UNIVERSIDAD DON BOSCO
DIRECCION DE EDUCACION A DISTANCIA

TRABAJO DE GRADUACIÓN:

TRANSFORMACIÓN RESILIENTE: ESTRATEGIAS DE RECUPERACIÓN ANTE DESASTRES EN EMPRESAS SALVADOREÑAS A TRAVÉS DE SERVICIOS CLOUD PARA SISTEMAS CRÍTICOS

PARA OPTAR AL GRADO DE:

MAESTRO(A) EN SEGURIDAD Y GESTION DE RIESGOS INFORMATICOS

AUTORES:

ALEXANDER JOSÉ GUTIÉRREZ MEJÍA	**GM151856**
NELSON JOSUÉ RODRÍGUEZ OCHOA	**RO222469**
DIANA STEPHANIE GARCÍA LANDAVERDE	**GL220399**

ASESOR:

MG. MAURICIO ORLANDO FIGUEROA CHICAS

JUNIO, 2024

Rector de Universidad Don Bosco

Dr. Mario Rafael Olmos

Secretaria General

Inga. Yesenia Xiomara Martínez Oviedo

Decano de la Facultad de Ingeniería

Mg. Mario Guillermo Juárez Pérez

Coordinador de la Maestría

Mg. Herson Miguel Serrano

Asesor del proyecto de graduación

Mg. Mauricio Orlando Figueroa Chicas

Lector del proyecto de graduación

INDICE

II. Tema de la investigación

El proyecto "Transformación Resiliente: Estrategias de Recuperación ante Desastres en Empresas Salvadoreñas a través de Servicios Cloud para Sistemas Críticos" tiene como objetivo abordar la necesidad imperante de fortalecer las capacidades de recuperación ante desastres en el tejido empresarial de El Salvador. Para lograr este propósito, se llevará a cabo un estudio exhaustivo que incluirá la realización de una encuesta a empresas de diversos sectores económicos en El Salvador.

Este proyecto busca proporcionar un marco teórico sólido, evaluando la aplicabilidad de soluciones basadas en la nube, considerando las características y necesidades específicas de las empresas del entorno salvadoreño. A través de la encuesta, se recopilarán datos detallados sobre las estrategias de recuperación ante desastres actualmente implementadas por las empresas, permitiendo así una evaluación precisa de sus fortalezas, debilidades y áreas de mejora en lo que respecta a la protección de sus sistemas críticos.

Los resultados de este estudio proporcionarán información valiosa que servirá como base para el desarrollo de recomendaciones prácticas y adaptadas a la realidad local, con el objetivo de mejorar la resiliencia empresarial y promover la adopción efectiva de servicios en la nube para la protección de sistemas críticos en El Salvador.

III. Formulación del problema

En la actualidad, las empresas se encuentran confrontando una serie de desafíos significativos en lo que respecta a la seguridad y disponibilidad de sus sistemas críticos. Estos desafíos se intensifican especialmente en situaciones de emergencia o desastres naturales, donde la capacidad de mantener la continuidad del negocio y proteger la integridad de los datos se vuelve aún más crucial.

IV. Justificación

La falta de un enfoque específico para la implementación de un Plan de Recuperación ante Desastres (DRP) en la nube en las empresas salvadoreñas deja a estas organizaciones expuestas a una serie de riesgos y vulnerabilidades ante eventos catastróficos. Esta vulnerabilidad puede traducirse en consecuencias financieras y operativas significativas, incluyendo pérdidas de datos críticos, interrupción de servicios esenciales y daños a la reputación de la empresa.

Por lo tanto, es fundamental abordar esta brecha ofreciendo a las empresas un plan práctico y adaptado a la realidad local. Un DRP en la nube diseñado específicamente para las necesidades y características del entorno empresarial salvadoreño puede fortalecer de manera efectiva la capacidad de recuperación ante desastres naturales e intrusiones de seguridad. Al proporcionar a las empresas herramientas y directrices claras para la gestión de crisis, el objetivo es minimizar el impacto de los eventos adversos y facilitar una rápida y eficiente recuperación de las operaciones comerciales.

En resumen, la implementación de un DRP en la nube adaptado a las empresas salvadoreñas no solo ayuda a mitigar los riesgos asociados con desastres y ataques cibernéticos, sino que también contribuye a la protección del tejido empresarial local, promoviendo la continuidad del negocio y la resiliencia frente a las adversidades.

V. Objetivo general del proyecto

Modelar estrategias de recuperación ante desastres naturales e intrusiones de seguridad, mediante el aprovechamiento de servicios en la nube, enfocadas en sistemas críticos, con el propósito de fortalecer la resiliencia de las empresas salvadoreñas.

VI. Objetivos específicos del proyecto

- Conducir una encuesta exhaustiva a empresas salvadoreñas para analizar a fondo sus estrategias actuales de recuperación ante desastres, con un enfoque particular en la evaluación de sus sistemas críticos, con el fin de identificar claramente sus puntos fuertes, debilidades y oportunidades de mejora.
- Evaluar estrategias específicas de recuperación ante desastres naturales e intrusiones de seguridad basadas en servicios en la nube, considerando las particularidades del entorno empresarial salvadoreño, como aspectos culturales, económicos y tecnológicos, con un enfoque especial en la protección y recuperación de sistemas críticos.
- Presentar las estrategias ante desastres naturales e intrusiones de seguridad desarrolladas para que estas puedan servir de referencia ante futuras implementaciones, mediante un artículo electrónico y webinar.

VII. Antecedentes de la investigación

1. Fundamentos de la computación en la nube

1.1 Conceptos y características

Empresas grandes como Amazon ([AWS | Informática en la nube. Ventajas y Beneficios], s. f.), HP ([¿Qué es la computación en la nube?], s. f.) y Google ([¿Qué es la computación en la nube? | Google Cloud], s. f.) definen la computación en la nube como modelo de prestación de servicios de computación a través de Internet, permitiendo a los usuarios acceder a recursos informáticos, como almacenamiento, servidores, bases de datos, redes, software, entre otros, de manera remota y según demanda. Entre los conceptos y características clave podemos destacar los siguientes:

- **Escalabilidad:** la capacidad de aumentar o disminuir recursos computacionales según las necesidades del usuario, lo que permite una flexibilidad sin precedentes en comparación con la infraestructura tradicional.
- **Pago por uso:** los usuarios pagan únicamente por los recursos que consumen, lo que puede ser más rentable que invertir en infraestructura propia.
- **Servicios bajo demanda:** los recursos están disponibles para ser utilizados de forma inmediata, sin necesidad de adquirir hardware o software adicional.
- **Virtualización:** la infraestructura en la nube se basa en la virtualización, lo que permite que múltiples usuarios compartan los mismos recursos físicos de manera segura y eficiente.
- **Elasticidad:** la capacidad de adaptarse automáticamente a fluctuaciones en la demanda de recursos, proporcionando más o menos capacidad según sea necesario.
- **Disponibilidad y fiabilidad:** los proveedores de servicios en la nube suelen garantizar altos niveles de disponibilidad y fiabilidad mediante la redundancia y la replicación de datos en múltiples ubicaciones.
- **Acceso global:** los usuarios pueden acceder a los servicios en la nube desde cualquier lugar del mundo, siempre que tengan conexión a Internet.
- **Automatización:** muchas tareas de administración y mantenimiento se pueden automatizar en la nube, lo que reduce la carga de trabajo para los usuarios y los administradores de sistemas.

- **Escalabilidad horizontal y vertical:** la nube permite tanto aumentar la capacidad de un recurso (escalabilidad vertical) como agregar más instancias del mismo recurso (escalabilidad horizontal) para manejar cargas de trabajo más pesadas.
- **Seguridad:** los proveedores de servicios en la nube suelen ofrecer medidas de seguridad avanzadas para proteger los datos y las aplicaciones de los usuarios, aunque la responsabilidad de la seguridad también recae en los propios usuarios.

1.2 Antecedentes de la computación en la nube

La computación en la nube, un paradigma tecnológico que ha evolucionado de conceptos como la virtualización y la infraestructura bajo demanda, ha transformado radicalmente la forma en que se ofrecen y consumen recursos informáticos a través de Internet. Desde sus orígenes hasta su adopción generalizada, la computación en la nube ha pasado por un desarrollo tecnológico y conceptual continuo, dando lugar a modelos de servicios como la Infraestructura como Servicio (IaaS), la Plataforma como Servicio (PaaS) y el Software como Servicio (SaaS). Estos modelos han permitido a las organizaciones y usuarios acceder a recursos informáticos escalables y flexibles de manera más eficiente y económica que nunca. Sin embargo, a pesar de sus beneficios, la computación en la nube también ha planteado desafíos significativos en términos de seguridad, privacidad, interoperabilidad y gestión de datos. La adopción empresarial y social de la computación en la nube ha sido impulsada por la necesidad de mejorar la agilidad y la capacidad de respuesta de las organizaciones frente a las demandas del mercado y la competencia global. Referencias bibliográficas como "A view of cloud computing" de Armbrust et al. Publicado en el año 2010 en la editorial ACM New York, NY, USA., "The NIST definition of cloud computing" de Mell y Grance, publicado en el año 2011, así como "Cloud computing: principles and paradigms" de Buyya et al. publicado en el año 2011 en la editorial Wiley., proporcionan un profundo análisis de los antecedentes, los modelos y las consideraciones clave relacionadas con la computación en la nube, permitiendo una comprensión más completa de su impacto y su potencial en el mundo actual.

1.3 Ventajas y desventajas de la computación en la nube

La computación en la nube ofrece una serie de ventajas significativas, pero también presenta algunas desventajas que deben ser consideradas. A continuación, se presentan algunas de estas ventajas y desventajas según la empresa Google ([Ventajas de la computación en la nube | Google Cloud], s. f.):

Ventajas

- **Costo reducido:** los servicios en la nube suelen ser más rentables ya que eliminan la necesidad de adquirir y mantener infraestructura física, lo que reduce los costos de capital y operativos.
- **Escalabilidad:** la capacidad de escalar recursos según la demanda permite a las empresas ajustar fácilmente sus capacidades informáticas para satisfacer los picos de uso sin tener que invertir en hardware adicional.
- **Acceso remoto:** los usuarios pueden acceder a los servicios en la nube desde cualquier lugar con conexión a Internet, lo que facilita el trabajo remoto y la colaboración entre equipos distribuidos geográficamente.
- **Actualizaciones automáticas:** los proveedores de servicios en la nube se encargan de mantener actualizadas las plataformas y aplicaciones, lo que garantiza que los usuarios siempre tengan acceso a las últimas características y mejoras de seguridad.
- **Mayor flexibilidad:** los servicios en la nube ofrecen una amplia gama de herramientas y servicios que pueden adaptarse a las necesidades específicas de cada empresa, permitiendo una mayor agilidad y capacidad de respuesta.
- **Respaldo y recuperación de datos:** los proveedores de servicios en la nube suelen ofrecer servicios de respaldo y recuperación de datos automáticos, lo que garantiza la integridad y disponibilidad de la información en caso de desastres o errores humanos.

Desventajas

- **Dependencia de la conexión a Internet:** la disponibilidad y el rendimiento de los servicios en la nube están directamente relacionados con la calidad de la conexión a Internet, lo que puede suponer un problema en áreas con conexiones poco fiables o lentas.
- **Seguridad y privacidad:** existen preocupaciones sobre la seguridad y privacidad de los datos almacenados en la nube, ya que los usuarios deben confiar en los proveedores de servicios para proteger su información de manera adecuada.
- **Posibles interrupciones del servicio:** los servicios en la nube pueden experimentar interrupciones temporales debido a fallas en el proveedor de servicios, ataques cibernéticos u otros problemas técnicos, lo que puede afectar la disponibilidad de los sistemas y aplicaciones.

- **Costos a largo plazo:** aunque inicialmente puede ser más económico utilizar servicios en la nube, a largo plazo los costos recurrentes pueden acumularse y superar el costo de la infraestructura propia.
- **Limitaciones de personalización:** algunos servicios en la nube pueden tener limitaciones en cuanto a la personalización y configuración, lo que puede ser una desventaja para empresas que requieren soluciones altamente personalizadas.
- **Cumplimiento normativo:** cumplir con ciertas regulaciones y estándares de cumplimiento puede ser más complicado en entornos de nube pública debido a preocupaciones sobre la ubicación de los datos y la conformidad con las leyes locales y sectoriales.

Evaluar estas ventajas y desventajas es crucial para determinar si la computación en la nube es la opción adecuada para una empresa o proyecto específico.

1.4 Modelos de computación en la nube

Existen diferentes modelos de computación en la nube de los cuales podríamos listar los siguientes:

- **Infraestructura como Servicio (IaaS):** en este modelo, los proveedores de servicios en la nube ofrecen infraestructura informática virtualizada, incluyendo servidores, redes y almacenamiento, a través de Internet. Los usuarios pueden aprovisionar y gestionar recursos de manera flexible según sus necesidades.
- **Plataforma como Servicio (PaaS):** en el modelo PaaS, los proveedores de servicios ofrecen una plataforma de desarrollo y despliegue que incluye herramientas, middleware y entornos de ejecución para que los desarrolladores creen, prueben y desplieguen aplicaciones de manera rápida y eficiente.
- **Software como Servicio (SaaS):** el modelo SaaS proporciona aplicaciones de software hospedadas y gestionadas por el proveedor de la nube y accesibles a través de Internet. Los usuarios pueden acceder a estas aplicaciones a través de un navegador web sin necesidad de instalar software adicional en sus dispositivos.
- **Nube Híbrida:** la nube híbrida combina recursos de infraestructura tanto en entornos de nube pública como privada, permitiendo a las organizaciones integrar y gestionar cargas de trabajo en diferentes plataformas de manera fluida.

- **Nube MultiCloud:** en un entorno MultiCloud, las organizaciones utilizan servicios de múltiples proveedores de nube para distribuir cargas de trabajo y minimizar dependencias de un proveedor único, aumentando la flexibilidad y la resiliencia.
- **Nube Federada:** la nube federada es un modelo que permite la interoperabilidad y la portabilidad de datos y cargas de trabajo entre múltiples entornos de nube, a menudo a través de estándares y protocolos comunes.

Los antes mencionados proporcionan una visión general de los diferentes modelos de computación en la nube y pueden ayudar a comprender sus características, beneficios y desafíos asociados. Además, hay una amplia gama de recursos disponibles para profundizar en cada uno de estos modelos y explorar su aplicación en diversos contextos empresariales y tecnológicos.

1.5 Desafíos presenta la computación en la nube

La computación en la nube ha revolucionado la forma en que las empresas gestionan sus recursos de tecnología de la información (TI). Este paradigma tecnológico ofrece una variedad de beneficios, desde la escalabilidad y la flexibilidad hasta la eficiencia operativa y la reducción de costos. Sin embargo, junto con estos beneficios vienen desafíos únicos que deben abordarse para una implementación exitosa y efectiva de la computación en la nube.

En este trabajo, exploraremos los conceptos generales de la computación en la nube y analizaremos en detalle aspectos fundamentales como la escalabilidad, los modelos de servicio, la virtualización, la seguridad y la gestión de costos. Además, examinaremos los desafíos y consideraciones adicionales asociados con la adopción de la computación en la nube, así como estrategias para superar estos desafíos y garantizar una implementación exitosa.

A través de una comprensión completa de estos conceptos y consideraciones, las empresas pueden aprovechar al máximo los beneficios de la computación en la nube mientras mitigar los riesgos y maximizar el retorno de la inversión. A lo largo de este trabajo, nos sumergiremos en el fascinante mundo de la computación en la nube y exploraremos cómo esta tecnología continúa transformando el panorama empresarial moderno.

- **Escalabilidad y Elasticidad**: uno de los aspectos más destacados de la computación en la nube es su capacidad para escalar recursos de forma rápida y eficiente. La escalabilidad permite a las empresas ajustar sus recursos en función de la demanda

del usuario, lo que resulta en un uso más eficiente de los recursos y una mejor capacidad de respuesta a las fluctuaciones en la carga de trabajo. Además, la elasticidad garantiza que los recursos se adapten dinámicamente a las necesidades cambiantes de la carga de trabajo, lo que implica la asignación y desasignación automática de recursos según sea necesario, optimizando así el rendimiento y minimizando los costos operativos.

- **Modelos de Servicio**: la computación en la nube se basa en varios modelos de servicio, cada uno con diferentes niveles de responsabilidad compartida entre el proveedor de la nube y el usuario final. El Software como Servicio (SaaS) ofrece aplicaciones alojadas y gestionadas por el proveedor de la nube, mientras que la Plataforma como Servicio (PaaS) proporciona una plataforma de desarrollo y herramientas para construir y desplegar aplicaciones. Por otro lado, la Infraestructura como Servicio (IaaS) ofrece recursos de infraestructura, como servidores virtuales y almacenamiento, que los usuarios pueden configurar y gestionar según sus necesidades.
- **Virtualización**: la virtualización es una tecnología subyacente clave en la computación en la nube que permite la creación de entornos de computación virtuales. Al virtualizar recursos de hardware, como servidores, redes y almacenamiento, la virtualización permite a los usuarios ejecutar múltiples sistemas operativos y aplicaciones en un solo servidor físico. Esto maximiza la utilización de recursos, reduce los costos de infraestructura y mejora la eficiencia operativa.
- **Seguridad**: la seguridad es una preocupación fundamental en la computación en la nube, especialmente porque los datos y las aplicaciones se almacenan y procesan fuera de las instalaciones de la empresa. Es esencial implementar medidas de seguridad robustas para proteger la información confidencial contra amenazas como el acceso no autorizado, la piratería informática y el robo de datos. Esto incluye prácticas como el cifrado de datos, la autenticación multifactorial, la gestión de accesos y la monitorización continua de la seguridad.
- **Gestión de Costos**: la gestión de costos es un aspecto crítico de la computación en la nube, ya que los servicios suelen basarse en un modelo de pago por uso. Para evitar costos excesivos y garantizar la rentabilidad de la inversión en la nube, las empresas deben monitorear y optimizar el consumo de recursos. Esto puede implicar la implementación de herramientas de gestión de costos, la planificación y asignación

adecuada de presupuestos, y la optimización de la arquitectura de la nube para maximizar la eficiencia y minimizar los gastos innecesarios.

- **Desafíos y Consideraciones Adicionales**: además de los beneficios, la adopción de la computación en la nube también plantea desafíos y consideraciones adicionales que deben abordarse. Estos incluyen la disponibilidad de una conectividad confiable a Internet, el cumplimiento normativo, la capacitación del personal, la gestión de proveedores de servicios en la nube y la integración con sistemas existentes.

1.6 Tendencias en Servicios en la Nube para la Recuperación de Sistemas Críticos ante Desastres

La adopción de servicios en la nube para la recuperación de sistemas críticos ante desastres se ha convertido en una prioridad para muchas empresas en todo el mundo. En un entorno empresarial cada vez más digital y dinámico, la capacidad de mantener la continuidad del negocio en situaciones de emergencia es fundamental para garantizar la supervivencia y el crecimiento a largo plazo. En este contexto, las empresas están recurriendo a soluciones innovadoras basadas en la nube para fortalecer sus estrategias de recuperación ante desastres, aprovechando tecnologías como el DRaaS, la automatización, la inteligencia artificial y la gestión de múltiples nubes. En este documento, exploraremos las tendencias más relevantes en servicios en la nube para la recuperación de sistemas críticos ante desastres, así como su impacto en el panorama empresarial actual.

- **Recuperación ante desastres como servicio (DRaaS)**: el DRaaS sigue creciendo en popularidad debido a su flexibilidad y ahorro de costos. Permite a las empresas externalizar la gestión de la recuperación ante desastres, lo que reduce la carga operativa y proporciona acceso a recursos de recuperación ante desastres de alta calidad sin la necesidad de inversiones significativas en infraestructura.
- **Automatización y orquestación**: la automatización y la orquestación están transformando la forma en que las empresas gestionan la recuperación ante desastres al agilizar los procesos y minimizar el tiempo de inactividad. Esto se logra mediante la implementación de herramientas y plataformas que permiten la ejecución automática de tareas de recuperación ante desastres, como la conmutación por error y la restauración de datos, sin intervención humana.
- **Integración de tecnologías emergentes**: la integración de tecnologías como la inteligencia artificial (IA) y el aprendizaje automático (ML) está mejorando la capacidad de detección y respuesta de las soluciones de recuperación ante desastres.

Estas tecnologías permiten a las empresas identificar y mitigar proactivamente las amenazas, reduciendo así el tiempo de detección y minimizando el impacto de los incidentes.

- **Enfoque en la seguridad y el cumplimiento normativo**: con el aumento de las amenazas cibernéticas y las regulaciones de privacidad, las empresas están priorizando la seguridad y el cumplimiento normativo en sus estrategias de recuperación ante desastres en la nube. Esto incluye la implementación de medidas de seguridad avanzadas, como el cifrado de datos, la autenticación multifactorial y el monitoreo continuo de amenazas.
- **Adopción de múltiples nubes**: las empresas están adoptando estrategias de múltiples nubes para diversificar sus opciones de recuperación ante desastres y mejorar la resiliencia de sus sistemas críticos. Al utilizar múltiples proveedores de servicios en la nube, las organizaciones pueden reducir la dependencia de un solo proveedor y mitigar el riesgo de interrupciones del servicio.
- **Enfoque en la sostenibilidad y la eficiencia energética**: las empresas están prestando más atención a la sostenibilidad ambiental en sus operaciones de TI, incluida la recuperación ante desastres en la nube. Al adoptar prácticas y tecnologías que reducen el consumo de energía y minimizan el impacto ambiental, las organizaciones pueden mejorar su huella ecológica y contribuir a la protección del medio ambiente.

Estas tendencias reflejan la evolución continua del panorama de la recuperación ante desastres en la nube y proporcionan una visión completa de las innovaciones y las mejores prácticas emergentes en este campo. Al adoptar estas tendencias y enfoques, las empresas pueden mejorar su capacidad para resistir y recuperarse de eventos catastróficos, garantizando así la continuidad del negocio y protegiendo sus activos críticos.

2. Elementos de un Plan de Recuperación ante Desastres (DRP)

2.1 Introducción al DRP

2.1.1 Definición y propósito del DRP

Empresas como IBM, Amazon, Microsoft, Google y CISCO definen el plan de recuperación ante desastres (DRP o disaster recovery plan) como la documentación y procesos estratégicos de una organización para restaurar el acceso a los sistemas e infraestructuras

comprometidos después de un ciberataque, error humano, desastre natural u otros eventos catastróficos.

Es la metodología sistemática mediante la cual un equipo asigna sus recursos para retomar eficazmente el control de sistemas clave de datos e información después de un desastre.

La recuperación ante desastres tiene un doble propósito: el mantenimiento y el restablecimiento de sistemas e infraestructuras de TI claves después de una incidencia. El mantenimiento funciona mediante la adecuada replicación y respaldo de datos y activos a puntos de restauración específicos. La recuperación es un esfuerzo reactivo para recuperar funcionalidad y control sobre sistemas y datos que resultan infectados o vulnerados.

Un plan de recuperación ante desastres se puede usar para resolver situaciones tanto leves como graves. Esto puede ser, por ejemplo, problemas como software con fallos. O también pueden ser tragedias devastadoras, como una filtración de datos general o una pandemia. Lo que vuelve eficaz a los planes de recuperación ante desastres es la capacidad de anticiparse a las amenazas antes de que surjan realmente, y probar con diversos escenarios de amenazas para garantizar que el plan esté funcionando bien.

2.1.2 Breve historia y evolución del concepto de DRP

La historia y evolución del concepto de Plan de Recuperación ante Desastres (DRP) está intrínsecamente ligada al desarrollo tecnológico y la creciente dependencia de las organizaciones en la informática y los sistemas de información (Galileus, 17 septiembre 2012). Una empresa tecnológica importante que ha desempeñado un papel fundamental en esta evolución es IBM.

En las décadas de 1960 y 1970, las computadoras comenzaron a ser ampliamente utilizadas por empresas y organizaciones gubernamentales para procesar datos y automatizar procesos (Galileus, 17 septiembre 2012). Sin embargo, estos sistemas iniciales eran grandes, costosos y propensos a fallas. En ese entonces, la preocupación principal era la protección de los datos contra pérdidas debido a fallos de hardware.

IBM (Herbane, 2010), una de las principales compañías de tecnología de la época, fue pionera en el desarrollo de soluciones para garantizar la disponibilidad y la integridad de los datos. En la década de 1970, IBM introdujo el concepto de "Plan de Continuidad del Negocio" (BCP, por sus siglas en inglés), que se centraba en mantener las operaciones

comerciales en funcionamiento durante situaciones de crisis, incluidos desastres naturales y fallas de equipos.

A medida que las tecnologías de la información evolucionaron y las empresas dependían cada vez más de los sistemas informáticos para operar, surgió la necesidad de planes más específicos para la recuperación de sistemas y datos en caso de desastres. Es en este punto donde se establece el concepto moderno de Plan de Recuperación ante Desastres (DRP).

IBM ([Recuperación de desastres: Introducción | IBM], s. f.) continuó liderando el camino en el desarrollo de tecnologías y prácticas relacionadas con la recuperación ante desastres. Introdujo soluciones de almacenamiento redundante, como RAID (Redundant Array of Independent Disks), que ayudaron a proteger los datos contra fallas de hardware. También proporcionó servicios de consultoría para ayudar a las organizaciones a desarrollar e implementar sus propios planes de recuperación ante desastres.

Con el tiempo, otras empresas tecnológicas importantes, como Microsoft (Martinekuan, s. f.), Oracle ([¿Qué es la recuperación ante desastres?], s. f.) y EMC (ahora parte de Dell Technologies), también han contribuido al desarrollo de soluciones y mejores prácticas en el ámbito de la recuperación ante desastres, ofreciendo una amplia gama de productos y servicios para respaldar la continuidad del negocio y la recuperación de datos.

En resumen, la evolución del concepto de DRP ha estado estrechamente relacionada con el avance tecnológico y la necesidad de proteger la integridad y la disponibilidad de los datos en un mundo cada vez más digitalizado. Grandes empresas tecnológicas como IBM han desempeñado un papel fundamental en esta evolución, proporcionando soluciones innovadoras y liderando el desarrollo de prácticas y estándares en el campo de la recuperación ante desastres.

2.2 Análisis de Riesgos

2.2.1 Identificación de amenazas y vulnerabilidades

Es un proceso integral que implica analizar detenidamente los riesgos a los que está expuesta una organización y tomar medidas proactivas para proteger sus operaciones comerciales y sus activos.

La identificación de amenazas y vulnerabilidades es un paso crítico en el proceso de análisis de riesgos y en la creación de un plan integral de recuperación de desastres. Sus procesos son los siguientes:

- **Recopilación de información:** el primer paso en la identificación de amenazas y vulnerabilidades es recopilar información sobre la organización, sus operaciones, infraestructura, sistemas y entorno operativo. Esto puede incluir revisar documentación existente, entrevistar a personal clave, revisar incidentes pasados y realizar análisis de datos relevantes.
- **Análisis de amenazas:** una vez recopilada la información, se procede a identificar y analizar las posibles amenazas que podrían afectar a la organización. Las amenazas pueden ser de origen natural, como desastres naturales (terremotos, inundaciones, tormentas), o pueden ser de origen humano, como ataques cibernéticos, actos de terrorismo o sabotaje interno.
- **Identificación de vulnerabilidades:** después de identificar las amenazas, se evalúa la vulnerabilidad de la organización frente a cada una de ellas. Las vulnerabilidades pueden ser debilidades en la infraestructura física, deficiencias en la seguridad de la información, dependencia excesiva de proveedores o cualquier otra brecha que pueda ser explotada por las amenazas identificadas.
- **Evaluación de impacto:** una vez que se han identificado las amenazas y vulnerabilidades, se evalúa el impacto potencial que podrían tener en las operaciones de la organización. Esto implica considerar cómo cada amenaza podría afectar a los procesos comerciales, la infraestructura, los activos críticos, la reputación y las finanzas de la organización.
- **Priorización de riesgos:** después de evaluar el impacto de las amenazas y vulnerabilidades, se priorizan los riesgos según su probabilidad de ocurrencia y su impacto potencial en la organización. Esto permite a la organización enfocar sus recursos y esfuerzos en abordar los riesgos más críticos y urgentes.

- **Desarrollo de estrategias de mitigación:** una vez que se han identificado y priorizado los riesgos, se desarrollan estrategias de mitigación para reducir la probabilidad de ocurrencia de las amenazas y minimizar su impacto en caso de que ocurran. Estas estrategias pueden incluir la implementación de controles de seguridad, la adopción de políticas y procedimientos, la mejora de la infraestructura y la capacitación del personal.

2.2.2 Evaluación del impacto potencial de los desastres

La evaluación del impacto potencial de los desastres es una etapa crucial en la planificación de la recuperación de desastres, que implica evaluar tanto la probabilidad como las posibles consecuencias de los riesgos que enfrenta su empresa. Con la creciente frecuencia de ciberataques y ransomware, comprender los riesgos de ciberseguridad esencialmente se vuelve crítico, así como también entender los riesgos específicos asociados con su industria y ubicación geográfica.

Al considerar una variedad de escenarios, desde desastres naturales hasta fallas de equipos y amenazas internas, es importante realizar una evaluación exhaustiva de los riesgos y su impacto en su negocio. Para lograrlo, es útil plantearse las siguientes preguntas:

- **Pérdidas financieras:** ¿Cuánto podrían afectar las interrupciones en las operaciones a su flujo de ingresos? ¿Qué pérdidas financieras podrían surgir debido a la pérdida de oportunidades de ventas o a la interrupción de actividades generadoras de ingresos?
- **Reputación de la marca y satisfacción del cliente:** ¿Qué tipo de daño podría sufrir la reputación de su marca? ¿Cómo se vería afectada la satisfacción del cliente como resultado de un evento disruptivo?
- **Productividad de los empleados:** ¿Cómo se vería afectada la productividad de los empleados en caso de un desastre? ¿Cuántas horas laborales podrían perderse?
- **Salud y seguridad humana:** ¿Qué riesgos podrían representar el incidente para la salud o la seguridad de las personas involucradas, ya sean empleados, clientes o la comunidad en general?
- **Progreso empresarial:** ¿Cómo podría verse afectado el progreso hacia los objetivos y metas empresariales establecidos? ¿Existen iniciativas críticas que podrían retrasarse o interrumpirse como resultado del desastre?

Al abordar estas preguntas, podrá identificar áreas clave de vulnerabilidad y priorizar los recursos y esfuerzos necesarios para mitigar los riesgos y garantizar la continuidad de su negocio ante posibles desastres.

2.2.3 Métodos y herramientas para el análisis de riesgos

- **Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas):** el análisis FODA, una técnica ampliamente utilizada para evaluar la posición estratégica de una organización, se adapta a la gestión de riesgos. Permite identificar las fortalezas y debilidades internas, así como las oportunidades y amenazas externas. Al aplicar este análisis a la gestión de riesgos, se logra una visión completa de la situación actual y futura de la organización. Esto facilita una mejor comprensión de los riesgos y la implementación de medidas apropiadas para minimizarlos o aprovechar las oportunidades disponibles.
- **Evaluación de riesgos cualitativa y cuantitativa:** la evaluación de riesgos, fundamental en la gestión de riesgos, puede llevarse a cabo de manera cualitativa o cuantitativa:
    - La evaluación cualitativa se basa en una evaluación subjetiva de los riesgos según su impacto y probabilidad. Esto permite clasificar los riesgos y asignarles una puntuación o categoría en función de su gravedad y probabilidad de ocurrencia, facilitando la identificación de los más críticos.
    - La evaluación cuantitativa, por otro lado, se apoya en el análisis numérico y cálculos estadísticos para determinar la probabilidad de ocurrencia y el impacto de los riesgos. Este enfoque proporciona una estimación más precisa de los riesgos y su impacto financiero.
- **Análisis de escenarios:** el análisis de escenarios implica identificar y evaluar diversas situaciones hipotéticas que podrían afectar a una organización. Permite prepararse para eventos adversos y desarrollar estrategias de mitigación de riesgos, facilitando la toma de decisiones informadas y la minimización de sorpresas.

- **Análisis de causa raíz:** cuando surge un problema o un riesgo se materializa, es crucial identificar su causa raíz para evitar recurrencias. Este análisis se centra en identificar y abordar las causas fundamentales de un problema o evento adverso, en lugar de tratar solo los síntomas superficiales.
- **Análisis Preliminar de Riesgos (APR):** el Análisis Preliminar de Riesgos, llevado a cabo en las etapas iniciales de un proyecto o proceso, busca identificar y evaluar los riesgos potenciales asociados con una actividad específica antes de su ejecución. Esto permite tomar decisiones informadas y establecer medidas preventivas y correctivas.
- **Matriz de riesgo:** una matriz de riesgo visualiza y prioriza los riesgos identificados en función de su impacto y probabilidad, facilitando la comprensión y gestión de los riesgos de manera efectiva.
- **Análisis costo-beneficio:** esta herramienta evalúa los costos y beneficios asociados con la implementación de medidas de mitigación de riesgos, ayudando a determinar la justificación financiera de dichas medidas.
- **Evaluación de proveedores y socios comerciales:** la evaluación de proveedores y socios comerciales busca mitigar los riesgos asociados con las relaciones comerciales externas, evaluando el cumplimiento normativo, la capacidad financiera y otros aspectos relevantes.
- **Monitoreo y análisis de datos:** el seguimiento y análisis de datos son fundamentales para detectar patrones y anomalías que puedan indicar riesgos emergentes, permitiendo una gestión de riesgos basada en evidencias y una mejora continua.
- **Planificación de contingencia y respuesta a crisis:** contar con un plan de contingencia y respuesta a crisis es esencial para minimizar el impacto de eventos adversos, proteger a empleados y clientes, y garantizar la continuidad del negocio, contribuyendo a la resiliencia y reputación de la organización.
- **Herramientas del análisis:**
    - **Inteligencia artificial (IA):** la IA se utiliza para anticipar y predecir posibles amenazas y ataques cibernéticos. Puede analizar grandes cantidades de datos para identificar patrones y anomalías, lo que permite a las organizaciones tomar medidas proactivas para proteger sus sistemas y datos.
    - **Software antivirus:** los programas antivirus son herramientas diseñadas para detectar, prevenir y eliminar software malicioso, como virus, troyanos, gusanos y ransomware, de los dispositivos informáticos. Protegen los

sistemas contra ataques cibernéticos y ayudan a mantener la integridad y seguridad de la información.

- **Firewall o cortafuegos:** un firewall es una barrera de seguridad que monitorea y controla el tráfico de red entre una red interna y externa. Ayuda a prevenir el acceso no autorizado a la red y protege los sistemas contra intrusiones, ataques y malware.
- **Plan de seguridad informática:** un plan de seguridad informática es un conjunto de políticas, procedimientos y controles diseñados para proteger los activos de información de una organización. Sirve para detectar y mitigar riesgos de seguridad, establecer roles y responsabilidades, y responder de manera efectiva a incidentes de seguridad.
- **Infraestructura de clave pública (PKI):** la PKI proporciona un marco de seguridad para el intercambio de información confidencial en línea. Utiliza un sistema de claves públicas y privadas para cifrar y firmar digitalmente datos, garantizando la autenticidad, integridad y confidencialidad de la información transmitida.
- **Pentesting:** el pentesting, o testeo de penetración, se utiliza para evaluar la seguridad de los sistemas informáticos al simular ataques cibernéticos controlados. Ayuda a identificar vulnerabilidades y puntos débiles en la seguridad de una organización, permitiendo tomar medidas correctivas para fortalecer la seguridad.
- **Personal capacitado:** el personal capacitado es fundamental para implementar y mantener eficazmente las herramientas y procesos de seguridad informática. Proporciona el conocimiento y las habilidades necesarias para gestionar la seguridad de la información, identificar y mitigar riesgos, y responder a incidentes de seguridad de manera adecuada.

2.3 Objetivos y Alcance del DRP

A continuación, se presentan algunos aspectos que se deben considerar en el establecimiento de los objetivos y el alcance de un DRP según IBM ([Recuperación de desastres: Introducción | IBM], s. f.).

2.3.1 Establecimiento de Objetivos Claros para el DRP

- **Identificación de los objetivos estratégicos del DRP:** los objetivos del DRP deben alinearse con los objetivos estratégicos de la organización. Estos pueden incluir

minimizar el tiempo de inactividad, proteger los datos críticos, mantener la continuidad de las operaciones y preservar la reputación de la empresa.

- **Definición de métricas de rendimiento:** se deben establecer métricas claras para evaluar la efectividad del DRP. Estas métricas pueden incluir el tiempo de recuperación objetivo (RTO), el punto de recuperación objetivo (RPO), la tasa de éxito de recuperación y la satisfacción del cliente interno y externo.

2.3.2 Definición del Alcance del DRP

- **Identificación de los activos críticos:** se deben identificar y priorizar los activos críticos de la organización, como datos, sistemas, infraestructura, personal clave y procesos comerciales.
- **Evaluación de riesgos y amenazas:** se debe realizar un análisis de riesgos exhaustivo para determinar las posibles amenazas que podrían afectar a los activos críticos y el impacto potencial de estas amenazas en las operaciones comerciales.
- **Determinación de los escenarios de desastre:** se deben definir los escenarios de desastre más probables, como fallas de hardware, ataques cibernéticos, desastres naturales, interrupciones en el suministro de energía, entre otros.

2.3.3 Consideraciones Legales y Regulatorias

- **Cumplimiento normativo:** el DRP debe cumplir con todas las regulaciones y normativas pertinentes, como la NRP-24, que rige la continuidad del negocio en El Salvador.
- **Requisitos contractuales:** se deben tener en cuenta los requisitos contractuales con clientes, proveedores y socios comerciales relacionados con la recuperación ante desastres. Esto puede incluir acuerdos de nivel de servicio (SLA) y cláusulas de continuidad del negocio en contratos comerciales.

2.4 Políticas y Procedimientos de Respuesta

2.4.1 El desarrollo de políticas de respuesta ante desastres

Mediante el uso de servicios en la nube para sistemas críticos, es una iniciativa crucial en un país propenso a desastres naturales como El Salvador. Estas políticas deben diseñarse considerando varios factores clave. En primer lugar, se debe realizar una evaluación exhaustiva de los sistemas críticos de la empresa y de su vulnerabilidad ante diferentes tipos de desastres, como terremotos, inundaciones o fallos de infraestructura (Rittinghouse, 2016).

A continuación, se deben identificar los servicios en la nube adecuados que puedan proporcionar redundancia, escalabilidad y recuperación ante desastres para estos sistemas críticos (Hashizume, 2013). Esto podría incluir el uso de servicios de almacenamiento en la nube para copias de seguridad, servicios de recuperación ante desastres para replicar entornos críticos en la nube, y servicios de alta disponibilidad para garantizar la continuidad del negocio incluso en situaciones de emergencia.

Además, es esencial establecer procedimientos claros de gestión de crisis y de activación de planes de respuesta ante desastres, así como realizar pruebas regulares para garantizar la eficacia de estos planes (Hugos, 2018). La formación del personal en el uso de servicios en la nube y en los procedimientos de respuesta ante desastres también es fundamental. Por último, es importante mantener una comunicación constante con los proveedores de servicios en la nube y con las autoridades locales para estar al tanto de las mejores prácticas y de las últimas actualizaciones en materia de seguridad y gestión de crisis (Velte, 2009). Este enfoque integral ayudará a las empresas salvadoreñas a estar mejor preparadas para hacer frente a cualquier eventualidad y a garantizar la continuidad de sus operaciones incluso en tiempos de crisis.

2.4.2 Establecimiento de procedimientos de acción

Es fundamental para garantizar la continuidad del negocio y la respuesta efectiva ante posibles crisis. Estos procedimientos deben diseñarse meticulosamente, considerando varios aspectos clave. En primer lugar, es esencial identificar y priorizar los sistemas críticos de la empresa respaldados por servicios en la nube, como sistemas de gestión de clientes o bases de datos financieras. Luego, se deben establecer protocolos claros para la configuración, implementación y gestión de estos servicios en la nube, incluyendo la asignación de roles y responsabilidades dentro del equipo de gestión de crisis.

Además, se deben definir procedimientos específicos para la monitorización y el mantenimiento continuo de los sistemas críticos en la nube, asegurando su disponibilidad y rendimiento óptimo en todo momento (Armbrust, abril 2010). Esto podría incluir la configuración de alertas automatizadas para detectar posibles fallos o anomalías, así como la realización de pruebas regulares de recuperación ante desastres para garantizar la eficacia de los procedimientos de respaldo y restauración de datos (Hugos, 2018). También es importante establecer una comunicación clara y efectiva entre los equipos internos de la

empresa y los proveedores de servicios en la nube, para coordinar la respuesta ante incidentes y resolver cualquier problema de manera rápida y eficiente.

Por último, es crucial realizar capacitaciones periódicas para el personal de la empresa sobre el uso de los servicios en la nube y los procedimientos de acción en caso de emergencia (Velte, 2009). Esto garantizará que todos los empleados estén familiarizados con los protocolos de respuesta ante desastres y puedan actuar de manera coordinada en situaciones críticas. En resumen, el establecimiento de procedimientos de acción para empresas salvadoreñas a través de servicios en la nube para sistemas críticos requiere una planificación cuidadosa, una coordinación efectiva y una formación adecuada del personal para garantizar la resiliencia y la continuidad del negocio en todo momento.

2.4.3 Roles y responsabilidades del personal durante un desastre

Durante un desastre, es crucial que el personal de una empresa salvadoreña respaldada por servicios en la nube para sistemas críticos asuma roles y responsabilidades definidos para garantizar una respuesta efectiva. Estos roles pueden incluir:

- **Líder del Equipo de Crisis:** encargado de coordinar y liderar las acciones de respuesta ante desastres, comunicarse con las partes interesadas internas y externas, y tomar decisiones estratégicas para garantizar la continuidad del negocio (Hugos, 2018).
- **Administrador de Sistemas en la Nube:** responsable de supervisar la infraestructura en la nube, gestionar la disponibilidad de los servicios críticos y coordinar con el proveedor de servicios en la nube para implementar medidas de recuperación ante desastres (Velte, 2009).
- **Especialista en Seguridad de la Información:** encargado de garantizar la seguridad de los datos y sistemas críticos durante la respuesta ante desastres, implementando medidas de protección y supervisando posibles vulnerabilidades (Hashizume, 2013).
- **Equipo de Soporte Técnico:** responsable de brindar asistencia técnica y resolver problemas relacionados con el uso de servicios en la nube y la recuperación de sistemas críticos, garantizando una rápida resolución de incidentes (Marston, 2011).
- **Comunicaciones y Relaciones Públicas:** encargado de gestionar la comunicación interna y externa durante el desastre, proporcionando actualizaciones regulares a los empleados, clientes, proveedores y otras partes interesadas (Fearn-Banks, 2019).

Es fundamental que cada miembro del personal esté capacitado y familiarizado con sus roles y responsabilidades específicos durante un desastre, y que exista una clara coordinación entre los diferentes equipos. La formación regular y la realización de simulacros de respuesta ante desastres pueden ayudar a garantizar una preparación adecuada y una respuesta efectiva en momentos críticos.

2.5 Recuperación de Datos y Sistemas

Entre las estrategias recomendadas por Google ([¿Qué es la recuperación ante desastres y por qué es importante? | Google Cloud], s. f.), IBM ([Recuperación de desastres: Introducción | IBM], s. f.) y Oracle ([¿Qué es la recuperación ante desastres? | Oracle México], s. f.) (algunas incluso definidas en la NRP-24 ([NRP-24: Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio], 14 de abril 2020)) a seguir para el respaldo y recuperación de sistemas y datos podemos mencionar las siguientes:

2.5.1 Estrategias de Respaldo y Recuperación de Datos

- **Implementación de copias de seguridad regulares:** se deben establecer políticas y procedimientos para realizar copias de seguridad periódicas de datos críticos. Esto puede incluir copias de seguridad completas, incrementales y diferenciales, dependiendo de los requisitos de recuperación y el volumen de datos.
- **Almacenamiento seguro de las copias de seguridad:** se deben definir ubicaciones seguras y fuera del sitio para almacenar las copias de seguridad, como centros de datos secundarios, servicios de almacenamiento en la nube o instalaciones de almacenamiento en frío.
- **Pruebas de restauración de datos:** se deben realizar pruebas periódicas para verificar la integridad y la accesibilidad de las copias de seguridad. Esto garantiza que los datos se puedan recuperar de manera efectiva en caso de un desastre.

2.5.2 Implementación de Sistemas de Respaldo y Redundancia

- **Uso de tecnologías de almacenamiento redundante:** se deben implementar tecnologías como RAID (Redundant Array of Independent Disks) para proporcionar redundancia de datos y aumentar la disponibilidad de los sistemas.
- **Replicación de datos:** se pueden utilizar soluciones de replicación de datos para crear copias en tiempo real de los datos en ubicaciones geográficamente dispersas. Esto garantiza la disponibilidad continua de los datos incluso en caso de falla de hardware o desastre en una ubicación.

- **Virtualización de servidores:** la virtualización de servidores permite la migración rápida y la recuperación de sistemas críticos en caso de desastre. Los servidores virtuales pueden ser replicados y restaurados en un entorno alternativo de manera rápida y eficiente.

2.5.3 Procedimientos para la Restauración de Sistemas y Datos

- **Priorización de la restauración:** se deben establecer criterios claros para priorizar la restauración de sistemas y datos en función de su importancia para las operaciones comerciales. Esto ayuda a minimizar el tiempo de inactividad y priorizar los recursos durante la recuperación.
- **Documentación detallada de los procedimientos de restauración:** se deben crear guías paso a paso y procedimientos detallados para la restauración de sistemas y datos. Esto garantiza que el personal encargado de la recuperación pueda seguir los pasos adecuados durante una situación de desastre.
- **Automatización de procesos de restauración:** se pueden utilizar herramientas de automatización para agilizar y simplificar el proceso de restauración de sistemas y datos. Esto reduce el riesgo de errores humanos y acelera la recuperación.

2.6 Infraestructura de Respuesta ante Desastres

2.6.1 Consideraciones sobre infraestructura física y tecnológica

Al migrar sistemas críticos a servicios en la nube, las empresas salvadoreñas deben considerar cuidadosamente las implicaciones de infraestructura física y tecnológica para garantizar una transición exitosa y una operación continua. Algunas de estas consideraciones incluyen:

- **Conectividad y Ancho de Banda:** la disponibilidad de una conexión a Internet confiable y de alta velocidad es crucial para acceder a los servicios en la nube de manera eficiente y mantener la continuidad del negocio (Toth, 2014).
- **Seguridad Física de los Centros de Datos:** es importante evaluar la seguridad física de los centros de datos de los proveedores de servicios en la nube para garantizar la protección adecuada de los servidores y la infraestructura crítica (Hashizume, 2013).
- **Respaldo y Recuperación de Datos:** implementar políticas robustas de respaldo y recuperación de datos para asegurar la disponibilidad y la integridad de la información crítica en caso de desastres o fallas del sistema (Hugos, 2018).

Estas consideraciones son fundamentales para garantizar una migración exitosa a la nube y para mantener la operación continua y segura de los sistemas críticos de una empresa salvadoreña.

2.6.2 Planificación de la continuidad del negocio

Esto es algo esencial para garantizar la resiliencia operativa en caso de interrupciones. Algunas consideraciones importantes en este proceso incluyen:

- **Evaluación de Riesgos y Vulnerabilidades:** realizar una evaluación exhaustiva de los riesgos y vulnerabilidades que puedan afectar los sistemas críticos en la nube, considerando amenazas tanto internas como externas (Hugos, 2018).
- **Identificación de Recursos Críticos:** identificar los recursos y servicios en la nube que son críticos para las operaciones del negocio y priorizar su protección y recuperación (Velte, 2009).
- **Desarrollo de Estrategias de Respaldo y Recuperación**: desarrollar estrategias detalladas de respaldo y recuperación de datos, incluyendo la implementación de copias de seguridad frecuentes y la utilización de servicios de recuperación ante desastres en la nube (Armbrust, 2010).
- **Establecimiento de Procedimientos de Respuesta ante Incidentes:** definir procedimientos claros y protocolos de actuación para el personal en caso de incidentes, asegurando una respuesta rápida y eficaz a situaciones de crisis (Marston, 2011).
- **Pruebas y Ejercicios de Simulación:** realizar pruebas regulares y ejercicios de simulación para evaluar la efectividad de los planes de continuidad del negocio y garantizar la preparación del personal para situaciones de emergencia (Toth, 2014).
- **Mantenimiento de la Formación y Concienciación del Personal**: proporcionar formación continua al personal sobre los procedimientos de continuidad del negocio y aumentar la concienciación sobre la importancia de la preparación para desastres (Doughty, 2014).

Estas medidas ayudarán a las empresas salvadoreñas a mitigar los riesgos y a mantener la operatividad de sus sistemas críticos incluso en situaciones adversas.

2.6.3 Recursos necesarios para la recuperación

La recuperación de sistemas críticos para empresas salvadoreñas mediante servicios en la nube requiere una cuidadosa consideración de los recursos necesarios para garantizar una restauración efectiva y oportuna. Algunos de estos recursos incluyen:

- **Almacenamiento en la Nube:** se necesitan capacidades de almacenamiento adecuadas en la nube para almacenar copias de seguridad de datos críticos y aplicaciones, lo que permite una rápida recuperación en caso de desastres (Armbrust, 2010).
- **Capacidad de Procesamiento:** es crucial contar con suficiente capacidad de procesamiento en la nube para ejecutar aplicaciones y cargas de trabajo críticas durante el proceso de recuperación, asegurando una rápida restauración de la funcionalidad del sistema (Velte, 2009).
- **Ancho de Banda y Conectividad:** se requiere una conectividad de red robusta y un ancho de banda adecuado para transferir datos entre los sistemas locales y los servicios en la nube durante el proceso de recuperación, minimizando el tiempo de inactividad (Marston, 2011).
- **Herramientas de Gestión y Automatización:** el uso de herramientas de gestión y automatización en la nube puede facilitar la implementación y supervisión de procesos de recuperación, mejorando la eficiencia y reduciendo el riesgo de errores humanos.
- **Personal Capacitado:** es fundamental contar con personal capacitado en la gestión de la nube y en los procedimientos de recuperación de desastres para garantizar una respuesta efectiva y coordinada durante situaciones de crisis (Hashizume, 2013).
- **Contratos de Nivel de Servicio (SLA):** establecer SLAs claros con los proveedores de servicios en la nube para garantizar niveles de rendimiento, disponibilidad y tiempo de respuesta específicos durante la recuperación de desastres (Doughty, 2014).

Al asegurar estos recursos, las empresas salvadoreñas pueden estar mejor preparadas para enfrentar y recuperarse de situaciones de emergencia que afecten a sus sistemas críticos.

2.7 Entrenamiento y Pruebas del Plan

La NRP-24 ([NRP-24: Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio], 14 de abril 2020) nos brinda los siguientes puntos que se deben tener al momento de realizar el entrenamiento y pruebas de nuestro DRP:

2.7.1 Programación de Simulacros y Pruebas de Recuperación

- **Planificación de simulacros regulares:** se deben programar simulacros de recuperación ante desastres de manera regular para garantizar que el personal esté familiarizado con los procedimientos y pueda responder de manera efectiva en situaciones reales de emergencia.
- **Diversificación de escenarios de prueba:** los simulacros deben incluir una variedad de escenarios de desastre, como fallas de hardware, ataques cibernéticos, desastres naturales, interrupciones en el suministro de energía, entre otros, para evaluar la capacidad de respuesta del DRP en diferentes situaciones.
- **Evaluación y análisis de resultados:** después de cada simulacro, se debe realizar una evaluación exhaustiva para identificar áreas de mejora y revisar los procedimientos según sea necesario. Esto ayuda a garantizar que el DRP esté actualizado y sea efectivo en la práctica.

2.7.2 Capacitación del Personal en los Procedimientos del DRP

- **Desarrollo de programas de capacitación:** se deben desarrollar programas de capacitación específicos para el personal involucrado en la implementación y ejecución del DRP. Esto puede incluir sesiones de entrenamiento en línea, clases presenciales, manuales de referencia y materiales de capacitación.
- **Inclusión de roles y responsabilidades:** la capacitación debe incluir una descripción detallada de los roles y responsabilidades de cada miembro del equipo durante una situación de desastre, asegurando que el personal esté preparado para asumir sus funciones de manera efectiva.
- **Pruebas de habilidades y competencias:** además de la capacitación teórica, se deben realizar pruebas prácticas para evaluar las habilidades y competencias del personal en la ejecución de los procedimientos del DRP. Esto garantiza que el personal esté listo para responder de manera efectiva en situaciones reales.

2.7.3 Evaluación y Mejora Continua del Plan

- **Análisis de lecciones aprendidas:** después de cada simulacro o evento de desastre real, se debe realizar un análisis exhaustivo de las lecciones aprendidas para identificar áreas de mejora y oportunidades de fortalecimiento del DRP.
- **Actualización y revisión del plan:** basado en los hallazgos del análisis de lecciones aprendidas, el DRP debe ser actualizado y revisado regularmente para reflejar cambios en la infraestructura tecnológica, los procesos comerciales y los requisitos regulatorios.
- **Participación de partes interesadas:** es importante involucrar a todas las partes interesadas relevantes en el proceso de evaluación y mejora continua del DRP, incluyendo a la alta dirección, los equipos de TI, los usuarios finales y los proveedores de servicios.

2.8 Gestión de la Comunicación durante un Desastre

La gestión de la comunicación durante un desastre es fundamental para coordinar eficazmente las acciones de respuesta y garantizar que la información llegue de manera oportuna y precisa a todas las partes involucradas.

2.8.1 Protocolos de comunicación interna y externa

- **Internamente:**
    - Establece canales de comunicación claros y eficientes entre los diferentes departamentos y equipos dentro de tu organización.
    - Designa un punto de contacto principal para la comunicación interna y asegúrate de que esté disponible y accesible en todo momento.
    - Desarrolla un plan de comunicación interna que incluya la distribución de roles y responsabilidades en caso de un desastre.
    - Implementa sistemas de alerta temprana internos para notificar al personal sobre emergencias y acciones requeridas.
- **Externamente:**
    - Identifica y establece canales de comunicación con las autoridades locales, regionales y nacionales relevantes, así como con otras organizaciones de respuesta a emergencias.
    - Coordina la divulgación de información con los medios de comunicación y las redes sociales para llegar al público en general.

- Proporciona actualizaciones regulares a los stakeholders externos sobre la situación y las acciones de respuesta de tu organización.

2.8.2 Coordinación con autoridades y otras organizaciones:

- **Establece relaciones previas:** antes de que ocurra un desastre, establece contactos y relaciones con las autoridades locales de gestión de emergencias y otras organizaciones relevantes, como ONGs y agencias gubernamentales.
- **Participa en ejercicios de simulación:** participa en simulacros y ejercicios de respuesta a desastres junto con las autoridades y otras organizaciones para familiarizarte con los protocolos de comunicación y coordinación.
- **Designa puntos de contacto:** designa puntos de contacto específicos en tu organización para interactuar con las autoridades y otras organizaciones durante un desastre y asegúrate de que estén disponibles y capacitados para esta función.

2.8.3 Estrategias de gestión de la información durante un desastre

- **Centraliza la información:** establece un centro de operaciones de emergencia donde se recopile, analice y distribuya la información relevante sobre el desastre.
- **Utiliza tecnología adecuada:** implementa sistemas de gestión de la información y tecnologías de comunicación que permitan compartir datos de manera eficiente entre los equipos de respuesta.
- **Prioriza la información crítica:** identifica y prioriza la información crítica que debe comunicarse de manera inmediata y asegúrate de que llegue a las partes interesadas pertinentes.
- **Verificación de la información:** confirma la veracidad de la información antes de compartirla para evitar la difusión de rumores o información incorrecta.

Al integrar estos elementos en tu plan de gestión de la comunicación durante un desastre, podrás mejorar la eficacia de tus acciones de respuesta y contribuir a una recuperación más rápida y coordinada.

2.9 Aspectos Financieros y de Seguros

2.9.1 Presupuesto para la implementación y mantenimiento del DRP

El presupuesto para la implementación y mantenimiento de un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés) para empresas salvadoreñas que utilizan servicios en la nube para sistemas críticos puede variar según varios factores, incluyendo el tamaño

de la empresa, la complejidad de los sistemas, y los requisitos de cumplimiento regulatorio. Algunos aspectos clave a considerar en el presupuesto incluyen:

- **Costos Iniciales de Implementación:** esto puede incluir la evaluación inicial de riesgos y vulnerabilidades, la planificación del DRP, la selección y configuración de servicios en la nube, y la capacitación del personal. Estos costos pueden ser significativos, pero son una inversión crucial para la preparación ante desastres (Hugos, 2018).
- **Costos de Servicios en la Nube:** los servicios en la nube utilizados para respaldar el DRP pueden tener costos variables, como tarifas mensuales por almacenamiento, procesamiento o ancho de banda. Es importante considerar estos costos al seleccionar proveedores y servicios en la nube (Marston, 2011).
- **Costos de Licenciamiento de Software:** si se utilizan aplicaciones específicas en la nube para respaldar el DRP, pueden existir costos asociados con licencias de software. Es importante tener en cuenta estos costos al planificar el presupuesto (Velte, 2009).
- **Costos de Mantenimiento y Actualización:** se deben asignar fondos para el mantenimiento continuo del DRP, incluyendo la revisión y actualización periódica de procedimientos, pruebas de recuperación de desastres, y capacitación del personal.
- **Costos de Consultoría Externa:** en algunos casos, puede ser necesario contratar consultores externos con experiencia en DRP y servicios en la nube para ayudar en la implementación y mantenimiento del plan. Estos costos deben considerarse en el presupuesto (Fearn-Banks, 2019).

Es importante realizar un análisis detallado de costos y beneficios al desarrollar un presupuesto para el DRP, asegurándose de equilibrar la efectividad y la asequibilidad de las medidas de preparación ante desastres.

2.9.2 Consideraciones sobre seguros y cobertura ante desastres

El seguro de continuidad del negocio para empresas salvadoreñas que dependen de servicios en la nube para sistemas críticos es esencial para mitigar los riesgos financieros asociados con interrupciones operativas. Según Hoyt y Liebenberg (2011), este tipo de seguro proporciona una cobertura financiera que puede ayudar a cubrir los costos de recuperación y los ingresos perdidos durante una interrupción del negocio. Además, el seguro de continuidad del negocio puede ser especialmente importante para empresas que dependen

en gran medida de la infraestructura en la nube, ya que pueden enfrentar riesgos adicionales relacionados con la seguridad de los datos y la disponibilidad de los servicios. Al obtener una cobertura adecuada de seguro de continuidad del negocio, las empresas salvadoreñas pueden protegerse contra los impactos financieros adversos de los desastres y mantener la estabilidad operativa incluso en situaciones de crisis (Hoyt, 2011).

Puntos importantes:

1. Mitigación de Riesgos Financieros
2. Protección ante Interrupciones en la Nube
3. Recuperación de Datos
4. Cumplimiento de Requisitos Legales
5. Respaldo en Caso de Eventos Inesperados
6. Planificación Integral de la Continuidad del Negocio

2.9.3 Análisis de costos y beneficios del DRP

El DRP para sistemas críticos en la nube puede ser costoso de implementar, pero los beneficios a largo plazo superan los costos iniciales. Según Marston (2011), los costos de implementación incluyen la evaluación de riesgos, la planificación del DRP y la configuración de servicios en la nube. Sin embargo, los beneficios incluyen una reducción significativa del tiempo de inactividad en caso de desastre, la protección de datos críticos y la capacidad de cumplir con los requisitos normativos. Aunque puede haber costos continuos de mantenimiento y tarifas de servicios en la nube, estos son necesarios para garantizar la efectividad continua del DRP y pueden ser más flexibles y escalables que la infraestructura local. En última instancia, el DRP en la nube proporciona una capa adicional de protección y preparación que puede ayudar a las empresas salvadoreñas a mantener la continuidad del negocio y mitigar los riesgos operativos (Marston, 2011).

Listado de algunos costos y beneficios:

Costos:

1. Costos iniciales de implementación, que incluyen la evaluación de riesgos, la planificación del DRP y la configuración de servicios en la nube.

2. Costos continuos de mantenimiento, como la revisión y actualización periódica del DRP, así como las pruebas regulares de recuperación ante desastres.
3. Costos de servicios en la nube, que pueden incluir tarifas mensuales por almacenamiento, procesamiento o ancho de banda.

Beneficios:

1. Reducción del tiempo de inactividad en caso de desastre, lo que minimiza la pérdida de ingresos y la interrupción de las operaciones comerciales.
2. Protección de datos críticos almacenados en la nube, que ayuda a prevenir la pérdida de información valiosa y la interrupción de los procesos comerciales.
3. Cumplimiento normativo, ya que un DRP bien diseñado puede ayudar a las empresas a cumplir con los requisitos regulatorios y de cumplimiento relacionados con la seguridad y la privacidad de los datos.

2.10 Cumplimiento Normativo y Auditorías

El cumplimiento normativo en relación con el DRP puede variar según la industria, el país y las regulaciones específicas a las que esté sujeta una organización. Algunas regulaciones comunes que pueden tener requisitos relacionados con el DRP incluyen:

- **Leyes de Protección de Datos:** regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos pueden requerir que las organizaciones implementen medidas de seguridad adecuadas para proteger los datos personales, lo que incluye tener un plan de recuperación ante desastres para evitar la pérdida de estos datos en caso de incidentes.
- **Normas de Seguridad de la Industria:** en algunos sectores, como la industria de servicios financieros o la salud, existen normas específicas de seguridad que requieren la implementación de medidas de recuperación ante desastres. Por ejemplo, en la industria de pagos, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) exige la implementación de un plan de contingencia para garantizar la disponibilidad de los sistemas de procesamiento de pagos.
- **Regulaciones Sectoriales:** algunas industrias pueden estar sujetas a regulaciones específicas relacionadas con la continuidad del negocio y la recuperación ante desastres. Por ejemplo, en el sector de la energía, pueden existir requisitos

regulatorios para garantizar la disponibilidad continua de los servicios energéticos en caso de desastres naturales u otros eventos.

- **Procesos de auditoría para garantizar el cumplimiento:** los procesos de auditoría son fundamentales para garantizar que las organizaciones cumplan con los requisitos legales y regulatorios relacionados con el DRP. Estos pueden incluir:
- **Auditorías Internas:** las organizaciones pueden realizar auditorías internas periódicas para evaluar la efectividad de sus planes de recuperación ante desastres y asegurarse de que cumplen con los requisitos normativos. Esto puede implicar revisar la documentación del DRP, realizar simulacros de recuperación, y verificar la implementación de medidas de seguridad y protección de datos.
- **Auditorías Externas:** además de las auditorías internas, las organizaciones pueden estar sujetas a auditorías externas realizadas por terceros, como agencias reguladoras o empresas de certificación. Estas auditorías pueden ser obligatorias según la regulación aplicable o pueden ser solicitadas por los socios comerciales para garantizar el cumplimiento contractual.
- **Sanciones por incumplimiento y medidas correctivas:** el incumplimiento de los requisitos legales y regulatorios relacionados con el DRP puede dar lugar a diversas sanciones y medidas correctivas, que pueden variar según la gravedad del incumplimiento y la regulación específica. Algunas posibles consecuencias del incumplimiento incluyen:
- **Multas y Sanciones Financieras:** las autoridades regulatorias pueden imponer multas monetarias significativas por el incumplimiento de las regulaciones relacionadas con el DRP. Estas multas pueden variar según la naturaleza y gravedad del incumplimiento, y pueden aumentar si se demuestra negligencia o malicia.
- **Suspensión de Operaciones:** en casos graves de incumplimiento, las autoridades reguladoras pueden ordenar la suspensión temporal o permanente de las operaciones de una organización hasta que se resuelvan los problemas de cumplimiento.
- **Reputación y Pérdida de Clientes:** el incumplimiento de los requisitos normativos relacionados con la seguridad y la protección de datos puede dañar la reputación de una organización y llevar a la pérdida de la confianza de los clientes, lo que puede tener consecuencias financieras a largo plazo.
- **Medidas Correctivas Obligatorias:** además de las sanciones monetarias, las autoridades reguladoras pueden exigir a las organizaciones que implementen

medidas correctivas específicas para abordar las deficiencias identificadas en sus planes de recuperación ante desastres. Estas medidas pueden incluir la revisión y actualización de los procedimientos del DRP, la mejora de la seguridad de la infraestructura de TI y la capacitación del personal en prácticas de seguridad adecuadas.

VIII. Hipótesis y metodología de la investigación

1. Hipótesis

La implementación de un Plan de Recuperación ante Desastres (DRP) en la nube, en línea con estándares internacionales como ISO/IEC 27031:2022, representa una estrategia clave para fortalecer la resiliencia de las empresas salvadoreñas frente a desastres naturales e intrusiones de seguridad. Este enfoque, respaldado por las mejores prácticas, busca reducir significativamente el riesgo de pérdida de información y la interrupción de servicios críticos.

La adopción de servicios en la nube para la implementación de un DRP mejorará significativamente la resiliencia de las empresas salvadoreñas ante desastres naturales e intrusiones de seguridad.

2. Tipo de investigación

La presente propuesta se enmarca en una investigación cuantitativa de tipo teórica, cuyo objetivo es explorar la viabilidad y los beneficios potenciales de la implementación de un plan de recuperación ante desastres (DRP) basado en la computación en la nube para las empresas de El Salvador. A través de encuestas diseñadas específicamente, se buscará comprender la situación actual de estas empresas en relación con la gestión de desastres y la disponibilidad de servicios críticos, así como sus percepciones y necesidades en cuanto a la adopción de tecnologías basadas en la nube para este fin.

La investigación también incluirá un componente exploratorio y descriptivo para comprender en profundidad los procesos existentes de gestión de desastres en las empresas salvadoreñas, así como los desafíos y limitaciones que enfrentan en este aspecto. Esto proporcionará un contexto sólido para la propuesta teórica de lineamientos de DRP basados en la nube, respaldada por estándares internacionales como la ISO/IEC 27031:2022.

El enfoque cuantitativo permitirá recopilar datos numéricos que respalden la propuesta teórica y brinden una comprensión más amplia de la situación actual y las necesidades

específicas de las empresas salvadoreñas en materia de gestión de desastres. A través de este enfoque, se podrán identificar tendencias y patrones que orienten la formulación de recomendaciones y lineamientos para la implementación de DRP basados en la nube, adaptados a las realidades y requerimientos locales.

3. Instrumentos de investigación

Encuesta

Se diseñarán una serie de preguntas dirigidas a las empresas salvadoreñas con el fin de evaluar su nivel de conocimiento y adopción de planes de recuperación ante desastres (DRP) basados en la computación en la nube. Estas preguntas buscarán indagar sobre el grado de familiaridad que tienen las empresas con los conceptos y las mejores prácticas en la gestión de desastres en la nube. Se explorará si actualmente cuentan con algún tipo de DRP, ya sea en la nube o no, y en caso afirmativo, qué tan efectivo consideran que es.

Asimismo, se buscará comprender las percepciones de las empresas sobre los beneficios y las posibles preocupaciones relacionadas con la adopción de un DRP basado en la nube. Se preguntará sobre aspectos como la seguridad de los datos, la disponibilidad de servicios, la escalabilidad y la capacidad de recuperación en caso de desastres. El objetivo es obtener información detallada que permita identificar las necesidades y los desafíos específicos que enfrentan las empresas salvadoreñas en materia de gestión de desastres en la nube, así como sus actitudes hacia la implementación de soluciones basadas en esta tecnología.

Cuestionario realizado a empresas

Con el propósito de evaluar la preparación empresarial frente a potenciales contingencias, se llevó a cabo un exhaustivo sondeo de preguntas cerradas dirigido a una muestra representativa de diversas empresas pertenecientes a una amplia gama de sectores industriales. Este sondeo tuvo como objetivo principal indagar acerca de la disponibilidad y utilización de infraestructura en la nube para la Planificación de la Recuperación ante Desastres (DRP). La implementación de esta tecnología emergente se ha vuelto esencial en el panorama actual de los negocios, donde la resiliencia ante eventos imprevistos es fundamental para asegurar la continuidad operativa y la protección de los activos empresariales. A través de este estudio, se buscó no solo identificar las empresas que ya han adoptado estas soluciones tecnológicas avanzadas, sino también comprender las razones detrás de estas decisiones, así como los obstáculos que puedan estar obstaculizando una adopción más amplia. El análisis detallado de estos datos proporcionará valiosas perspectivas sobre el estado actual de la preparación empresarial frente a desastres y ayudará a informar futuras estrategias de gestión de riesgos y continuidad del negocio en el ámbito empresarial salvadoreño.

La encuesta diseñada para evaluar el nivel de conocimiento y adopción de planes de recuperación ante desastres (DRP) basados en la computación en la nube entre las empresas salvadoreñas consta de una serie de preguntas estructuradas en secciones temáticas (ver anexo 1). Esta estructura facilita la recolección y análisis de datos de manera sistemática.

A continuación, se detallan las secciones y los tipos de preguntas incluidas en el instrumento de investigación:

Sección 1: Información General de la Empresa

Objetivo: Recopilar datos básicos sobre las empresas participantes para contextualizar las respuestas.

- Pregunta 1: Seleccione su tipo de empresa
- Pregunta 2: ¿Cuántos empleados maneja su empresa?

Sección 2: Uso de la Computación en la Nube

Objetivo: Evaluar la adopción de servicios en la nube y su integración en la infraestructura tecnológica de las empresas.

- Pregunta 3: ¿Su empresa utiliza actualmente servicios de computación en la nube para alojar alguna parte de su infraestructura tecnológica?
- Pregunta 4: En caso de utilizar servicios en la nube, ¿Qué porcentaje de su infraestructura tecnológica se encuentra alojada en la nube?
- Pregunta 5: ¿Qué tipo de servicios en la nube utiliza su empresa? (Puede seleccionar varias opciones)

Sección 3: Planes de Recuperación ante Desastres (DRP)

Objetivo: Evaluar la existencia, efectividad y características de los DRP en las empresas.

- Pregunta 6: ¿Su empresa tiene un plan de recuperación ante desastres (DRP) establecido?
- Pregunta 7: En caso de tener un plan de recuperación ante desastres, ¿Este plan incluye estrategias específicas para la recuperación de datos y sistemas alojados en la nube?

- Pregunta 8: ¿Con qué frecuencia se realizan pruebas o simulacros del plan de recuperación ante desastres?
- Pregunta 9: ¿Quién es el responsable de la implementación y gestión del plan de recuperación ante desastres en su empresa?
- Pregunta 10: ¿Cuál es su percepción sobre la eficacia del plan de recuperación ante desastres de su empresa?
- Pregunta 11: ¿Su empresa cuenta con un presupuesto asignado específicamente para la implementación y mantenimiento del plan de recuperación ante desastres?
- Pregunta 12: Seleccione el rango del presupuesto para implementación del DRP
- Pregunta 13: Seleccione el rango del presupuesto mensual para el mantenimiento del DRP

Sección 4: Percepciones y Actitudes hacia los DRP

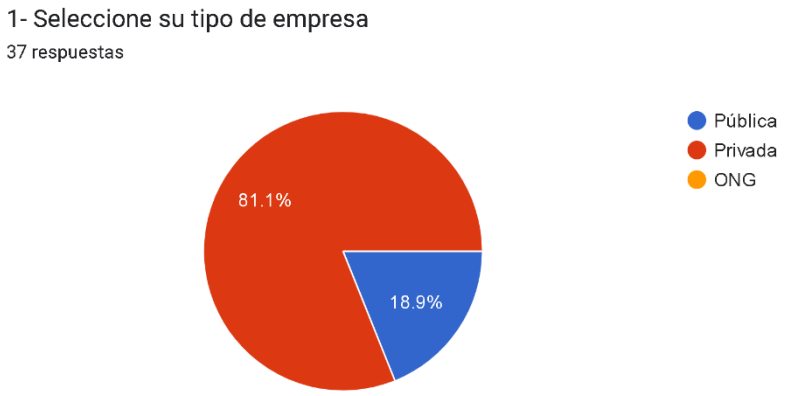
Objetivo: Comprender las percepciones y actitudes de las empresas sobre los beneficios y preocupaciones asociados con los DRP basados en la nube.

- Pregunta 14: ¿Qué áreas considera que podrían mejorarse en el plan de recuperación ante desastres de su empresa?
- Pregunta 15: En caso de que su respuesta a la pregunta 6 fue NO, favor indicar ¿Por qué motivo no poseen DRP?

Así mismo, se detalla el resumen de los resultados obtenidos de 37 empresas encuestadas:

Pregunta 1 - Seleccione su tipo de empresa

Se obtuvieron 37 respuestas donde el 81.1% de las empresas son de tipo privada y el 18.9 son empresas públicas.

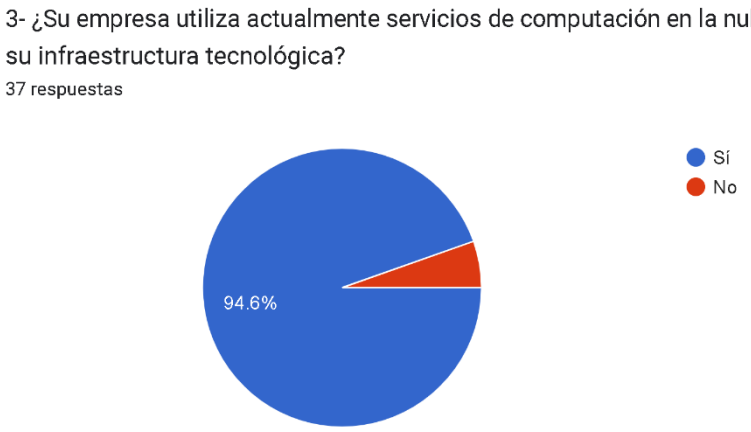


Pregunta 2 - ¿Cuántos empleados maneja su empresa?

De 37 respuestas el 59.5% indicó que la cantidad de empleados que manejan son mayor de 250, el 18.9% indicó que es de 50 a 250.

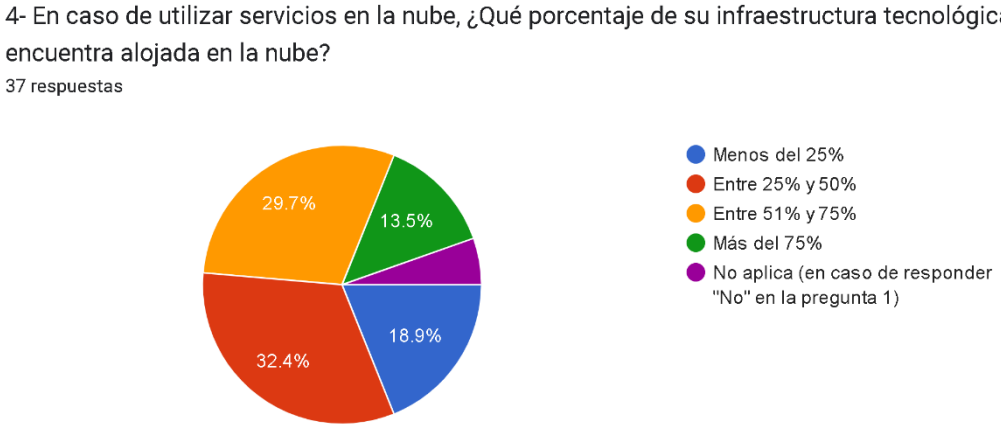
Pregunta 3 - ¿Su empresa utiliza actualmente servicios de computación en la nube para alojar alguna parte de su infraestructura tecnológica?

De 37 empresas 94.6% contestaron que si poseen servicios de computación en la nube.

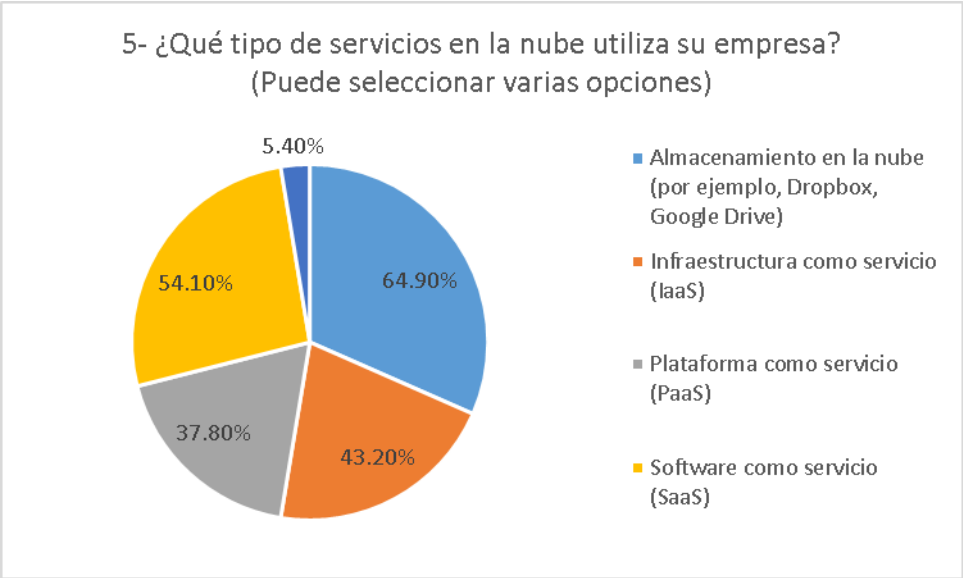


Pregunta 4 - En caso de utilizar servicios en la nube, ¿Qué porcentaje de su infraestructura tecnológica se encuentra alojada en la nube?

De 37 empresas encuestadas, el 32.4% indicó que su porcentaje de infraestructura alojada en la nube es entre 25% y 50%, el 29.7% indicó que es de 51% y 75%, el 18.9% indicó que es menos del 25% y el 13.5% indicó que es más del 75%.

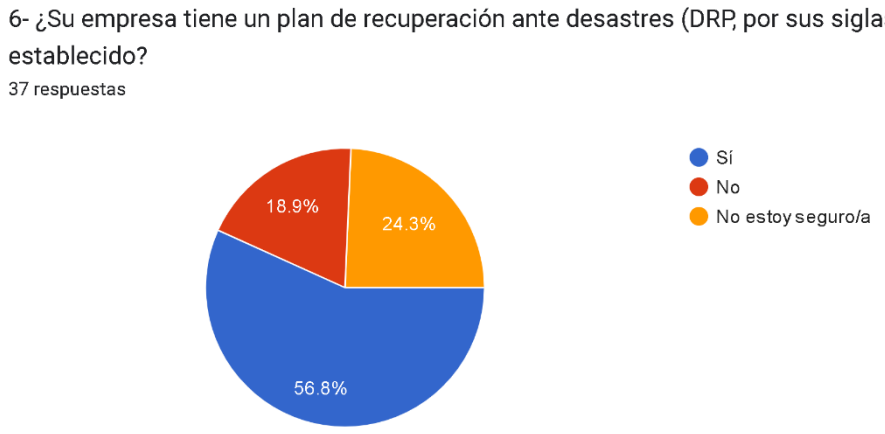


Pregunta 5 - ¿Qué tipo de servicios en la nube utiliza su empresa? (Puede seleccionar varias opciones)



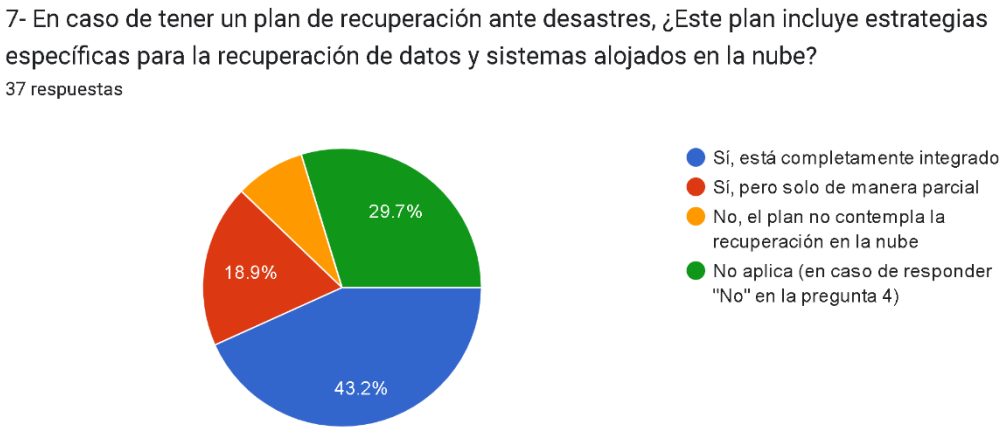
Pregunta 6 - ¿Su empresa tiene un plan de recuperación ante desastres (DRP, por sus siglas en inglés) establecido?

De 37 respuestas recibidas de empresas, el 58.8% indicó que, si posee un plan de recuperación ante desastres, 24.3% indicó que no estaban seguros y el 18.9% indicó que no posee un plan de recuperación ante desastres.



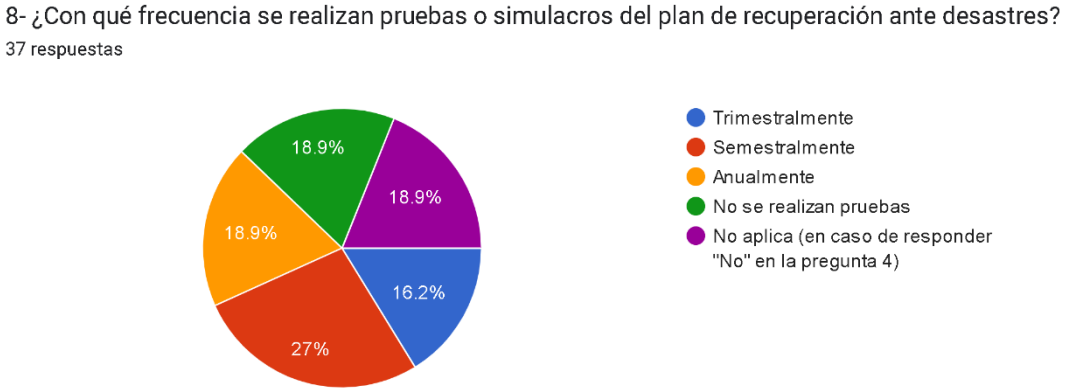
Pregunta 7 - En caso de tener un plan de recuperación ante desastres, ¿Este plan incluye estrategias específicas para la recuperación de datos y sistemas alojados en la nube?

De 37 respuestas de empresas, el 43.2% indicó que su plan de DRP incluye estrategias especificas está completamente integrado, el 29.7% indicó que no aplica, el 18.9% indicó que sí, pero solamente de manera parcial.



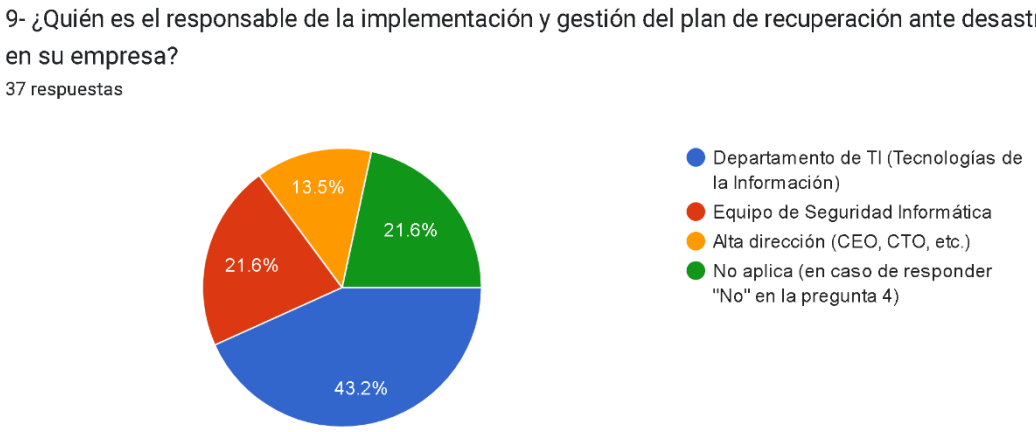
Pregunta 8 ¿Con qué frecuencia se realizan pruebas o simulacros del plan de recuperación ante desastres?

De 37 respuestas de empresas el 27% indicó que semestralmente realizan pruebas o simulacros de DRP, el 18.9% contestaron que anualmente, no realizan pruebas y no aplica porque no cuentan con el servicio. El 16.2% indicó que trimestralmente.

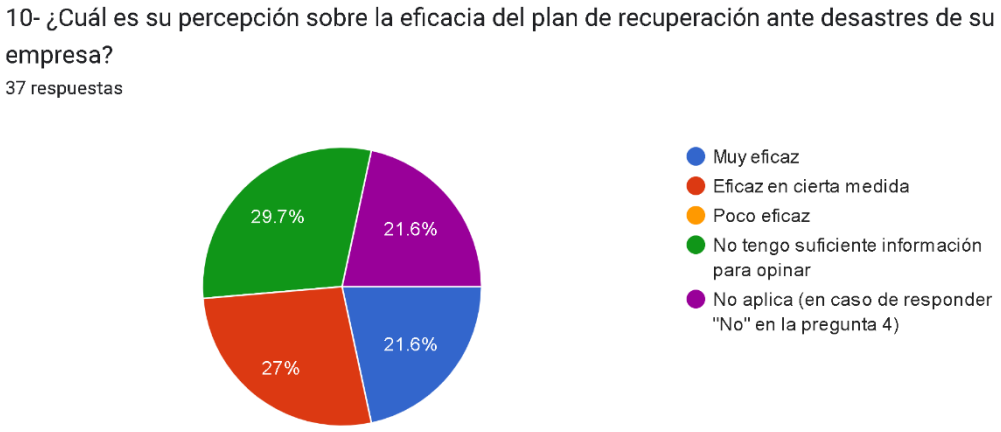


Pregunta 9 - ¿Quién es el responsable de la implementación y gestión del plan de recuperación ante desastres en su empresa?

De 37 respuestas realizadas por empresas, el 43.2% indicó que el departamento de TI es el responsable de la implementación y gestión del DRP, el 21.6% indicó que el encargado es el equipo de seguridad informática, otro grupo indicó que no aplica. El 13.5% indicó que el responsable es la Alta dirección.



Pregunta 10 - ¿Cuál es su percepción sobre la eficacia del plan de recuperación ante desastres de su empresa?

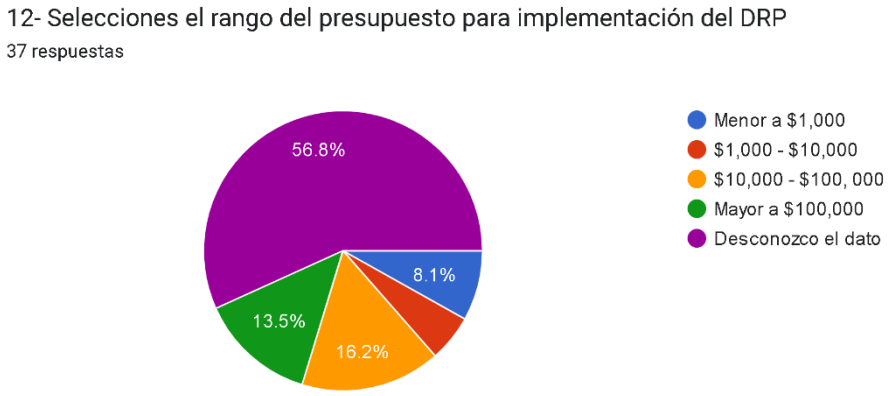


Pregunta 11 - ¿Su empresa cuenta con un presupuesto asignado específicamente para la implementación y mantenimiento del plan de recuperación ante desastres?

De 37 respuestas por las empresas el 45.9% indican que, si poseen presupuesto asignado para la implementación de DRP, el 27% indicaron que no poseen o no están seguros.

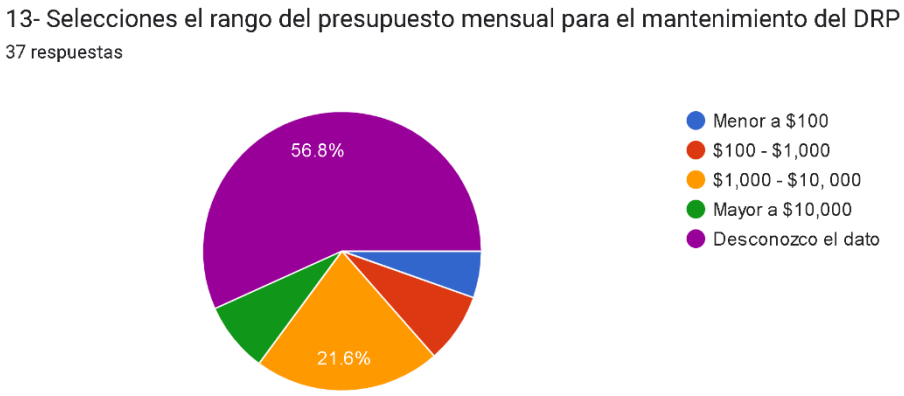
Pregunta 12 - Selecciones el rango del presupuesto para implementación del DRP

De 37 respuestas por las empresas el 56.8% indican que desconocen el dato del rango del presupuesto para implementación de DRP, el 16.2% indica que es de $10,000 a $100,000, el 13.5% indica que es mayor a $100,000, el 8.1% indica menor a $1,000.



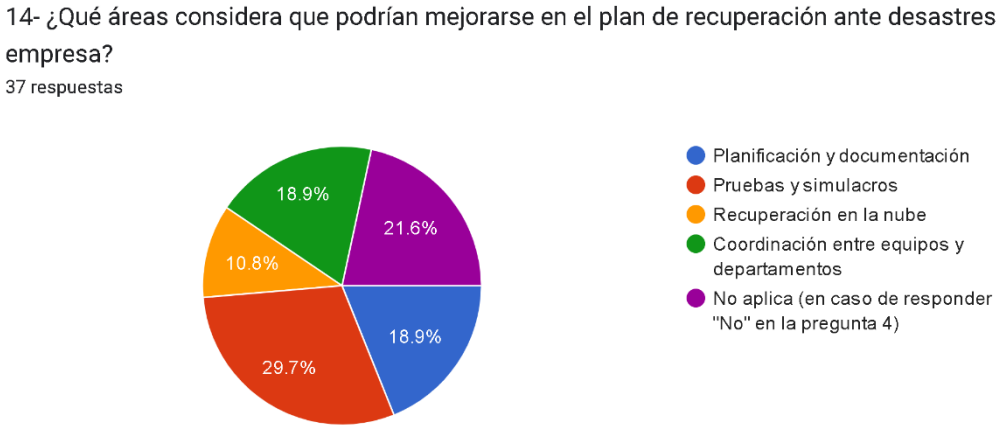
Pregunta 13 - Selecciones el rango del presupuesto mensual para el mantenimiento del DRP

De 37 respuestas por las empresas el 56.8% desconoce el dato del rango del presupuesto mensual para el mantenimiento del DRP, el 21.6% es de $1,000 a $10,000.



Pregunta 14 - ¿Qué áreas considera que podrían mejorarse en el plan de recuperación ante desastres de su empresa?

De 37 respuestas por las empresas el 29.7% que el área de mejora para un DRP es con pruebas y simulacros, el 21.6% indico que no aplica, el 18.9% indicaron que coordinación entre equipos y departamentos también planificación y documentación. El 10.8% la recuperación en la nube.

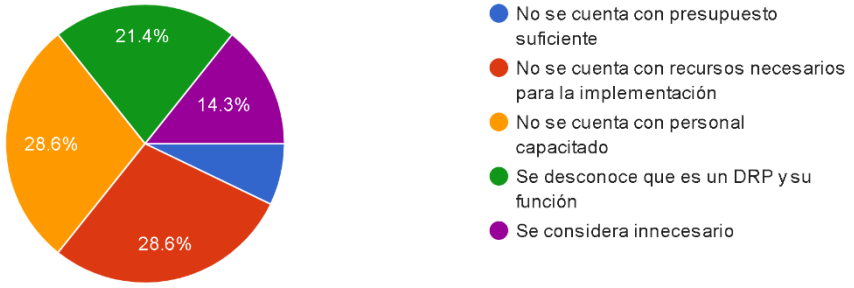


Pregunta 15 En caso de que su respuesta a la pregunta 4 fue NO, favor indicar ¿Por qué motivo no poseen DRP?

De 37 respuestas por las empresas el 28.6% contestaron que no se cuenta con los recursos necesarios para la implementación de un DRP y no se cuenta con personal capacitado, el 21.4% indicó que se desconoce que es un DRP y cuál es su función. El 14.3% indicaron que no es necesario la implementación de un DRP.

15- En caso de que su respuesta a la pregunta 4 fue NO, favor indicar ¿Por qué motivo no poseen DRP?

14 respuestas



IX. Presentación de resultados

1. Muestra

La encuesta se llevó a cabo en 37 empresas ubicadas en el país de El Salvador, abarcando una diversidad de sectores industriales. Durante el proceso de investigación, se analizó qué empresas contaban con servicios de infraestructura en la nube para la Planificación de la Recuperación ante Desastres (DRP, por sus siglas en inglés). Los resultados revelaron que, aunque la adopción de estos servicios es incipiente, algunas empresas están comenzando a reconocer su importancia estratégica para garantizar la continuidad del negocio en situaciones adversas. Es importante destacar que la población de muestreo fue limitada, ya que solo unas pocas empresas optaron por participar en la encuesta, lo que podría reflejar la reticencia o la falta de conciencia sobre la relevancia de estas prácticas para la gestión de riesgos empresariales en el entorno actual.

2. Análisis de resultados de la encuesta realizada

Los resultados de la encuesta sugieren una tendencia positiva hacia la adopción y la preparación para el uso de tecnologías de computación en la nube, así como la implementación de planes de recuperación ante desastres. Sin embargo, también destacan áreas de mejora, como la realización de pruebas periódicas, la asignación adecuada de presupuesto y la concienciación sobre la importancia del DRP. Estos hallazgos pueden servir como guía para desarrollar estrategias efectivas de gestión de riesgos y continuidad del negocio en el entorno empresarial actual.

- **Tipo de Empresa y Tamaño:** la encuesta abarcó un total de 37 empresas, con una predominancia de empresas del sector privado (81.1%) en comparación con el sector público (18.9%). Respecto al tamaño de las empresas, la mayoría (59.5%) tienen más de 250 empleados, lo que sugiere que la muestra incluye principalmente medianas y grandes empresas.
- **Adopción de Computación en la Nube:** se observa una alta adopción de servicios de computación en la nube, ya que el 94.6% de las empresas encuestadas indicaron utilizar estos servicios para alojar parte de su infraestructura tecnológica. Esto refleja una tendencia hacia la adopción de tecnologías de nube para mejorar la eficiencia operativa y la escalabilidad.
- **Porcentaje de Infraestructura en la Nube:** el porcentaje de infraestructura tecnológica alojada en la nube varía entre las empresas encuestadas. Se destaca que un 32.4% tiene entre el 25% y el 50% de su infraestructura en la nube, mientras que un 29.7% aloja entre el 51% y el 75%. Esto sugiere que algunas empresas están migrando una parte significativa de su infraestructura a la nube.
- **Plan de Recuperación ante Desastres (DRP):** casi el 60% de las empresas encuestadas tienen un plan de recuperación ante desastres (DRP) establecido. Esto demuestra una conciencia creciente sobre la importancia de la preparación para contingencias y la continuidad del negocio en caso de desastres o interrupciones.
- **Estrategias para Recuperación en la Nube:** del grupo de empresas con un plan de DRP, un 43.2% incluye estrategias específicas para la recuperación de datos y sistemas alojados en la nube. Esto indica una consideración especial hacia la protección y recuperación de los activos tecnológicos en la nube.
- **Frecuencia de Pruebas del Plan DRP:** el 27% de las empresas realizan pruebas o simulacros de su plan de DRP semestralmente. Esto sugiere un compromiso con la revisión y mejora continua del plan para garantizar su eficacia en situaciones de emergencia.
- **Responsabilidad de Implementación del Plan DRP:** el departamento de Tecnologías de la Información (TI) es mayoritariamente responsable (43.2%) de la implementación y gestión del plan de DRP en las empresas encuestadas. Esto resalta el papel crucial de los equipos de TI en la protección de los sistemas y datos empresariales.

- **Presupuesto Asignado:** alrededor del 46% de las empresas tienen un presupuesto asignado para la implementación del DRP. Sin embargo, una parte significativa (27%) no posee o no está segura de tener asignado un presupuesto para este fin, lo que podría ser un área de mejora en términos de asignación de recursos.
- **Áreas de Mejora en el Plan DRP:** las áreas de mejora más mencionadas incluyen la realización de pruebas y simulacros, la coordinación entre equipos y departamentos, y la planificación y documentación. Estos aspectos son fundamentales para garantizar la efectividad del plan en situaciones de crisis.
- **Razones para la Falta de DRP:** entre las empresas que no tienen un plan de DRP, las principales razones citadas incluyen la falta de recursos y personal capacitado, el desconocimiento sobre el tema y la percepción de que no es necesario. Estos hallazgos resaltan la necesidad de concienciar sobre la importancia del DRP y de proporcionar recursos adecuados para su implementación.

X. Recomendaciones de buenas prácticas para un DRP en la nube para empresas salvadoreñas

1. **Evaluación de riesgos y análisis de impacto empresarial (BIA)**
    - Identificar y evaluar los riesgos potenciales que podrían afectar la continuidad del negocio, tanto internos como externos (por ejemplo, desastres naturales, ciberataques, errores humanos).
    - Realizar un análisis de impacto empresarial para comprender las consecuencias financieras y operativas de estos riesgos y establecer prioridades.
2. **Definición de objetivos y requisitos**
    - Establecer objetivos claros para el DRP en términos de tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO).
    - Determinar los requisitos específicos de la empresa en términos de capacidad de almacenamiento, redundancia, seguridad y cumplimiento normativo.
3. **Selección de proveedores de servicios en la nube**
    - Evaluar y seleccionar proveedores de servicios en la nube que cumplan con los estándares de seguridad y disponibilidad requeridos.

- Priorizar proveedores con experiencia en DRP y certificaciones relevantes (por ejemplo, ISO 27001 para seguridad de la información).

4. **Diseño de la arquitectura de DRP en la nube**
   - Desarrollar una arquitectura de DRP que incluya redundancia geográfica y copias de seguridad automatizadas.
   - Utilizar servicios de nube como almacenamiento en caliente y en frío, máquinas virtuales replicadas y servicios de base de datos gestionados para garantizar la disponibilidad y la integridad de los datos.
5. **Implementación y configuración**
   - Configurar la infraestructura de DRP en la nube de acuerdo con el diseño previamente establecido.
   - Automatizar procesos de copia de seguridad, replicación de datos y conmutación por error para minimizar el tiempo de inactividad en caso de un desastre.
6. **Pruebas y validación**
   - Realizar pruebas regulares de los procedimientos de recuperación ante desastres para verificar su eficacia.
   - Documentar y analizar los resultados de las pruebas para identificar áreas de mejora y realizar ajustes en consecuencia.
7. **Capacitación y concientización**
   - Capacitar al personal sobre los procedimientos de recuperación ante desastres y su papel en su implementación.
   - Fomentar una cultura de concientización sobre la importancia de la preparación para desastres y la responsabilidad compartida en la protección de los activos empresariales.
8. **Mantenimiento y actualización**
   - Realizar mantenimiento regular de la infraestructura de DRP en la nube para garantizar su funcionamiento óptimo.
   - Actualizar continuamente el plan de DRP en función de los cambios en la infraestructura, los riesgos empresariales y las lecciones aprendidas de incidentes pasados.

9. **Auditoría y cumplimiento**
    - Realizar auditorías periódicas del DRP en la nube para garantizar el cumplimiento de los estándares de seguridad y regulaciones aplicables.
    - Mantener documentación detallada de los procedimientos de DRP y los resultados de las auditorías para demostrar la conformidad con los requisitos regulatorios.
10. **Gestión de incidentes**
    - Establecer un proceso claro de gestión de incidentes para responder de manera efectiva a eventos disruptivos.
    - Designar un equipo de respuesta a incidentes y definir roles y responsabilidades para mitigar rápidamente los impactos de cualquier interrupción en el negocio.
11. **Consideraciones legales y regulatorias**
    - Realizar un análisis exhaustivo de las leyes y regulaciones locales que puedan afectar el almacenamiento y la gestión de datos en la nube.
    - Garantizar el cumplimiento de normativas como la Ley de Protección de Datos Personales y la Ley de Firmas Electrónicas, adaptando los procedimientos de DRP en consecuencia.

XI. Discusión

La presente investigación aborda la implementación de un Plan de Recuperación ante Desastres (DRP) en la nube, conforme a los estándares internacionales como ISO/IEC 27031:2022, y su impacto en la resiliencia de las empresas salvadoreñas frente a desastres naturales e intrusiones de seguridad. Los resultados de la encuesta muestran tendencias positivas y áreas de mejora significativas, lo que permite un análisis profundo de los hallazgos y sus implicaciones.

Importancia y Novedad de los Resultados

Los resultados obtenidos son cruciales para comprender la adopción y efectividad de los DRP en la nube dentro del contexto empresarial salvadoreño. La alta adopción de servicios de computación en la nube, con un 94.6% de las empresas utilizando estos servicios, subraya una clara tendencia hacia la modernización y escalabilidad operativa. Esta adopción masiva

refleja una conciencia creciente sobre la necesidad de mantener la continuidad del negocio y proteger la información sensible frente a interrupciones.

Uno de los hallazgos novedosos es la proporción significativa de empresas que han trasladado entre el 25% y el 75% de su infraestructura tecnológica a la nube. Este dato destaca un enfoque estratégico en la migración de infraestructura crítica, lo cual es vital para la implementación efectiva de un DRP en la nube. Además, el hecho de que casi el 60% de las empresas tengan un DRP establecido demuestra una creciente concienciación sobre la importancia de la preparación para desastres.

Validación de la Hipótesis

La hipótesis planteada en este estudio se valida parcialmente, ya que la implementación de DRP en la nube ha mostrado ser una estrategia efectiva para mejorar la resiliencia de las empresas. Sin embargo, la encuesta también revela áreas de mejora que deben abordarse para maximizar los beneficios de estos planes. La realización de pruebas periódicas, la asignación adecuada de presupuesto y la concienciación sobre la importancia del DRP son factores críticos que requieren atención para fortalecer aún más la resiliencia empresarial.

Comparación con Otros Estudios

Al comparar estos hallazgos con investigaciones previas, se observa una consonancia con estudios que sugieren la efectividad de los DRP en la nube para mejorar la continuidad del negocio. Sin embargo, el nivel de adopción y preparación entre las empresas salvadoreñas parece ser más alto de lo reportado en algunos contextos internacionales, lo que podría indicar una respuesta proactiva a los riesgos naturales y de seguridad específicos de la región. Esta proactividad destaca la importancia de contextos regionales en el análisis de la adopción de DRP en la nube.

Implicaciones Prácticas

Las implicaciones prácticas de estos resultados son significativas. Las empresas deben enfocar esfuerzos en áreas críticas de mejora identificadas, tales como:

- **Realización de Pruebas Periódicas:** solo el 27% de las empresas realizan pruebas semestrales de su DRP, lo que indica una necesidad urgente de aumentar esta práctica para asegurar la eficacia del plan.

- **Asignación de Presupuesto:** aunque el 46% de las empresas tienen presupuesto asignado para DRP, un 27% no tiene o no está seguro de tener uno. Asignar recursos adecuados es esencial para la implementación y mantenimiento efectivo del DRP.
- **Concienciación y Capacitación:** la falta de recursos y personal capacitado es una razón significativa para la no implementación de un DRP. Programas de capacitación y concienciación podrían cerrar esta brecha.

Limitaciones del Estudio

Este estudio presenta varias limitaciones que deben considerarse. Primero, la muestra de la encuesta está compuesta principalmente por medianas y grandes empresas, lo que podría no representar completamente la realidad de las pequeñas empresas en El Salvador. Además, la predominancia del sector privado en la muestra podría sesgar los resultados, dado que las necesidades y capacidades del sector público pueden diferir significativamente. Finalmente, la autoevaluación de las empresas puede introducir sesgos en la precisión de los datos reportados.

Cierre de discusión

Podemos decir que la implementación de DRP en la nube conforme a estándares internacionales como ISO/IEC 27031:2022 es una estrategia efectiva para mejorar la resiliencia empresarial en El Salvador. Sin embargo, la necesidad de pruebas periódicas, asignación adecuada de presupuesto y mayor concienciación son áreas críticas que deben ser abordadas para maximizar los beneficios de estos planes. Este estudio no solo valida parcialmente la hipótesis, sino que también proporciona una hoja de ruta clara para futuras mejoras y adopciones en el campo de la recuperación ante desastres y la continuidad del negocio.

XII. Conclusiones y recomendaciones

Conclusiones

El presente estudio ha explorado la implementación de un Plan de Recuperación ante Desastres (DRP) en la nube, siguiendo los estándares internacionales como ISO/IEC 27031:2022, y su impacto en la resiliencia de las empresas salvadoreñas. Los resultados obtenidos permiten llegar a las siguientes conclusiones:

1. **Alta Adopción de la Computación en la Nube:** la mayoría de las empresas encuestadas (94.6%) utilizan servicios de computación en la nube, lo que subraya una tendencia significativa hacia la modernización y escalabilidad operativa. Esto refleja una conciencia creciente sobre la necesidad de mantener la continuidad del negocio y proteger la información sensible.
2. **Presencia de Planes de Recuperación ante Desastres (DRP):** casi el 60% de las empresas encuestadas cuentan con un DRP, demostrando una creciente conciencia sobre la importancia de la preparación para desastres y la continuidad del negocio.
3. **Migración de Infraestructura a la Nube:** un porcentaje considerable de empresas ha trasladado entre el 25% y el 75% de su infraestructura tecnológica a la nube. Esta migración es un paso estratégico clave para la implementación efectiva de DRP en la nube.
4. **Necesidad de Pruebas Periódicas y Asignación de Presupuesto:** solo el 27% de las empresas realizan pruebas semestrales de su DRP, y alrededor del 27% no están seguras de tener un presupuesto asignado para DRP. Estas áreas representan oportunidades críticas para mejorar la efectividad y la preparación.
5. Roles y Responsabilidades: el departamento de Tecnologías de la Información (TI) es mayoritariamente responsable de la implementación y gestión del DRP, resaltando su papel crucial en la protección de los sistemas y datos empresariales.
6. **Áreas de Mejora y Desafíos:** las principales áreas de mejora identificadas incluyen la realización de pruebas y simulacros, la coordinación entre equipos y departamentos, y la planificación y documentación del DRP. La falta de recursos y personal capacitado, junto con el desconocimiento sobre el tema, son los desafíos más significativos para aquellas empresas que no cuentan con un DRP.

Recomendaciones

A partir de las conclusiones del estudio, se proponen las siguientes recomendaciones para fortalecer la resiliencia empresarial a través de la implementación efectiva de DRP en la nube:

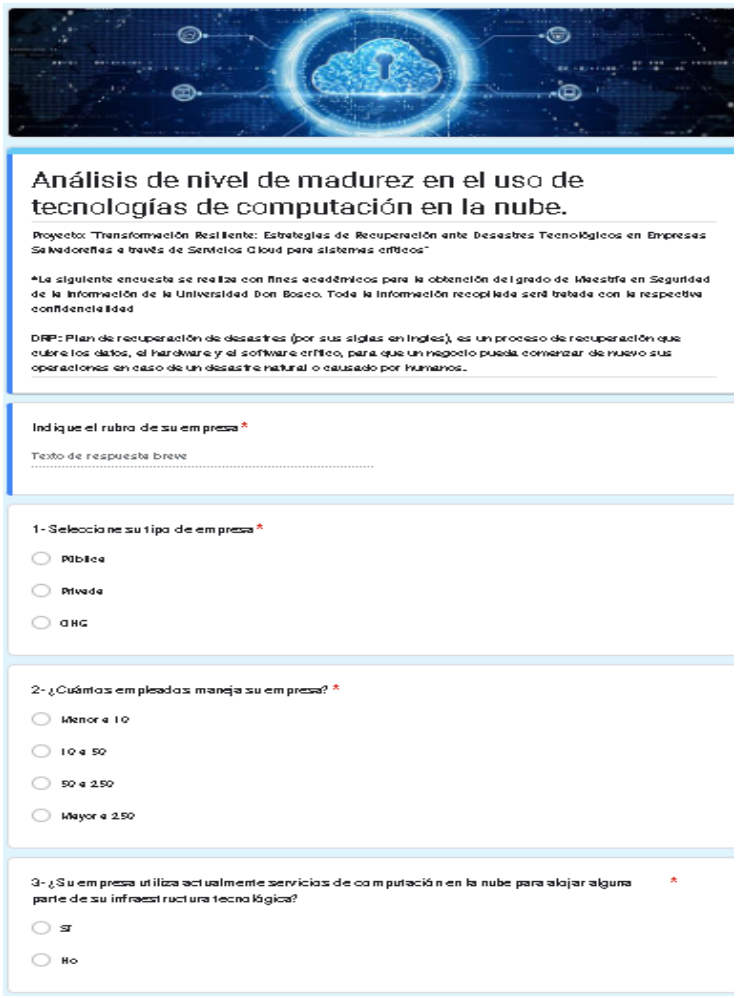
1. **Aumentar la Frecuencia de Pruebas del DRP:** es fundamental que las empresas realicen pruebas periódicas de sus planes de recuperación ante desastres. Se recomienda implementar pruebas semestrales o trimestrales para asegurar la eficacia del plan y mejorar la preparación ante situaciones de emergencia.
2. **Asignación Adecuada de Recursos:** las empresas deben asegurar la asignación de un presupuesto adecuado para el desarrollo, implementación y mantenimiento del DRP. Esto incluye la inversión en infraestructura, software, y capacitación del personal.
3. **Capacitación y Concienciación:** implementar programas de capacitación continua para el personal sobre la importancia y los procedimientos del DRP. Además, campañas de concienciación pueden ayudar a superar la percepción de que el DRP no es necesario.
4. **Mejora de la Documentación y Planificación:** las empresas deben trabajar en la documentación detallada y la planificación exhaustiva de sus DRP. Esto incluye la definición clara de roles y responsabilidades, así como la creación de protocolos específicos para diferentes tipos de desastres.
5. **Coordinación Interdepartamental:** fomentar la colaboración y coordinación entre los distintos departamentos para asegurar una respuesta cohesiva y efectiva ante cualquier interrupción o desastre. Esto puede lograrse mediante simulacros conjuntos y reuniones de planificación interdepartamental.
6. **Evaluación Continua y Actualización del DRP:** establecer procesos para la evaluación continua y la actualización regular del DRP, adaptándose a las nuevas amenazas y tecnologías emergentes. Esto garantizará que el plan permanezca relevante y efectivo.
7. **Explorar Nuevas Tecnologías y Mejores Prácticas:** las empresas deben mantenerse informadas sobre las nuevas tecnologías y mejores prácticas en el ámbito de la recuperación ante desastres y la computación en la nube. La adopción de soluciones innovadoras puede ofrecer ventajas adicionales en términos de resiliencia y eficiencia operativa.

Implementar estas recomendaciones permitirá a las empresas salvadoreñas mejorar su preparación y respuesta ante desastres, asegurando la continuidad del negocio y la protección de sus activos tecnológicos y de información. Esto no solo valida la hipótesis inicial, sino que también proporciona un marco claro para fortalecer la resiliencia empresarial en un entorno cada vez más digital y susceptible a amenazas.

XIII. Anexos

Anexo 1

Se muestra la encuesta realizada en Google Forms para su distribución entre las empresas que colaboraron para realizar sus aportes en las preguntas mostradas a continuación.



Análisis de nivel de madurez en el uso de tecnologías de computación en la nube.

Proyecto: "Transformación Resiliente: Estrategias de Recuperación ante Desastres Tecnológicos en Empresas Salvadoreñas a través de Servicios Cloud para sistemas críticos"

*La siguiente encuesta se realiza con fines académicos para la obtención del grado de Maestría en Seguridad de la Información de la Universidad Don Bosco. Toda la información recopilada será tratada con la respectiva confidencialidad

DRP: Plan de recuperación de desastres (por sus siglas en inglés), es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

Indique el rubro de su empresa *

Texto de respuesta breve

1- Seleccione su tipo de empresa *

- Pública
- Privada
- GHG

2- ¿Cuántos empleados maneja su empresa? *

- Menor a 10
- 10 a 50
- 50 a 250
- Mayor a 250

3- ¿Su empresa utiliza actualmente servicios de computación en la nube para alojar alguna parte de su infraestructura tecnológica? *

- Si
- No

4- En caso de utilizar servicios en la nube, ¿Qué porcentaje de su infraestructura tecnológica se encuentra alojada en la nube? *

- Menos del 25%
- Entre 25% y 50%
- Entre 51% y 75%
- Más del 75%
- No aplica (en caso de responder "No" en la pregunta 1)

5- ¿Qué tipo de servicios en la nube utiliza su empresa? (Puede seleccionar varias opciones) *

- Almacenamiento en la nube (por ejemplo, Dropbox, Google Drive)
- Infraestructura como servicio (IaaS)
- Plataforma como servicio (PaaS)
- Software como servicio (SaaS)
- No aplica (no se tiene servicios en la nube)

6- ¿Su empresa tiene un plan de recuperación ante desastres (DRP, por sus siglas en inglés) establecido? *

- Sí
- No
- No estoy seguro/a

7- En caso de tener un plan de recuperación ante desastres, ¿Este plan incluye estrategias específicas para la recuperación de datos y sistemas alojados en la nube? *

- Sí, está completamente integrado
- Sí, pero solo de manera parcial
- No, el plan no contempla la recuperación en la nube
- No aplica (en caso de responder "No" en la pregunta 4)

8- ¿Con qué frecuencia se realizan pruebas o simulacros del plan de recuperación ante desastres? *

- Trimestralmente
- Semestralmente
- Anualmente
- No se realizan pruebas
- No aplica (en caso de responder "No" en la pregunta 4)

9- ¿Quién es el responsable de la implementación y gestión del plan de recuperación ante desastres en su empresa? *

- Departamento de TI (Tecnologías de la Información)
- Equipo de Seguridad Informática
- Alta dirección (CEO, CTO, etc.)
- No aplica (en caso de responder "No" en la pregunta 4)

10- ¿Cuál es su percepción sobre la eficacia del plan de recuperación ante desastres de su empresa? *

- Muy eficaz
- Eficaz en cierta medida
- Poco eficaz
- No tengo suficiente información para opinar
- No aplica (en caso de responder "No" en la pregunta 4)

11- ¿Su empresa cuenta con un presupuesto asignado específicamente para la implementación y mantenimiento del plan de recuperación ante desastres? *

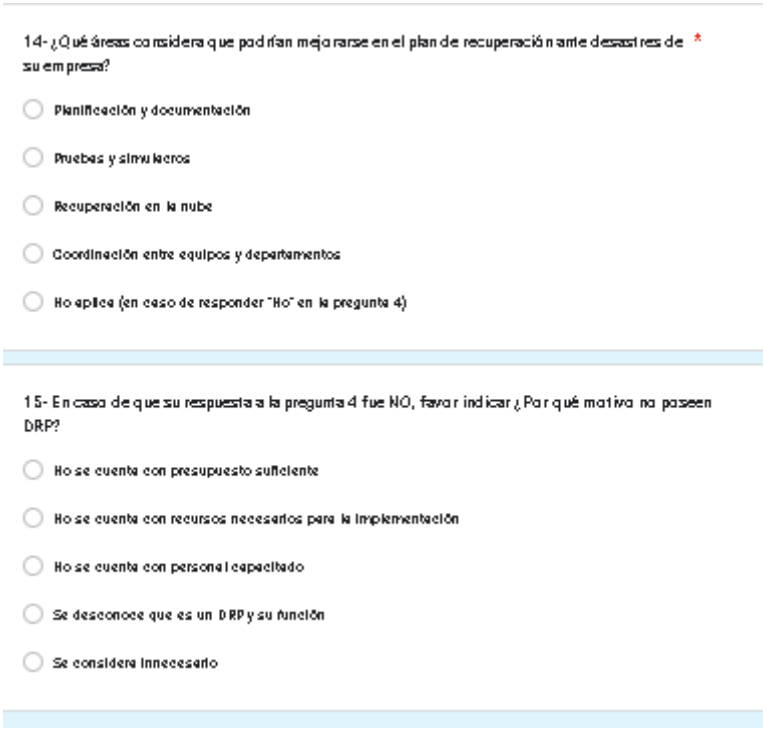
- Sí
- No
- No estoy seguro/a

12- Seleccione el rango del presupuesto para implementación del DRP *

- Menor a $1,000
- $1,000 - $10,000
- $10,000 - $100, 000
- Mayor a $100,000
- Desconozco el dato

13- Seleccione el rango del presupuesto mensual para el mantenimiento del DRP *

- Menor a $100
- $100 - $1,000
- $1,000 - $10, 000
- Mayor a $10,000
- Desconozco el dato



XIV. Referencias

I. AWS | Informática en la nube. Ventajas y Beneficios (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is-cloud-computing/

II. ¿Qué es la computación en la nube? | Glosario. (s. f.). HPE LAMERICA. https://www.hpe.com/lamerica/es/what-is/cloud-computing.html

III. ¿Qué es la computación en la nube? | Google Cloud. (s. f.). Google Cloud. https://cloud.google.com/learn/what-is-cloud-computing?hl=es-419

IV. Ventajas de la computación en la nube | Google Cloud | Google Cloud. (s. f.). Google Cloud. https://cloud.google.com/learn/advantages-of-cloud-computing?hl=es-419

V. Mell, P., & Grance, T. (2011). "The NIST definition of cloud computing (NIST Special Publication 800-145)". National Institute of Standards and Technology, 7.

VI. Buyya, R., Broberg, J., & Goscinski, A. M. (2011). "Cloud computing: principles and paradigms". John Wiley & Sons.

VII. ¿Qué es la recuperación ante desastres y por qué es importante? | Google Cloud | Google Cloud. (s. f.). Google Cloud. https://cloud.google.com/learn/what-is-disaster-recovery?hl=es-419

VIII. Galileus. (2012, 17 septiembre). Antecedentes históricos de la Continuidad del Negocio. Apuntes sobre continuidad del negocio. https://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html

IX. Herbane, Brahim. (2010). The Evolution of Business Continuity Management: A Historical Review of Practices and Drivers. Business History. 52. 978-1002. 10.1080/00076791.2010.511185.

X. Recuperación de desastres: Introducción | IBM. (s. f.). IBM. Recuperado 16 de marzo de 2024, de https://www.ibm.com/mx-es/topics/disaster-recovery

XI. Martinekuan. (s. f.). Recuperación ante desastres de escala empresarial - Azure Architecture Center. Microsoft Learn. https://learn.microsoft.com/es-es/azure/architecture/solution-ideas/articles/disaster-recovery-enterprise-scale-dr

XII. ¿Qué es la recuperación ante desastres? | Oracle México (s. f.). Oracle México. https://www.oracle.com/mx/cloud/backup-and-disaster-recovery/what-is-disaster-recovery/

XIII. NRP-24: Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio. (2020, 14 abril). SSF. https://ssf.gob.sv/descargas/Normas/Normas_Prudenciales/Bancos/NRP-24.pdf

XIV. Rittinghouse, J. W., & Ransome, J. F. (2016). "Cloud Computing: Implementation, Management, and Security" - Publicado en 2016 por CRC Press.

XV. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). "An Analysis of Security Issues for Cloud Computing" - Publicado en 2013 en el Journal of Internet Services and Applications.

XVI. Hugos, M. H., & Hulitzky, D. (2018). "Business Continuity and Disaster Recovery Planning for IT Professionals" - Publicado en 2018 por Apress.

XVII. Velte, A. T., Velte, T. J., & Elsenpeter, R. C. (2009). "Cloud Computing: A Practical Approach" - Publicado en 2009 por McGraw-Hill Osborne Media.

XVIII. "Above the Clouds: A Berkeley View of Cloud Computing", publicado en la revista Communications of the ACM, volumen 53, número 4, páginas 50-58, en abril de 2010. Los autores son Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica y Matei Zaharia.

XIX. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). "Cloud computing—The business perspective." Decision support systems. Publicado en enero de 2011.

XX. Fearn-Banks, K. (2019). "Crisis communications: A casebook approach." Routledge. Publicado en el año 2019.

XXI. Toth, A., & Koppen, V. (2014). "Business continuity management: Global best practices." Publicado en el año 2014. Editorial: Rothstein Associates Inc

XXII. "Doughty, K. (2014). Business continuity for dummies." Publicado en el año 2014. Editorial: John Wiley & Sons.

XXIII. Hoyt, R. E., & Liebenberg, A. P. (2011). "Fundamentals of Risk and Insurance" escrito por Hoyt, R. E., & Liebenberg, A. P. es 2011. La editorial es John Wiley & Sons.