al aprovechar el conocimiento acumulado. Cabe decir que este proceso resulta importante para tener documentada la información de las causas raíz y soluciones de los incidentes de ciberseguridad.

- Dominio de Respuesta a crisis (RAC): Este dominio se concentra en detallar las actividades necesarias para responder de manera efectiva, oportuna y completa a una crisis, abarcando los procesos necesarios para su gestión.
    - Gestión de crisis: Componente principal del marco, donde se detallan las actividades necesarias para gestionar una crisis de manera rápida y eficiente, de tal forma que se manejen los incidentes de forma oportuna, se proteja la reputación de la empresa y se minimicen los impactos negativos sobre ella.
    - Gestión de la comunicación en crisis: Este proceso resulta crucial para proporcionar información precisa, oportuna y transparente sobre las acciones que se están tomando para gestionar la crisis a todas las partes interesadas (internas y externas).
    - Gestión de equipos de respuesta: Proceso para definir, monitorear y supervisar los roles y responsabilidades asignados al personal para hacer frente a las crisis generadas por incidentes de ciberseguridad.

4. Evaluación del artefacto

Una vez construido el artefacto se procede con la validación de los componentes del marco. Para ello se realizará una evaluación al 100% de la lista de componentes identificados por un especialista que pueda brindar sus observaciones y dar su aprobación.

5. Conclusiones

Se presentó un conjunto de componentes que conforman el marco de trabajo para la gestión de incidentes y crisis de ciberseguridad. Cabe decir que estos componentes se encuentran divididos en dominios con la finalidad de mantener una estructura organizada para abordar los diferentes aspectos claves del marco.

Finalmente, resulta importante mencionar que toda la investigación realizada se enfocó solo en la gestión de crisis producidas por incidentes de ciberseguridad; sin embargo, se podría generalizar el uso de los componentes para gestionar cualquier tipo de crisis dentro de una organización.

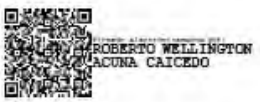
Anexo D: Acta de validación del resultado esperado R1

Lima, 11 de septiembre del 2023

Validación de la lista de componentes a alto nivel del marco para hacer frente a crisis producidas por incidentes de ciberseguridad

Por medio de la presente acta se hace constar que el **Ing. Roberto Wellington Acuña Caicedo, PhD** ha revisado el proyecto de tesis titulado **"Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361"** del alumno **Mauricio Maldonado Alvarez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del informe de hoja de ruta para la creación de la lista de componentes del marco, correspondiente al resultado R1 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,



Ing. Roberto Wellington Acuña Caicedo PhD.

Anexo E: Acta de validación del resultado esperado R2

Lima, 28 de septiembre del 2023

Validación del modelo de procesos, actividades y métricas de cada uno de los componentes del marco para hacer frente a crisis producidas por incidentes de ciberseguridad

Por medio de la presente acta se hace constar que **Roberto Wellington Acuña Caicedo** ha revisado el proyecto de tesis titulado "**Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361**" del alumno **Mauricio Maldonado Alvarez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del documento que contiene el modelo de procesos, actividades y métricas de cada uno de los componentes, correspondiente al resultado R2 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

Ing. Roberto Wellington Acuña Caicedo, PhD.

Anexo F: Acta de validación del resultado esperado R3

Lima, 28 de septiembre del 2023

Validación de la lista de roles y responsabilidades por proceso del marco para hacer frente a crisis producidas por incidentes de ciberseguridad

Por medio de la presente acta se hace constar que **Roberto Wellington Acuña Caicedo** ha revisado el proyecto de tesis titulado "**Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361**" del alumno **Mauricio Maldonado Alvarez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del documento que contiene las matrices de roles y responsabilidades por proceso, correspondiente al resultado R3 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

Ing. Roberto Wellington Acuña Caicedo, PhD.

Anexo G: Acta de validación del resultado esperado R4

Lima, 22 de octubre del 2023

Validación de la guía de implementación del marco para hacer frente a crisis generadas por incidentes de ciberseguridad

Por medio de la presente acta se hace constar que **Roberto Wellington Acuña Caicedo** ha revisado el proyecto de tesis titulado "**Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361**" del alumno **Mauricio Maldonado Alvarez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del documento que contiene la guía de implementación del marco paso a paso, correspondiente al resultado R4 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

ROBERTO
WELLINGTON ACUÑA
CAICEDO

Ing. Roberto Wellington Acuña Caicedo, PhD.
CI: 1307094936

Anexo H: Acta de validación del resultado esperado R5

Lima, 22 de octubre del 2023

Validación del caso de estudio elegido sobre una crisis producida por un incidente de ciberseguridad

Por medio de la presente acta se hace constar que **Roberto Wellington Acuña Caicedo** ha revisado el proyecto de tesis titulado **"Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361"** del alumno **Mauricio Maldonado Alvarez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del documento que contiene la descripción detallada del caso de estudio que puede ser tomado de la realidad, y que haya sido exitosamente o no resuelto, correspondiente al resultado R5 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

ROBERTO
WELLINGTON ACUNA
CAICEDO

Ing. Roberto Wellington Acuña Caicedo, PhD.
CI: 1307094936

Anexo I: Acta de validación del resultado esperado R6

Lima, 30 de octubre del 2023

Validación del Informe de aplicación del marco de trabajo al caso de estudio seleccionado

Por medio de la presente acta se hace constar que **Roberto Wellington Acuña Caicedo** ha revisado el proyecto de tesis titulado "**Diseño de un marco de trabajo para la gestión de incidentes y crisis de ciberseguridad basado en la norma ISO 22361**" del alumno **Mauricio Maldonado Alvarez**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del documento que contiene el análisis comparativo entre la gestión de crisis real seguida en el caso de estudio versus la gestión de crisis aplicando el marco de trabajo elaborado, correspondiente al resultado R6 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

Ing. Roberto Wellington Acuña Caicedo, PhD.
CI: 1307094936