# DESARROLLO DE UN PLAN DE CONTINGENCIA PARA EL ÁREA DE TECNOLOGÍA DE ZONA SEGURA S.A.S


Carlos Alberto Carvajal Pérez

FACULTAD DE INGENIERÍAS

Ingeniería de Sistemas

Alicia Osorio Builes


**INSTITUTO TECNOLÓGICO METROPOLITANO**

**07/06/2018**

# RESUMEN

El presente proyecto se implementó en el área de tecnología de Zona Segura S.A.S, empresa enfocada en la transferencia de conocimiento mediante un modelo FCT (Formación, Consultoría y Tecnología), suministrando herramientas Web Clouding y Mobile para el acompañamiento de los procesos de diversas organizaciones.

La empresa no contaba con una estrategia que respaldara sus procesos tecnológicos en caso de una catástrofe natural, errores humanos o actos malintencionados de terceros, lo que podría provocar la pérdida de información confidencial de los diferentes clientes adscritos a la compañía.

Se desarrolló un plan de contingencia, basado en normas internacionales: ISO 31000:2009 de gestión de riesgos, la ISO 27001:2013 que aborda cómo gestionar la seguridad de la información y la metodología MAGERIT V.3 que facilitó la evaluación y disminución en el impacto de los riesgos por medio de salvaguardas que se implementaron antes, durante y después de un incidente. Esto, con el fin de garantizar la operatividad de la organización en caso de que uno o varios riesgos se materialicen.

El alcance del proyecto partió de la planificación de procesos, escenarios y activos de la empresa. Posterior a ello, la evaluación de riesgos, el desarrollo de los procedimientos e instructivos que se efectuaran como salvaguardas en caso de la materialización de incidentes y finalizó con la simulación de eventos que permitieron implementar el plan de contingencia, quedando a disposición de la compañía.

Finalmente, se logró la sistematización del plan de contingencia de los procesos tecnológicos de Zona Segura S.A.S, aportando en la disminución del impacto de riesgos críticos encontrados, optimizando así, la disponibilidad, integridad, confidencialidad y los niveles de seguridad de la información.

*Palabras clave*: Riesgo, MAGERIT, Ciclo Deming, Gestión de riesgos, Gestión de la seguridad de la información.

# RECONOCIMIENTOS

Agradezco a Dios por darme salud y la fuerza necesaria para alcanzar las metas que me tracé durante mi carrera universitaria. A mi familia, en especial a mis padres y hermanos quienes me brindaron un apoyo incondicional.

A mis amigos, quienes me impulsaron cada día a ser una mejor persona y a los profesores con los que tuve oportunidad de compartir en el ITM, que con su conocimiento y enseñanzas, me ayudaron a ser un mejor profesional.

A la profesora Alicia Osorio Builes, quien fue mi asesora y me guio durante el proceso del proyecto de grado.

A mis compañeros de trabajo y jefes de Zona Segura S.A.S quienes me dieron la oportunidad de realizar mi proyecto de grado enfocado en la empresa, impactando positivamente mi vida profesional.

# ACRÓNIMOS

| | |
|---|---|
| *ISO* | Organización Internacional de Normalización (International Organization for Standardization) |
| *PHVA* | Planificar, Hacer, Verificar y Actuar |
| *NTC* | Norma Técnica Colombiana |
| *AVARMS* | Software de la empresa Zona Segura S.A.S |
| *BRAVA* | Software de la empresa Zona Segura S.A.S |
| *MAVA* | Mesa de ayuda de la empresa Zona Segura S.A.S |
| *APP* | Aplicación para dispositivos móviles |
| *MGI-004* | Macroproceso Gestión de la Información |
| *MFCT-003* | Macroproceso Desarrollo FCT |
| *PR-MGI-001* | Proceso Desarrollo y Actualizaciones del Macroproceso Gestión de la Información |
| *PR-MGI-002* | Proceso Soporte (MAVA) del Macroproceso Gestión de la Información |
| *PR-MGI-003* | Proceso Mantenimiento y Manejo de Datos del Macroproceso Gestión de la Información |
| *PR-MGI-004* | Proceso Infraestructura del Macroproceso Gestión de la Información |
| *PR-MFCT-003* | Proceso Tecnología del Macroproceso Desarrollo FCT |
| *IN-MGI-001* | Instructivo del Macroproceso Gestión de la Información - proceso Desarrollo y Actualizaciones |
| *IN-MGI-002* | Instructivo del Macroproceso Gestión de la Información - proceso Soporte (MAVA) |
| *IN-MGI-003* | Instructivo del Macroproceso Gestión de la Información - proceso Mantenimiento y Manejo de Datos |
| *IN-MGI-004* | Instructivo del Macroproceso Gestión de la Información - proceso Infraestructura |

# TABLA DE CONTENIDO

# 1. INTRODUCCIÓN

En la actualidad las empresas buscan entender su fenómeno de riesgo para así realizar una gestión integral por procesos, que les permita monitorear toda la operación de su organización con el fin de tomar acciones correctivas y de mejora.

La empresa Zona Segura S.A.S ofrece un modelo que soporta dicho fenómeno apoyado en los principios y directrices que proporciona la ISO 31000:2009, y se hace a través de un software donde uno de los mayores valores es la entrega de la información, indicadores y demás componentes de la aplicación en tiempo real, por lo tanto, es necesario garantizar la operatividad del servicio incluso ante la materialización de incidentes en la compañía.

Aunque la empresa dispone de servidores en un Datacenter fuera del país, que garantizan la disponibilidad de los datos, no está exenta de algún episodio que ponga en riesgo la información, especialmente cuando no se cuenta con una estrategia que respalde los procesos tecnológicos en caso de una catástrofe natural, errores humanos o actos malintencionados de terceros, lo que provocaría la pérdida de información confidencial y afectaría la integridad de los datos de los diferentes clientes adscritos a la empresa, y esto puede repercutir en que los procesos de las mismas colapsen ya que estos dependen de nuestro sistema para gestionar sus riesgos, desencadenando afectaciones legales, económicas y/o reputacionales para Zona Segura S.A.S. De igual manera a nivel interno, se pueden presentar incidentes operativos que pongan en riesgo el normal desarrollo de las actividades de la empresa y sus colaboradores.

Por lo anterior es preciso desarrollar un plan de contingencia que contenga los procedimientos necesarios para reaccionar a tiempo y garantizar la operatividad continua de los procesos tecnológicos de la compañía, dando cumplimiento a su razón de ser “Asegurar la vida de su empresa”.

Para llevar a cabo el objeto de este proyecto, se realizó una identificación de procesos, escenarios, activos y riesgos del área implicada a través de la metodología MAGERIT V.3, facilitando el análisis y la evaluación de los mismos, posterior a ello, se formularon acciones correctivas y de mejora con base a las normas ISO 31000 de gestión de riesgos e ISO 27001:2013 sobre la gestión de seguridad de la información que garanticen la continuidad de los procesos tecnológicos de Zona Segura S.A.S.

Buscando que la empresa se apropie del tema con el fin de obtener una respuesta oportuna y activación efectiva del plan de contingencia, se sensibilizó el personal de Zona Segura S.A.S por medio de capacitaciones y sesiones de trabajo para el manejo de los procedimientos a llevar a cabo ante las eventualidades que puedan presentase. Luego, se dejó a disposición el plan para su posterior implementación ante futuros incidentes. Esto a su vez, apoyó el proceso de certificación en la norma ISO 9001:2015 (Sistema de gestión de calidad) lo que fortalecerá la exportación al mercado internacional.

Este proyecto se enmarca en cuatro (4) capítulos, donde el primero es el marco teórico en el cual se encuentran todas las definiciones y los temas necesarios para entender el desarrollo del mismo. El segundo capítulo es la metodología donde por medio de un ciclo Deming PHVA se muestra la elaboración de cada uno de los componentes que permitieron cumplir con los objetivos específicos. Luego, en el tercer capítulo se detallan los resultados obtenidos con las pruebas realizadas en la verificación y la mitigación de los riesgos más críticos por medio de las salvaguardas.

Para finalizar, en el cuarto capítulo que abarca las conclusiones, recomendaciones y trabajo a futuro, se dejan plasmadas las mejoras, sugerencias y el seguimiento que se le debe dar al plan de contingencia a través del tiempo.

## 1.1 OBJETIVOS

### General

- Desarrollar un plan de contingencia para el área de tecnología de la empresa Zona Segura S.A.S, el cual permita el normal funcionamiento de sus diferentes procesos, garantizando la operatividad de la organización en caso de que uno o varios incidentes se materialicen.

### Específicos

- Identificar los riesgos del área de tecnología a través de la metodología MAGERIT V.3 facilitando el análisis y la evaluación de estos.

- Formular acciones correctivas y de mejora con base a las normas ISO 31000:2009 de gestión de riesgos y la ISO 27001:2013 sobre la gestión de seguridad de la información que garanticen la continuidad de los procesos tecnológicos de Zona Segura S.A.S.

- Sensibilizar el personal de Zona Segura S.A.S por medio de capacitaciones sobre el plan de contingencia y sus procedimientos, permitiendo la activación y respuesta oportuna del plan ante las eventualidades que puedan presentase al interior de la empresa.

- Fortalecer el proceso de certificación en la NTC-ISO 9001:2015 (Sistema de gestión de calidad), a partir de la elaboración de los procedimientos desarrollados en el plan de contingencia, que hacen parte de los requisitos establecidos para las acciones de contingencia pertinentes dentro de la misma. Esto con el fin de expandir la exportación de servicios hacia el mercado internacional.

# 2. MARCO TEÓRICO

En este capítulo, se establecen los diferentes conceptos, metodologías, normas y elementos utilizados en el proyecto, con el fin de otorgar bases para el entendimiento de este.

Con la experiencia ganada en la entrega de servicios de TI, especialmente en el diseño, construcción y el suministro de herramientas en web clouding y mobile entre 2009 y 2017, Zona Segura S.A.S se ha venido constituyendo en un jugador importante en el sector de TI, por lo novedoso y útil de la plataforma, en la resolución de cálculos y determinación de las brechas que existían en la creación, monitoreo y lectura de informes estratégicos y operativos, que fueran útiles a la hora de la toma de decisiones por parte de los directivos y administradores de cualquier tipo y tamaño de negocio.

Por lo anterior la empresa necesita mecanismos que puedan respaldar los procesos más críticos y eviten poner en riesgo la información de sus clientes, haciendo que la construcción de un **Plan de Contingencia aplicado a las tecnologías de la información** sea prioritaria.

Un plan de contingencia es una estrategia planificada con un conjunto de procedimientos alternativos a la operatividad normal de cada empresa, el cual facilita u orienta a tener una solución que permita restituir rápidamente los servicios ante la eventualidad de algún incidente interno o externo de la organización, por medio de normas y acciones básicas de respuesta que se deberían tomar para afrontar de manera oportuna, adecuada y efectiva. (Ortiz Anderson, 2017).

En este proyecto se alinearán los planes de acción y los procedimientos alternativos para el normal funcionamiento de las Tecnologías de Información y Comunicación, cuando alguno de sus servicios se vea afectados por la materialización de un incidente interno o externo a la organización.

Lo anterior considerando 3 acciones: "**Antes**, como un plan de respaldo o de prevención para mitigar los incidentes. **Durante**, como un plan de ejecución en el momento de presentarse el incidente y **Después**, como un plan de recuperación una vez superado el incidente, regresando al estado previo a la contingencia" (Ortiz Anderson, 2017).

Antes de desarrollar un plan de contingencia que respalde la operatividad de los procesos, se necesita tener conocimiento del fenómeno de **riesgo** en la organización, entendiendo el riesgo como la interacción entre la amenaza y la vulnerabilidad. La amenaza es la probabilidad de que un fenómeno de origen natural, socionatural o antrópico se presente con cierta intensidad en un sitio específico y dentro de un período de tiempo, con potencial de producir efectos adversos sobre las personas, los bienes y el medio ambiente. La vulnerabilidad, por su parte, expresa las características y circunstancias de una comunidad, sistema o bien, que los vuelven susceptibles a los efectos dañinos de una amenaza. (Ortiz Anderson, 2017)

"Los riesgos se pueden eliminar, transferir, mitigar o aceptar. Esto dependerá de varios factores tales como la probabilidad de ocurrencia o impacto del riesgo" (Ortiz Anderson, 2017).

Zona Segura S.A.S entiende que el aseguramiento integral es un seguro de vida para las empresas y que los riesgos son dinámicos, por lo que, la medición del estado del riesgo debe ser dinámica y oportuna. Lo anterior solo se puede llevar a cabo con una buena gestión de riesgos.

**Gestión integral de riesgos**

"La Gestión Integral del Riesgo es un proceso coordinado entre varias instituciones para reducir, prevenir, responder y apoyar la rehabilitación y recuperación frente a eventuales

emergencias y desastres, en el marco de un desarrollo sostenible" (SINAE (Sistema Nacional de Emergencias Uruguay), 2012).

La ISO 31000 es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones. Fue publicada en noviembre del 2009 por la Organización Internacional de Normalización (ISO), y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades. Como complemento está la norma ISO 31010 "Gestión del riesgo. Técnicas de evaluación de riesgos" que tiene una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos. (ISOTools, 2017)

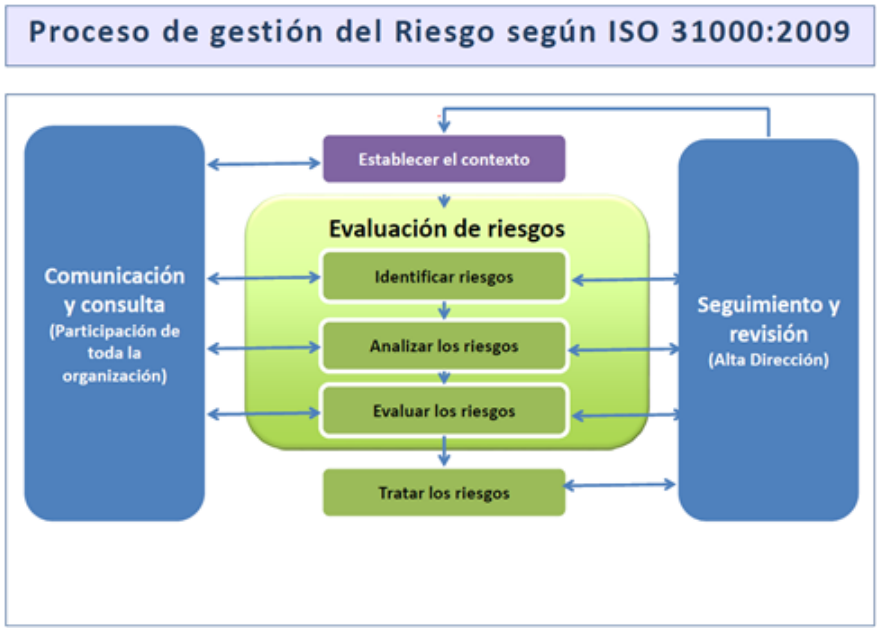



*Figura 1.* Proceso gestión del riesgo. Fuente: ISO 31000:2009.

La Gestión Integral del Riesgo tiene seis fases: la **prevención** para impedir que ocurra un incidente, la **mitigación** para atenuar el impacto de los fenómenos adversos, asumiendo que no siempre es posible evitar los incidentes, la **preparación** para generar actividades

orientadas a asegurar la disponibilidad de los recursos y efectividad de los procedimientos para enfrentar una situación de emergencia, la **atención de emergencias** para dar respuesta ante la ocurrencia de un evento adverso, la **rehabilitación** para la puesta en marcha en el menor tiempo posible de los servicios básicos afectados por un evento adverso y por último la **recuperación,** para que luego de un evento adverso, se genere la reactivación del desarrollo económico y social de la comunidad en condiciones más seguras. (SINAE (Sistema Nacional de Emergencias Uruguay), 2012)

Teniendo en cuenta que el mayor activo de Zona Segura S.A.S es la información, no basta con hacer una gestión de riesgos basada solo en la ISO 31000:2009, sino que se debe abordar un **Sistema de gestión de seguridad de la información.**

Podemos entender por información todo el conjunto de datos que se organizan en una empresa y otorgan un valor añadido para ésta. El Sistema de Gestión de Seguridad de la Información, según ISO 27001:2013 consiste en preservar la **confidencialidad** donde la información no se pone a disposición de terceros, ni se revela a individuos o entidades no autorizados, la **integridad** donde se mantiene de forma completa y exacta la información y los métodos de proceso, por último, la **disponibilidad** que permite acceder y utilizar la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO 27001, 2013)

“El SGSI (Sistema de Gestión de Seguridad de la Información) es el principal concepto sobre el que se conforma la norma ISO 27001:2013. La gestión de la Seguridad de la Información se debe realizar mediante un proceso sistémico, documentado y conocido por toda la empresa” (ISO 27001, 2013).

La ISO 27001:2013 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que

la procesan. El estándar ISO 27001:2013 para los Sistemas de Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. (ISOTools, 2017) La cual "(…) ofrece herramientas que tienen el objetivo de facilitar la implementación de los **planes de contingencia** y de continuidad en las empresas, existen diferentes pasos a seguir si se produce un incidente de seguridad" (ISOTools Excellence, 2015).

Por otro lado, para realizar una buena evaluación de riesgos es necesario apoyarse de una metodología para su análisis y gestión, puesto que las normas ISO 27001:2013 e ISO 31000:2009 sólo describen los pasos y directrices a seguir para la gestión del riesgo, mas no explica las actividades que se deben llevar a cabo específicamente, por lo que se hace necesario abordar alguna metodología que ayude en este proceso.

**MAGERIT V.3**

Esta metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica en España. Ofrece un método sistemático para analizar los riesgos derivados del uso de **tecnologías de la información** y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los **riesgos mitigados**. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el **análisis de riesgos**. (Gutiérrez Amaya, 2013)

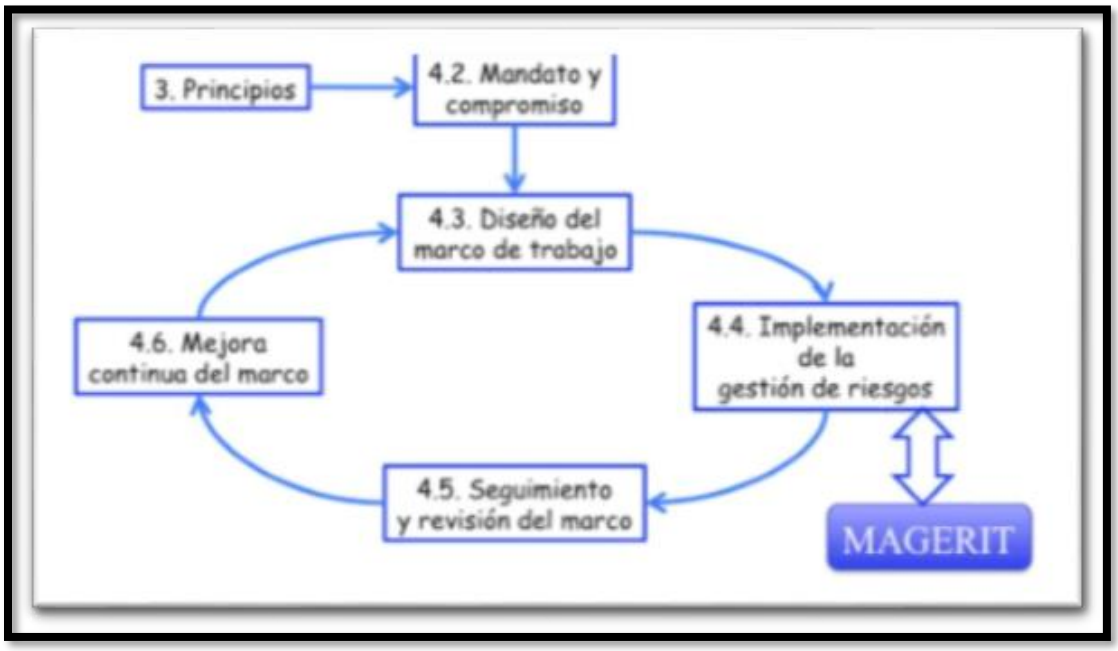



*Figura 2.* ISO 31000:2009, Marco de trabajo para la gestión de riesgos. Fuente: MAGERIT V3 Libro I: Método

MAGERIT persigue los siguientes objetivos: concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC) y por último, ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. (Gobierno de España, 2012)

MAGERIT permite estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. (Gobierno de España, 2012)

“Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o

controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios" (Gobierno de España, 2012).

MAGERIT V3 se ha estructurado en tres guías:

1) **Método,** se estructura de la siguiente forma:

**El capítulo 2** presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos. **El capítulo 3** concreta los pasos y formaliza las actividades de análisis de los riesgos. **El capítulo 4** describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos. **El capítulo 5** se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente. **El capítulo 6** formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos. **El capítulo 7** se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo. **El capítulo 8** se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos. (Gobierno de España, 2012)

2) **Catálogo de Elementos,** marca unas pautas en cuanto a:

- Tipos de activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información

3) **Guía de Técnicas,** aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos. Técnicas específicas para el análisis de riesgos:

- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

Cabe anotar, que en la empresa se viene adelantando un proceso de certificación en la ISO 9001:2015, la cual, "es la norma que proporciona los requisitos básicos para tener en cuenta a la hora de desarrollar e implementar un sistema de gestión de calidad" (ICONTEC, 2015, págs. 17-19). Esto con el fin de expandir la exportación de servicios hacia el mercado internacional.

Esta norma pertenece a la familia ISO 9000 de sistemas de gestión de la calidad (junto con ISO 9004), y ayuda a las organizaciones a cumplir con las expectativas y necesidades de sus clientes. Un sistema de gestión ISO 9001:2015 le ayudará a gestionar y controlar de manera continua la calidad en todos los procesos. (BSI (The British Standars Institution), 2017)

Aunque pareciera que este tema no compete con el desarrollo del proyecto, colateralmente fortalecerá la certificación en la NTC-ISO 9001:2015 que está realizando la empresa donde en el numeral 8.2.1 de la norma se habla de los requisitos para los productos y servicios, en el cual, el literal e) dice: "se debe establecer los requisitos específicos para las acciones de contingencia, cuando sea pertinente" (ICONTEC, 2017). Además, se hace referencia al tema en uno de los ítems de PRODUCCIÓN Y PROVISIÓN DEL SERVICIO, donde dice: "La

organización debe implementar la producción y provisión del servicio bajo **condiciones controladas** como la implementación de acciones para prevenir los errores humanos, la implementación de actividades de liberación, entrega y posteriores a la entrega, entre otros" (ICONTEC, 2015).

Como casos de éxito, tenemos la implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad Nuestra Señora de Gracia, alineado tecnológicamente con la norma ISO 27001:2013.

En un artículo publicado en la web, se muestra el resultado de un proyecto de investigación, adelantado por un grupo de estudiantes de ingeniería de sistemas con el fin de implementar un SGSI en la Comunidad Nuestra Señora de Gracia, en Bogotá Colombia. Este sistema se basa en las directrices indicadas en la norma ISO/IEC 27001. El proyecto permitió evidenciar un nivel de brechas significativo en la mencionada Comunidad, con base en el cual se estableció políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado. (Díaz, Collazos, Cortez Lozano, Ortiz, & Herazo Pérez, 2018)

Gracias al proyecto que se desarrolló, se concretaron principios y políticas de control de información y de comunicación de seguridad, los cuales produjeron los siguientes resultados:

- Entrega de un sistema de información para una mayor seguridad integral.
- Propuesta de un plan de continuidad del negocio permitiendo que la empresa pueda recuperarse después de algún incidente que pudiese presentarse**. (Lo cual es fundamental para este proyecto).**
- Capacitación y concientización al Departamento de Sistemas sobre el impacto favorable que tendría el establecimiento de una política en ISO 27001:2013.

También, se encontró otro artículo donde se evalúa la seguridad de la información del proceso de admisión de estudiantes de pregrado en la Universidad Tecnológica Equinoccial basado en la norma internacional ISO/IEC 27000, con el fin de determinar el nivel de seguridad y elaborar un plan de tratamiento de riesgos que permita dar respuesta a los riesgos de seguridad de la información asociados a este proceso. (Universidad de las Fuerzas Armadas ESPE, 2018)

En el desarrollo de dicho trabajo se utilizó una metodología de evaluación de seguridad de la información basada en riesgos con su fundamento en la norma NTE INEN-ISO/IEC 27005:2012 elaborada por los autores, donde se establecen los pasos a seguir y las actividades a realizar en cada etapa del proceso hasta obtener los resultados finales sobre la brecha de seguridad respecto a la norma ISO/IEC 27001:2005 y el plan de tratamiento que mitiguen los riesgos priorizados acorde a los criterios de aceptación que definieron. (Universidad de las Fuerzas Armadas ESPE, 2018)

Por último, se evidenció un artículo donde se presenta la aplicación de la metodología **OCTAVE-s** para el análisis y gestión del riesgo en la seguridad de la información, adaptada al proceso "Inscripciones y Admisiones", en la División de Admisión, Registro y Control Académico (DARCA) de la Universidad del Cauca; siguiendo las directrices de la norma ISO/IEC 27005:2011. Además, se incluye la estructura del proceso, y el procedimiento escogido como caso de estudio para aplicar el tratamiento del riesgo. (Espinosa T., Martínez P., & Amador D., 2014)

Como conclusión de este proyecto, se tiene que no es suficiente gestionar el riesgo de la seguridad de la información solo con la norma ISO 27005:2011. Es necesario apoyarse de una metodología para el análisis y gestión del riesgo, como por ejemplo OCTAVE-s o MAGERIT, pues la norma ISO 27005:2011 solo describe los pasos que se deben seguir para la gestión del riesgo, pero no explica las actividades que se deben llevar a cabo específicamente, lo que OCTAVE-s y MAGERIT si determina.

# 3. METODOLOGÍA

## 3.1 CONTEXTUALIZACIÓN

El presente proyecto se implementó en el área de tecnología de Zona Segura S.A.S, una empresa enfocada en la transferencia de conocimiento mediante un modelo FCT (Formación, Consultoría y Tecnología), suministrando herramientas web clouding y mobile para el acompañamiento de los procesos de diversas organizaciones.


*Figura 3. Esquema organizacional de Zona Segura S.A.S.*

Este plan estará direccionado a la Gerencia de Innovación y desarrollo, quien está encargada de la operación del área de tecnología de la compañía y busca garantizar la operatividad continua de sus procesos tecnológicos.

### 3.1.1 Personal responsable del área de tecnología de Zona Segura S.A.S y actores principales del proyecto

En la tabla 1 se pueden visualizar los colaboradores principales que participaron en la obtención de la información utilizada. Son los encargados de la gerencia de innovación y desarrollo de la empresa, la cual maneja los procesos tecnológicos y por ende son los actores principales en este proyecto.

| CARGOS DEL PERSONAL | CANTIDAD |
|---|---|
| Gerente de Innovación y Desarrollo | 1 |
| Ingeniero de Desarrollo | 1 |
| Analista de Desarrollo | 1 |
| Analista de Soporte a Usuarios | 1 |
| Analista de Procesos | 1 |
| **Total** | **5** |

*Tabla 1.* Personal a cargo de los procesos del área de Tecnología de Zona Segura S.A.S.

## 3.2 METODOLOGÍA DE LA INVESTIGACIÓN

El proceso investigativo y de recolección de la información requerida para el plan de contingencia de Zona Segura S.A.S se desarrolló en el siguiente orden:

- Investigación de la norma ISO 27001:2013 y la ISO 31000:2009.
- Exploración de la metodología MARGERIT V3 para la evaluación de riesgos.
- Consulta de antecedentes relacionados a planes de contingencia informáticos.
- Recopilación de referencias bibliográficas.
- Sesiones de trabajo con el personal del área encargada de los procesos tecnológicos. **(Ver Apéndice I)**

### 3.3 DESARROLLO DEL PLAN DE CONTINGENCIA

El desarrollo de este plan de contingencia se rigió en tres aspectos importantes para garantizar la seguridad de la información, que fueron la confidencialidad, la integridad y la disponibilidad, los cuales se deben asumir en los sistemas de información.

Se puso en marcha un ciclo de mejora continua Deming (PHVA), el cual permitió llevar mayor control en el desarrollo del plan de contingencia pues gracias a este se dividió en 4 grandes fases la solución del plan:

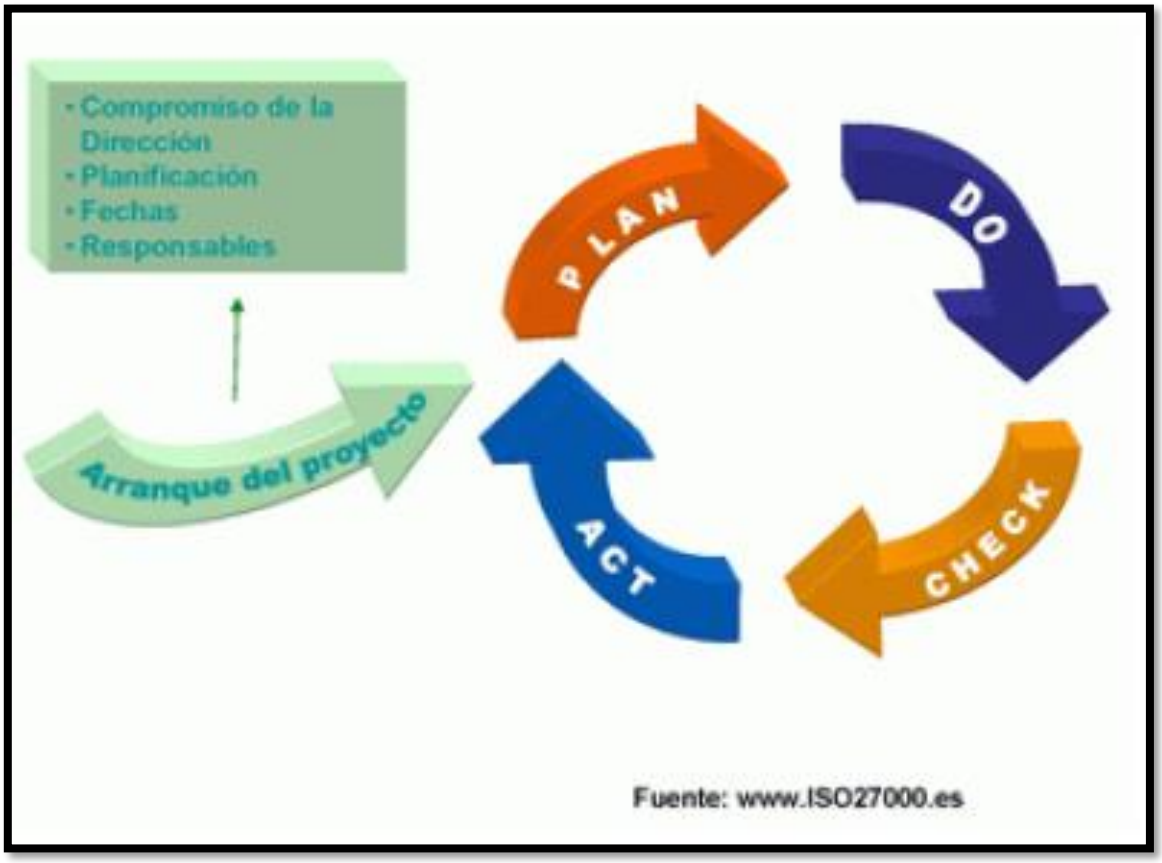



*Figura 4.* Ciclo PHVA (PDCA en Ingles). Fuente: www.ISO27000.es

### 3.3.1 Planificación (P)

Tras un análisis de diversas metodologías aplicadas para el análisis y evaluación de riesgos, se logra determinar que MAGERIT V. 3.0 resulta ser la opción más efectiva y completa ya que protege la información con base a los aspectos de disponibilidad, confidencialidad e integridad de la información. Además, posee otras características importantes para garantizar la seguridad de los sistemas y procesos de la organización. Dicha metodología facilitará la identificación de los activos de la empresa al dividirlos en diferentes grupos con el fin de valorizar de forma amplia los riesgos y elaborar medidas específicas evitando la presencia de incidentes.

#### 3.3.1.1 Definición de procesos críticos

Los Macroprocesos críticos del área de tecnología de Zona Segura S.A.S son **MGI-004 Gestión de la Información** y **MFCT-003 Desarrollo FCT** los cuales están compuestos por los siguientes procesos definidos en procedimientos.

Para **MGI-004 Gestión de la Información** tenemos los procesos:

- PR-MGI-001 Desarrollo y Actualizaciones
- PR-MGI-002 Soporte (MAVA)
- PR-MGI-003 Mantenimiento y Manejo de Datos
- PR-MGI-004 Infraestructura

Para **MFCT-003 Desarrollo FCT** tenemos el proceso:

- PR-MFCT-003 Tecnología

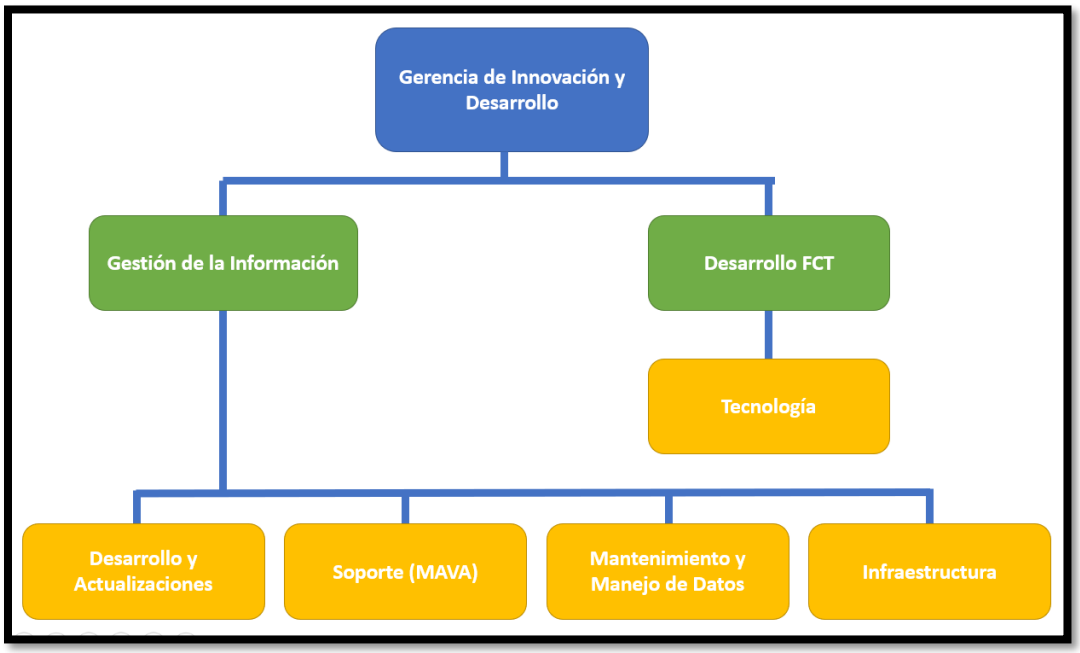



*Figura 5. Esquema de Macroprocesos y procesos del área de Tecnología de Zona Segura S.A.S.*

**MGI-004 Gestión de la Información**

| **Nombre del Macroproceso:** | **GESTIÓN DE LA INFORMACIÓN** |
|---|---|
| **Responsable - Líder del Proceso** | Gerente de Innovación y Desarrollo |
| **Objetivo** | Garantizar la disponibilidad, confidencialidad e integridad del software AVARMS®, brava®, los datos ingresados por nuestros clientes, información de las otras partes interesadas y la información interna de Zona Segura S.A.S. |
| **Alcance** | Desde que se recibe la información por parte de todas las partes interesadas, el desarrollo de nuevos productos y sus actualizaciones, hasta el manejo y custodia de la misma por parte de Zona Segura S.A.S. |

*Tabla 2. Descripción del Macroproceso Gestión de la Información de Zona Segura S.A.S.*

**PR-MGI-001 Desarrollo y Actualizaciones**

**Objetivo:** Innovar a través de nuevos desarrollos y actualizaciones, de acuerdo con las tendencias mundiales de gestión del riesgo

**Alcance:** Tanto para los clientes como para ZONA SEGURA, desde la historia del usuario hasta la satisfacción del cliente interno o externo.

**Definiciones:**

- **Historia de usuario**: Todos los requerimientos por fallas en el manejo en la plataforma o necesidades de mejora
- **App:** Aplicaciones en formatos Mobile.
- **Trello:** Herramientas de registros de historias de usuarios

**Descripción:**

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **1** | Montaje de servicio AVARMS | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Gerente innovación de desarrollo | No aplica | Instructivo de Implantación del AVA RMS |
| **2** | Publicar y actualizar la aplicación AVA RMS y/o brava en Play Store. | • Ingeniero de desarrollo<br>• Analista de desarrollo | No aplica | Instructivo de publicación de app. |
| **3** | Historias de usuario<br>• Clientes<br>• ZONA SEGURA S.A.S<br>• Adquisición de conocimiento<br>• Clientes de prospecto | • Todos los colaboradores de ZONA SEGURA<br>• Clientes<br>• Clientes de prospectos | • TRELLO<br>• Correo electrónico | No aplica |
| **4** | Evaluación de requerimiento, su objetivo y generación de su valor | • Ingeniero de desarrollo<br>• Analista de desarrollo | • TRELLO | Formato de costos |

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| | | • Gerente innovación de desarrollo<br>• Gerente general | • Correo electrónico | |
| **5** | Ingeniería de software<br>• Levantamiento y análisis de requerimiento<br>• Desarrollo de requerimiento<br>• Prueba y ajustes<br>• Implantación de desarrollo<br>• Guías (documentación)<br>• Mantenimiento | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Gerente innovación de desarrollo<br>• Analista de procesos | • TRELLO<br>• Guía de usuario | Instructivo de implantación de desarrollo |
| **6** | Comunicación y satisfacción del cliente | Todos los colaboradores de ZONA SEGURA | • Acta de entrega<br>• TRELLO | Ver procedimiento de comunicaciones e instructivo de PQRS |

*Tabla 3. Descripción del Proceso Desarrollo y Actualizaciones de Zona Segura S.A.S.*

**PR-MGI-002 Soporte (MAVA)**

**Objetivo**: Brindar a los usuarios de AVARMS y BRAVA un servicio ágil oportuno y preciso.

**Alcance:** Para todos nuestros clientes desde Historia de usuario hasta la satisfacción del cliente.

**Definiciones:**

- **Historia de usuario**: Todos los requerimientos por fallas en el manejo en la plataforma o necesidades de mejora.
- **Esquema organizacional:** La estructura de 4 niveles compuesta por: (organización, unidad de negocio, región y sedes)
- **Petición:** Es la acción de solicitar o demandar a la organización que haga intervenga o realice algún encargo.

- **Queja:** Reclamación o protesta que se hace ante la organización a causa de un desacuerdo o inconformidad.
- **Reclamo:** Es la solicitud de inconformidad y la consecuente corrección del fallo para la búsqueda de la satisfacción del cliente.
- **Sugerencia:** A modo de recomendación, es la acción que realiza un cliente o una de las partes interesadas tendiente al mejoramiento de un proceso.
- **Felicitación:** Expresión de la satisfacción a través de una comunicación.
- **Trello:** Herramientas de registros de historias de usuarios.

**Descripción:**

| ITEM | DESCRIPCIÓN ACTIVIDAD | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **1** | • Historia del Usuario<br>• Correo Electrónico<br>• Llamadas del cliente<br>• Actas de reunión<br>• PQRS | USUARIOS | • Correo Electrónico<br>• Llamada<br>• Actas<br>• Clientes de prospecto | No aplica |
| **2** | Evaluación de la historia | | | |
| **2.1** | La creación del usuario | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Analista de procesos | TRELLO | Instructivos de Soporte |
| **2.2** | Creación del esquema organizacional | • Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | Instructivos de Soporte |
| **2.3** | Parametrización de las sedes | • Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | Instructivos de Soporte |

| ITEM | DESCRIPCIÓN ACTIVIDAD | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| | | • Gerente innovación y desarrollo<br>• Analista de procesos | | |
| **2.4** | Borrar evento | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Analista de procesos | TRELLO | Instructivos de Soporte |
| **2.5** | Ajustes del sistema | • Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | Instructivos de Soporte |
| **2.6** | Orientación del usuario | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Gerente innovación y desarrollo<br>• Analista de procesos | TRELLO | Instructivos de Soporte |
| **2.7** | Generar informes | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Gerente innovación y desarrollo<br>• Analista de procesos | TRELLO | Instructivos de Soporte |
| **2.8** | Preparación de datos y carga masiva | • Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | Instructivos de Soporte |

| ITEM | DESCRIPCIÓN ACTIVIDAD | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **2.9** | Modificar perfil y permisos de acceso | • Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | Instructivos de Soporte |
| **3** | Ejecución y comunicación | • Ingeniero de desarrollo<br>• Analista de desarrollo<br>• Gerente innovación y desarrollo<br>• Analista de procesos | • TRELLO<br>• Correo electrónico<br>• llamada | No aplica |
| **4** | Medición de la satisfacción del cliente | Gerente general | • TRELLO<br>• Correo electrónico<br>• Llamada | Instructivo de PQRS |

*Tabla 4. Descripción del Proceso Soporte (MAVA) de Zona Segura S.A.S.*

**PR-MGI-003 Mantenimiento y Manejo de Datos**

**Objetivo:** Garantizar la disponibilidad, integridad y confidencialidad de la información interna y externa

**Alcance:** Desde la obtención (creación de la información o captura de la información) hasta su disposición final.

**Definiciones**:

- **Información interna**: Aquella que se necesita para el cumplimiento de los objetivos de cada uno de los procesos de zona segura.
- **Información externa**: Información de terceros que está bajo nuestra custodia en virtud de nuestro modelo de licenciamiento (por servicio).
- **Información estratégica**: Se requiere para el cumplimiento de los objetivos de cada uno de los procesos.
- **Información confidencial:** La que por sus características solo usuarios con privilegios pueden acceder a ella.
- **Información pública**: Se puede publicar páginas web, redes sociales y medios de comunicación masiva.

**Descripción:**

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **1** | Obtención de la información<br>• Archivos planos<br>• Servicios web<br>• Base de datos | • Todos los colaboradores de ZONA SEGURA S.A.S<br>• clientes | • Acta de recepción de información<br>• TRELLO | No aplica |
| **2** | Clasificación de la información:<br>• Estratégica<br>• Confidencial<br>• Publica | • Gerente innovación y desarrollo<br>• Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | No aplica |
| **3** | Tratamiento:<br>• Confidencial (seguridad)<br>• Estratégicas (seguridad y disponibilidad)<br>• Publica (disponibilidad)<br>• Confidencial (seguridad) integra<br>• Estratégicas (seguridad y disponibilidad) integra<br>• Publica (disponibilidad) integral<br>• Backup interno<br>• Backup externo<br>• Certificados de seguridad<br>• Actualización de dominios<br>• Amazon AWS<br>• Contraseña segura<br>• Cuentas de usuarios internas | • Gerente innovación y desarrollo<br>• Ingeniero de desarrollo<br>• Analista de desarrollo | TRELLO | • Instructivo de Seguridad de<br>• Información Interna y Externa |

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| 4 | • Almacenamiento<br>• Entrega o eliminación | • Gerente innovación y desarrollo<br>• Ingeniero de desarrollo<br>• Analista de desarrollo | • TRELLO<br>• Acta de entrega de la información | No aplica |

*Tabla 5. Descripción del Proceso Mantenimiento y Manejo de Datos de Zona Segura S.A.S.*

**PR-MGI-004 Infraestructura**

**Objetivo**: Brindar los recursos tecnológicos necesarios para la prestación de servicio.

**Alcance:** Desde procesos internos de ZONA SEGURA hasta la información de los clientes.

**Definiciones:**

- **Logs firewall**: Registro de transacciones (ataque, reinicios entre otros).
- **Servicio Asterisk:** Servidor de telecomunicaciones.
- **Hostmonster:** Servicio de hosting que se emplea para publicar la página web de una organización.
- **Dimensionamiento:** Selección de componentes y capacidades para un proyecto y servicio.

**Descripción:**

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| 1 | Dimensionamiento de la infraestructura requerida | • Gerente de innovación y desarrollo<br>• Ingeniero de desarrollo<br>• Analista de desarrollo | No aplica | No aplica |

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **2** | Evaluación de tarifas de infraestructura | • Gerente de innovación y desarrollo<br>• Gerente general | Formato de costos | No aplica |
| **3** | Adquisición de infraestructura | • Gerente de innovación y desarrollo<br>• Gerente general | Órdenes de compra | Instructivo de compras |
| **4** | Pruebas y puestas en producción | • Gerente de innovación y desarrollo<br>• Ingeniero de desarrollo<br>• Analista de desarrollo | Informe de prueba | No aplica |
| **5** | **Monitoreo**<br>• Base de datos<br>• Tamaño (servidor de aplicaciones)<br>• Disponibilidad de internet y telefonía<br>• Servicios de correos<br>• Servicios de web<br>• Servidor Asterisk<br>• Logs firewall<br>• Pago asociado a infraestructura<br>• AWS<br>• Dominio (zonasegura.com.co, avarms.com, brava.com.co)<br>• Certificados digitales<br>• Hostmoster<br>• Línea Santo Domingo | • Gerente de innovación y desarrollo<br>• Ingeniero de desarrollo<br>• Analista de desarrollo | Informes de monitoreo | • Instructivo de compras<br>• Instructivo de Monitoreo<br>• Instructivo de Renovación de Certificado Digital |

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| | • Ampliación de espacio Gmail | | | |

*Tabla 6. Descripción del Proceso Infraestructura de Zona Segura S.A.S.*

**MFCT-003 Desarrollo FCT**

| Nombre del Macroproceso: | DESARROLLO DE FCT |
|---|---|
| Responsable - Líder de Proceso | Gerente de Innovación y Desarrollo |
| Objetivo | Ejecutar la propuesta de servicios mediante la combinación de la oferta de Formación, Consultoría y Tecnología aplicada al Modelo de Aseguramiento Integral del Riesgo. |
| Alcance | Inicia en el proceso de planeación del servicio hasta la puesta en operación de la oferta de Formación, Consultoría y Tecnología en el cliente. |

*Tabla 7. Descripción del Macroproceso Desarrollo FCT de Zona Segura S.A.S.*

**PR-MFCT-003 Tecnología**

**Objetivo**: Apalancar y simplificar el modelo de gestión de riesgos a través de nuestro software AVA RMS® y BRAVA®.

**Alcance:** Desde la creación del cliente y atención de historias de usuario hasta la identificación de mejoras

**Definiciones:**

- **BI (Inteligencia de negocios):** Generación de conocimiento con base a la información.
- **KRI:** Key Risk Indicator (Indicador Clave de Riesgo).

**Descripción:**

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **1** | Socialización de los compromisos contractuales y del cronograma de actividades de cada proyecto | • Gerente de Innovación y Desarrollo<br>• Gerente de Conocimiento | • Cronograma de trabajo<br>• Brief de Riesgos | |
| **2** | Recepción y análisis de requerimiento<br>• Parametrización cliente<br>• Creación esquema organizacional<br>• Inventario de riesgos de la organización<br>• Cargue masivo de histórico de evento | • Gerente de innovación y desarrollo<br>• Analista de procesos<br>• Analista de desarrollo<br>• Ingeniero de desarrollo | • TRELLO<br>• Correo electrónico | • Procedimiento de elaboración de la propuesta<br>• Instructivo de costos |
| **3** | Desarrollo de los requerimientos | • Gerente de innovación y desarrollo<br>• Analista de desarrollo<br>• Ingeniero de desarrollo | • Evaluación de la satisfacción<br>• PQRS<br>• Evaluación de la efectividad y del conocimiento | No aplica |
| **4** | Implantación del desarrollo | • Gerente de innovación y desarrollo<br>• Analista de desarrollo<br>• Ingeniero de desarrollo | No aplica | No aplica |
| **5** | Mantenimiento (Soporte) | • Gerente de innovación y desarrollo<br>• Analista de desarrollo<br>• Ingeniero de desarrollo | No aplica | No aplica |

| ITEM | DESCRIPCIÓN | RESPONSABLE | REGISTROS | DOCUMENTACIÓN DE REFERENCIA |
|---|---|---|---|---|
| **6** | Monitoreo<br>• Usuarios<br>• Informes de **KPI** | • Gerente de innovación y desarrollo<br>• Analista de desarrollo<br>• Ingeniero de desarrollo | Informe de monitoreo de usuario de KPI | No aplica |
| **7** | Identificación de mejoras | ZONA SEGURA | Actas de requerimientos | No aplica |
| **8** | BI (Inteligencia de negocios) | Gerente de innovación y desarrollo | Informe de devolución cliente | Formato de devolución |

*Tabla 8. Descripción del Proceso Tecnología de Zona Segura S.A.S.*

#### 3.3.1.2 Escenarios de riesgo

Los escenarios de riesgos son el lugar de desarrollo de un suceso, es decir, donde se puede materializar uno de los riesgos que la empresa establece como críticos. La definición de estos se hace con base a los procesos que antes fueron establecidos y van directamente relacionados dado que con esto se logra una mejor identificación de los riesgos que deben ser evaluados.

En la tabla 9 se definieron los escenarios de riesgo de Zona Segura S.A.S, los cuales se subdividen en tres tipos:

- Escenarios de infraestructura.
- Escenarios de subproceso.
- Escenarios de actividad.

La definición de los escenarios de riesgo en estos tres tipos permite realizar una mejor identificación de los activos y de los riesgos de la empresa, lo cual es fundamental en el proyecto.

En los escenarios de tipo subproceso se definieron los procesos establecidos en los macroprocesos de Gestión de la Información y Desarrollo FCT. En los escenarios de tipo actividad, quedaron plasmadas cada una de las actividades de los procesos teniendo en cuenta que en cada una de ellas se puede dar la materialización de riesgos. Por último, en los escenarios tipo infraestructura se definieron algunos de los activos en los que podría ocurrir algún incidente que ponga en riesgo la seguridad de la información. Lo anterior se realizó manteniendo su relación con los macroprocesos de la empresa.

| ESCENARIOS DEL ÁREA DE TECNOLOGÍA DE ZONA SEGURA S.A.S | | | |
|---|---|---|---|
| **MACROPROCESO** | **ESCENARIOS DE INFRAESTRUCTURA** | **ESCENARIOS DE SUBPROCESOS** | **ESCENARIOS ACTIVIDADES** |
| **Gestión de la Información** | Servidores | Desarrollo y Actualizaciones | Montaje de servicio AVA RMS y BRAVA |
| | Sede Zona Segura | | Publicar y actualizar la aplicación en Play Store |
| | Equipos de Cómputo | | Historia de usuario |
| | Cableado Eléctrico | | Evaluación de requerimiento |
| | Cableado de Red | | Ingeniería de software |
| | Bases de datos | | Comunicación y satisfacción del cliente |
| | Equipos de Cómputo | Soporte (MAVA) | Historia de usuario |
| | Cableado de Red | | Correo electrónico |
| | Bases de datos | | Llamadas del cliente |
| | Módulos internos | | Actas de reunión |
| | Cableado Eléctrico | | PQRS |
| | Fibra óptica | | Creación de usuario |

| | | | |
|---|---|---|---|
| | Sede Zona Segura | | Creación del esquema organizacional |
| | Correo electrónico | | Parametrización de las sedes |
| | Brava® | | Borrar evento |
| | Discos Duros | | Ajustes del sistema |
| | Apps | | Orientación al usuario |
| | Puntos de Red | | Generar informes |
| | AVARMS® | | Preparación de datos y carga masiva |
| | periféricos de los equipos | | Modificar perfil y permisos de acceso |
| | | | Ejecución y comunicación |
| | | | Medición de la satisfacción del cliente |
| | Servidores | Mantenimiento y Manejo de Datos | Obtención de la información |
| | Web Clouding | | |
| | Equipos de Cómputo | | Clasificación de la información |
| | Sede Zona Segura | | |
| | Discos Duros | | Tratamiento |
| | Correo electrónico | | |
| | Bases de Datos | | Almacenamiento, entrega o eliminación |
| | NAS | | |
| | Servidores | Infraestructura | Dimensionamiento de la infraestructura requerida |
| | Fibra óptica | | |
| | Sede Zona Segura | | Evaluación de costos |
| | Cableado de Red | | Adquisición de infraestructura |
| | UPS | | |
| | Puntos de Red | | Pruebas y puesta en producción |
| | Equipos de Cómputo | | Monitoreo |
| | AVARMS® | Tecnología | Parametrización del cliente |
| | Bases de Datos | | Creación del esquema organizacional |

| | | | |
|---|---|---|---|
| **Desarrollo FCT** | Amazon AWS | | Inventario de riesgos de la organización |
| | | | Carga masiva de histórico de evento |
| | Brava® | | Desarrollo de los requerimientos |
| | | | Implantación del desarrollo |
| | Apps | | Mantenimiento (Soporte) |
| | Equipos de Cómputo | | Usuarios |
| | | | Informe de KPI |
| | Fibra Óptica | | Identificación de mejoras |
| | | | BI ( Inteligencia de negocios) |

*Tabla 9. Escenarios Identificados en Zona Segura para los Procesos Críticos del Área de Tecnología.*

#### 3.3.1.3 Servicios Funcionales

El área de Tecnologías proporciona los siguientes servicios, a sus colaboradores para el desempeño de las funciones en la empresa y a sus clientes como los servicios que provee la compañía:

- Correo Electrónico Institucional
- Desarrollo de aplicaciones para dispositivos móviles
- Desarrollo de aplicaciones Web
- Instalación, configuración y mantenimiento de Software
- Instalación y Mantenimiento del Cableado Estructurado
- Internet de fibra óptica
- Intranet
- VoIP telefonía IP
- Mantenimiento Preventivo y Correctivo a los equipos de cómputo de los colaboradores

- Mantenimiento de servidores
- Redes Inalámbricas
- Soporte a usuarios (MAVA)
- Servicios Web
- Consultoría
- Sistema de alarma monitoreado

La definición de estos servicios ayudó a tener un punto de enfoque para el levantamiento de riesgos de las operaciones tecnológicas de la empresa, debido a que estos pueden verse afectados por la materialización de incidentes en el trabajo del día a día, facilitando así su identificación.

#### 3.3.1.4 Inventario de activos del área de tecnología

La metodología MAGERIT V.3 permite hacer un listado de activos de la empresa, esto con el fin de identificarlos y organizarlos según su tipo. Tener un mayor control de lo que pueda causar pérdidas o daños en la organización, ayuda en la realización de una gestión de riesgos acertada porque al relacionar procesos, escenarios, activos y riesgos en la empresa, se tiene una mejor percepción del entorno.

**Servicios**

- Internet de fibra óptica
- Soporte a usuarios
- Consultoría
- Desarrollo de Software
- Correo electrónico
- Red inalámbrica
- Servicios de aplicaciones web

- Mensajería de aplicativos

**Software**

- Aplicativo AVARMS®
- Aplicativo BRAVA®
- Módulos internos
- Sistemas Operativos
- Antivirus
- Ofimática
- Visual Studio 2017
- SQL Server 2014
- Virtualización
- Tableau 10.5

**Hardware**

- Servidor de aplicación
- Servidor de respaldo
- Servidor de base de datos
- Equipos de cómputo
- Periféricos
- Impresoras
- Escáneres
- Switches
- Routers
- Antenas

**Comunicación**

- Internet de fibra óptica
- Red local
- Red inalámbrica
- Red alámbrica

- Dispositivos móviles

**Soporte de Información**

- Discos duros externos
- NAS
- Memorias USB
- Información en la nube
- Bases de datos
- Carpetas de archivos

**Equipamiento Auxiliar**

- Cableado eléctrico
- UPS

**Instalaciones**

- Los servidores donde se encuentran alojados las aplicaciones en producción y las bases de datos se encuentran en Amazon AWS en Estados Unidos.
- Sede principal de la empresa Zona Segura S.A.S, ubicada en la ciudad de Medellín, Antioquia Colombia, donde se desenvuelven las actividades de soporte técnico a usuarios, desarrollo de software, consultorías, entre otras.

**Personal**

- Gerente de Innovación y Desarrollo
- Ingenieros de Desarrollo
- Analistas de Desarrollo
- Analistas de Soporte a Usuarios
- Analista de Procesos
- Consultores

#### 3.3.1.5 Inventario de Riesgos para los procesos de Gestión de la Información y Desarrollo FCT (Tecnología)

Al igual que con los procesos y escenarios, por medio de sesiones y reuniones de trabajo en equipo de los diferentes miembros del área de Tecnología de Zona Segura S.A.S, donde cada colaborador hizo un listado de riesgos relacionados a su cargo y a las actividades de su día a día, se identificó el siguiente inventario:

1 Acceso no Autorizado a la Información
2 Alteración de la Información (Integridad)
3 Ataque Cibernético (DoS, Virus informático, Hackeo)
4 Caía de los Servidores (Disponibilidad)
5 Caída de Red
6 Corto Circuito
7 Daño de Equipos de Cómputo
8 Errores u Omisiones
9 Falla en la Infraestructura
10 Falla en los Sistemas
11 Falta de Mantenimiento
12 Falta de Suministro de Energía
13 Falta en el Suministro de Internet
14 Fuga de Información Confidencial (Confidencialidad)
15 Hurto
16 Incendio
17 Inundación
18 Pérdida de la Información
19 Personal no Calificado
20 Terremoto

Para ver la relación entre los activos definidos y los riesgos encontrados en el área de tecnología de la empresa, ir al Apéndice M.

### 3.3.1.6 Matriz de riesgo

La matriz de riesgo en este caso 6x4, permite calificar los riesgos por probabilidad y consecuencia de acuerdo con unas tablas de valoración cualitativa y cuantitativa determinadas por la empresa, facilitando llegar a la calificación de una primera matriz que llamaremos inherente, donde los riesgos están en su estado puro.

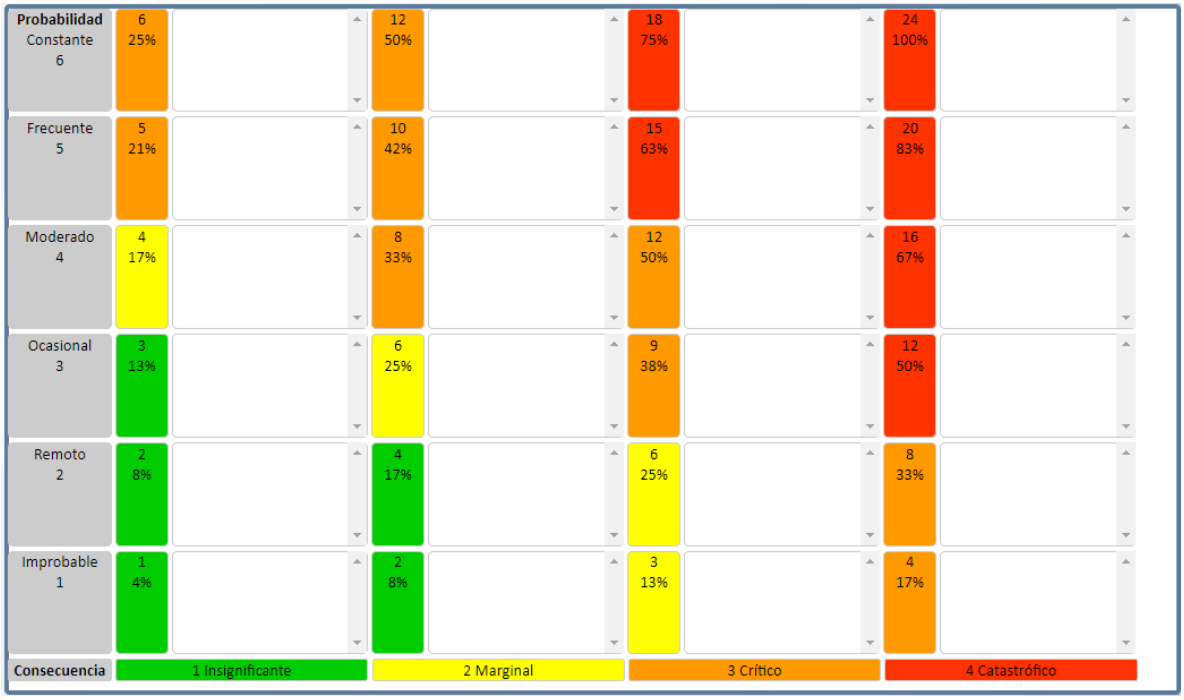



*Figura 6. Matriz de Riesgo por probabilidad y consecuencia definida por la empresa Zona Segura S.A.S.*

*Fuente Software AVARMS®*

La ubicación del riesgo en la matriz, es decir, el nivel de riesgo está determinado por la multiplicación de la probabilidad de ocurrencia por la consecuencia o impacto que genera la materialización del incidente.

**Nivel Riesgo = Probabilidad x Consecuencia**

### 3.3.1.7 Probabilidad de ocurrencia de los riesgos

La probabilidad es la frecuencia con la que se genera la materialización de un riesgo determinado, ya sea en días, semanas, meses o años. Lo anterior lo determina la empresa según su necesidad o apetito del riesgo. En la tabla 10 se puede observar los valores que Zona Segura S.A.S adoptó para la valoración de los riesgos en las matrices.

| PROBABILIDAD | | | | |
|---|---|---|---|---|
| **Valor** | **Tipo** | **Descripción** | **Probabilidad** | **Nivel** |
| 1 | Improbable | Difícil que ocurra | 1 o menos eventos al año | |
| 2 | Remoto | Baja probabilidad de ocurrencia | De 2 a 4 eventos al año | |
| 3 | Ocasional | Limitada probabilidad de ocurrencia | De 5 a 7 eventos al año | |
| 4 | Moderado | Mediana probabilidad de ocurrencia | De 8 a 10 eventos al año | |
| 5 | Frecuente | Significativa probabilidad de ocurrencia | 11 eventos al año | |
| 6 | Constante | Alta probabilidad de ocurrencia | Más de 11 eventos al año | |

*Tabla 10. Definición de criterios de Probabilidad para la evaluación de riesgos de Zona Segura S.A.S.*

### 3.3.1.8 Consecuencia (Magnitud o gravedad de la materialización del riesgo)

La consecuencia es el impacto o daño generado por la materialización de uno o varios riesgos. En la tabla 11 se puede observar la definición que adoptó la empresa Zona Segura S.A.S tanto cualitativa como cuantitativa en una escala del 1 al 4, considerando 1 como insignificante y 4 como catastrófica para la organización.

| CONSECUENCIA | | | | |
|---|---|---|---|---|
| **Valor** | **Tipo** | **Descripción cualitativa** | **Descripción cuantitativa** | **Nivel** |
| 1 | Insignificante | Suspensión momentánea de actividades operacionales (1 hora) | $20.000.000 o menos | |
| 2 | Marginal | Suspensión temporal de actividades operacionales (hasta 8 horas) | entre $20.000.001 y $50.000.000 | |

| | | | | |
|---|---|---|---|---|
| 3 | Crítico | Suspensión parcial de actividades operacionales (hasta 72 horas) | entre $50.000.001 y $250.000.000 | |
| 4 | Catastrófico | Suspensión definitiva de actividades operacionales (mayor a 72 horas) | mayor a $ 250.000.000 | |

*Tabla 11. Definición de criterios de Consecuencia para la evaluación de riesgos de Zona Segura S.A.S.*

### 3.3.1.9 Matriz de riesgo inherente

La matriz inherente permite calificar los riesgos en su estado puro, es decir, sin la utilización de ningún salvaguarda, control, protocolo o instructivo para sobrellevar los incidentes materializados o mitigar el impacto de estos. El fin de realizar el análisis de riesgos inherentes es el de obtener la seguridad de estar contemplando todos los posibles riesgos que podrían llegar a materializarse.

En la tabla 12 se puede observar la calificación de los 20 riesgos encontrados por el área de tecnología de Zona Segura S.A.S, nótese que al valorar un riesgo con probabilidad 3 y consecuencia 4 da como resultado un valor del riesgo igual a 12 (50%), ubicándolo en un nivel de riesgo catastrófico (Rojo), mientras que al valorar un riesgo con probabilidad 4 y consecuencia 3, arroja el mismo valor de riesgo igual a 12 (50%), pero con un nivel de riesgo crítico (Naranja).

| RIESGOS DEL ÁREA DE TECNOLOGÍA DE ZONA SEGURA S.A.S | PROBABILIDAD | CONSECUENCIA | Valor del Riesgo | % |
|---|---|---|---|---|
| Acceso no Autorizado a la Información | 3 | 4 | 12 | 50% |
| Alteración de la Información (Integridad) | 3 | 4 | 12 | 50% |
| Ataque Cibernético (DoS, Virus informático, Hackeo) | 4 | 3 | 12 | 50% |
| Caída de los Servidores (Disponibilidad) | 4 | 4 | 16 | 67% |
| Caída de Red | 3 | 3 | 9 | 38% |
| Corto Circuito | 4 | 3 | 12 | 50% |
| Daño de Equipos de Cómputo | 2 | 2 | 4 | 17% |
| Errores u Omisiones | 2 | 3 | 6 | 25% |
| Falla en la Infraestructura | 3 | 3 | 9 | 38% |
| Falla en los Sistemas de Información | 3 | 3 | 9 | 38% |

| | | | | |
|---|---|---|---|---|
| Falta de Mantenimiento | 3 | 2 | 6 | 25% |
| Falta de Suministro de Energía | 4 | 2 | 8 | 33% |
| Falta en el Suministro de Internet | 3 | 2 | 6 | 25% |
| Fuga de Información Confidencial (Confidencialidad) | 3 | 4 | 12 | 50% |
| Hurto | 3 | 2 | 6 | 25% |
| Incendio | 4 | 4 | 16 | 67% |
| Inundación | 5 | 3 | 15 | 63% |
| Pérdida de la Información (Falta de Backup) | 4 | 4 | 16 | 67% |
| Personal no Calificado | 2 | 3 | 6 | 25% |
| Terremoto | 2 | 4 | 8 | 33% |

*Tabla 12. Calificación de riesgos inherente para el listado de riesgos definido.*

### 3.3.2 Hacer (H)

En el proyecto se alinean los planes de acción y los procedimientos alternativos para el normal funcionamiento de las Tecnologías de Información y Comunicación, cuando alguno de sus servicios se vea afectados por la materialización de un incidente interno o externo a la organización.

Lo anterior considerando 3 acciones: "**Antes**, como un plan de respaldo o de prevención para mitigar los incidentes. **Durante**, como un plan de ejecución en el momento de presentarse el incidente y **Después**, como un plan de recuperación una vez superado el incidente, regresando al estado previo a la contingencia" (Ortiz Anderson, 2017).

En esta etapa se definieron los controles o salvaguardas que se utilizarán para mitigar los riesgos que fueron determinados anteriormente, además, una serie de instructivos y procedimientos que pueden ayudar a la hora de enfrentar un incidente (Ver Apéndices). Los efectos de los salvaguardas en el tratamiento de riesgos pueden ser **preventivos** ayudando a reducir la probabilidad de ocurrencia y de **protección,** los cuales ayudan a aminorar el impacto o consecuencia que conlleva la materialización de riesgos. Esto se

tratará en detalle en la evaluación de eficiencia de los controles y la calificación de matriz residual.

### 3.3.2.1 Eficiencia en las salvaguardas

Las salvaguardas además de su existencia dentro del tratamiento del riesgo, se califican también por su nivel de eficacia ante los riesgos. Este nivel está representado en un rango de 0% a 100%, dependiendo de un punto de vista técnico y operacional de la salvaguarda.

| Factor | Nivel | Significado |
|---|---|---|
| 0% | L0 | Inexistente |
| 20% | L1 | Inicial |
| 40% | L2 | Reproducible, pero intuitivo |
| 60% | L3 | Proceso definido |
| 80% | L4 | Gestionado y medible |
| 100% | L5 | Optimizado |

*Tabla 13. Eficacia y madurez de las salvaguardas. Fuente: MAGERIT V3.*

### 3.3.2.2 Evaluación de salvaguardas utilizadas antes de la materialización de un riesgo

| Como un plan de prevención | | | | |
|---|---|---|---|---|
| **Accesos No Autorizados a la Información** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Concienciar a los usuarios de la red acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables. Contraseñas seguras | **C1** | **L2** | **L4** | **Prevención** |

| | | | | |
|---|---|---|---|---|
| Evitar correos electrónicos que no provengan de un remitente de confianza | **C2** | **L2** | **L4** | **Prevención** |
| Utilizar una conexión Segura | **C3** | **L3** | **L5** | **Prevención** |
| Instalar firewall que evite ingresos desde redes externas hacia la red de la institución. | **C4** | **L3** | **L5** | **Protección** |
| Deshabilitar los servicios que no sean necesarios y verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos. | **C5** | **L2** | **L5** | **Prevención** |
| Sistema de alarma monitoreado | **C6** | **L3** | **L5** | **Protección** |
| Control de acceso | **C7** | **L3** | **L4** | **Protección** |
| **Alteración de la Información (Integridad)** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Contraseñas seguras | **C1** | **L2** | **L4** | **Protección** |
| Cifrado de datos | **C2** | **L0** | **L5** | **Protección** |
| Instalar firewall que evite ingresos desde redes externas hacia la red de la institución. | **C3** | **L3** | **L5** | **Protección** |
| IN-MGI-003-2 instructiva seguridad de información interna y externa. **(Ver Apéndice H)** | **C4** | **L3** | **L5** | **Prevención** |
| **Ataque Cibernético (DoS, Virus informático, Hackeo)** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Instalación de antivirus en equipos de cómputo | **C1** | **L1** | **L4** | **Protección** |
| Instalación de antivirus en los servidores | **C2** | **L3** | **L5** | **Protección** |
| Establecer políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo | **C3** | **L0** | **L4** | **Prevención** |
| Evitar ejecutar programas de origen desconocidos | **C4** | **L2** | **L4** | **Prevención** |
| Impedir el uso de Pendrive, CD a personal no autorizado por el Director de Sistemas | **C5** | **L0** | **L3** | **Prevención** |
| Habilitar la opción de logging (logs) para llevar un control adecuado de las conexiones que existen con dichos routers | **C6** | **L1** | **L4** | **Protección** |
| **Caída de los Servidores (Disponibilidad)** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |

| | | | | |
|---|---|---|---|---|
| Realizar monitoreo constante de los servidores instructivo IN-MGI-004-1 **(Ver en Apéndice A)** | **C1** | **L3** | **L5** | **Prevención** |
| Ventana de manteamiento preventivo Instructivo IN-MGI-003-1 (**Ver Apéndice G)** | **C2** | **L3** | **L5** | **Prevención** |
| Activar alertas de correo electrónicos en los servidores | **C3** | **L3** | **L5** | **Prevención** |
| Alojamiento de los servidores con Amazon AWS que posee una infraestructura robusta | **C4** | **L3** | **L5** | **Protección** |
| Realización de backups alojados en diferentes lugares | **C5** | **L2** | **L5** | **Prevención** |
| **Caída de Red** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Mantenimiento preventivo | **C1** | **L2** | **L4** | **Prevención** |
| Hacer actualizaciones periódicas de inventarios de los equipos de comunicaciones. | **C2** | **L0** | **L4** | **Prevención** |
| Verificar el correcto funcionamiento de las tarjetas de red y dispositivos de comunicaciones como switch, router, Access point | **C3** | **L1** | **L4** | **Prevención** |
| **Corto Circuito** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Desconectar algunos aparatos cuando no se estén utilizando | **C1** | **L0** | **L3** | **Prevención** |
| Alejar aparatos eléctricos de fuentes de agua | **C2** | **L1** | **L3** | **Prevención** |
| Mantener los cables de los aparatos en buen estado | **C3** | **L2** | **L4** | **Prevención** |
| Actualizar correctamente las instalaciones eléctricas y cableado del edificio | **C4** | **L1** | **L4** | **Prevención** |
| Ubicar enchufes y cables apartados de muebles | **C5** | **L1** | **L3** | **Prevención** |
| Si se observa alguna chispa, hay que desconectar y solicitar la revisión a los expertos. | **C6** | **L1** | **L3** | **Protección** |
| No se debe reparar un fusible, sino sustituirlo por uno nuevo. | **C7** | **L2** | **L3** | **Prevención** |
| **Falla en la Infraestructura** | | | | |

| Salvaguardas | | Situación Actual | Se Propone | Tipo |
|---|---|---|---|---|
| Ventana de manteamiento preventivo Instructivo IN-MGI-003-1 **(Ver Apéndice G)** | **C1** | **L3** | **L5** | **Prevención** |
| **Falla en los Sistemas** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Realizar monitoreo constante de los servidores instructivo IN-MGI-004-1 **(Ver Apéndice A)** | **C1** | **L4** | **L5** | **Prevención** |
| Ventana de manteamiento preventivo Instructivo IN-MGI-003-1 **(Ver Apéndice G)** | **C2** | **L3** | **L5** | **Prevención** |
| Instructivo para la renovación del certificado SSL IN-MGI-004-2 **(Ver Apéndice B)** | **C3** | **L3** | **L5** | **Prevención** |
| Instructivo de actualización hosting IN-MGI-004-3 **(Ver Apéndice C)** | **C4** | **L3** | **L5** | **Prevención** |
| **Falta de Suministro de Energía** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Implementación de UPS por cada equipo | **C1** | **L3** | **L5** | **Protección** |
| Mantenimiento preventivo a las UPS con el fin de que soporte por lo menos 15 minutos la operación | **C2** | **L2** | **L4** | **Prevención** |
| Analizar los lugares alternos de trabajo en caso de inundaciones | **C3** | **L2** | **L3** | **Prevención** |
| **Fuga de Información Confidencial (Confidencialidad)** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Implementar política de seguridad en el área de tecnología | **C1** | **L0** | **L5** | **Prevención** |
| Sistema de detección de intrusos para monitorear los accesos o tentativas de accesos a la red | **C2** | **L3** | **L5** | **Protección** |
| Mantener actualizados los sistemas antimalware, firewalls para que sean eficientes | **C3** | **L2** | **L4** | **Prevención** |
| Cerrar los puertos abiertos que no estén siendo utilizados | **C4** | **L3** | **L4** | **Protección** |

| | | | | |
|---|---|---|---|---|
| Promover el uso de contraseñas seguras a los colaboradores de la empresa | **C5** | **L2** | **L3** | **Prevención** |
| IN-MGI-003-2 instructivo seguridad de información interna y externa. **(ver Apéndice H)** | **C6** | **L3** | **L5** | **Prevención** |
| **Incendio** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Sistemas contra incendio | **C1** | **L4** | **L5** | **Protección** |
| Alarma contra incendio | **C2** | **L3** | **L4** | **Protección** |
| Uso y mantenimiento de extintores | **C3** | **L2** | **L4** | **Protección** |
| Rutas de evacuación señalizadas | **C4** | **L4** | **L4** | **Protección** |
| Realizar simulacros contra incendios en la copropiedad | **C5** | **L0** | **L3** | **Protección** |
| **Inundación** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Analizar los lugares alternos de trabajo en caso de inundaciones | **C1** | **L2** | **L3** | **Prevención** |
| Ubicar los equipos en lugares estratégicos, fuera de lugares propensos a roturas de tuberías de agua | **C2** | **L1** | **L4** | **Prevención** |
| Realizar simulacros sobre inundaciones | **C3** | **L0** | **L3** | **Protección** |
| **Pérdida de la Información** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Realización de backups alojados en diferentes lugares | **C1** | **L3** | **L5** | **Prevención** |
| Implementación de UPS en todos los equipos de cómputo | **C2** | **L2** | **L4** | **Protección** |
| IN-MGI-003-2 instructivo seguridad de información interna y externa. **(ver Apéndice H)** | **C3** | **L3** | **L5** | **Prevención** |
| **Terremoto** | | | | |
| **Salvaguardas** | | **Situación Actual** | **Se Propone** | **Tipo** |
| Realización de simulacros periódicamente | **C1** | **L2** | **L4** | **Protección** |
| Rutas de evacuación señalizadas | **C2** | **L2** | **L4** | **Protección** |
| Desarrollo de un plan de emergencias ante desastres | **C3** | **L1** | **L3** | **Protección** |

| | | | | |
|---|---|---|---|---|
| Tener un inventario de implementos necesarios para emergencias como kit de primeros auxilios, linternas, cascos, entre otros. | **C4** | **L0** | **L3** | **Prevención** |

*Tabla 14. Salvaguardas para antes de la materialización de un riesgo.*

### 3.3.2.3 Evaluación de salvaguardas utilizadas durante la materialización de un riesgo

| **Como un plan de Ejecución** | |
|---|---|
| **Accesos No Autorizados a la Información** | |
| **Protocolo** | **Responsable** |
| • Deshabilitar los servicios prioritarios de los sistemas hasta identificar los intrusos. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Verificar todos los puertos por los cuales pudieron haber ingresado los intrusos al sistema de la empresa. | |
| • Analizar el listado de personas que ingresaron al sistema y verificar su información para posibles investigaciones. | |
| • En caso de que la información implicada sea a nivel físico, llamar a las porterías del edificio para informar del incidente y evitar que escape el responsable. | |
| • Verificar grabaciones con el fin de encontrar el intruso. | |
| • De ser necesario llamar a las autoridades pertinentes para la detención del intruso | |
| **Alteración de la Información (Integridad)** | |
| **Protocolo** | **Responsable** |
| • Realizar respaldos de la información para evitar más pérdidas. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Analizar todos los puertos por los que se pudieron haber accedido a la información. | |
| • Validar la magnitud de la alteración. | |
| • Buscar si existe un respaldo para la información perdida y en caso afirmativo, proceder con su restauración. | |
| • Restaurar la información afectada. | |
| **Ataque Cibernético (DoS, Virus informático, Hackeo)** | |

| Protocolo | Responsable |
|---|---|
| • Desconectar los equipos afectados de la red de la empresa.<br>• Realizar respaldos de la información para evitar pérdida de la misma.<br>• Analizar todos los puertos por los que se pudo generar el ataque.<br>• Desplegar medidas para proteger la información.<br>• Si el equipo fue infectado por algún virus, realizarle un análisis con el fin de eliminar el agente causante de la infección.<br>• Revisar la configuración de Routers y Firewalls para detener IPs inválidas, así como también el filtrado de protocolos que no sean necesarios.<br>• Solicitar ayuda al proveedor de servicios de Internet para ayudar a bloquear el tráfico más cercano al origen sin necesidad de que alcance a la empresa.<br>• Tomar acciones como:<br>• Limitar la tasa de tráfico proveniente de un único host.<br>• Limitar el número de conexiones concurrentes al servidor.<br>• Restringir el uso del ancho de banda por aquellos hosts que cometan violaciones.<br>Realizar un monitoreo de las conexiones TCP/UDP que se llevan a cabo en el servidor (permite identificar patrones de ataque). (Catoira, 2012) | Personal encargado del área de tecnología. (Ver tabla 17) |
| **Caída de los Servidores (Disponibilidad)** | |
| **Protocolo** | **Responsable** |
| • Validar si es posible acceder a los sistemas de información alojados en los servidores y además, validar las bases de datos.<br>• Aplicar medidas de contingencia utilizando el servidor de respaldo para que la prestación del servicio no se vea afectada. | Personal encargado del área de tecnología. (Ver tabla 17) |

| | |
|---|---|
| • En caso de ser necesario ir al instructivo IN-MGI-001-1 de implantación de los sistemas. **(ver Apéndice E).** | |
| • Redireccionar los servicios al servidor de respaldo como contingencia mientras se da tratamiento al incidente. | |
| • Tratar de encontrar la fuente del problema para tomar un plan de acción para la recuperación del servidor. | |
| **Caída de Red** | |
| **Protocolo** | **Responsable** |
| • utilizar otras alternativas de comunicación como el celular corporativo para realizar llamadas, contestar correos urgentes, y de ser necesario utilizar los datos móviles del mismo en el computador si este le permite hacerlo. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • En caso de que el daño haya sido grave y se demore en restablecer el servicio de red en la empresa, validar otros lugares alternos donde se pueda trabajar durante la contingencia, puede aplicarse el teletrabajo. | |
| **Corto Circuito** | |
| **Protocolo** | **Responsable** |
| • Si se genera fuego a causa del corto circuito no emplear agua para tratar de apagarlo. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Cortar el suministro eléctrico de las instalaciones. | |
| • Desconectar los demás equipos, servidores, entre otros para evitar más posibles daños. | |
| • Si se propaga fuego a raíz del corto circuito, utilizar los extintores de tipo C para equipos eléctricos. **(Solo por personal calificado)** | |
| • Tratar de continuar la operación desde un lugar alterno a la empresa, aplica el teletrabajo mientras se soluciona el incidente. | |
| **Falla en la Infraestructura** | |
| **Protocolo** | **Responsable** |
| • Validar si es posible continuar con la operación de manera parcial para tomar medidas. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Tratar de corregir la falla en el menor tiempo posible. | |

| | |
|---|---|
| • Si los recursos afectados son críticos y están interfiriendo con la operación de la empresa, buscar el reemplazo para continuar con la operación. | |
| **Falla en los Sistemas** | |
| **Protocolo** | **Responsable** |
| • Validar el tipo de falla que se está presentando y si está afectando a un sistema en específico o a varios sistemas a la vez. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Tratar de corregir la falla en el menor tiempo posible haciendo un análisis del sistema implicado. | |
| • Validar la posibilidad de restablecer el sistema a un punto donde no se había presentado la falla. | |
| • Si es necesario, restablecer el sistema con otros recursos. Ver instructivo IN-MGI-001-1 de implantación de los sistemas. **(ver Apéndice E).** | |
| **Falta de Suministro de Energía** | |
| **Protocolo** | **Responsable** |
| • Dar seguimiento a las UPS para validar si hay que tomar acciones diferentes. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Apagar y desconectar los equipos eléctricos que no sean de vital importancia. | |
| • Comunicarse con el área encargada de la copropiedad para informarse de la magnitud del problema y así analizar qué medidas tomar al respecto. | |
| • En caso de que el incidente se prolongue por más de una hora, analizar la posibilidad de ir a un lugar alterno para continuar con la operación normal mientras se restablece la energía. Puede aplicar el teletrabajo. | |
| **Fuga de Información Confidencial (Confidencialidad)** | |
| **Protocolo** | **Responsable** |
| • Verificar los puertos por los que los intrusos pudieron haber entrado al sistema | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Si la información es física llamar a las porterías para evitar que se lleven la información | |
| • Analizar las cámaras de seguridad para identificar el sospechoso | |
| • Llamar a la Policía Nacional | |

| **Incendio** | |
|---|---|
| **Protocolo** | **Responsable** |
| • Activar la alarma contra incendios | Personal encargado del área de tecnología. (Ver tabla 17)<br><br>Personal de emergencia de la copropiedad donde se encuentra la empresa, encargados de evacuar el edificio. |
| • Si el fuego no tiene grandes proporciones, tratar de apagarlo utilizando los extintores que se encuentran en la empresa (Sólo por personal calificado). | |
| • Llamar a la línea de emergencia de bomberos de la zona. | |
| • Mover a lugares no afectados los aparatos susceptibles al fuego. | |
| • Evacuar las instalaciones si el fuego está fuera de control. | |
| **Inundación** | |
| **Protocolo** | **Responsable** |
| • Desconectar servidores, computadores y demás artefactos eléctricos de la corriente eléctrica. | Personal encargado del área de tecnología. (Ver tabla 17)<br><br>Personal de emergencia de la copropiedad donde se encuentra la empresa, encargados de evacuar el edificio. |
| • Encontrar de donde proviene la inundación y tratar de detener el fluido de agua. | |
| • Mover a lugares no afectados los aparatos susceptibles a la humedad | |
| • Secar las zonas afectadas lo antes posible | |
| **Pérdida de la Información** | |
| **Protocolo** | **Responsable** |
| • Validar la magnitud de la pérdida | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Verificar que las UPS estén debidamente conectadas y encendidas | |
| • Buscar si existe un respaldo para la información perdida y en caso afirmativo, proceder con su restauración. | |
| • Si no existe un backup de la información perdida, validar si se puede devolver el sistema a un punto en el tiempo donde aún estaba la información (Sin perjudicar otra información). | |
| **Terremoto** | |
| **Protocolo** | **Responsable** |
| • Apagar los equipos de cómputo y desconectarlos del fluido eléctrico si el incidente lo permite. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Suspender el fluido eléctrico si es posible. | |

| | |
|---|---|
| • Conservar la calma, buscar las rutas de evacuación y seguirlas sin correr y sin empujar a los demás. | Personal de emergencia de la copropiedad donde se encuentra la empresa, encargados de evacuar el edificio. |
| • Por ningún motivo usar ascensores durante la evacuación. | |
| • En la medida de lo posible abrir las puertas que encuentra a su paso en la ruta de evacuación, con el fin de que algunas personas no queden atrapadas. | |
| • Ir lo antes posible a un punto de encuentro lo más apartado que se pueda de edificaciones altas y cables de alta tensión. | |

*Tabla 15. Salvaguardas durante la materialización de un riesgo.*

### 3.3.2.4 Evaluación de salvaguardas utilizadas después de la materialización de un riesgo

| Como un plan de Recuperación | |
|---|---|
| **Accesos No Autorizados a la Información** | |
| **Protocolo** | **Responsable** |
| • Aplicar acciones correctivas de posibles puertos que utilizaron para ingresar en el sistema de la empresa. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Encontrar el método que se utilizó para efectuar el robo de la información o por donde pudo filtrarse con el fin de realizar los correctivos necesarios para que no vuelva a ocurrir un incidente de este tipo. | |
| • Actualizar sistemas buscando posibles vulnerabilidades para corregirlas. | |
| • Mantener un inventario de toda la documentación e información de la empresa e implementar medidas de seguridad más fuertes. | |
| **Alteración de la Información (Integridad)** | |
| **Protocolo** | **Responsable** |
| • Presentar un informe con el detalle de la información que se vio afectada. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Proceder a realizar la restauración de la información por medio de los backups. | |

| | |
|---|---|
| • Tomar acciones correctivas con el fin de evitar posibles incidentes relacionados. | |
| **Ataque Cibernético (DoS, Virus informático, Hackeo)** | |
| **Protocolo** | **Responsable** |
| • Verificar los archivos infectados con el virus informático para corregir posibles alteraciones | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Aplicar acciones correctivas de posibles puertos que utilizaron para ingresar en el sistema de la empresa | |
| • Corroborar el buen funcionamiento de los equipos de cómputo, servidores, entre otros con el fin de continuar con la operación | |
| **Caída de los Servidores (Disponibilidad)** | |
| **Protocolo** | **Responsable** |
| • Validar en las plataformas el estado de las mismas y de ser posible reanudar el servicio. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • En caso de que el servidor este presentando aun inconvenientes, dejar implementados los servicios en el servidor de respaldo mientras se soluciona el problema. | |
| • IN-MGI-001-1 instructivo de implantación de los sistemas. **(ver Apéndice E).** Utilizarlo en caso de ser necesario, en este se indica paso a paso como restaurar las bases de datos y los sistemas de información que suministra la empresa. | |
| **Caída de Red** | |
| **Protocolo** | **Responsable** |
| • Realizar un análisis de todos los equipos de red y comunicación afectados | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Comprobar conexiones a internet y a la red interna | |
| • Restaurar en el menor tiempo posible la comunicación de los sistemas | |
| • De ser necesario adquirir nuevos equipos en caso de que el daño haya sido grave | |
| • Hacer pruebas para comprobar el correcto funcionamiento de los equipos | |
| **Corto Circuito** | |
| **Protocolo** | **Responsable** |

| | |
|---|---|
| • No conectar y encender ningún equipo hasta que se haya revisado todo el sistema eléctrico y cableado de las instalaciones.<br>• En caso de ser necesario cambiar los tomas afectados, al igual que los cables.<br>• Si el corto circuito provocó un incendio, tomar las medidas definidas para el riesgo de **INCENDIO** definidas en esta misma tabla.<br>• Realizar el respectivo informe de daños causados por el incidente. | Personal encargado del área de tecnología. (Ver tabla 17) |
| **Falla en la Infraestructura** | |
| **Protocolo** | **Responsable** |
| • Evaluación de Daños.<br>• Priorización de Actividades del Plan de Acción.<br>• Ejecución de Actividades.<br>• Evaluación de Resultados. | Personal encargado del área de tecnología. (Ver tabla 17) |
| **Falla en los Sistemas** | |
| **Protocolo** | **Responsable** |
| • Validar que todos los formularios de las aplicaciones estén funcionando correctamente.<br>• Si la aplicación se implanto en otro servidor durante la contingencia, llevar nuevamente la aplicación al servidor de producción.<br>• Dejar documentado el incidente especificando su causa para evitar futuras eventualidades. | Personal encargado del área de tecnología. (Ver tabla 17) |
| **Falta de Suministro de Energía** | |
| **Protocolo** | **Responsable** |
| • Determinar el tiempo máximo para restablecer los servicios que presta la empresa a sus colaboradores y clientes<br>• Determinar la causa por la cual se presentó el incidente y hacer su respectivo registro con el fin de alimentar una matriz de riesgo real y prevenir posibles incidencias del mismo tipo<br>• Notificar el restablecimiento de los servicios tanto a empleados como a clientes<br>• Validar que la planta eléctrica de la copropiedad se encuentre en buen estado para prevenir futuras incidencias de este tipo | Personal encargado del área de tecnología. (Ver tabla 17) |

| | |
|---|---|
| • Verificar que las UPS se encuentren lista para afrontar otra posible incidencia de este tipo | |
| **Fuga de Información Confidencial (Confidencialidad)** | |
| **Protocolo** | **Responsable** |
| • Verificar el nivel de importancia de la información y los problemas legales que podría enfrentar la empresa a causa de este incidente. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Encontrar el método que se utilizó para efectuar el robo de la información o por donde pudo filtrarse con el fin de realizar los correctivos necesarios para que no vuelva a ocurrir un incidente de este tipo. | |
| • Actualizar sistemas buscando posibles vulnerabilidades para corregirlas. | |
| • Mantener un inventario de toda la documentación e información de la empresa e implementar medidas de seguridad más fuertes. | |
| **Incendio** | |
| **Protocolo** | **Responsable** |
| • Realizar un inventario de equipos afectados, indicando el nivel de daño de cada uno | Personal encargado del área de tecnología. (Ver tabla 17)<br><br>Personal de emergencia de la copropiedad donde se encuentra la empresa, encargados de evacuar el edificio. |
| • Hacer una evaluación de daños en la infraestructura física, redes eléctricas, entre otros | |
| • Reanudar con la operación lo antes posible ya sea en otras instalaciones o por medio de teletrabajo | |
| • Limpiar el área afectada por el incendio definiendo el personal encargado de esta labor | |
| • En caso de que haya personal afectado que se encuentra incapacitado, tomar las medidas necesarias para que la operación no se detenga utilizando la documentación existente del cargo de la persona afectada | |
| • Reanudar los servicios implementando respaldos de ser necesario | |
| • Recargar los extintores utilizados en el incidente para que queden listos para cualquier otra eventualidad. | |
| **Inundación** | |
| **Protocolo** | **Responsable** |

| | |
|---|---|
| • Secar el área afectada por el agua con el fin de limpiar y tratar de restablecer la operación en el menor tiempo posible | |
| • No utilizar o encender los equipos eléctricos hasta que se haya secado correctamente el área afectada y un experto revise las instalaciones eléctricas | |
| • Verificar los daños causados por el agua desde equipos de cómputo, servidores, documentación física, entre otros | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Hacer un informe con las pérdidas encontradas en la empresa | Personal de emergencia de la copropiedad donde se encuentra la empresa, encargados de evacuar el edificio. |
| • Si la afectación por el agua es grande, buscar un lugar alterno donde continuar con la operación mientras se adecuan las instalaciones nuevamente | |
| • Restaurar los respaldos de información en caso de ser necesario | |
| **Pérdida de la Información** | |
| **Protocolo** | **Responsable** |
| • Verificar si la información perdida es vital para la empresa y puede generar repercusiones graves para la misma. | |
| • Validar los backups con el fin de encontrar la información que se pudo haber perdido. | |
| • Reforzar posibles vulnerabilidades de los sistemas y de la red. | Personal encargado del área de tecnología. (Ver tabla 17) |
| • Encontrar el cómo se perdió la información con el fin de aplicar correctivos. | |
| • Reforzar la implementación de backups en la empresa, tomando la información como el principal activo de la compañía. | |
| **Terremoto** | |
| **Protocolo** | **Responsable** |
| • Estar alerta a posibles replicas que puedan presentarse | |
| • Prestar primeros auxilios a quien lo necesite o llamar a emergencias para que llegue personal calificado | |
| • Realizar un inventario de los equipos, documentos y todos los recursos evaluando su estado y su funcionalidad | Personal encargado del área de tecnología. (Ver tabla 17) |

| | |
|---|---|
| • Verificar que todo el personal se encuentre a salvo | Personal de emergencia de la copropiedad donde se encuentra la empresa, encargados de evacuar el edificio. |
| • Evitar entrar a las instalaciones sin la verificación de que los muros, techos, tuberías y demás infraestructura del edificio afectado se encuentre estable para ser habitado nuevamente | |
| • Tratar de adecuar las instalaciones limpiando las zonas afectadas por el sismo | |
| • Mirar la posibilidad de restablecer servicios verificando los servidores, los equipos de cómputo, los servicios de comunicación, cableado eléctrico, entre otros | |
| • En caso de ser imposible el acceso a las instalaciones de la empresa, implementar un plan de acción para ubicar una sede alterna donde trabajar o realizar teletrabajo mientras se encuentra otra solución posible | |

*Tabla 16. Salvaguardas después de la materialización de un riesgo.*

**NOTA:** Para todos y cada uno de los incidentes que ocurran en la empresa en el área de tecnología, se debe realizar un reporte donde se relacione el proceso, escenario y riesgo materializado con su respectiva descripción, fecha y hora, y un estimado de la pérdida generada por el incidente. Este reporte les llegará a los responsables del proceso para tomar las medidas necesarias contra el incidente. Esto a su vez, ayudará a la empresa a tener una matriz Real donde se podrá visualizar las afectaciones en el tiempo con el fin de mejorar controles y de tomar acciones correctivas y de mejora.

#### 3.3.2.5 Información de contacto

En la tabla 17 se encuentra la información de contacto del personal encargado de los procesos de la gerencia de innovación y desarrollo, que es la encargada del área de

tecnología de Zona Segura S.A.S y la cual estará a cargo de cualquier eventualidad relacionada con lo planificado en este proyecto.

| NOMBRES | CARGO | CORREO ELECTRÓNICO | TELÉFONO |
|---|---|---|---|
| Juan Manuel Saumet Galvis | Gerente de Innovación y Desarrollo | jsaumet@zonasegura.com.co | 4442098 ext. 105 |
| Jonathan Perez Vivas | Ingeniero de Desarrollo | jperez@zonasegura.com.co | 4442098 ext. 102 |
| Carlos Alberto Carvajal Pérez | Analista de Desarrollo | ccarvajal@zonasegura.com.co | 4442098 ext. 103 |
| Soporte a usuarios | Analista de Soporte a Usuarios | soporte@zonasegura.com.co | 4442098 ext. 101 |
| Angélica María Henao Gutiérrez | Analista de Procesos | ahenao@zonasegura.com.co | 4442098 ext. 104 |

*Tabla 17. Información de contacto del personal responsable de poner en marcha el Plan de Contingencia.*

#### 3.3.2.6 Control de cambios

Es necesario manejar un control para los cambios que se realicen al plan de contingencia en general o a uno de sus instructivos o procedimientos en específico, por lo tanto, se diseñó el siguiente formato de control de cambios, el cual se puede observar en la tabla 18.

| CONTROL DE CAMBIOS | | | | |
|---|---|---|---|---|
| N° | VERSIÓN INICIAL | NATURALEZA DEL CAMBIO | IDENTIFICACIÓN DEL CAMBIO | VERSIÓN FINAL |
| 1 | 1.0 | Nuevo | No aplica | Actual |
| | | | | |

*Tabla 18. Formato para el control de cambios de todos los procedimientos, instructivos y del plan mismo.*

### 3.3.3 Verificación (V)

En esta fase se realizó una revisión en general de todo el plan de contingencia, se midió la eficiencia de las salvaguardas definas en la etapa del **Hacer (H)** con el fin de determinar una

matriz residual o controlada donde los riesgos están mitigados, mostrando así, el estado actual de riesgos de la empresa. Luego de tener la relación entre los procesos críticos afectados, escenarios, activos y riesgos involucrados en la operación de servicios tecnológicos de Zona Segura S.A.S, se realizó un simulacro a manera de prueba, validando el funcionamiento de algunos de los instructivos definidos anteriormente.

#### 3.3.3.1 Evaluación de eficiencia de los controles

La evaluación de la eficiencia de los controles se realizó tomando las salvaguardas definidas anteriormente en la tabla 14, donde se establecieron las que tenían un efecto de prevención ante los riesgos y las que tenían un efecto de protección. En la tabla 19 se puede visualizar el nivel de eficiencia de cada uno de los controles por riesgo, el cual se determinó a través de la tabla 13 anteriormente definida, donde se especifica el nivel de validez de los controles para sacar un promedio y un porcentaje por riesgo y tipo.

| RIESGOS | Valor del Riesgo | Controles | Nivel de Eficiencia | Tipo | Promedio Eficiencia | % Eficiencia |
|---|---|---|---|---|---|---|
| Acceso no Autorizado a la Información | 12 | C1 | 2 | Prevención | 2,25 | 45% |
| | | C2 | 2 | | | |
| | | C3 | 3 | | | |
| | | C5 | 2 | | | |
| | | C4 | 3 | Protección | 3 | 60% |
| | | C6 | 3 | | | |
| | | C7 | 3 | | | |
| Alteración de la Información (Integridad) | 12 | C1 | 2 | Protección | 1,6 | 32% |
| | | C2 | 0 | | | |
| | | C3 | 3 | | | |
| | | C4 | 3 | Prevención | 3 | 60% |
| Ataque Cibernético (DoS, Virus informático, Hackeo) | 12 | C1 | 1 | Protección | 1,7 | 34% |
| | | C2 | 3 | | | |
| | | C6 | 1 | | | |
| | | C4 | 2 | Prevención | 0,66 | 13,2% |
| | | C5 | 0 | | | |
| | | C3 | 0 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Caída de los Servidores (Disponibilidad) | 16 | C1 | 3 | Prevención | 2,75 | 55% |
| | | C2 | 3 | | | |
| | | C3 | 3 | | | |
| | | C5 | 2 | | | |
| | | C4 | 3 | Protección | 3 | 60% |
| Caída de Red | 9 | C1 | 2 | Prevención | 1 | 20% |
| | | C2 | 0 | | | |
| | | C3 | 1 | | | |
| Corto Circuito | 12 | C1 | 0 | Prevención | 1,17 | 23,4% |
| | | C2 | 1 | | | |
| | | C3 | 2 | | | |
| | | C4 | 1 | | | |
| | | C5 | 1 | | | |
| | | C7 | 2 | | | |
| | | C6 | 1 | Protección | 1 | 20% |
| Falla en la Infraestructura | 9 | C1 | 3 | Prevención | 3 | 60% |
| Falla en los Sistemas | 9 | C1 | 4 | Prevención | 3,25 | 65% |
| | | C2 | 3 | | | |
| | | C3 | 3 | | | |
| | | C4 | 3 | | | |
| Falta de Suministro de Energía | 8 | C1 | 3 | Protección | 3 | 60% |
| | | C2 | 2 | Prevención | 2 | 40% |
| | | C3 | 2 | | | |
| Fuga de Información Confidencial (Confidencialidad) | 12 | C1 | 0 | Prevención | 2 | 40% |
| | | C3 | 3 | | | |
| | | C6 | 3 | | | |
| | | C5 | 2 | | | |
| | | C4 | 3 | Protección | 3 | 60% |
| | | C2 | 3 | | | |
| Incendio | 16 | C1 | 4 | Protección | 2,6 | 52% |
| | | C2 | 3 | | | |
| | | C3 | 2 | | | |
| | | C4 | 4 | | | |
| | | C5 | 0 | | | |
| Inundación | 15 | C1 | 2 | Prevención | 1,5 | 30% |
| | | C2 | 1 | | | |
| | | C3 | 0 | Protección | 1 | 20% |

| | | | | | | |
|---|---|---|---|---|---|---|
| Pérdida de la Información (Falta de Backup) | 16 | C1 | 3 | Prevención | 3 | 60% |
| | | C3 | 3 | | | |
| | | C2 | 2 | Protección | 2 | 40% |
| Terremoto | 8 | C1 | 2 | Protección | 1,67 | 33,4% |
| | | C2 | 2 | | | |
| | | C3 | 1 | | | |
| | | C4 | 0 | Prevención | 0 | 0% |

*Tabla 19. Eficiencia de los controles definidos para la mitigación de riesgos.*

### 3.3.3.2 Matriz de riesgo residual o controlada

Habiendo definido los controles y determinado el porcentaje de eficiencia de cada uno de ellos, se puede pasar a un estado del riesgo que se llama residual. Esta metodología se basa en la ISO 27001:2013 donde se explica que esta fase es el estado resultante del riesgo habiéndolo tratado con los controles antes especificados, dando un estado más real de la situación en cuanto a riesgos de la empresa.

En la tabla 20 se puede observar en la primera columna el riesgo al que se le está dando tratamiento; en la segunda columna está situada la calificación inicial o inherente, la cual fue realizada en la etapa de la **Planificación (P)**. Luego, la tercera columna da referencia de los controles definidos anteriormente en la tabla 14, siguiendo con su respectivo tipo y su porcentaje de eficiencia promediado. En la última columna está situada la calificación residual donde se realizó el cálculo de la probabilidad y consecuencia de los riesgos después de haber sido mitigados con controles.

Este cálculo se basa en la norma ISO 27001:2013 donde sugiere que el nivel de riesgo residual es igual al riesgo inherente dividido por el promedio de eficacia de los controles:

**Riesgo residual = Riesgo inherente / eficacia de los controles**

En la empresa Zona Segura S.A.S se tomó como referencia esta norma para realizar la calificación de riesgo residual, adoptando el siguiente modelo:

**PR = PI - ((PE * PI) / 100)**

**CR = CI - ((PE * CI) / 100)**

**RR = PR * CR**

Donde,

- PI = Probabilidad de ocurrencia inherente
- PR = Probabilidad de ocurrencia residual
- CI = Consecuencia o impacto inherente
- CR = Consecuencia o impacto residual
- PE = Porcentaje de eficiencia de los controles
- RR = Nivel de riesgo residual

| RIESGOS | Calificación Riesgo Inherente | | | Controles | Tipo | % Eficiencia | Calificación Riesgo Residual | |
|---|---|---|---|---|---|---|---|---|
| Acceso no Autorizado a la Información | 12 | Probabilidad | 3 | C1 | Prevención | 45% | 2 | 4 |
| | | | | C2 | | | | |
| | | | | C3 | | | | |
| | | | | C5 | | | | |
| | | Consecuencia | 4 | C4 | Protección | 60% | 2 | |
| | | | | C6 | | | | |
| | | | | C7 | | | | |
| Alteración de la Información (Integridad) | 12 | Consecuencia | 4 | C1 | Protección | 32% | 3 | 3 |
| | | | | C2 | | | | |
| | | | | C3 | | | | |
| | | Probabilidad | 3 | C4 | Prevención | 60% | 1 | |
| Ataque Cibernético (DoS, Virus | 12 | Consecuencia | 3 | C1 | Protección | 34% | 2 | 6 |
| | | | | C2 | | | | |
| | | | | C6 | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| informático, Hackeo) | | Probabilidad | 4 | C4<br>C5<br>C3 | Prevención | 13% | 3 | |
| Caída de los Servidores (Disponibilidad) | 16 | Probabilidad | 4 | C1<br>C2<br>C3<br>C5 | Prevención | 55% | 2 | 4 |
| | | Consecuencia | 4 | C4 | Protección | 60% | 2 | |
| Caída de Red | 9 | Probabilidad | 3 | C1<br>C2<br>C3 | Prevención | 20% | 2 | 6 |
| | | Consecuencia | 3 | No | Protección | 0% | 3 | |
| Corto Circuito | 12 | Probabilidad | 4 | C1<br>C2<br>C3<br>C4<br>C5<br>C7 | Prevención | 23% | 3 | 6 |
| | | Consecuencia | 3 | C6 | Protección | 20% | 2 | |
| Falla en la Infraestructura | 9 | Probabilidad | 3 | C1 | Prevención | 60% | 1 | 3 |
| | | Consecuencia | 3 | No | Protección | 0% | 3 | |
| Falla en los Sistemas | 9 | Probabilidad | 3 | C1<br>C2<br>C3<br>C4 | Prevención | 65% | 1 | 3 |
| | | Consecuencia | 3 | No | Protección | 0% | 3 | |
| Falta de Suministro de Energía | 8 | Consecuencia | 2 | C1 | Protección | 60% | 1 | 2 |
| | | Probabilidad | 4 | C2<br>C3 | Prevención | 40% | 2 | |
| Fuga de Información Confidencial | 12 | Probabilidad | 3 | C1<br>C3<br>C6<br>C5 | Prevención | 40% | 2 | 4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| (Confidencialidad) | | Consecuencia | 4 | C4<br>C2 | Protección | 60% | 2 | |
| Incendio | 16 | Consecuencia | 4 | C1<br>C2<br>C3<br>C4<br>C5 | Protección | 52% | 2 | 8 |
| | | Probabilidad | 4 | No | Prevención | 0% | 4 | |
| Inundación | 15 | Probabilidad | 5 | C1<br>C2 | Prevención | 30% | 4 | 8 |
| | | Consecuencia | 3 | C3 | Protección | 20% | 2 | |
| Pérdida de la Información (Falta de Backup) | 16 | Probabilidad | 4 | C1<br>C3 | Prevención | 60% | 2 | 4 |
| | | Consecuencia | 4 | C2 | Protección | 40% | 2 | |
| Terremoto | 8 | Consecuencia | 4 | C1<br>C2<br>C3 | Protección | 33% | 3 | 6 |
| | | Probabilidad | 2 | C4 | Prevención | 0% | 2 | |

*Tabla 20. Valoración de Riesgo Residual, basado en ISO 27001:2013.*

### 3.3.3.3 Simulacro

Para garantizar que toda la etapa de la **Planificación (P)** y del **Hacer (H)** se consolidó de manera acertada, fue necesario realizar pruebas en un ambiente controlado donde se tomó partes específicas del Plan de contingencia, con el objetivo de validar la efectividad de los procedimientos e instructivos consignados en el plan. Esto a su vez, permitió probar las habilidades de coordinación y de trabajo en equipo del personal asignado para afrontar las contingencias.

La realización de estas pruebas tuvo el consentimiento de la empresa, fueron desarrolladas en sus instalaciones y en un día no laboral, con el fin de no interferir con las actividades

habituales de la compañía. Además del día, se tuvo en cuenta un horario de poca concurrencia por parte de los clientes para evitar posibles inconvenientes.

**Encargados del Simulacro**

| NOMBRES | CARGO | Responsabilidad |
|---|---|---|
| Carlos Alberto Carvajal Pérez | Analista de Desarrollo | Ejecución |
| Jonathan Perez Vivas | Ingeniero de Desarrollo | Supervición |

*Tabla 21. Personal a cargo del simulacro.*

En la primera prueba se simularon fallas en el servidor de aplicación, donde se encuentran alojadas las aplicaciones que proporciona Zona Segura S.A.S a sus clientes. La prueba se hizo específicamente a la aplicación BRAVA®, la cual maneja el proceso de seguridad física a nivel nacional de diferentes empresas. Esta cuenta con una versión web y una aplicación móvil que se utiliza para realizar reportes, con los cuales a través de graficas y estadísticas, los directivos pueden tomar decisiones para sus compañías.

Se asume que la plataforma no está permitiendo ingresar, por lo que no es posible realizar la reportaría habitual. También se asume que no es un daño del servidor de aplicación considerando que las demás aplicaciones continúan operativas. Por lo tanto, se debe entrar a validar únicamente lo que sucede con el sistema BRAVA® y de momento no es necesario configurar un nuevo servidor para su operación.

Cabe aclarar que se parte del hecho de que existen los backups necesarios para la restauración del sistema en caso de que sea necesario y de que existe el instructivo IN-MGI-001-1 (Ver Apéndice E), el cual nos permite hacer la implantación parcial o completa de los servicios de Zona Segura S.A.S.

Se valida en los navegadores de internet que se pueda acceder a la aplicación, pero se encuentra con el siguiente mensaje de error (Ver Figura 7).

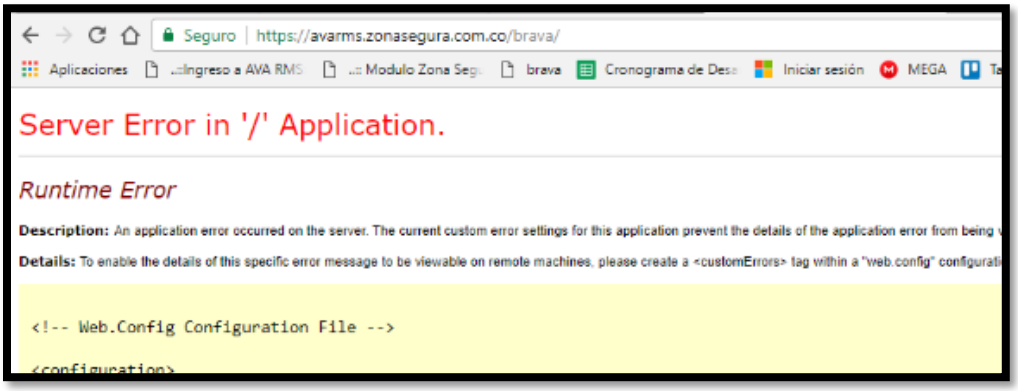



*Figura 7. Inconveniente con la aplicación BRAVA®. Fuente: (autor).*

En la etapa del **Hacer (H)** se crearon una serie de salvaguardas para antes, durante y después de un incidente, por lo que este escenario indica que las salvaguardas preventivas fallaron o no fueron suficientes para impedir la materialización del riesgo y es momento de poner en marcha las estrategias definidas para ejecutar durante el incidente con el fin de darle solución lo antes posible.

- Validar el tipo de falla que se está presentando y si está afectando a un sistema en específico o a varios sistemas a la vez.
- Tratar de corregir la falla en el menor tiempo posible haciendo un análisis del sistema implicado.
- Validar la posibilidad de restablecer el sistema a un punto donde no se había presentado la falla.
- Si es necesario, restablecer el sistema con otros recursos. Ver instructivo IN-MGI-001-1 de implantación de los sistemas. (Ver Apéndice E).

Siguiendo los pasos del instructivo IN-MGI-001-1:

Se ingresó al Server Manager para adicionar algunas extensiones. Se ingresó a la opción Features y luego se presionó en Add-Features para seleccionar la opción IIS Server extensión.

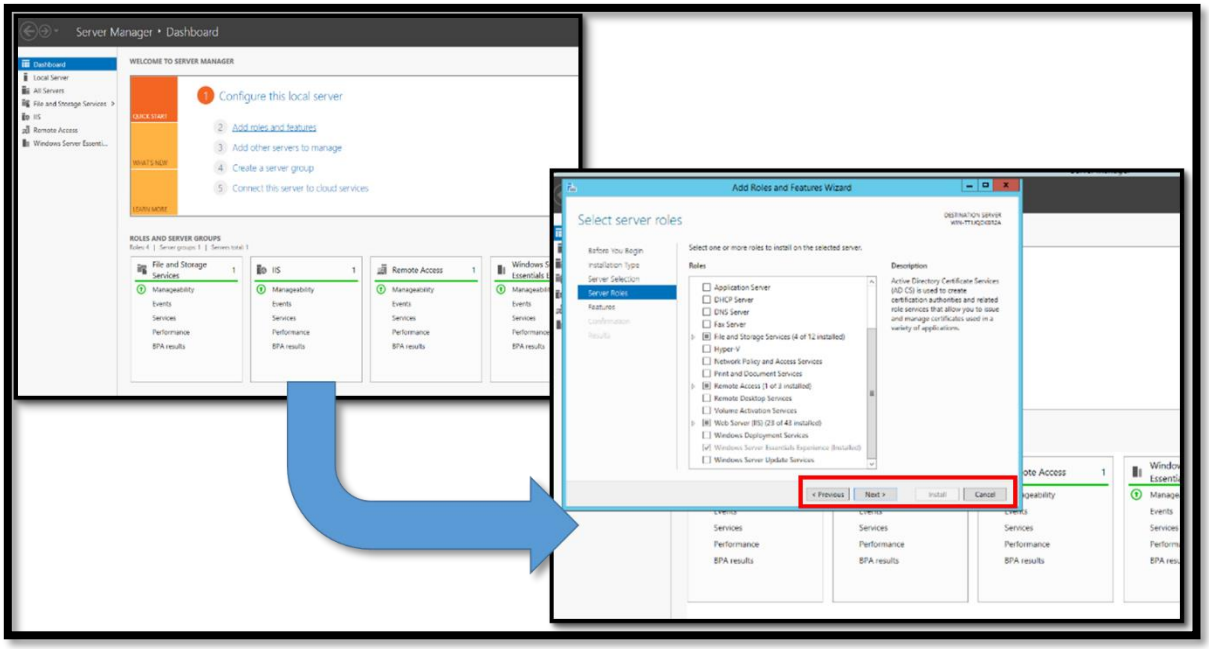



*Figura 8. Configuración Server Manager. Fuente: (autor).*

Luego se agregó un grupo de aplicación para FRAMEWORK 4.5 como se puede observar en la figura 9.

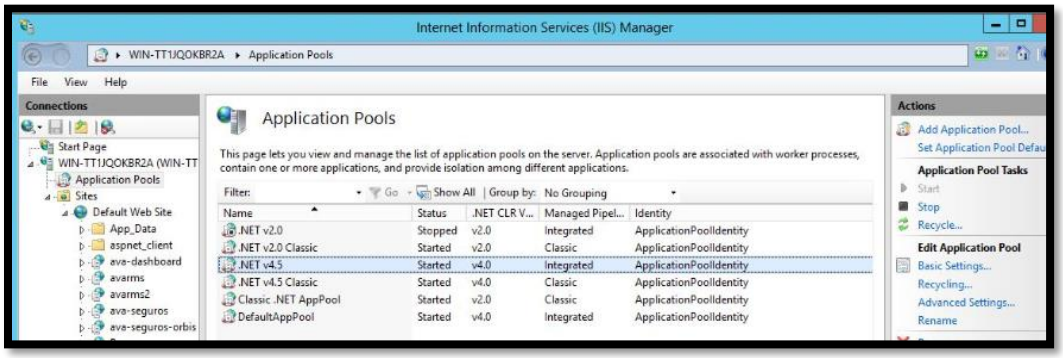



*Figura 9. Configuración del Internet Information Services (IIS). Fuente: (autor).*

Se añadieron excepciones al FIREWALL de los protocolos y puertos para el SQL server, SMTP e Internet.

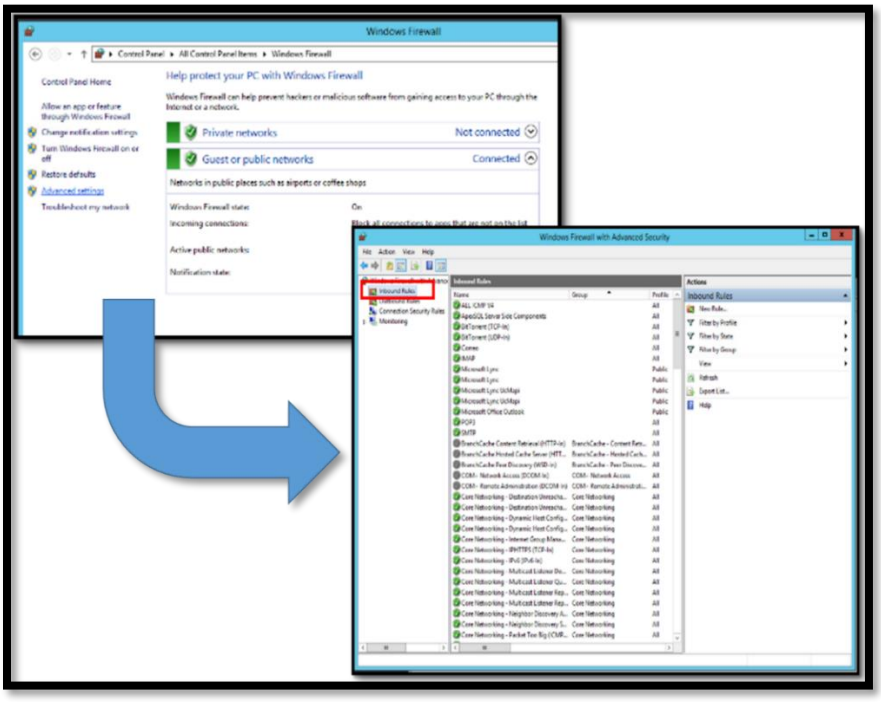



*Figura 10. Configuración del FIREWALL. Fuente: (autor).*

Se tomó el archivo del sitio web para Subirlo al servidor en la ruta **C:\inetpub\wwwroot**

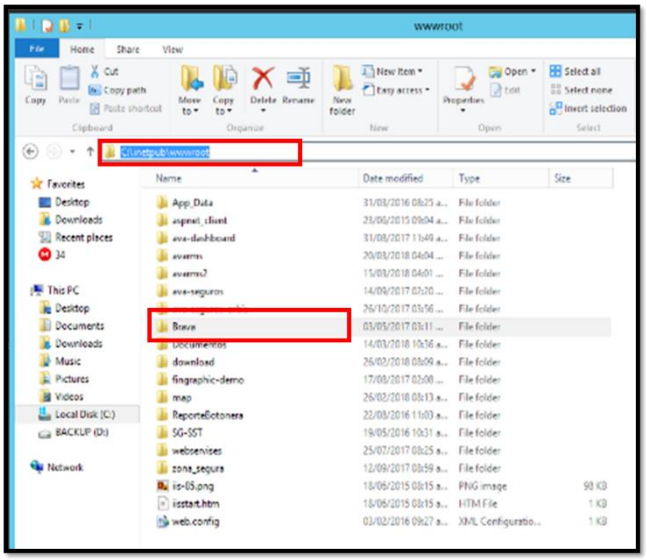



*Figura 11. Subir el archivo del sitio web al servidor. Fuente: (autor).*

Se prosiguió Ingresando al **IIS,** en el panel de conexiones se desplegó el árbol del servidor y luego la carpeta **SITES,** la carpeta **Default web sites** y en la carpeta BRAVA se le dio clic derecho en ella para convertirla en aplicación.

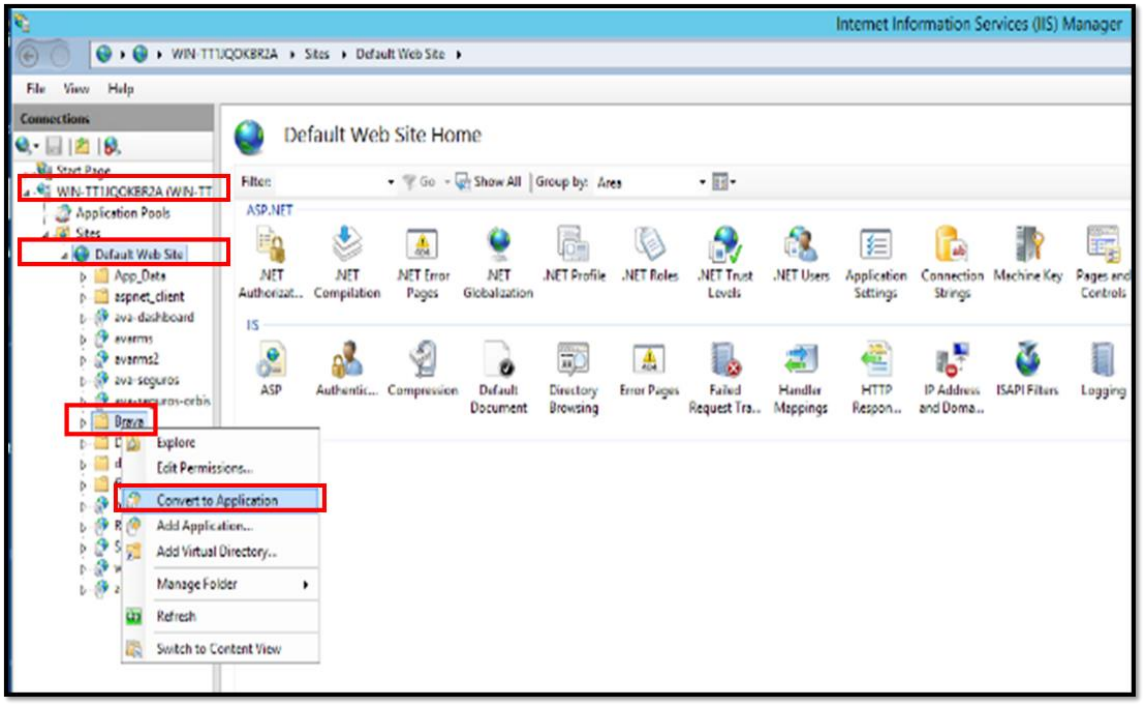



*Figura 12. Convertir en aplicación el sitio web. Fuente: (autor).*

En el menú de opciones del sitio **BRAVA HOME** se hizo doble clic en la opción **Default Document**, luego en el menú **Actions** en la opción **ADD** y se escribió el nombre del formulario inicial (Login.aspx). Se abrió un navegador de internet y validando nuevamente el sitio web respondió satisfactoriamente. Lo siguiente fue ingresar en la aplicación a realizar pruebas de los formularios.

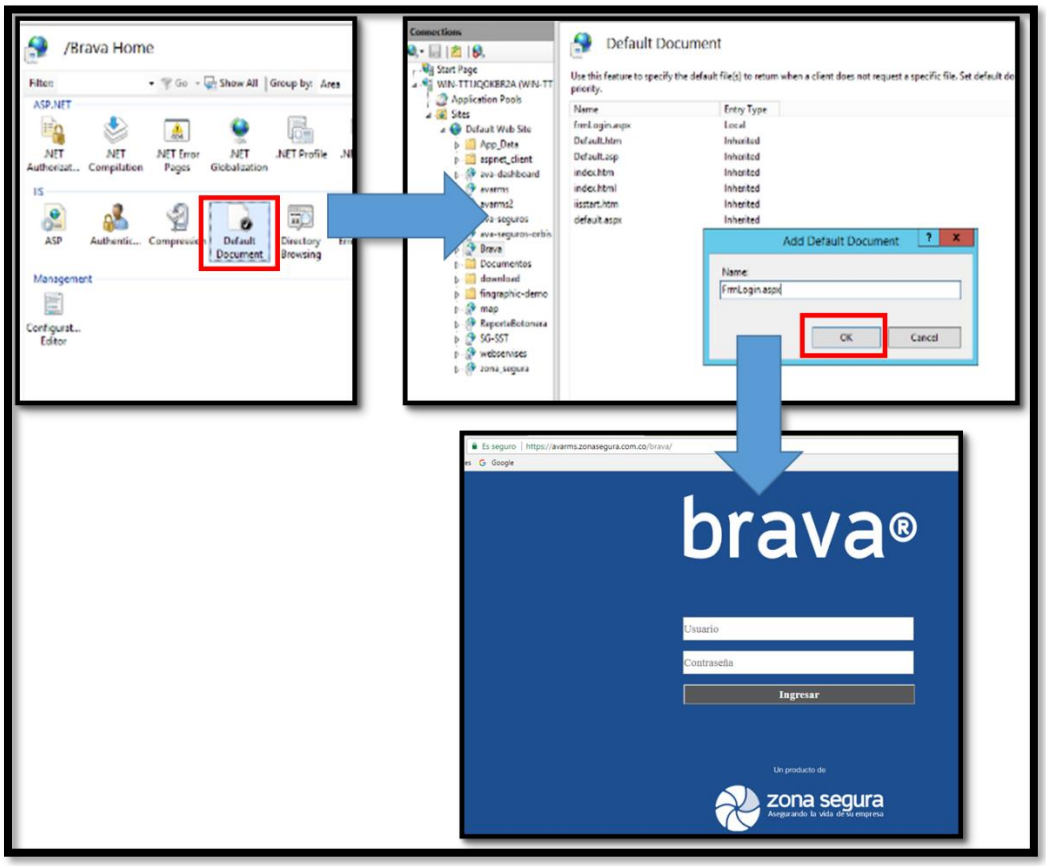



*Figura 13. Ultimas configuraciones y validación de ingreso a la aplicación BRAVA®. Fuente: (autor).*

En la segunda prueba se buscó un escenario enfocado a la afectación de las bases de datos de la empresa, lo cual es uno de los contextos más críticos de la compañía ya que en ellas reposan tanto información propia de la empresa como información de sus clientes. Por ello, en esta simulación se tomó una instancia de base de datos que existe para pruebas con el fin de no interrumpir la disponibilidad del servicio durante la prueba.

Se realizaron una serie de consultas de grandes volúmenes de información a la base de datos y como esta no cuenta con grandes recursos asignados, se logró llegar al escenario deseado (Ver figura 14). Lo anterior generó la activación de una alarma que llega al correo electrónico del ingeniero y el analista de desarrollo cuando el uso de la CPU de la instancia está por encima de 90% durante 60 segundos (Ver figura 15).

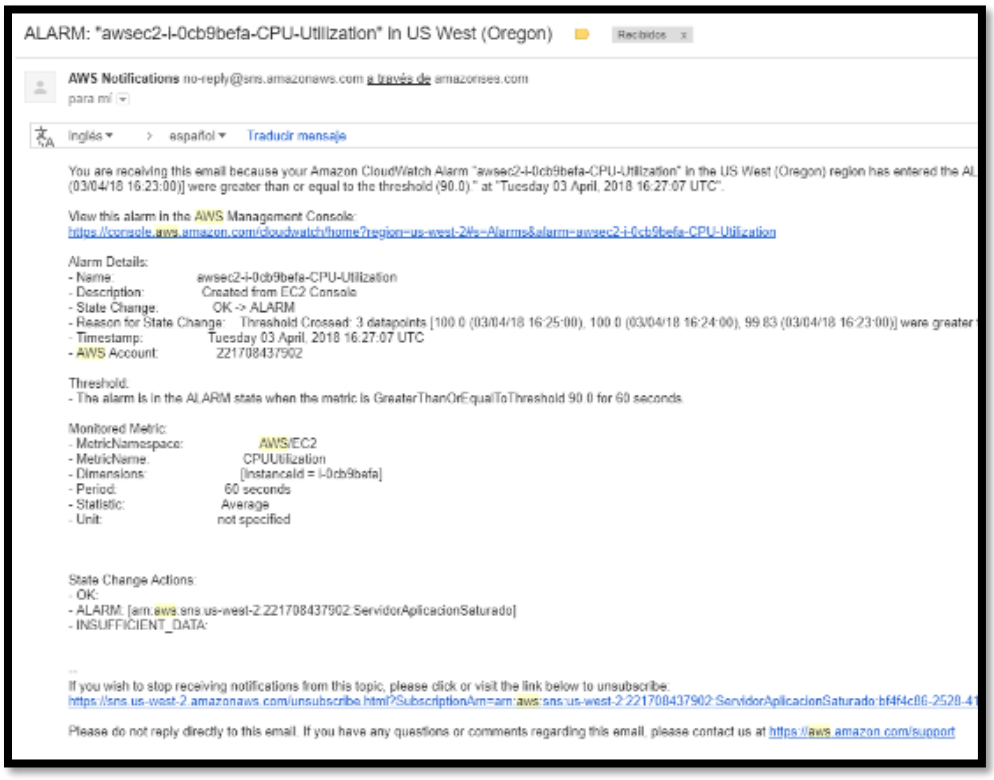



*Figura 14. Alerta del servidor indicando su estado por correo electrónico. Fuente: (autor).*

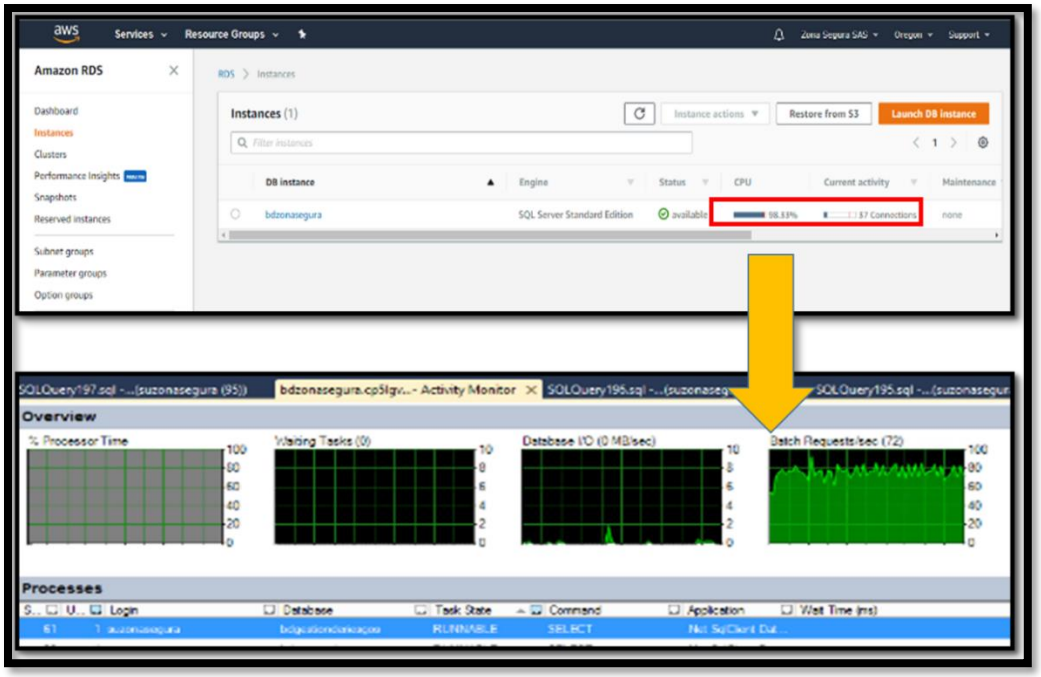



*Figura 15. Instancia de la base de datos y monitor del SQL Server. Fuente: (autor).*

Como la base de datos está alojada en las plataformas de Amazon AWS, es raro que ocurra un incidente que afecte gravemente las instancias de las bases de datos, pero en caso de que algo ocurriese la plataforma brinda diversas formas para dar solución al problema, una de ellas es la que se utilizó en esta simulación, donde siguiendo los procedimientos propuesto en la etapa del **Hacer (H),** se seleccionó la opción **Reboot** de la base de datos.

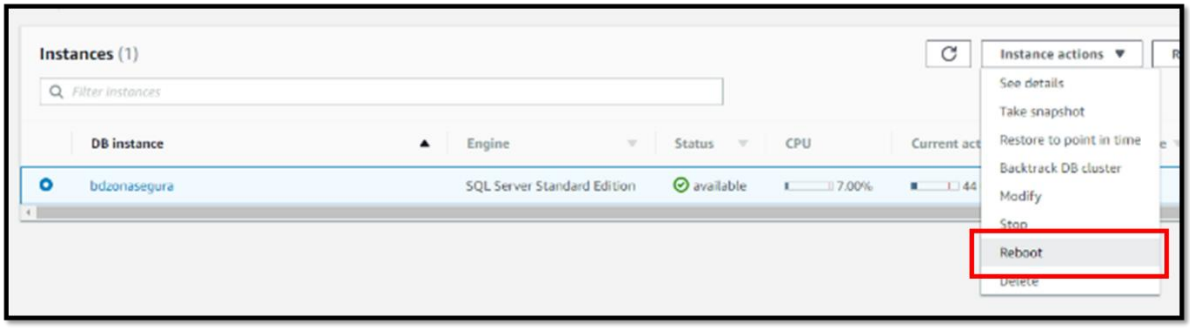



*Figura 16. Reiniciar la instancia de la base de datos. Fuente: (autor).*

Estado óptimo de la instancia de base de datos luego de haberla reiniciado (Figura 17)

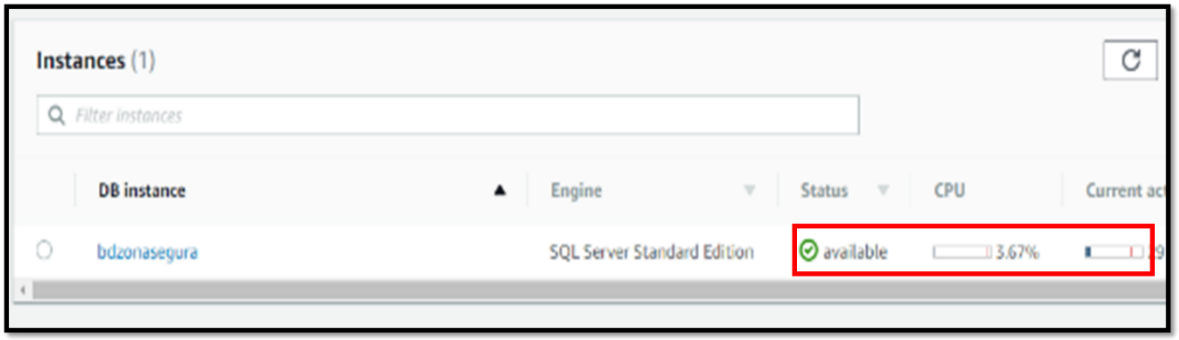



*Figura 17. Estado óptimo de la base de datos. Fuente: (autor).*

También, de ser necesario la plataforma brinda otras opciones como la de restaurar la base de datos a un punto específico en el tiempo, donde aún no se haya presentado el incidente (Ver Figura 18) y la utilización de Snapshots (ver figura 19), actualizados cada día de manera incremental.

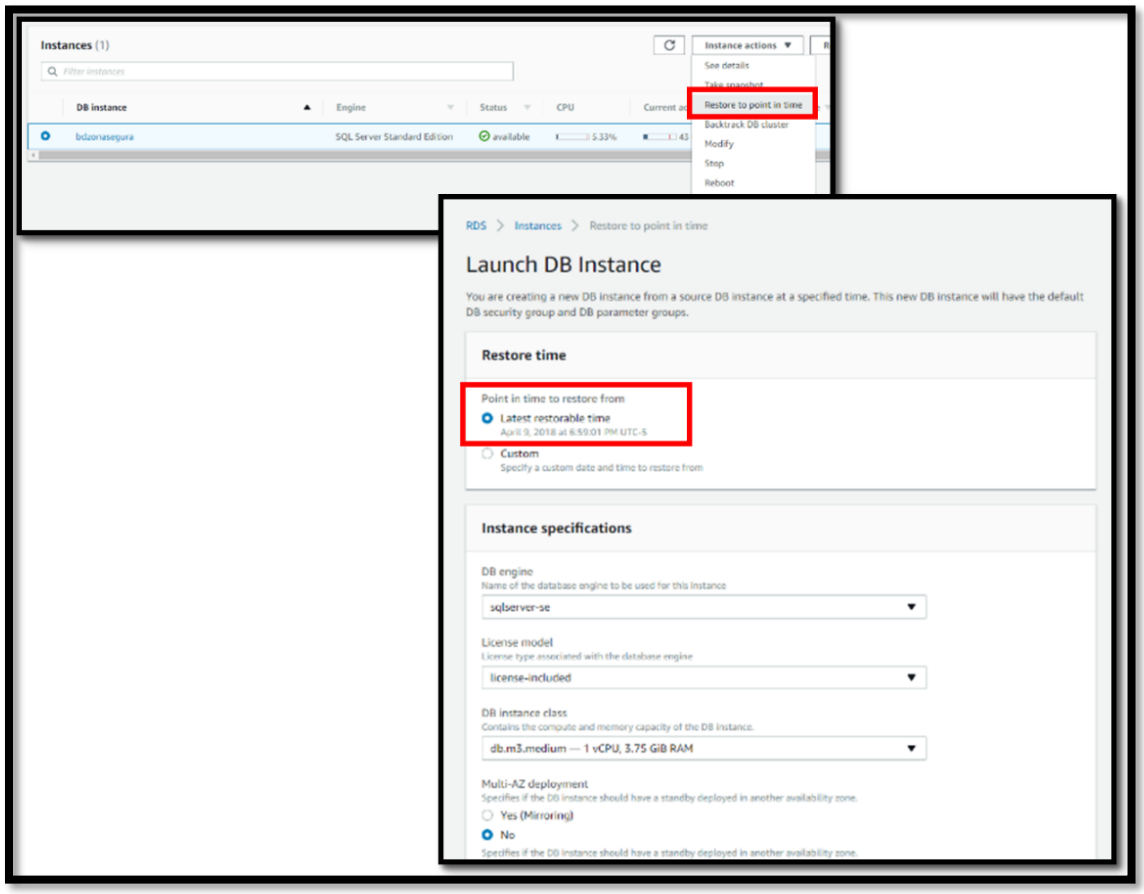



*Figura 18. Restaurar la instancia de base de datos a un punto en el tiempo. Fuente: (autor).*

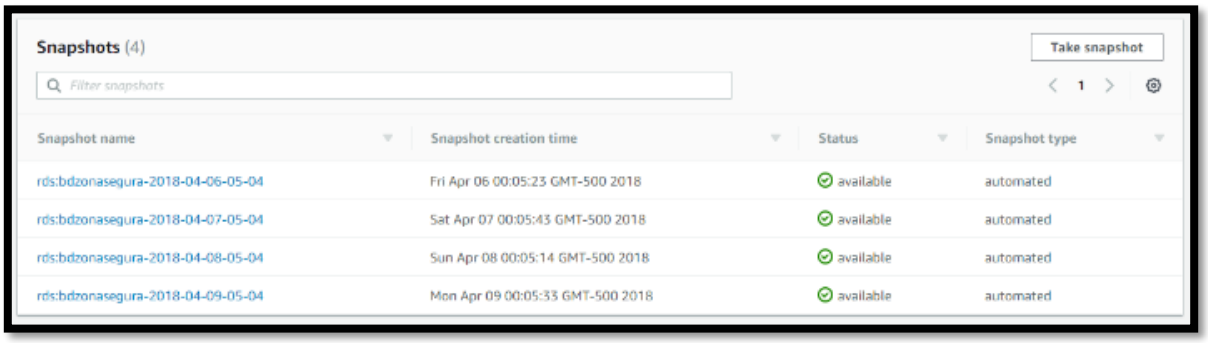



*Figura 19. Utilización de Snapshots de la instancia de base de datos. Fuente: (autor).*

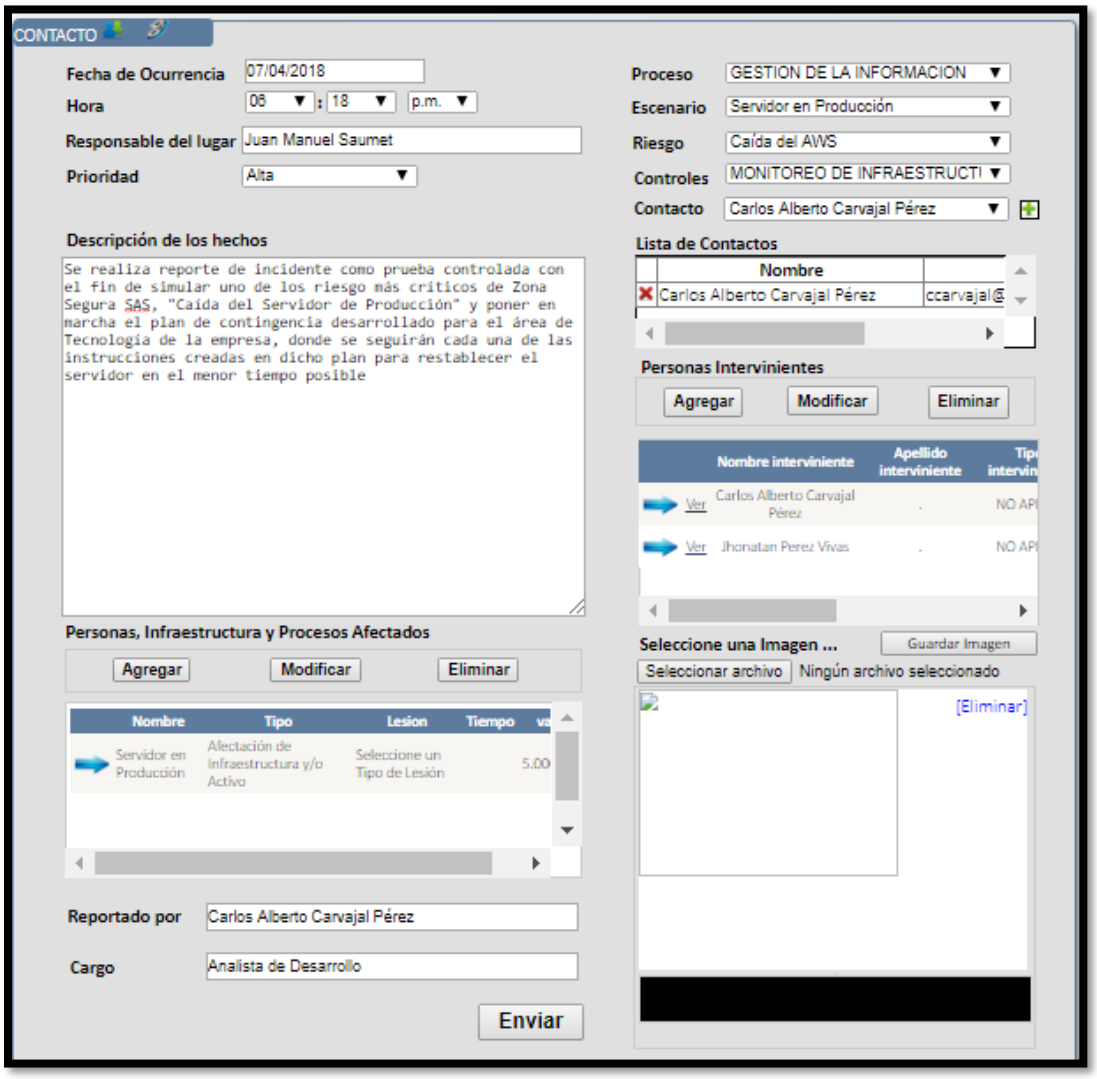



*Figura 20. Reporte del Simulacro realizado. Fuente Software AVARMS®*

La realización del evento en la plataforma sirve para dos cosas: la primera es para comenzar a llenar un histórico de los eventos que ocurren en la empresa, los cuales servirán para la construcción de una matriz real, la cual ayudará a corroborar la eficiencia de los controles o en su defecto, ayudará a mejorar las estrategias de prevención y retención de los riesgos presentes en el área de tecnología de Zona Segura S.A.S.

La segunda razón por la cual es importante dejar el registro de estos eventos es que al realizar este reporte, el sistema está configurado para enviar un correo electrónico (Ver

figura 8) a los responsables del proceso afectado para que estén enterados de la situación y puedan empezar a tomar medidas para afrontar el riesgo.

# Reporte de Incidente

**Ubicación:** GESTION DE RIESGOS/ANTIOQUIA/Principal
**Consecutivo de Reporte #:** 9 **Fecha de Ocurrencia:** 07/04/2018 **Hora:** 06:32:00 a.m.
**Lugar:** Servidor en Producción **Responsable del Lugar:** Juan Manuel Saumet **Prioridad:** Alta

**Descripción de los hechos**
Se realiza reporte de incidente como prueba controlada con el fin de simular uno de los riesgo más críticos de Zona Segura SAS, "Caída del Servidor de Producción" y poner en marcha el plan de contingencia desarrollado para el área de Tecnología de la empresa, donde se seguirán cada una de las instrucciones creadas en dicho plan para restablecer el servidor en el menor tiempo posible.

**PROCESO:**
GESTIÓN DE LA INFORMACIÓN
**ESCENARIO:**
Servidor en Producción
**RIESGO:**
Caída del AWS
**CONTROL:**
MONITOREO DE INFRAESTRUCTURA
**PERSONAS IMPLICADAS:**
Carlos Alberto Carvajal Pérez . C.C. sin documento Tipo de intervención: NO APLICA
Jhonatan Perez Vivas . C.C. sin documento Tipo de intervención: NO APLICA
**PERSONAS Y/O BIENES AFECTADOS:**
NOMBRE: Servidor en Producción TIPO DE AFECTACIÓN: Afectación de Infraestructura y/o Activo COSTO: 5000000
**TOTAL PERDIDA:** 5.000.000,00
**Reportado por:** Carlos Alberto Carvajal Pérez
**Cargo:** Analista de Desarrollo
**Fecha de Reporte:** 07/04/2018 **Hora:** 06:34:01 p. m.

# Análisis

**Análizado por:** Carlos Alberto Carvajal Pérez
**Cargo:** Analista de Desarrollo
**Fecha de Análisis:** 07/04/2018 **Hora:** 06:34:01 p. m.

# Seguimiento

*Figura 21. Correo electrónico generado del Simulacro realizado. Fuente Software AVARMS®*

### 3.3.4 Actuar (A)

Como la metodología de este trabajo se llevó a cabo por medio de un ciclo Deming de mejora continua, en la última etapa se debe analizar todo lo que se planificó y creó, con el fin de ir perfeccionando en el tiempo el plan de contingencia. Por ello, en esta fase se hizo un seguimiento de los resultados obtenidos en las pruebas realizadas en la **Verificación (V),** donde se implementó de manera controlada los instructivos y procedimientos elaborados en el **hacer (H).** Esto se profundizará más en el capítulo cuatro, **Resultados y Discusión.**

Además de lo anterior, la etapa del **Actuar (A)** se dividió en dos fases: La primera fue donde se socializó a la empresa y a las personas implicadas los procedimientos creados que se deben efectuar en caso de la materialización de un riesgo y la segunda fue donde se dispuso el plan de contingencia para su implementación ante la posible materialización de riesgos.

#### 3.3.4.1 Socialización y capacitación sobre el plan de contingencia

Para que un plan de contingencia sea en verdad una herramienta de utilidad que permita afrontar de manera más fácil los incidentes que se puedan presentar en la compañía, no basta solo con una buena planificación de procesos, un levantamiento de escenarios y una adecuada evaluación de riesgos, de hecho, tampoco bastaría con la creación de instructivos y procedimientos a seguir en determinados escenarios. Lo más importante es manejar una **cultura de riesgos** en la empresa, mostrar la importancia de tener planes alternos específicos para que la operación no se vea afectada durante la materialización de riesgos y esto se logra involucrando a las personas en el proceso, no solo a los actores principales de este proyecto, que son el personal del área de innovación y desarrollo, sino también a los demás miembros de la compañía.

Como la empresa Zona Segura S.A.S no es una empresa muy grande, esto facilitó la posibilidad de reunir a los colaboradores para hacer la respectiva divulgación del plan de contingencia, además, otro factor que favoreció con la difusión del plan fue el hecho de que la empresa se encuentra realizando un proceso de certificación en la ISO 9001:2015 en estos momentos, por lo cual se han venido realizando constantes reuniones extra laborales y sesiones de trabajo donde se pudo aprovechar para hacer recolección de información importante de cada uno de los cargos y los procesos **(Ver Apéndice I)**, del mismo modo, sirvió para ir socializando los instructivos, lo cual fue de gran ayuda ya que con la participación de todos se pudo ajustar detalles de los procesos de cada persona. De esta manera se logró involucrar desde el inicio del proyecto al personal de la empresa. **(Se llevó un control de estas sesiones con listas de asistencia, ver Apéndice L)**

### 3.3.4.2 Disposición del plan de contingencia para la implementación

Para la entrega del plan de contingencia a la empresa Zona Segura S.A.S se tuvo en cuenta que la ubicación de este fuera estratégica y asequible, considerando que todos deben tener acceso al plan y a sus instructivos y procedimientos, en algunos casos con ciertas restricciones en procedimientos que contengan claves e información que no debe ser divulgada para el resto del personal. Para ello, se tomó la decisión de tener el plan en una carpeta física en las instalaciones de la empresa, por otro lado, se determinó que era necesario también alojarlo en una estructura de documentación que se ha venido trabajando en la nube, donde todo el personal tiene acceso a sus procesos y está definido por carpetas con códigos y nombres. Por último, se decidió implantar el plan en uno de los sistemas de información que tiene la empresa, ya que se adaptaba perfectamente a su estructura y como es una aplicación web, se puede acceder a esta información en cualquier momento con el usuario y contraseña suministrado a los empleados de la empresa.

La sistematización del plan de contingencia en el software de la empresa ayudará con el proceso de actualización del mismo, pues la información es mucho más fácil de leer y encontrar a través de los sistemas gracias a su interactividad. Además, servirá para la realización de reportes sobre incidentes que se presenten y llevar un historial de estos para la matriz de riesgos real.

Para iniciar con el proceso, se creó una instancia con el nombre de la empresa “ZONA SEGURA S.A.S” donde se ingresó en primer lugar, los procesos que se definieron en la planificación con sus respectivos responsables, para después registrar los escenarios y riesgos encontrados en el proyecto para su relación.


*Figura 22. Creación y selección de procesos en el software. Fuente Software AVARMS®*

Se asignaron los responsables del proceso con su respectivo correo, esto con el fin de que cuando se genere un reporte de algún incidente dentro de la compañía, le llegue un aviso a los encargados del procesos y puedan tomar medidas en el asunto.

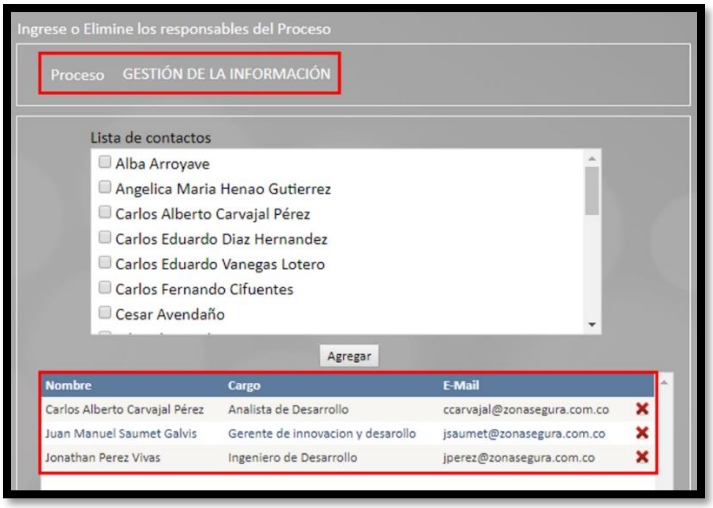



*Figura 23. Asignación de responsables de procesos en el software. Fuente Software AVARMS®*

Se ingresaron los escenarios encontrados durante el desarrollo del proyecto y se asociaron los procesos antes ingresados, creando así su respectiva relación.


*Figura 24. Selección de escenarios y relación con los procesos en el software. Fuente Software AVARMS®*

De igual manera se registraron los riesgos, los cuales apuntan a los procesos. Como se puede observar en la figura 25, se pueden añadir y quitar riesgos de una manera sencilla desde el software, facilitando el proceso de actualización del plan.

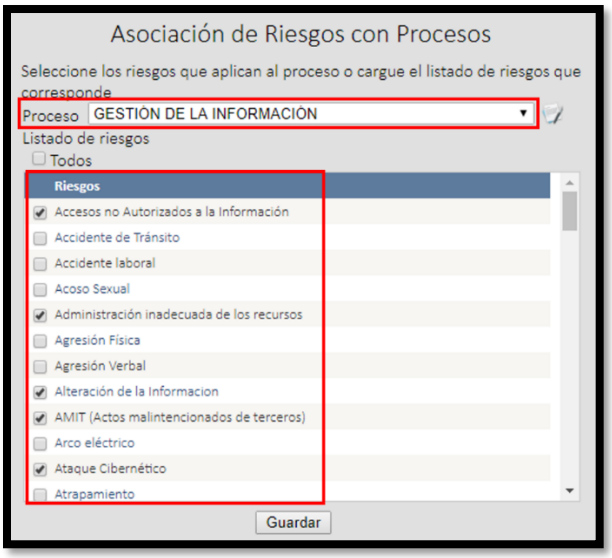



*Figura 25. Creación y selección de riesgos en el software según en el proceso. Fuente Software AVARMS®*

Por último, se hizo la asociación de los escenarios con los riesgos como se puede visualizar en la figura 26, terminando así con la parametrización en el software.

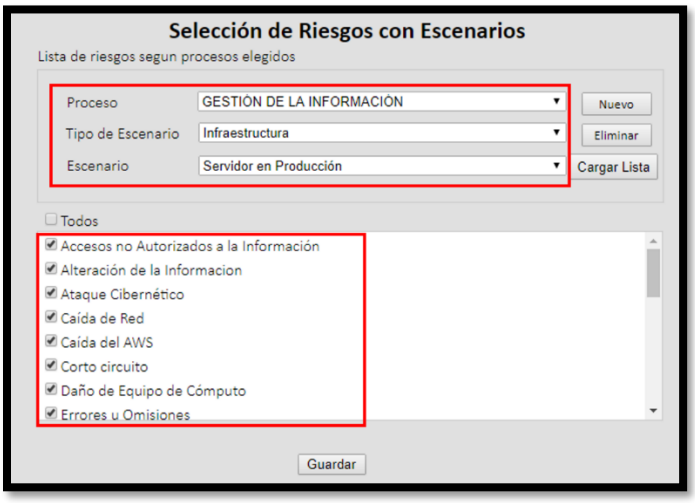



*Figura 26. Relación de procesos, escenarios y riesgos en el software. Fuente Software AVARMS®*

La asociación de todos los elementos antes mencionados se puede simplificar con el siguiente esquema (figura 27) y es la base para realizar una gestión integral de riesgos. Dicho esquema quedó implementado en el software, lo que facilitará su modificación y mejoramiento en el futuro.

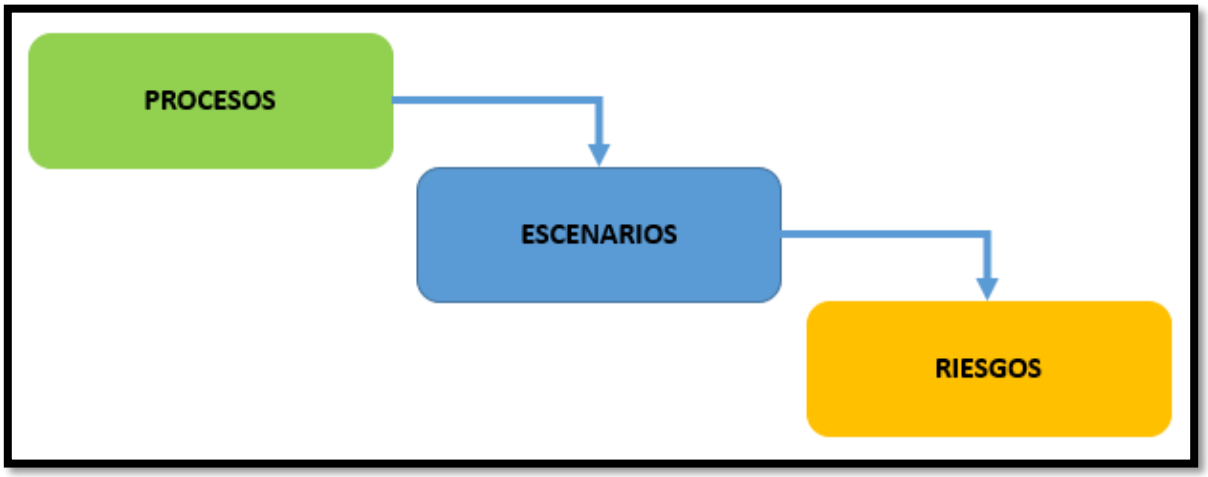



*Figura 27. Relación de procesos, escenarios y riesgos para la calificación de matrices. Fuente: (autor)*

Visualización de matriz inherente en el software (figura 28)


*Figura 28. Visualización de Matriz de Riesgo Inherente en el software. Fuente Software AVARMS®*

En la figura 29 se puede ver la matriz residual o controlada plasmada en el software

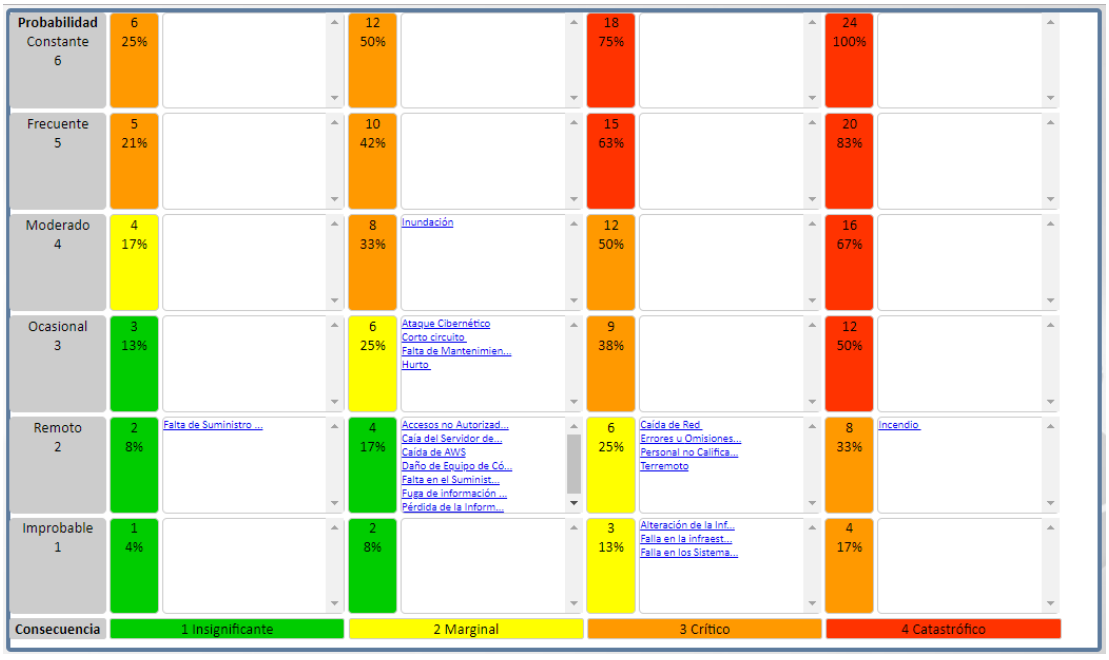



*Figura 29. Visualización de Matriz de Riesgo Controlada en el software. Fuente Software AVARMS®*

# 4. RESULTADOS Y DISCUSIÓN

Al finalizar este proyecto se puede observar los resultados obtenidos después de haber realizado la gestión de riesgos llegando a un estado residual, y esto a su vez fue posible gracias a una buena planificación de los procesos, escenarios y riesgos del área de tecnología de Zona Segura S.A.S.

En la tabla 22 se encuentran el estado inicial de los 14 riesgos seleccionados para darles tratamiento y el estado final de los mismos después de haber valorado la eficacia de los controles establecidos.

| RIESGOS | Calificación Riesgo Inherente | | | Calificación Riesgo Residual | | |
|---|---|---|---|---|---|---|
| Acceso no Autorizado a la Información | Probabilidad | 3 | 12 | Probabilidad | 2 | 4 |
| | Consecuencia | 4 | | Consecuencia | 2 | |
| Alteración de la Información (Integridad) | Probabilidad | 3 | 12 | Probabilidad | 1 | 3 |
| | Consecuencia | 4 | | Consecuencia | 3 | |
| Ataque Cibernético (DoS, Virus informático, Hackeo) | Probabilidad | 4 | 12 | Probabilidad | 3 | 6 |
| | Consecuencia | 3 | | Consecuencia | 2 | |
| | Probabilidad | 4 | 16 | Probabilidad | 2 | 4 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Caída de los Servidores (Disponibilidad) | | | | | | |
| | Consecuencia | 4 | | Consecuencia | 2 | |
| Caída de Red | Probabilidad | 3 | 9 | Probabilidad | 2 | 6 |
| | Consecuencia | 3 | | Consecuencia | 3 | |
| Corto Circuito | Probabilidad | 4 | 12 | Probabilidad | 3 | 6 |
| | Consecuencia | 3 | | Consecuencia | 2 | |
| Falla en la Infraestructura | Probabilidad | 3 | 9 | Probabilidad | 1 | 3 |
| | Consecuencia | 3 | | Consecuencia | 3 | |
| Falla en los Sistemas | Probabilidad | 3 | 9 | Probabilidad | 1 | 3 |
| | Consecuencia | 3 | | Consecuencia | 3 | |
| Falta de Suministro de Energía | Probabilidad | 4 | 8 | Probabilidad | 2 | 2 |
| | Consecuencia | 2 | | Consecuencia | 1 | |
| Fuga de Información Confidencial (Confidencialidad) | Probabilidad | 3 | 12 | Probabilidad | 2 | 4 |
| | Consecuencia | 4 | | Consecuencia | 2 | |
| Incendio | Probabilidad | 4 | 16 | Probabilidad | 2 | 8 |
| | Consecuencia | 4 | | Consecuencia | 4 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Inundación | Probabilidad | 5 | 15 | Probabilidad | 4 | 8 |
| | Consecuencia | 3 | | Consecuencia | 2 | |
| Pérdida de la Información (Falta de Backup) | Probabilidad | 4 | 16 | Probabilidad | 2 | 4 |
| | Consecuencia | 4 | | Consecuencia | 2 | |
| Terremoto | Probabilidad | 2 | 8 | Probabilidad | 2 | 6 |
| | Consecuencia | 4 | | Consecuencia | 3 | |

*Tabla 22. Comparativo de riesgo inherente y riesgo residual.*

De acuerdo a la tabla 22, mediante la calificación de riesgo residual se obtuvo la reducción en la probabilidad y el impacto de cada uno de los riesgos tratados y con ayuda a la tabla 23 se pudo valorar desde aceptables a inaceptables los niveles de riesgo resultantes.

| **Estimación de Riesgo Residual** | |
|---|---|
| **Nivel de Riesgo Residual** | **Nivel** |
| Inaceptable | |
| Importante | |
| Tolerable | |
| Aceptable | |

*Tabla 23. Valoración del riesgo residual basado en la ISO 27001:2013 y en la matriz de riesgos definida en la empresa.*

- El mayor nivel de riesgo residual obtenido recae sobre el riesgo **incendio** con una probabilidad **remota** (2) y una consecuencia **catastrófica** (4) y el riesgo **inundación** con una probabilidad **moderada** (4) y una consecuencia **marginal** (2). Aunque ambos quedaron con un nivel de riesgo **importante (8)** y se deben tener en constante observación y monitoreo, se puede apreciar la gestión en ellos teniendo en cuenta que **incendio** contaba con un nivel de riesgo igual a **dieciséis (16)** e **inundación** a **quince (15).**

- Los menores niveles residuales alcanzados fueron para los riesgos **Falta de Suministro de Energía** con una probabilidad **remota (2)** y consecuencia **insignificante (1)** para un nivel de riesgo **Aceptable (2)** según la tabla 23, seguido de los riesgos: **Acceso no Autorizado a la Información**, **Caída de Servidores**, **Fuga de Información Confidencial** y **Pérdida de la Información** todos con una probabilidad **remota (2)** y consecuencia **marginal (2)** para un nivel de riesgo **Aceptable (4).**

- Los demás riesgos quedaron con un nivel de riesgo **Tolerable**.

Los resultados de las pruebas realizadas en la **Verificación (V)** fueron satisfactorios debido a que se corroboró la eficiencia de uno de los instructivos más importantes (**IN-MGI-001-1**) y que le va a ser de mucha utilidad a la empresa al dar las pautas para la implantación de los sistemas de manera parcial o completa de los sistemas que la compañía ofrece a sus clientes.

De igual manera, se puede observar las ventajas de tener alojadas las bases de datos en un Datacenter como Amazon AWS, que brindan una serie de recursos para la protección de la información y que de ser bien administrados, difícilmente se verá perjudicada dicha información, que es el activo más importante de la empresa Zona Segura S.A.S.

# 5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

**CONCLUSIONES**

- La elaboración del proyecto "Desarrollo de un plan de contingencia para el área de tecnología de Zona Segura S.A.S" favorece a la empresa, dado que no se cuenta con una estrategia, ni con una serie de procedimientos que brinden ayuda a la hora de restaurar la operación e incluso continuar con los procesos de la compañía durante la materialización de uno o varios incidentes.

- Con la ayuda de la metodología MAGERIT se logra identificar un inventario de riesgos que afectan los procesos del área de Tecnología de Zona Segura S.A.S, permitiendo así, evidenciar el estado actual de la empresa para finalmente hacer una gestión de riesgos logrando mitigar el impacto de los mismos.

- Con la implementación de normas como la ISO 31000:2009 de gestión de riesgos y la ISO 27001:2013 de gestión de seguridad de la información se logra la elaboración de procedimientos e instructivos que brindan a la empresa un conjunto de acciones para abordar las eventualidades que puedan afectar los procesos tecnológicos e impedir su normal desarrollo.

- Se concluye que la mejor manera de desarrollar el proyecto es con la participación activa de cada uno de los responsables de los procesos implicados, ya que son ellos quienes los conocen a profundidad y sus aportes son de gran ayuda a la hora de realizar el análisis de riesgo de una manera completa. Además, con esto los

colaboradores toman conciencia de la importancia de tener un plan de contingencia que respalde sus procesos y de esta manera se logra difundir entre los empleados y las partes interesadas el plan mediante sesiones de trabajo (ver Apéndice I, L).

- Con la realización de este proyecto se logra dar un aporte valioso para la certificación en la NTC-ISO 9001:2015 (Sistema de gestión de calidad) fortaleciendo uno de los requisitos de la misma en cuanto a las acciones de contingencia. Concluyendo así, que las certificaciones son importantes para las empresas en muchos sentidos, uno de ellos es la documentación de sus procesos y la gestión de riesgos, los cuales no se deben tomar como gastos, sino como una inversión que tiene el objetivo de **"Asegurar la vida de su empresa"**.

**RECOMENDACIONES**

- Se recomienda a la gerencia de Innovación y Desarrollo, quien es la encargada de los procesos tecnológicos de Zona Segura S.A.S, hacer la difusión del plan de contingencia para los sistemas de información a los colaboradores futuros que presten sus servicios a la empresa, con el fin de mantener contextualizado el personal en caso de cualquier eventualidad.

- Hacer una revisión del plan por lo menos una vez al año, con el fin de validar si los procedimientos están funcionando correctamente. Además, se sugiere hacer la misma revisión y actualización del plan en caso de que algún proceso critico en la organización se haya modificado.

- Se sugiere buscar la certificación de la empresa en la norma ISO 27001:2013, considerando que la información es el activo más importante de Zona Segura S.A.S, y es primordial tener el personal calificado para dar seguridad a la información.

- Implementar simulacros periódicos del plan de contingencia, probando diferentes materializaciones de riesgos con el fin de ir perfeccionando el plan con cada revisión.

**TRABAJO FUTURO**

Tras el proceso de identificación de la matriz inherente y posterior a ello el análisis de la mitigación de los riesgos en la matriz residual, será necesario diligenciar un formulario ante la materialización de incidentes, que contenga datos como fecha, descripción del evento, proceso afectado, escenario, riesgo materializado y control fallido; lo que dará pie a la creación de una matriz real que permita un registro continuo y preciso de la incidentalidad al interior de la empresa, con el fin de corroborar la eficiencia y pertinencia de los controles contenidos en el plan según la necesidad en tiempo real.

Después de la realización de este plan de contingencia que fue enfocado inicialmente a los procesos tecnológicos de Zona Segura S.A.S, se proyecta desarrollar en los procesos de las diferentes áreas de la empresa un plan de contingencia que aborde las necesidades de los mismos, con el fin de consolidar planes de acción específicos que permitan a Zona Segura S.A.S dar continuidad a su operación ante la materialización de riesgos y así asegurar la continuidad de la empresa.

# REFERENCIAS

BSI (The British Standars Institution). (25 de Noviembre de 2017). *Gestión de la Calidad ISO 9001:2015*. Obtenido de https://www.bsigroup.com/es-ES/Gestion-de-Calidad-ISO-9001/

Catoira, F. (28 de Marzo de 2012). *WeliveSecurity ESET*. Obtenido de https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

Díaz, A. F., Collazos, G. I., Cortez Lozano, H., Ortiz, L. J., & Herazo Pérez, G. A. (13 de Enero de 2018). *Implementación de un (SGSI) en la comunidad Nuestra Señora de Gracia, alineado tecnológicamente con la norma ISO 27001*. Obtenido de http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf

Espinosa T., D., Martínez P., J., & Amador D., S. (2014). *Gestión del Riesgo en la Seguridad de la Información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodoloía OCTAVE-S, Vol. 5*. Obtenido de http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

García, D. (19 de Julio de 2016). *GESTIÓN DE RIESGOS*. Obtenido de http://www.ealde.es/metodologias-gestion-riesgos/

Gobierno de España. (13 de noviembre de 2012). *PAe portal administración electrónica*. Obtenido de https://administracionelectronica.gob.es/ctt/magerit#.Wtf3Li7wbIU

Gutiérrez Amaya, C. (2013). *MAGERIT: Metodología Práctica para Gestionar Riesgos*. Obtenido de https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

ICONTEC. (2015). Sistema de Gestión de la Calidad. Requisitos. En ICONTEC, *NORMAS FUNDAMENTALES SOBRE GESTIÓN DE LA CALIDAD* (págs. 1-33). Bogotá: Instituto Colombiano de Normas y Certificaciones (ICONTEC).

ICONTEC. (2017). Guía de aplicación de la ISO 9001:2015. Bogotá: ICONTEC.

ISO 27001. (2013). *Sistema de Gestión de la Seguridad de la Información*. Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

ISOTools. (02 de Diciembre de 2017). *Norma ISO 27001*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools. (02 de DIciembre de 2017). *Norma ISO 31000*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000

ISOTools Excellence. (02 de Junio de 2015). *Planes de Contigencia y la Continuidad de Negocio*. Obtenido de http://www.pmg-ssi.com/2015/06/iso-27001-planes-de-contingencia-y-la-continuidad-de-negocio/

Ortiz Anderson, C. (2017). *La Importancia de un Plan de Contingencia*. Obtenido de http://www.forodeseguridad.com/artic/discipl/4132.htm

SINAE (Sistema Nacional de Emergencias Uruguay). (12 de Noviembre de 2012). *GESTIÓN INTEGRAL DEL RIESGO*. Obtenido de http://sinae.gub.uy/conceptos-basicos/gestion-integral-del-riesgo/

Universidad de las Fuerzas Armadas ESPE. (15 de Enero de 2018). *Evaluación de Seguridad de la Información al Proceso de Admisión de Estudiantes de la UTE basada en ISO /IEC 27000*. Obtenido de Maestría en Evaluación y Auditoría en Sistemas Tecnológicos: http://www.bibliotecasdelecuador.com/Record/ir-:21000-9025/Description#tabnav

# APÉNDICE

**APÉNDICE A**

| IN-MGI-004-1 INSTRUCTIVO DE MONITOREO DE INFRAESTRUCTURA AVARMS® Y BRAVA® | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | **Ingresar a la página: https: //aws.amazon.com/es/**, luego ingresar a la opción ***Mi cuenta > Consola de administración AWS.*** | Equipo de Desarrollo | Como mínimo una vez por día |
| **2** | Ingresar con las credenciales suministradas por la gerencia de Innovación y Desarrollo. | | |
| **3** | Hacer clic en el menú ***Services***, luego en la categoría ***DataBases*** hacer clic en la opción ***Relactional Database Service***, luego en la parte izquierda hacer clic en la opción ***Instances***. | | |
| **4** | Seleccionar la base de datos ***bdZonaSegura*** y luego en la opción ***Instance Actions*** hacer clic en ***See details.*** Verificar el comportamiento de la base de datos con base a las gráficas. | | |
| **5** | Ingresar al servidor de aplicaciones y verificar en el administrador de tareas el consumo de recursos del servidor. | | |
| **6** | Verificar el estado de los servicios web encardados del envío de correos y recepción de datos hacia nuestra plataforma. | | |
| **7** | Tomar el print screen del monitoreo de la infraestructura del AVA RMS y guardar la evidencia en el equipo del Ingeniero de Desarrollo, compartida con el Analista e Desarrollo y sincronizada a la nube: **D:\DESARROLLO\Mis documentos\Estratégica\Monitoreo de infraestructura** | | |

*Tabla 24. Instructivo para el monitoreo de la infraestructura de la empresa Zona Segura S.A.S.*

**APÉNDICE B**

| IN-MGI-004-2 INSTRUCTIVO PARA LA RENOVACIÓN DEL CERTIFICADO SSL | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | Desde el **LLS**, hacer clic en el servidor (**localhost**), luego en el icono de "**Server Certificates**". | Equipo de desarrollo | Máximo 24 horas después y antes del vencimiento del certificado actual. |
| **2** | Luego hacer clic en la opción "**Create Certificate Request**" | | |
| **3** | Diligenciar los datos y luego hacer clic en el botón "**Next**". | | |
| **4** | Seleccionar el tamaño de bits 2048, hacer clic en el botón "**Next**". | | |
| **5** | Seleccione la ruta y el nombre del archivo donde se guardará el código de solicitud, terminar haciendo clic en el botón "**Finish**". | | |
| **6** | Ingresar al archivo, copiar y pegar el código de solicitud en el formulario web de **RapidSSL**. | | |
| **7** | Vía correo electrónico llegará el link para descargar el asistente para la instalación del certificado en el servidor. | | |
| **8** | Seleccione el sistema operativo (**Microsoft**) y la versión del **IIS** (**Windows 2012 – IIS 8.0-8.5**) y descargue el archivo. | | |
| **9** | Descomprimir el archivo descargado e ingrese a la carpeta **SSLAssistant** y allí ejecute el asistente de instalación. | | |
| **10** | En el asistente hacer clic en el botón "**Install certificate**". | | |

*Tabla 25. Instructivo para renovación de certificado SSL de la empresa Zona Segura S.A.S.*

## APÉNDICE C

| IN-MGI-004-3 INSTRUCTIVO DE ACTUALIZACION HOSTING | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | Ingresar a www.hostmonster.com | Gerencia de innovación de desarrollo | Renovación cada dos (2) meses |
| **2** | Hacer clic en el icono Control panel **login.** | | |
| **3** | Ingresar el usuario y contraseña documentados. | | |
| **4** | Dar clic en el botón **CPANEL.** | | |
| **5** | Dar clic en **UPGRADE HOSTING.** | | |
| **6** | Validar o ingresar los datos de la Tarjeta de Crédito o el medio de pago. | | |
| **7** | Dar clic en **checkout.** | | |

*Tabla 26. Instructivo para actualización de Hosting de la empresa Zona Segura S.A.S.*

**APÉNDICE D**

| **IN-MGI-004-4 INSTRUCTIVO DE ACTUALIZACIÓN GODADDY www.brava.com.co - www.avarms.com** | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | Ingresar a la página **https://co.godaddy.com** | Gerencia de innovación y desarrollo | Cada Año |
| **2** | Dar clic en el botón **INICIAR SESION** | | |
| **3** | Ingresar con el Usuario y **Password** documentado | | |
| **4** | Dar clic en el Botón **MIS PRODUCTOS** | | |
| **5** | Seleccionar los **DOMINIOS A CANCELAR** | | |
| **6** | Dar clic en el botón CONTINUAR AL CARRITO | | |
| **7** | Seleccionar el tiempo de renovación y dar clic en el botón **CONTINUAR COMPRA** | | |
| **8** | Dar clic en el botón **PAGAR AHORA** | | |

*Tabla 27. Instructivo para actualizar GODADDY de la empresa Zona Segura S.A.S.*

**APÉNDICE E**

| IN-MGI-001-1 INSTRUCTIVO DE IMPLANTACIÓN DEL AVARMS® Y Brava® | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | Ingresar al Server manager | Equipo de desarrollo | Cada vez que se presente una migración de servidor |
| **2** | Hacer clic en la opción **Features** y luego el **Add-Features** | | |
| **3** | Seleccionar la opción ISS server extensión | | |
| **4** | Agregar un grupo de aplicación para **FRAMEWORK 4.5** | | |
| **5** | Agregar excepciones al **FIREWALL** de los siguientes protocolos y puertos<br>• 1**3 SQL server<br>• 2* SMTP<br>• *0 Internet | | |
| **6** | Subir archivo de sitio web del computador al servidor en la ruta **C:\inetpub\wwwroot** | | |
| **7** | Ingresar al **IIS,** en el panel de conexiones desplegar el árbol del servidor luego la carpeta **SITES,** luego la carpeta **Default web sites** e ir a la carpeta **AVARMS** hacer clic derecho en ella y luego hacer clic en la opción convertir en aplicación (Aplica para el sitio web **brava**) | | |
| **8** | En el menú de opciones del sitio **AVARMS HOME** hacer doble clic en la opción **Default Document**, luego en el menú **Actions** hacer clic en la opción **ADD** y escribir el nombre del formulario inicial (**Login.aspx**) (Aplica para el sitio web **brava**) | | |
| **9** | Subir el archivo **backup** (**.bak**) al servidor | | |

| IN-MGI-001-1 INSTRUCTIVO DE IMPLANTACIÓN DEL AVARMS® Y Brava® | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **10** | Ingresar al **SQL server management studio**, desplegar la opción | Equipo de desarrollo | Cada vez que se presente una migración de servidor |
| **11** | Hacer clic derecho en la opción **Databases** y luego en la opción **Restore databases**.<br><br>En la sección de ruta seleccionar la opción **Device** y hacer clic en el botón de puntos suspensivos **(…)**, luego hacer clic en el botón de **ADD** y seleccionar el archivo **(.BAK)** de la base de datos y terminar haciendo clic en el botón OK.<br><br>En la sección D**estino** escribir el nombre de la base de datos (**bdZonaSegura)** y finalizar con el botón **OK (BDBRAVA** para **brava)** | | |
| **12** | Subir los instaladores **Reporteria_ava_sevicol.msi** de la ruta<br><br>**D:\desarrollo\misdocumentos\estrategica\reporteria_ava_sevicol\setup_reporteria_ava_sevicol\debug\reporteria_ava_sevicol.msi** y el instalador **setup servicio mail.msi** de la ruta<br><br>**D:\DESARROLLO\Mis documentos\Estrategica\Desarrollo remoto\ServicioEnvioEmailAVARMS\Setup Servicio Mail\Debug\Setup Servicio Mail.msi** al servidor e instalar las aplicaciones y ejecutarlas | | |
| **13** | En la barra de tareas en el área de notificaciones dar clic derecho al servicio de envió de email de **AVARMS** y le da en la opción **Configurar** y diligenciar la siguiente información:<br><br>• Intervalo de tiempo de envió (**30**) minutos<br>• Número de email a enviar (**999**)<br>• Cuenta (**a*****@avarms.com**) | | |

| IN-MGI-001-1 INSTRUCTIVO DE IMPLANTACIÓN DEL AVARMS® Y Brava® | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| | • Clave **(*******)**<br>• Servidor **(Poner el nombre del servidor de correo electrónico)**<br>• Poner el Puerto **(**)**<br>• SSL **(chequear)**<br><br>Presionar el botón guardar y en el icono **reporteria *****  clic derecho reportar | | |

*Tabla 28. Instructivo para implantar los sistemas desde cero en servidores para la empresa Zona Segura S.A.S.*

## APÉNDICE F

| IN-MGI-001-2 INSTRUCTIVO DE IMPLANTACIÓN DE APLICACIONES MÓVILES | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | Ingresar a la aplicación **Android Studio** | Equipo de desarrollo | Cada que se actualice la app |
| **2** | Hacer clic en la opción **Build** y luego presionar la opción **Generate signed APK** | | |
| **3** | Ingresar las credenciales de la firma que está en el archivo **datosfirma.txt** en la ruta **D:\DESARROLLO\Mis documentos\Estrategica\workspace** | | |
| **4** | Presionar el botón **Next** y luego **Finish** | | |
| **5** | Esperar a que se genere el archivo **AVARMSMOBILE.apk** ,luego buscarlo en la ruta ***D:\DESARROLLO\Mis documentos\Estrategica\workspace\AVARMSMOBILE\out\production\AVARMSMOBILE*** | | |
| **6** | Ingresar a la siguiente página web **https://play.google.com/apps/publish** e ingresar las credenciales: **Usuario: ******@zonasegura.com.co, Contraseña:** ********** | | |
| **7** | Seleccionar la app que corresponda, luego en la opción de **Administración de lanzamientos**, luego presionar en **Versiones de la app** | | |
| **8** | Seleccionar la opción **Administrar versiones de producción** y luego presionar el botón **Crear versión** | | |
| **9** | Hacer clic en el botón **examinar archivos** y seleccionar el archivo **AVARMSMOBILE.apk** de la ruta ***D:\DESARROLLO\Misdocumentos\Estrategica\workspace\AVARMSMOBILE\out\production\AVARMSMOBILE*** | | |
| **10** | Finalizar haciendo clic en **Revisar** y luego en **Publicar** | | |
| **NOTA: EL INSTRUCTIVO TAMBIÉN APLICA PARA LA APP BRAVA** | | | |

*Tabla 29. Instructivo para implantar Apps de la empresa Zona Segura S.A.S.*

## APÉNDICE G

| IN-MGI-003-1 INSTRUCTIVO PARA LA VENTANA DE MANTENIMIENTO | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | **VENTANA DE MANTENIMIENTO** | | |
| **1.1.** | Previo a la ventana de Mantenimiento | | |
| **1.1.1.** | Redactar el mensaje sobre la realización de la ventana de mantenimiento en el formato definido, el cual está en el computador DESARROLLO-ZS en la ruta **D:\DESARROLLO\Mis documentos\correo.html** | Equipo de desarrollo | Máximo una semana antes de la realización de la ventana de mantenimiento |
| **1.1.2.** | Realizar la comunicación del mensaje a través de correo electrónico a los contactos definidos por cada cliente. El listado de contactos está en el computador **DESARROLLO-ZS** en la ruta **D:\DESARROLLO\Mis documentos\CONTACTOS PARA VENTANAS DE MANTENIMIENTO.doc** | | |
| **1.2.** | Durante la ventana de mantenimiento | | |
| **1.2.1.** | Detener los servicios relacionados a nuestras plataformas. (Envío de correo, servicios web, IIS y Bases de datos). | Equipo de desarrollo | Dentro del tiempo de duración definido para la ventana de mantenimiento |
| **1.2.2.** | Realizar las actividades definidas en la ventana de mantenimiento. | | |
| **1.2.3.** | Activar los servicios relacionados a nuestras plataformas. (Envío de correo, servicios web, IIS y Bases de datos). | | |
| **1.2.4.** | Realizar pruebas del correcto funcionamiento de todas las plataformas y servicios. | | |
| | **Se guarda el video de la ventana de mantenimiento.** | | |

*Tabla 30. Instructivo para realizar una ventana de mantenimiento en la empresa Zona Segura S.A.S.*

**APÉNDICE H**

| IN-MGI-003-2 INSTRUCTIVO SEGURIDAD DE INFORMACIÓN INTERNA Y EXTERNA | | | |
|---|---|---|---|
| **ITEM** | **DESCRIPCIÓN** | **RESPONSABLE** | **TIEMPO DE REALIZACION** |
| **1** | **POLÍTICA DE TRATAMIENTO DE DATOS DE ZONA SEGURA (MAGNETICAMENTE)** | | |
| **1.1.** | Todos los cargos tienen una carpeta asociada a su correo, en la que se copiará la información estratégica (archivos necesarios para el cumplimiento de los objetivos del cargo).<br>• Ger - General<br>• Ger - Conocimiento<br>• Ger - I+D<br>• Asis - Admin<br>• Ing - Desarrollo<br>• Analista - Desarrollo<br>• Analista - Soporte<br>• Analista - Riesgos<br>• Analista - Comercial<br>• Sistema Gestión Calidad | Gerente de Innovación y Desarrollo | Cada que ingrese una persona nueva o se cambie de cargo o funciones. |
| **1.2.** | Se creará una carpeta con el nombre de cada cliente asociada al dominio **@zonasegura.com.co** que contendrá las siguientes carpetas:<br>• Contrato<br>• Facturas<br>• Otro si<br>• Actas con clientes<br>**NOTA: La información asociada a cada uno de los usuarios son responsabilidad del empleado de Zona Segura.** | Gerente de Innovación y Desarrollo | Con la nueva contratación de cada cliente |
| **1.3.** | Datos Considerados confidenciales de **CLIENTES**:<br>• Información de Riesgos<br>• Información Eventos<br>• Base de datos de Intervinientes | Todos los empleados de Zona Segura | No aplica |

| | | | |
|---|---|---|---|
| | • Base de datos de Contactos<br>• Cualquier otra información cubierta bajo el acuerdo de confidencialidad. | | |
| **1.4.** | Datos Considerados confidenciales de **Zona Segura S.A.S:**<br><br>• Información personal de los empleados<br>• Presupuesto<br>• Estrategias comerciales<br>• Código Fuente de AVARMS® y BRAVA®<br>• Actas de Junta de Socios (Comités de Gerencia)<br><br>**NOTA: Se considera información confidencial, cuando por lo menos uno de los empleados no puede tener acceso a la misma.** | Todos los empleados de Zona Segura | No aplica |
| **1.5.** | Información **Pública Interna:**<br><br>Es la información que se puede compartir con todos los empleados de Zona Segura:<br><br>• Políticas<br>• Manuales<br>• Directrices | Gerente de Innovación y Desarrollo | No aplica |
| **1.6.** | Información **Estratégica y Confidencial:**<br><br>• Base de Datos de Clientes<br>• Base de Datos Comerciales<br>• Información confidencial de clientes.<br>• Estrategia de Mercadeo<br>• Direccionamiento Estratégico.<br><br>**NOTA: Esta Información NO debe ser compartida por USB o con terceros y NO debe ser enviada por correo fuera del dominio @zonasegura.com.co** | Gerente de Innovación y Desarrollo | No aplica |
| **1.7.** | Todos los equipos de cómputo en Zona Segura S.A.S deben estar protegidos por la contraseña del sistema operativo. | Gerente de Innovación y Desarrollo | Se asigna cada que una persona ingresa y se le da acceso a su carpeta y pc. |

*Tabla 31. Instructivo de seguridad de la información interna y externa de la empresa Zona Segura S.A.S.*

## APÉNDICE I

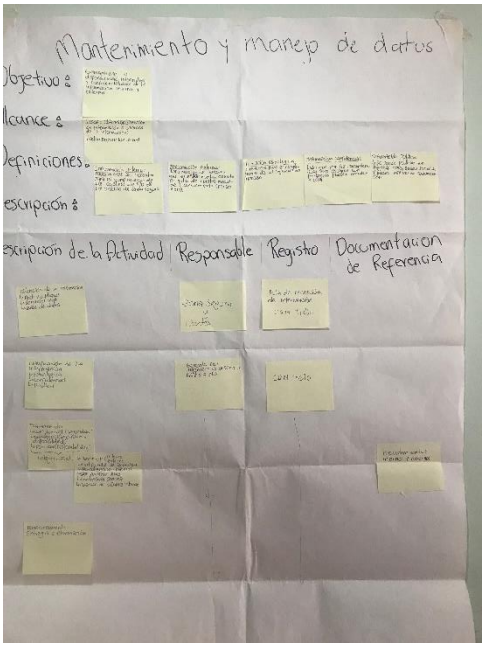



*Figura 30. Creación en equipo del proceso mantenimiento y manejo de dato.*

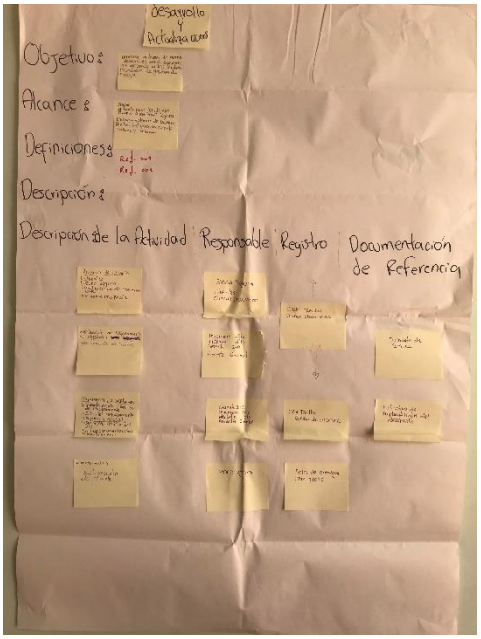



*Figura 31. Creación en equipo del proceso desarrollo y actualizaciones.*

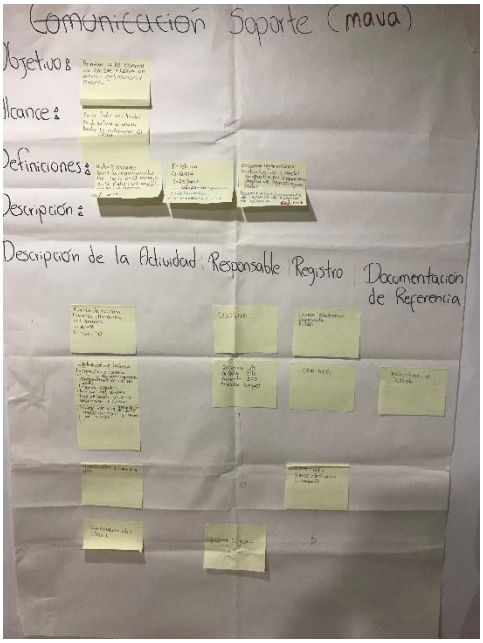



*Figura 32. Creación en equipo del proceso Soporte (MAVA)*

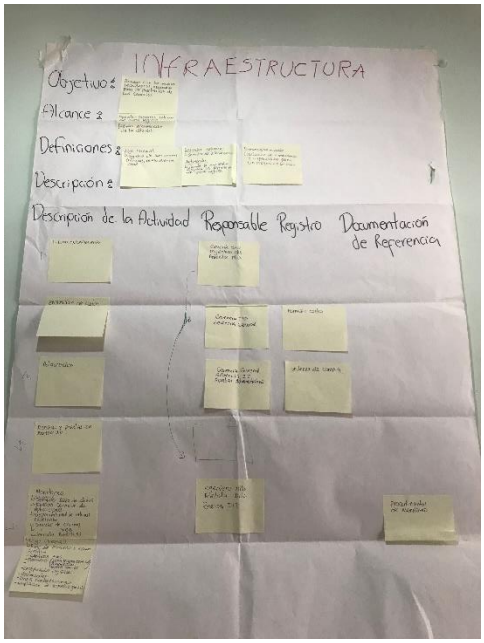



*Figura 33. Creación en equipo del proceso infraestructura.*

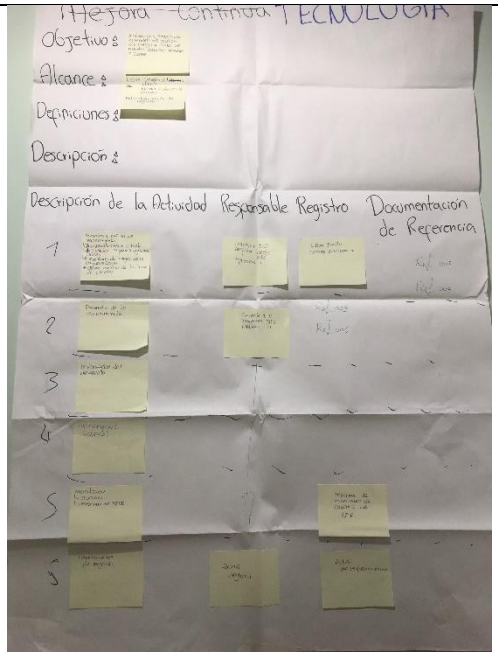



*Figura 34. Creación en equipo del proceso Tecnología.*

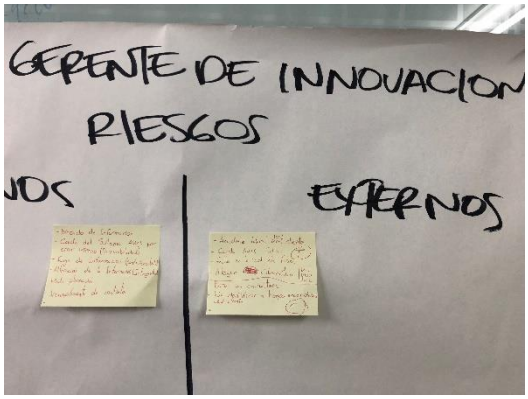



*Figura 35. Determinación de riesgos por cargo (Gerente de innovación y desarrollo)*

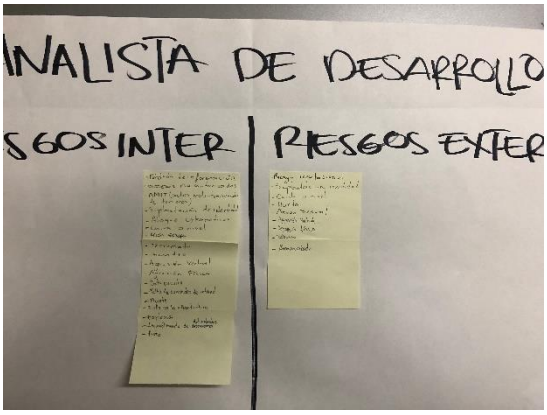



*Figura 36. Determinación de riesgos por cargo (Ingeniero y analista de desarrollo)*

*Tabla 32. Levantamiento de información a través de sesiones de trabajo con el personal de Zona Segura S.A.S.*

## APÉNDICE J

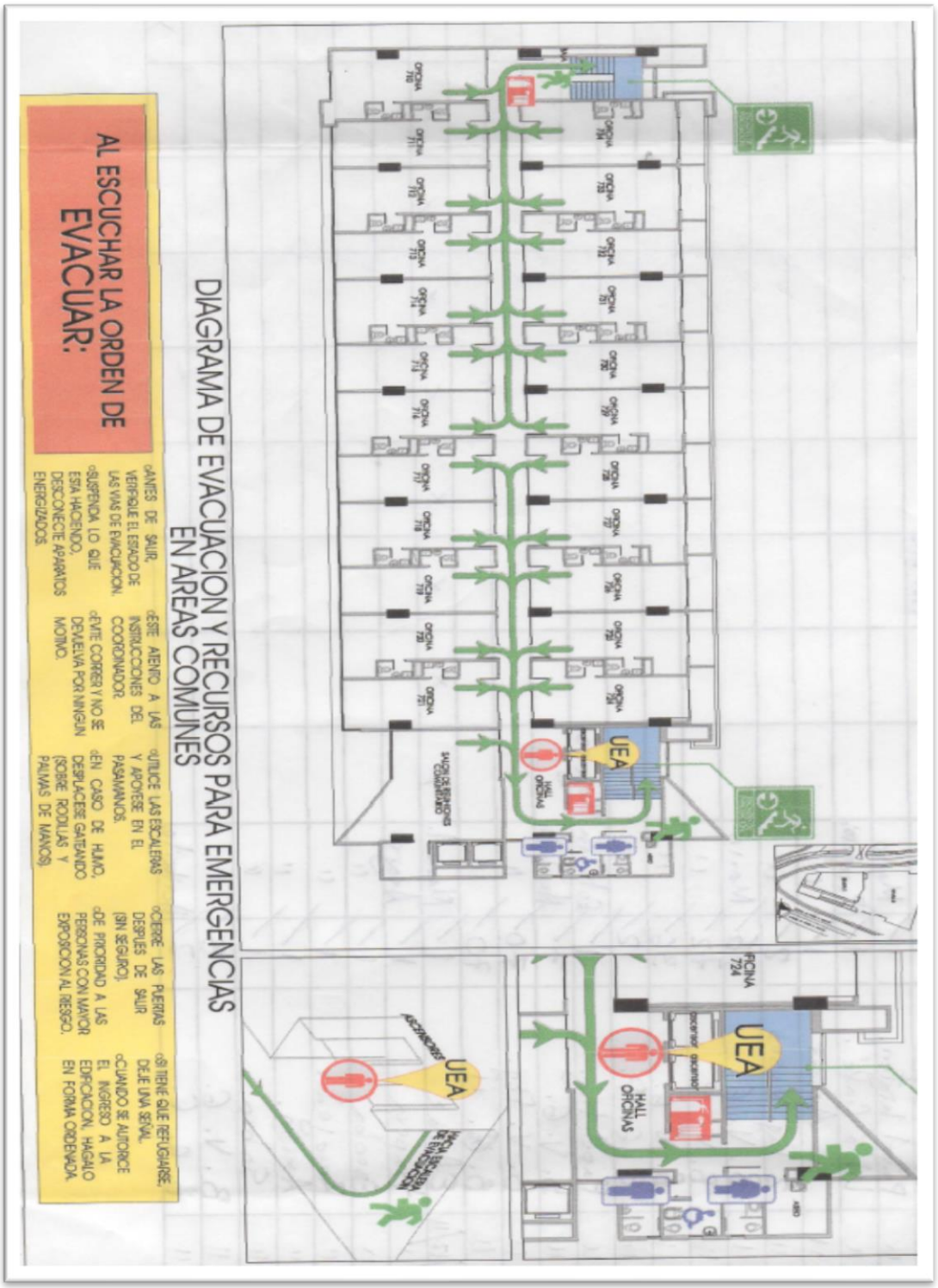



*Figura 37. Mapa de las instalaciones y ruta de evacuación ante desastres de la copropiedad.*

## APÉNDICE K

zona segura®

F-MGE-001-2
Versión: 1.0
Fecha: 01-01-2018

Medellín, abril-07-2018

Acta N°: 001

**Simulacro y prueba de instructivo del Plan de Contingencia del área de Tecnología de Zona Segura SAS**

**Inicio:** 06:18 PM **Fin:** 07:30 PM

**Asistentes:** Carlos Alberto Carvajal Pérez – Analista de Desarrollo
Jonathan Perez Vivas – Ingeniero de Desarrollo

**Orden del día:**

1. Realizar simulación del incidente "Falla en los sistemas" con la aplicación BRAVA® la cual es utilizada a nivel nacional para la seguridad operativa de diferentes empresas de seguridad.
2. Hacer una simulación de un incidente relacionado con las bases de datos.
3. Poner en marcha el instructivo IN-MGI-001-1 creado para el proceso Gestión de la Información donde se especifica como restablecer los sistemas y las bases de datos de la empresa.
4. Hacer el registro en las plataformas de la empresa para simular cómo sería la comunicación del incidente.

**Compromisos de los asistentes:**

1. Verificar que todos los servicios queden sin ningún problema después de las pruebas.
2. Realizar el registro del evento en nuestras plataformas como historial.
3. Hacer las correcciones (si se requiere) con base a lo encontrado en las pruebas

zona segura

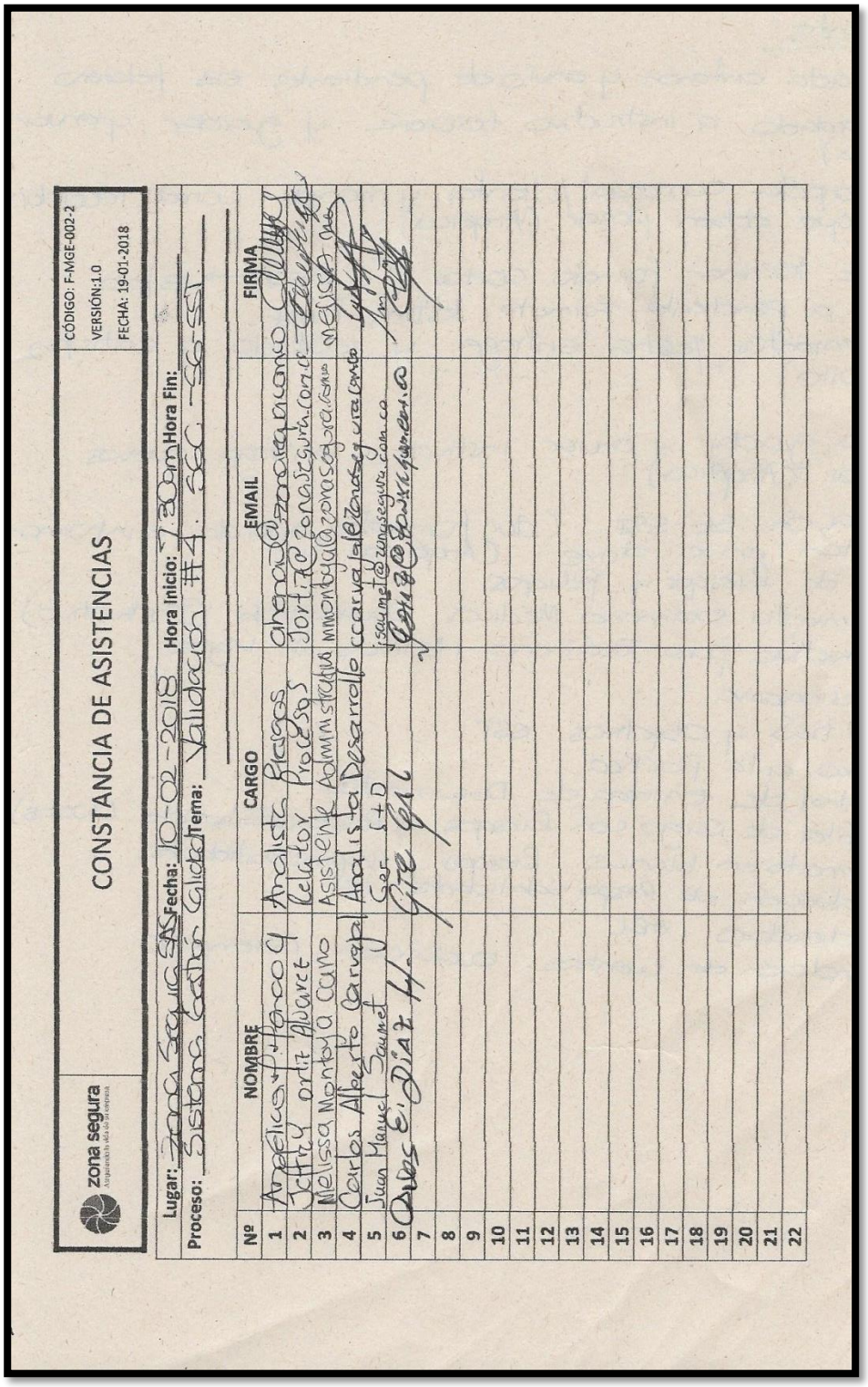
**Elaboró:**

Carlos Alberto Carvajal Pérez
Analista de Desarrollo

Jonathan Perez Vivas
Ingeniero de Desarrollo

*Figura 38. Acta de la realización del simulacro para el plan de contingencia.*

## APÉNDICE L



zona segura

CONSTANCIA DE ASISTENCIAS

CÓDIGO: F-MGE-002-2
VERSIÓN:1.0
FECHA: 19-01-2018

Lugar: Zona Segura SAS Fecha: 10-02-2018 Hora Inicio: 7:30am Hora Fin:

Proceso: Sistema Gestión Calidad Tema: Validación #4. Sec. -Go-SST

| Nº | NOMBRE | CARGO | EMAIL | FIRMA |
|---|---|---|---|---|
| 1 | Angelica Patricia Q | Analista Riesgos | ahenao@zonasegura.com.co | |
| 2 | Jeffry ortiz Alvarez | Relator Procesos | jortiz@zonasegura.com.co | |
| 3 | Melissa Montoya Cano | Asistente Administrativa | mmontoya@zonasegura.com.co | melissa |
| 4 | Carlos Alberto Carvajal | Analista Desarrollo | ccarvajal@zonasegura.com.co | |
| 5 | Juan Manuel Saumet J. | Ger. S+D | jsaumet@zonasegura.com.co | |
| 6 | Jules E. Diaz H. | Gte Gal | jediaz@zonasegura.com.co | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |
| 21 | | | | |
| 22 | | | | |

*Figura 39. Lista de asistencia de una de las sesiones de trabajo realizadas en la empresa.*

**APÉNDICE M**

| Activos contra riesgos | |
|---|---|
| **Riesgos** | **Tipos de Activos** |
| Acceso no Autorizado a la Información | Soporte de Información, Software |
| Alteración de la Información | Soporte de Información, Software |
| Ataque Cibernético | Software, Soporte de Información |
| Caída de los Servidores | Software, Soporte de Información, Hardware |
| Caída de Red | Servicios, Comunicación |
| Corto Circuito | Hardware, Instalaciones |
| Daño de Equipos de Cómputo | Hardware |
| Errores u Omisiones | Personas |
| Falla en la Infraestructura | Hardware, Equipamiento Auxiliar |
| Falla en los Sistemas de Información | Software, Hardware |
| Falta de Mantenimiento | Hardware, Instalaciones |
| Falta de Suministro de Energía | Servicios, Instalaciones, Hardware |
| Falta en el Suministro de Internet | Servicios, Comunicación |
| Fuga de Información Confidencial | Soporte de Información |
| Hurto | Personas, Hardware, Software, Soporte de Información |
| Incendio | Instalaciones |
| Inundación | Instalaciones |
| Pérdida de la Información | Soporte de Información |
| Personal no Calificado | Personas |
| Terremoto | Instalaciones |

*Tabla 33. Activos y riesgos del área de tecnología de Zona Segura S.A.S.*

FIRMA ESTUDIANTES _____

_____

_____

FIRMA ASESOR Alexis Andrés Builes

FECHA ENTREGA: 7/06/2018

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____