UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en

ADMINISTRACIÓN DE EMPRESAS

RCP-SO-37-No.696-2017

Opción de titulación:

PROPUESTAS METODOLÓGICAS Y TECNOLÓGICAS AVANZADAS

TEMA:

DISEÑO DEL PLAN DE CONTINUIDAD DE NEGOCIO APLICADO A SEGURIDAD DE INFORMACIÓN EN PYME INTERVISIÓN DE GUAYAQUIL

AUTOR:

ARMANDO JOSE GUTIERREZ MENDOZA

DIRECTOR:

CAMILO ENRIQUE OÑATE HUAYAMABE

Guayaquil - Ecuador
2022

COHORTE
2019-2021

Autor:

Armando José Gutiérrez Mendoza

Ingeniero en Sistemas Computacionales
Candidato a Magíster en Administración de Empresas con mención en Proyectos por la Universidad Politécnica Salesiana – Sede Guayaquil.
argume@gmail.com

Dirigido por:

Camilo Enrique Oñate Huayamabe

Licenciado en Electrónica de controles Industriales
Magister en Gestión de Proyectos
conate@ups.edu.ec

INDICE GENERAL

Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

1. INTRODUCCIÓN

1.1 Situación Problemática

Intevisión es una empresa Ecuatoriana fundada en al año 2008 por un conjunto de Oftalmologos radicados en la ciudad de Guayaquil cuya sede se encuentra ubicada al norte de la ciudad, cuya actividad económica está orientada a la atención de la salud humana por medio de sus servicios de diagnóstico clínico e investigación terapeutica de la visión.

En atención a la situación actual de la pandemia mundial y por el tratamiento de la información fisica y lógica actual de la empresa, reconocen que pueden exisitr riesgos en materia de seguridad informática en función de cómo se están utilizando la tecnología dentro de la organización. A continuación describimos los principales vectores de ataques o vulnerabilidades a la que pueden estar expuestos: correo electrónico, página web, tabletas, smartphones, sistemas de información y repaldos de la información. Traduciendose en posibles brechas de seguridad explotadas por ciberdelincuentes. Por ello considereamos necesario diseñar el plan de continuidad de negocio aplicado a la seguridad de la información, el que estará enfocado en los niveles de riesgo personas, procesos y tecnología.

Frente a la situación anómala la mayoría de las organizaciones al inicio de la pandemia SARCS 2 – COVID 19, no tenían considerado como hacerle frente por el el desconocimiento de su tratamiento a nivel munidal y en muchas ocasiones las empresas no tenían considerado desarrollar un plan de continuidad de negocio para contrarestar la situación. Esto a demando a las organizaciones a improvisar el trabajo de manera remota exponiendo a las empresas a posibles brechas de seguridad. Por ello se dieron ciertas paralizaciones a nivel local sobre las operaciones en las organizaciones hasta poder implementar las medidas de bioseguridad y seguridades informáticas con las que se establecieron controles para precautelar las salud de los empleados y el accesos sobre los activos fisicos y lógicos de las organizaciones.

De la mano de la pandemia se ha observado a nivel mundial ciber delincuentes explotando brechas de seguridad sobre ciertas plataformas tecnológicas para causar pánico y dejarlos sin poder operar por medio de ataques distribuidos de denegación de servicios (DDOS). Acorde al informe de kasperky describre que en el Q2 del año es notable el número de ataues de abril a junio, lo cuál se a incrementado en realción al Q1. Esto se da practicamente por las medidas restrictivas del coronavirus a nivel mundial (Oleg Kupreev, 2020).

Adicionalmente a lo expuesto se han incrementado ataques por medio spam, suplantación de identidad (phishing) vía correo electrónico o técnicas de ingeniería social para explotar las brechas de seguridad de sus victimas. Según Kaspersky en su portal de análisis reporta que la proporción de spam en el tráfico de correos en el Q1 y Q2 del año 2020 correspodne al 52.39%, es decir mas correo no deseado circulando en el los buzones de correo (Tatyana Kulikova, 2020).

Ahora bien aterrizando al entorno local lo descrito previamente no estamos distantes de las consecuencias que podrían ocurrir si no se mantienen controles de seguridad de la información bien implementados y con las debidas configuraciones de seguridad correspondientes. Estos podrían contrarrestar lo que se describe a continuación en el mapa de ciberamaneza en tiempo real según Kaspersky, ya que nos encontramos en la ubicación 39 como País más atacado a nivel mundial. Ver figura 1 y 2

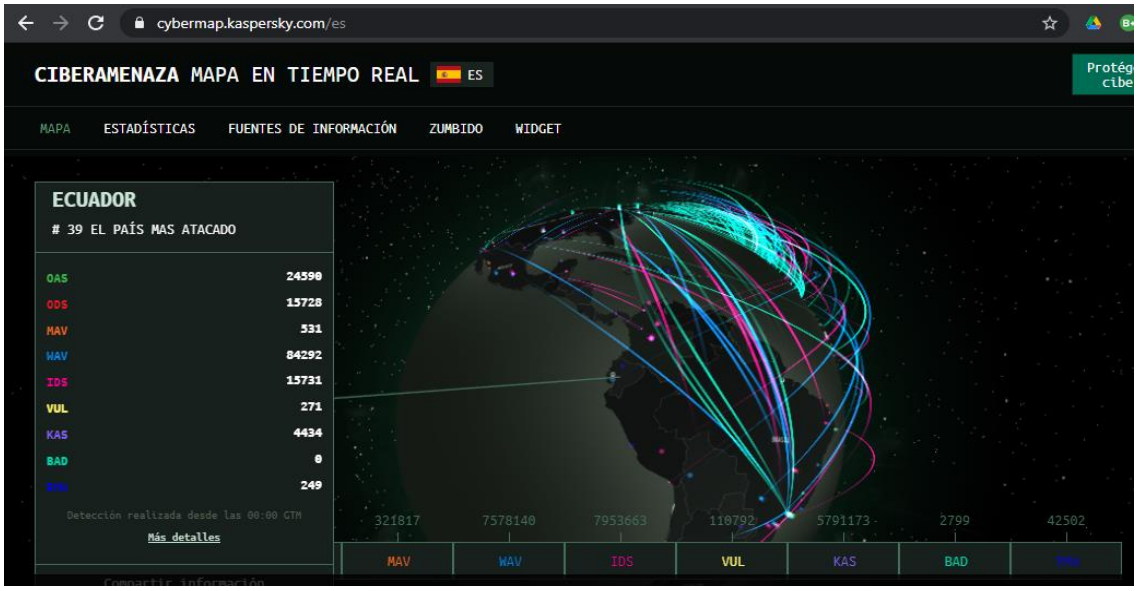


Figura 1. Mapa Cibermanezas en tiempo real – Ecuador
Fuente: Extraído del portal de Ciberamenzas de Kaspersky (Kaspersky, 2021)

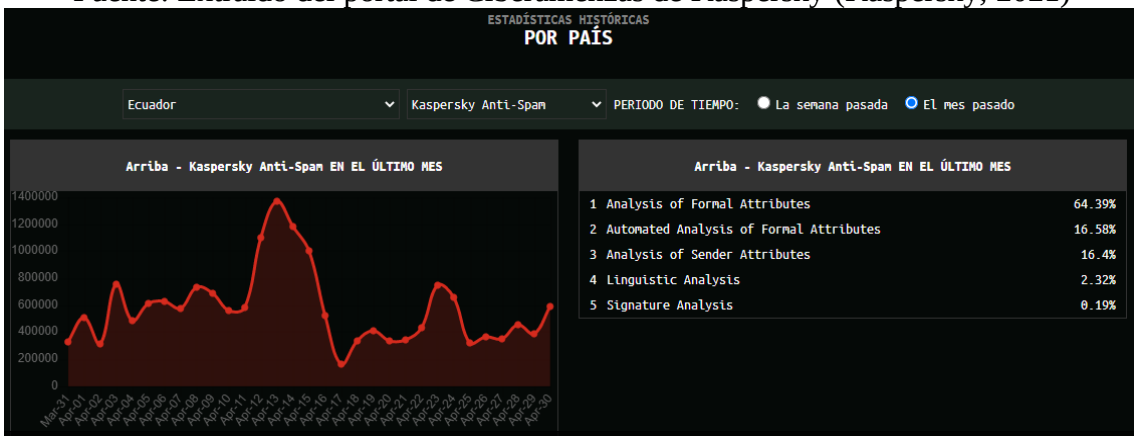


Figura 2. Estadística histórica Ecuador mes abril por Spam
Fuente: Extraído del portal de Ciberamenzas de Kaspersky, (Kaspersky, 2021)

1.2 Formulación Problema

1.2.1 Formulación del problema general

¿Cómo el plan de continuidad del negocio garantiza los servicios operativos frente a eventos de vulnerabilidad y/o ataques cibernéticos?

1.2.2 Formulación de los problemas específicos

¿Cómo los servicios críticos se podrían afectar frente a un evento de vulnerabilidad Intervisión?

¿Cómo las amenazas de vulnerabilidades podrían anular los servicios críticos de Intervisión?

¿Cómo la ausencia de una matriz de riesgos sobre los servicios críticos de Intervisión puede impactar la operatividad del negocio frente a un evento de vulnerabilidad?

¿Cómo las estrategias de recuperación de los servicios críticos pueden impactar la continuidad de las operaciones de Intervisión, frente a un evento de vulnerabilidad?

¿Cómo los tiempos de recuperación de los servicios críticos pueden incidir en la operatividad de Intervisión, frente a un evento de vulnerabilidad?

1.3 Justificación Teórica

La presente investigación tiene como finalidad diseñar el plan de Continuidad de negocio aplicado a la seguridad de la información en la compañía Intervisión PYME de Guayaquil, con base en el modelo de referencia de procesos Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT), siglas en inglés, aplicado a la metas del negocio y su relación con el gobierno de Tecnología de la Información (TI) sobre los dominios Alinear, Planificar y Organizar (APO13), siglas en inglés y Gestionar la Seguridad, el dominio Entrega, Servicio y Soporte (DSS04) , siglas en inglés.

Adicionalmente el marco del Instituto Nacional de Estándares y Tecnología (NIST), el mismo que proporciona una estructura de organización común para múltiples enfoques de seguridad cibernética mediante la conformación de estándares, directrices y prácticas que funcionan de manera efectiva en la actualidad, siglas en inglés. Cuyo objetivo es que las empresas de cualquier tamaño apliquen los principios y mejores prácticas de gestión de riesgos para mejorar la seguridad cibernética y la capacidad de recuperación. (NIST, Marco de trabajo NIST, s.f.)

También tomaremos las referencias del Instituto de Ciberseguridad Español (INCIBE), bajo sus distintas herramientas y mejores prácticas en términos de la concientización de ciberseguridad de la información.

1.4 Justificación Práctica

La presente investigación tiene como objetivo dar a conocer lineamientos que se pueden aplicar para prevenir, preparar, responder, administrar y recuperar el negocio frente algún caso de disrupción (Desastre naturales, pandemia, ataques cibernéticos, corte de servicios básicos entre otros)

Para la aplicación de la seguridad de la información se analizará el Marco de Trabajo para el mejoramiento de Ciberseguridad (NIST), considerando 5 dimensiones: identificación,

protección, detección, respuesta y recuperación. Las dimensiones se medirán por medio de un análisis inicial de la situación actual de la empresa en términos de seguridad, de la mano de la matriz de riesgos, la cual será el punto de partida para el análisis de nuestra propuesta. que describirá la situación real de la empresa en cuanto al cumplimiento del plan de continuidad del negocio (PCN) y su aplicación a la ciberseguridad.

1.5 Objetivos de la Investigación

1.5.1 Objetivo General

Diseñar un plan de continuidad de negocio aplicado a la seguridad de la información en la empresa Intervisión de la ciudad Guayaquil.

1.5.2 Objetivos específicos

- Identificar los servicios críticos que podrían afectarse frente a un evento de vulnerabilidad.
- Establecer los servicios críticos que Intervisión debe mantener operativos frente a un evento de vulnerabilidad.
- Elaborar una matriz de riesgos referente a los servicios críticos y analizar su impacto frente a un evento de vulnerabilidad.
- Proponer las estrategias de recuperación de los servicios críticos, frente a un evento de vulnerabilidad.
- Establecer los tiempos de recuperación de los servicios críticos frente a un evento de vulnerabilidad.

1.6 Principales Resultados

Durante nuestro relevamiento para conocer la situación actual de la empresa aprovechamos una herramienta de INCIBE que proporciona una encuesta electrónica en el siguiente enlace https://adl.incibe.es/, cuyo resultado presenta el nivel de riesgo al que está expuesta la organización.

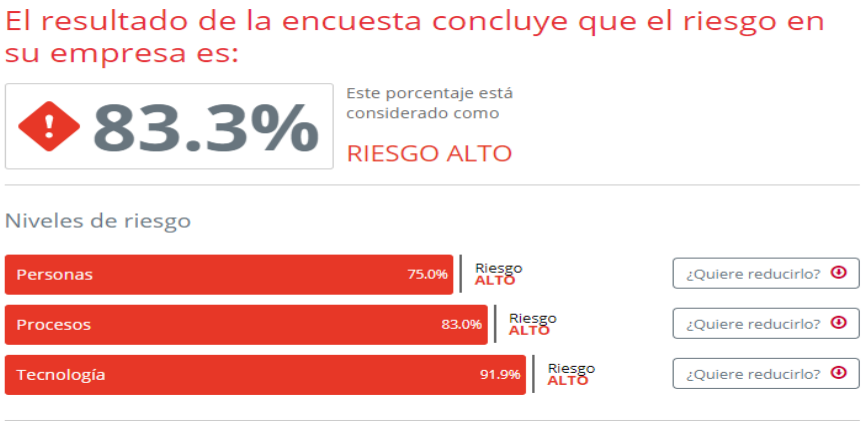


Figura 3. Niveles de Riesgos resultados de encuesta
Fuente: (INCIBE, Protege tu empresa, s.f.)

Resumen del diagnóstico proporcionado por la herramienta.

Aún no considera que la seguridad de la información es importante para su empresa o bien cree que la información no es muy esencial para su actividad.

- Analice y clasifique la información que maneja en su empresa (facturas, bases de datos de clientes, contratos, etc.) en función de su confidencialidad, integridad y disponibilidad. Consulte la sección de Protección de la información. (INCIBE, Protege tu empresa, s.f.)

- Revise si la información que maneja está sujeta al Reglamento General de Protección de Datos (RGPD) y si en su web tiene que cumplir con la La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) según el apartado de Cumplimiento Legal. (INCIBE, Cumplimiento Legal, s.f.) Para el ámbito local el LSSI es el reglamento a ley de comercio electrónico. (Telecomunicación, s.f.) Lo descrito en el párrafo previo llevándolo al ámbito local debería estar enmarcado en la Ley de Protección de Datos y la Ley de Comercio Electrónico.

- Considere empezar a formar a sus empleados, como indica el apartado de Desarrollar una cultura de seguridad. (INCIBE, Cultura en términos de seguridad con los empleados, s.f.)

2. MARCO TEÓRICO

2.1. Marco conceptual.

Continuidad de negocio: La continuidad de un negocio podría definirse como la situación en que la operativa de una entidad tiene lugar de forma continuada y sin interrupción. Sucesos de gravedad alto o fuerte impacto como algunos de los ocurridos en los últimos años (ataques terroristas, pandemias o catástrofes naturales), ponen de manifiesto el riesgo de que se puedan producir graves perturbaciones o interrupciones en la operativa del sector financiero y la necesidad de paliar sus consecuencias, abordando la cuestión de forma global y coordinada. (España)

La continuidad en todo tipo de negocio es importante en la actualidad debido a la prioridad que se proporciona al servicio a los clientes, los resultados financieros y la supervivencia en el mercado, son prioritarios con el objetivo de estar a la vanguardia de la competencia que se ha generado en los últimos tiempos. (Gonzalez, 2017) Página 9

Plan de continuidad del negocio: Establece la continuidad de una organización independientemente de su tamaño y tomando en consideración las siguientes perspectivas: infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores. (Incibe, Incibe - Protege tu Empresa)

El desarrollo del Plan define objetivamente los procesos críticos de la compañía y permite una consolidación de intereses entre la alta dirección y las diferentes unidades organizativas al constatar que diferentes áreas apoyan a procesos idénticos y generar estrategias efectivas para los incidentes no previstos. (Bustamante, 2017) Si bien gestionar los riesgos no es una garantía de control para todas las eventualidades que puedan suceder, si permite prevenir muchos acontecimientos que podrían poner en riesgo la continuidad del negocio. El plan de continuidad del negocio es una estrategia de gestión

de riegos que permite la prevención de contingencias y la provisión de estrategias y recursos que permitan la sobrevivencia de la empresa. La seguridad es parte fundamental de los planes de continuidad de negocio, para poder restablecer y restituir los activos de la empresa. (Guzmán E. H., 2015)

Seguridad de la información: es el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques accidentales o intencionados.

La seguridad informática a su vez está dividida en seis componentes a saber:

• SEGURIDAD FÍSICA: Es aquella que tiene relación con la protección del computador mismo, vela por que las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos. (Pino, 2016)

• SEGURIDAD DE DATOS: Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma, protege la integridad de los sistemas de datos.

• BACK UP Y RECUPERACIÓN DE DATOS: Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra daños o se pierda.

• DISPONIBILIDAD DE LOS RECURSOS: Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accesados por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.

• LA POLÍTICA DE SEGURIDAD: Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera.

• ANÁLISIS FORENSE: El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de seguridad informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas.

Servicios Críticos: Estos van a corresponder en la medida en que cada negocio pueda identificar y determinar en cuanto a los activos de la organización para establecer su criticidad.

Tabla 1. Servicios Críticos

Personas	Inventario	Operaciones	Información	Equipos	Edificio
•Empleados •Clientes •Proveedores	•Stock •Pedidos •Entrega •Despacho	•Fabricación •Facturación •Cobros / Pagos •Nómina	•Bases de Datos. •Respaldos de Seguridad •Sistemas •Documentos	•Servidores •Estaciones de Trabajo •Teléfonos •Mobiliario •Comunicación (Redes)	•Oficina •Bodegas •Taller •Almacen

Elaborado por: Gutiérrez, 2021

Si un servicio crítico produce un fallo puede ocasionar pérdidas económicas significativas, paralización de operación por tiempos indeterminados, daños físicos o en el peor de los casos amenazas a la vida humana.

Vulnerabilidad: (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Debilidad que presentan los activos y que facilita la materialización de las amenazas. (Incibe, Gestión de riesgos , 2015)

Amenazas: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas. (Incibe, Amenaza vs Vulnerabilidad, 2017)

Ataques cibernéticos: los ciberataques pueden generar robos de información, borrado de información, cifrado de información para solicitar un rescate, indisponibilidad de servicios, paralizar empresas públicas o privadas. También puede darse problemas entre naciones que mantienen este tipo de ataques por presiones de poder económico o de territorio.

Riesgo: Es la probabilidad de ocurrencia de un evento no deseado, cuyo impacto puede ser catastrófico, desastroso, serio, menor o insignificante. Adicionalmente las organizaciones pueden tratarlos bajo cuatro estrategias: Transferirlo, asumirlo, eliminarlo e implantar medidas para mitigarlo.

2.2. Bases teóricas. Discusión de enfoques de diferentes autores

2.2.1 Servicios críticos, riesgos y amenazas de continuidad

Las organizaciones se dan cuenta más de la importancia de adoptar enfoques de manera proactiva, es esencial salvaguardar los procesos comerciales y la relación entre ellos, con el fin de lograr los objetivos comerciales (N. Sahebjamnia, 2018). Así, las organizaciones deben prepararse en caso de disrupciones en su productividad y capacidad competitiva, especialmente en los procesos de negocio, apoyados en los servicios de Tecnologías de la Información y la Comunicación (TIC), puestos a disposición de la organización.

Teniendo esto en cuenta, las organizaciones deben desarrollar un conjunto de políticas y procedimientos para minimizar el impacto. Se destaca la importancia de estas medidas, cuyo impacto puede afectar la productividad y la capacidad competitiva, especialmente

en el caso de organizaciones cuya dependencia se de en los servicios de tecnología y comunicaciones. Este es el concepto fundamental de la continuidad del negocio, en el que una organización debe tener la capacidad estratégica y táctica para planificar y responder a incidentes e interrupciones comerciales (R. K.Ramakrishnan, 2011)

En la actualidad, la tecnología de la información se a convertido en una importante herramienta para que la gesitón del conocimiento en la toma de decisiones y aprovechar la oportunidad lo antes posible. Además la tecnología ayuda a las organizaciones a construir repositorios e indentificar el objeto de conocimiento como requerimiento para alcanzar lo requerido. (T. H. Davenport, 2001)

La continuidad del negocio debe tener en cuenta la valoración del riesgo tecnológico y su efecto sobre los activos infomaticos, la valoración de los riesgos físico y su efecto en la producción o en el servicio, las valoración de las tareas desarolladas por las personas y su redundacia para manejar procesos críticos y la planificación y reserva de los recursos para poder soportar de manera temporal el funcionamiento temporal (Guzmán E. H.)

La gestión de riesgos es el programa para identificar debilidades, amenazas y evaluaciones de impacto que podrían causar daños sobre las organizaciones. En términos de servicios, productos y maximmización de beneficios en una organización, la gestión de riesgos ayuda en minimizar las oportunidades de riesgos inesperados. (Wheeler, 2011) Explica que la gestión de riesgos es un proceso iterativo que discute análisis, planificación, implementación, control y supervisión de los riesgos llevados a cabo en determinados momentos (por ejemplo, una vez al año, etc.). La gestión de riesgos ayuda a las organizaciones a centrarse en zonas que pueden verse afectadas por un alto riesgo, también aseguran si hay una pérdida, entonces no previene ni impide la gestión de la búsqueda; el objetivo es preservar los activos y realizar el valor esperado de la inversión.

Como la continuidad del servicio (business-as-usual) es de suma importancia para los propietarios, gestores de activos y las disponibilidad del servicio en cualquier instancia, se ha definido el «indicador de rendimiento» (PI) del sistema, en este estudio. Cabe destacar que el PI para cualquier sistema es definido por los criterios de toma de decisiones, esto está vinculado a la prestación de "continuidad del servicio" a los usuarios

finales. Un sistema ideal es responsable de la prestación del servicio al 100% de sus usuarios, en cualquier momento dado (Donya Hajializadeh, 2021)

Implementar cultura de previsión, prevención y de riesgo, no es una tarea fácil en las empresas puesto que requiere de inversiones de dinero importantes y dadas las crisis y contingencias del mercado muchos gestores las consideran poco costo-efectivas. (Guzmán E. H., 2015), sin embargo, las nuevas organizaciones tienen presente que la identificación de los riesgos de manera temprana puede ayudarles a robustecer su operación y aplicar de lecciones aprendidas.

2.2.2 Metodologías y estándares internacionales

Objetivos de Control para Tecnologías de Información (COBIT 5)

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

COBIT 5 se basa en cinco principios claves:

Figura 4. Principios de Cobit 5
Fuente: (ISACA, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa)

1. Satisfacer las necesidades de las partes interesadas: Mantener el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.
2. Cubrir la empresa extrema a extremo: Integra el gobierno y la gestión de TI en el gobierno corporativo.
    a. Cubriendo todas las funciones y procesos dentro de la empresa.
    b. Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos
3. Aplicar un marco de referencia único integrado: COBIT 5 se alinea a alto nivel con otros

    estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

4. Hacer posible un enfoque holístico: Para ello define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. El marco define siete categorías de catalizadores:
    a. Principios, Políticas y Marcos de Trabajo
    b. Procesos
    c. Estructuras Organizativas
    d. Cultura, Ética y Comportamiento
    e. Información
    f. Servicios, Infraestructuras y Aplicaciones
    g. Personas, Habilidades y Competencias
5. Separar el Gobierno de la Gestión: establece una clara distinción entre gobierno y gestión.
    a. El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.
    b. La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Esto proporciona un modelo de referencia de procesos que representa todos los procesos encontrados normalmente en una empresa respecto a las actividades de TI, ofreciendo un modelo de referencia común entendible para gerentes de operativa TI y de negocio. El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica. (ISACA, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa)

Figura 5. Modelo de referencia de proceos de COBIT 5
Fuente: (ISACA, Cobit 5 - Marco de Trabajo - Procesos Catalizadores)

Instituto Nacional de Estándares y Tecnología (NIST)

Las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de los sistemas de infraestructura crítica, lo que pone en riesgo la seguridad de la nación, su economía y la salud y seguridad pública. Similar a los riesgos financieros y de reputación, el riesgo de la seguridad cibernética afecta el resultado final de una empresa. Puede aumentar los costos y afectar los ingresos de la misma. Puede afectar la capacidad de una organización para innovar, añadir y mantener clientes. La seguridad cibernética puede ser un componente importante y amplificador de la gestión general de riesgos de una organización.

El Marco proporciona una taxonomía común y un mecanismo para que las organizaciones realicen lo siguiente:

1. Describir su postura actual de seguridad cibernética.
2. Describir su objetivo deseado para seguridad cibernética.
3. Identificar y priorizar oportunidades de mejora dentro del contexto de un proceso continuo y repetible.
4. Evaluar el progreso hacia el objetivo deseado.

El Marco proporciona un lenguaje común para comprender, gestionar y expresar el riesgo de seguridad cibernética para las partes interesadas internas y externas. Se puede utilizar para ayudar a identificar y priorizar acciones para reducir el riesgo de seguridad cibernética, y es una herramienta para alinear los enfoques de políticas, negocios y tecnología para manejar dicho riesgo. También se puede utilizar para administrar el riesgo de seguridad cibernética en todas las partes de una organización o se puede enfocar en la entrega de servicios críticos dentro de una parte de la organización. (NIST, Marco para la mejora de la seguridad cibernética en infraestructuras críticas, 2018)

Funciones: Ayudan a una organización a expresar su gestión del riesgo de seguridad cibernética organizando información, habilitando decisiones de gestión de riesgos, abordando amenazas y mejorando el aprendizaje de actividades previas. Las Funciones también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en seguridad cibernética.

Categorías: Subdivisiones de una Función en grupos de resultados de seguridad cibernética.

Subcategorías: Resultados específicos de actividades técnicas o de gestión.

Referencias informativas: Son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría

Las cinco funciones del marco para formar una cultura operativa que aborde el riesgo dinámico de seguridad cibernética.

Tabla 2. Funciones del marco:

Identificar	Proteger	Detectar	Responder	Recuperar
•Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades	•Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos	•Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética	•Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.	•Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

Fuente: Elaboración propia en base a la metodología NIST, Gutiérrez, 2021

Niveles de implementación

Nos permiten conocer el contexto sobre cómo la organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar el riesgo. (Ver Tabla 3)

La implementación exitosa del marco se basa en el logro de los resultados descritos en el Perfil(s) Objetivo(s) de la organización y no en la determinación del nivel. Sin embargo, la selección y la designación ayudará a establecer el tono general de cómo se gestionará el riesgo de seguridad cibernética dentro de la organización, y deberá influir la priorización dentro de un Perfil Objetivo y en las evaluaciones del progreso para abordar las brechas

Tabla 3. Niveles de implementación

Niveles	Tipo	Proceso de gestión de riesgos	Programa integrado de gestión de riesgos	Participación externa

Nivel 1	Parcial	Riesgos de seguridad cibernética de la organización no están formalizadas y se gestionan de manera reactiva.	Organizaciones con una conciencia limitada sobre el riesgo de seguridad cibernética, se implementa la gestión de forma irregular y puede no tener procesos de ciberseguridad definidos dentro de la organización.	La organización no comprende su función en el ecosistema más amplio con respecto a sus dependencias o dependientes
Nivel 2	Riesgo Informado	Riesgos de seguridad cibernética identificados, pero no se han establecido políticas para toda la organización.	No se ha establecido un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética.	La organización no comprende su función en el ecosistema más amplio con respecto a sus dependencias o dependientes.
Nivel 3	Repetible	Los riesgos de la organización se aprueban formalmente y se expresan como políticas. Se mantienen actualizados periódicamente.	Existe un enfoque de toda la organización para gestionar el riesgo de seguridad cibernética. Las políticas, procesos y procedimientos. Existen métodos para responder a los cambios.	Colabora y recibe regularmente información de otras entidades que complementan la información generada internamente, y comparte información con otras entidades.
Nivel 4	Adaptable	La organización adapta sus prácticas de seguridad cibernética, incluye las lecciones aprendidas y los indicadores predictivos. Continuamente se adapta a un	Existe un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética que utiliza las políticas, los procesos y los procedimientos informados sobre riesgos para abordar posibles eventos de seguridad cibernética.	La organización entiende su rol, sus dependencias y sus dependientes en el ecosistema más amplio y contribuye a una mayor comprensión de los riesgos por parte de la comunidad.

		panorama cambiante de amenazas y tecnologías, y responde de manera eficaz y oportuna a las nuevas y sofisticadas amenazas.		

Fuente: (NIST, Marco para la mejora de la seguridad cibernética en infraestructuras críticas, 2018)

Instituto de Ciberseguridad España (INCIBE)

Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permitan a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza poder dar una respuesta planificada ante cualquier fallo de seguridad. (Incibe, INCIBE, s.f.)

También es importante mencionar que el término continuidad del negocio no hace referencia exclusivamente a aspectos relacionados con las tecnologías de la información.

Cada organización establece las medidas necesarias y proporcionales a sus necesidades para garantizar su continuidad en caso de desastre. Si hablamos del ámbito tecnológico, por ejemplo, mientras que una gran organización puede requerir el despliegue de un centro de respaldo alternativo, tanto de comunicaciones, sistemas como servidores en una ubicación remota, en otros casos podría ser más óptimo realizar copias de seguridad en la nube, primando el rendimiento frente al coste.

Podemos describir los tres tipos según el alcance o ámbito:

1. Plan de Continuidad de Negocio (PCN): establece la continuidad de una organización desde múltiples perspectivas:infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales,

infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico.

2. Plan de Continuidad TIC: es uno de los planes que forman el plan de continuidad de negocio de nuestra organización, pero restringido al ámbito TIC
3. Plan de Recuperación ante Desastres (PRD): En este caso, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe.

El mantener un plan de continuidad de negocio nos ayuda a:

- Mantener el nivel de servicio requeridos.
- Establecer un periodo mínimos de recuperación.
- Recuperar la situación inicial antes de cualquier incidente de seguridad.
- Analizar los resultados y los motivos de los incidentes.
- Evitar que las actividades de la empresa se interrumpan.

Los factores que pueden garantizar la continuidad de una empresa

- Fase 0. Determinación del alcance: Por departamentos o áreas con mayor importancia y progresivamente ir ampliando la continuidad a toda la organización.
- Fase 1. Análisis de la organización: Identificación de procesos de negocio críticos, los activos que les dan soporte y cuáles son las necesidades temporales y de recursos.
    a. Levantamiento de información (reuniones con equipo de trabajo)
    b. Análisis de Impacto (BIA)
        i. El BIA (Análisis de Impacto sobre el Negocio), es uno de los ejes principales del PCTIC (Plan de Continuidad TIC), al contener las necesidades de los procesos definidos como alcance. Así podremos clasificarlos según su criticidad y su dependencia de los activos tecnológicos. Identificar los requisitos temporales y de recursos de

los procesos dentro del alcance y, junto con el Análisis de Riegos define las iniciativas a implantar para recuperar los procesos en situación de contingencia. INCIBE, Plan de contingencia y continuidad de negocio.

c. Análisis de Riesgo

i. Trasnferir el riesgo a un tercero.

ii. Eliminar el riesgo.

iii. Asumir el riesgo.

iv. Implantar medidas de seguridad para mitigarlo.

Figura 6. Etapas del Analisis de Riegos (Incibe, Incibe, 2020)

- Fase 2. Determinación de la estrategia de continuidad: Una vez identificados los activos que soportan los procesos críticos, debemos determinar si en caso de desastre, seremos capaces de recuperar dichos activos en el tiempo necesario. En caso de no tenerlos identificados se debe establecer estrategias de recuperación.
- Fase 3. Respuesta a la contingencia: Sobre las estrategias seleccionadas se realiza la selección e implantación de las iniciativas necesarias, y se documenta el Plan de Crisis y los respectivos documentos para la recuperación de los entornos.

- Fase 4. Prueba, mantenimiento y revisión: desarrollo de planes de prueba y mantenimiento.
- Fase 5. Concienciación: Tanto el personal técnico como los responsables de nuestra empresa conozcan qué es y qué supone el Plan de Continuidad de Negocio así como qué se espera de ellos.

Al elegir la estrategia de continuidad determinaremos la más adecuada para nuestra empresa. Implantaremos políticas de copias de seguridad, donde definiremos la información que debe incluirse en dichas copias, qué tipo de soporte se utilizará, con qué periodicidad y en qué instalaciones físicas. Asimismo, se deberían definir pruebas periódicas para verificar la integridad y la correcta recuperación de la información. Por otro lado, estudiaremos la conveniencia de implantar un centro de respaldo a raíz de los resultados obtenidos durante la elaboración del BIA (Análisis del Impacto en el Negocio). Esto es especialmente importante si el alcance del Plan es el CPD (Centro de procesamiento de datos) . (INCIBE, Continuidad de negocio para pyme)

3. METODOLOGÍA

3.1. Unidad de análisis

En la presente investigación la unidad de análisis se basará en las entrevistas a los miembros de Intervisión y los encargados de las soluciones tecnológicas, cargos gerenciales y quienes participan en los procesos claves de la organización.

3.2. Población

Para la presente investigación, la población de estudio fue 5 colaboradores de las cuales se detalla los cargos: Gerente General, Jefe de servicio, Contador, Jefe Financiero y Jefe Administrativo; quienes participan en los procesos claves de la empresa Intervisión de la ciudad Guayaquil.

Tamaño y selección de muestra

La propuesta del estudio fue No probabilistica: Intencionada, en vista que se considero a los 5 colaboradores de mandos altos y medios de la empresa Intervision de la ciudad de Guayaquil.

3.4. Métodos a emplear.

La investigación se desarrolló de forma transversal, bajo el método inductivo, que parte de apreciaciones particulares para obtener conocimientos generales, El estudio fue descriptivo, con un enfoque cualitativo que utilizó a la entrevista como técnica que permitió identificar el desconocimiento de las mejores prácticas además fue necesario realizar un levantamiento de información para conocer la situación actual de Intervisión, para ello utilizamos las guías del Instituto de Ciberseguridad de España (INCIBE), planes, encuestas electrónicas y metodologías como NIST, COBIT 5; lo cual permitió identificar qué medidas paliativas se deben llevar acabo en cuanto a los riesgos expuestos y la mejoras que se deben aplicar para mitigar eventos no deseados o catastróficos y saber cómo responder en caso de que se presenten.

3.5. Identificación de las necesidades de información. Fuentes primarias o secundarias

Fuentes Primarias

“Son todas aquellas de las cuales se obtiene información directa, es decir, de donde se origina la información. Es también conocida como información de primera mano o desde el lugar de los hechos.” (César, 2010, pág. 191)

Se tomaron como datos primaros la información recabada durante las entrevistas con los cargos de mandos medios, altos y la encuesta electrónica. (Ver Anexo 1)

Fuentes Secundarias

“Son todas aquellas que ofrecen información sobre el tema que se va a investigar, pero que no son la fuente original de los hechos o las situaciones, sino que sólo los referencian. Las principales fuentes secundarias para la obtención de la información son los libros, las

revistas, los documentos escritos (en general, todo medio impreso), los documentales, los noticieros y los medios de información.” (César, 2010, pág. 192)

Por ello, se considera, fuentes secundarias a las referencias y soportes de las metodologías empleadas, marcos de trabajo, artículos y libros referente al problema de investigación.

3.6. Técnicas de recolección de datos

Las técnicas de recolección de datos de la presente propuesta metológica están basados en el apoyo instituciones de ciberseguridad y los marcos de trabajo con sus buenas prácticas descritos a continuación:

Instituto Nacional de Cyberseguridad de España (Incibe)

Se evaluó de manera preliminar el nivel de riesgo de seguridad de Intervisión en función del uso de la tecnología: correo electrónico, página web, tabletas, smartphones, entre otros.

La información recolectada para conocer el nivel de riesgo de seguridad de la información será de manera automática, para lo cual deberá ingresar al enlace siguiente: https://adl.incibe.es/

El resultado dió a conocer el estado de ciberseguridad de la empresa y cuáles son los riesgos a primar vista que te afectan a la organización, con ello se podrá evaluar y priorizar la atención de las debilidades observadas.

Posteriormente con el preambulo identificado realizamos un enfoque por procesos con el objetivo de mejorar su continuidad. Para ello se realizó el análisis de impacto del negocio, con lo cual será posible determinar las actividades o procesos y recursos TIC más críticos, así como determinar en qué casos hay que aplicar medidas para cumplir con los requerimientos de negocio.

Adicionalmente para elaborar la matriz de análisis de riesgos se tomó como referencia el levantamiento del proceso de la organización durante las entrevistas realizadas y el análisis BIA para la Pyme Inversión. (Ver Anexo N°2 y N°3)

Marco de Trabajo NIST

El marco de trabajo cuenta con salidas claves de ciberseguridad identificadas por las organizaciones como una ayuda en la administración de los riesgos de ciberseguridad. Este esta compuesto por cuatro elementos: Funciones, categorias, subcategorias y referencias informativas de varios marcos de trabajo.

Aplicando el marco NIST la organización podrá:

1) Describir su estado actual en terminos de ciberseguridad.

2) Describir cual es objetivo deseado en terminos de ciberseguridad.

3) Identificar y priorizar las oportunidades de mejoras de los procesos.

4) Evaluar el progreso hacia el objetivo deseado.

5) Comunicar a las partes interesadas internas y externas sobre los riesgos de ciberseguridad.

Matriz RACI del marco de Trabajo COBIT 5

En base al marco de trabajo COBIT 5 utilizamos los modelos de referencia de procesos aplicados a la metas del negocio y su relación con el gobierno de TI sobre la propuesta planteada aplican los dominios APO 13 – Gestionar la Seguridad,

DSS04 - Gestionar la Continuidad. Sobre estos dominios realizamos la entrevista con los responsables destacados en la matriz RACI[1]. (Ver Anexo N°5 y N°6)

También usamos el marco de trabajo COBIT 5 acorde a los objetivos de control que cubran los problemas especificos descritos.

El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica. (ISACA, Cobit 5 - Marco de Trabajo - Procesos Catalizadores)

3.8. Herramientas utilizadas para el análisis e interpretación de la información

Para el análisis de la propuesta metodológica se tomaron como referencia los planes de seguridad de la información de INCIBE y los marcos de trabajo NIST, COBIT5.

En relación a los descrito en párrafo anterior y atendiendo la propuesta planteada de presentar una alternativa para el diseño de un plan de continuidad de negocio aplicado a la seguridad de la información de la pyme INTERVISION, pudimos identificar en base a la información levantada la situación actual de cada uno de los procesos de la organización. Adicionalmente realizamos un mapeo de cada uno de los marcos de trabajo para aterrizarlos a la necesidad de la organización (Ver Anexo N°7)

---

[1] La Matriz RACI también se conoce como una matriz de asignación de responsabilidad.

Responsible (Responsable);

Accountable (Autoridad);

Consulted (Consultor);

Informed (Informado).

4. RESULTADOS Y DISCUSIÓN

4.1. Análisis, interpretación y discusión de resultados

4.1.1 Identificar los servicios críticos que podrían afectarse frente a un evento de vulnerabilidad en la PYME INTERVISIÓN.

Para la identificación se determinó el alcance del plan de continuidad de negocio, el cual incluye el análisis de activos y procesos para garantizar la continuidad de las operaciones acorde a su criticidad.

Durante el análisis de identificación de activos pudimos identificar cuales estarían siendo expuestos a alguna vulnerabilidad dentro de la organización y que requieren atención:

- Servidor de Aplicaciones
- Servidor Web
- Equipos de computación
- Equipos de comunicación
    - Switch
    - Routers
- Dispositivos móviles

4.1.2 Establecer los servicios críticos que Intervisión debe mantener operativos frente a un evento de vulnerabilidad.

Frente a los activos críticos realizamos un análisis de impacto del negocio (BIA) considerando los tiempos de recuperación o RTO, es decir el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado.

También revisamos el grado de dependencia de los datos o RPO, es decir el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de respaldos de la organización.

De los resultados obtenidos pudimos identificar que no existen implementadas políticas de respaldo de información sobre los activos tecnológicos críticos de la operación.

4.1.3 Elaborar una matriz de riesgos referente a los servicios críticos y analizar su impacto frente a un evento de vulnerabilidad.

Para analizar la situación actual de la empresa posterior al análisis de impacto del negocio como premisa tuvimos la novedad de los tiempos de respuesta para restablecer las operaciones en base a la información, para lo cual no se contaba con mecanismos de recuperación establecidos como parte de la estrategia del negocio. Posteriormente elaboramos la matriz de riesgos en base a los activos críticos de la organización identificando las amenazas de mayor impacto y su probabilidad (Ver Anexo N°4) descritos a continuación:

- Alteración de la información: El efecto conlleva a la baja reputación institucional, lo cual puede trasladarse en el desprestigio de la marca y en la imagen frente a sus clientes.
- Caída del sistema por sobrecarga: cuando los sistemas no mantienen un plan de recuperación o una definición de un plan de mantenimiento para medir el rendimiento de su infraestructura
- Denegación de servicio: Se presenta cuando la vulnerabilidad bloquea las peticiones y genera sobre carga en los servicios ocasionando interrupciones que pueden trasladarse en horas, días y semanas si no se logra contener o identificar el problema.
- Destrucción de información: También observamos la exposición a la que se encuentra la organización por mantener ciertos privilegios especiales sobre recursos que no ameritan mantener este perfil habilitado.
- Errores de configuración: Fallas en la configuración de dispositivos de comunicación conllevan a filtraciones de externos para exponer datos de la organización.

- Errores de mantenimiento / actualización de equipos (hardware): el no contar con un procedimiento que permita identificar la programación del mantenimiento y la actualización de servidores, podría dejar expuesta a la organización por los vectores de ataque que se despliegan d manera frecuente por la red de redes.
- Errores del administrador: Se presentan por dos motivos; una por desconocimiento y otra por no contar con un ambiente que le permita ejecutar los cambios sin generar alteraciones sobre los ambientes productivo.
- Fuga de información: La información de la organización está expuesta ya que no existen mecanismos de seguridad como la prevención sobre la pérdida de datos que en algunas ocasiones no se tiene identificada su prioridad.
- Interceptación de información (escucha): Fallas o brechas de seguridad explotadas por terceros se pueden traducir en daños severos o fuga de información para conocer las debilidades internas. (man in the middle)

4.1.4 Proponer las estrategias de recuperación de los servicios críticos, frente a un evento de vulnerabilidad.

- Determinar el alcance en cuanto a la atención de los servicios críticos y desarrollar la estrategia a seguir en base a la matriz de riesgos levantada.
- Definir responsabilidades para la ejecución de actividades a llevar a cabo. Matriz RACI
- Establecer una política de comunicación para culturizar al equipo interno y externos.
- Revisar la caducidad de las actividades en cuanto a las estrategias de recuperación, definir una periodicidad.
- Detallar los procedimientos y controles específicos a ejecutar ante la aparición de un desastre.
- Desarrollar actividades para verificar, revisar y evaluar las estrategias de recuperación propuestas.

4.1.5 Establecer los tiempos de recuperación de los servicios críticos frente a un evento de vulnerabilidad.

En la tabla 4 se detalla los tiempos de recuperación mínimos en horas de los servicios críticos extraídos de la matriz de riesgos clasificados con mayor impacto y probabilidad de afectación.

Tabla 4. Tiempo de recuperación de los servicios críticos

Amenaza	Activo	Nivel de Riesgo	Tiempo de recuperación mínimo en horas
Alteración de la información	Servidor web - Sitio web alojado y gestionada por un proveedor externo	6	Alta Disponibilidad
Caída del sistema por sobrecarga	Router Wifi	6	8
Denegación de servicio	Servidor web - Sitio web alojado y gestionada por un proveedor externo	6	Alta Disponibilidad
	Switch 01	6	8
Destrucción de información	Equipos de Computación	6	8
	Servidor web - Sitio web alojado y gestionada por un proveedor externo	6	Alta Disponibilidad
Errores de configuración	Dispositivos móviles para telefonía y datos	6	8
	Router Wifi	6	8
	Servidor 01 (Aplicaciones)	6	8
Errores de mantenimiento / actualización de equipos (hardware)	Servidor 01 (Aplicaciones)	6	8
Errores del administrador	Servidor 01 (Aplicaciones)	6	Alta Disponibilidad
	Servidor web - Sitio web alojado y gestionada por un proveedor externo	6	8
Fuga de información	Servidor 01 (Aplicaciones)	6	8
Interceptación de información (escucha)	Dispositivos móviles para telefonía y datos	6	8

Elaborado por: Gutiérrez, 2021

4.2. Propuesta Metodológica o Tecnológica

Teniendo como base los resultados de las matrices de la cual se seleccionaron los activos con mayor afectación acorde al nivel de riesgo, describimos el plan de mejora a seguir a continuación ver tabla 5.

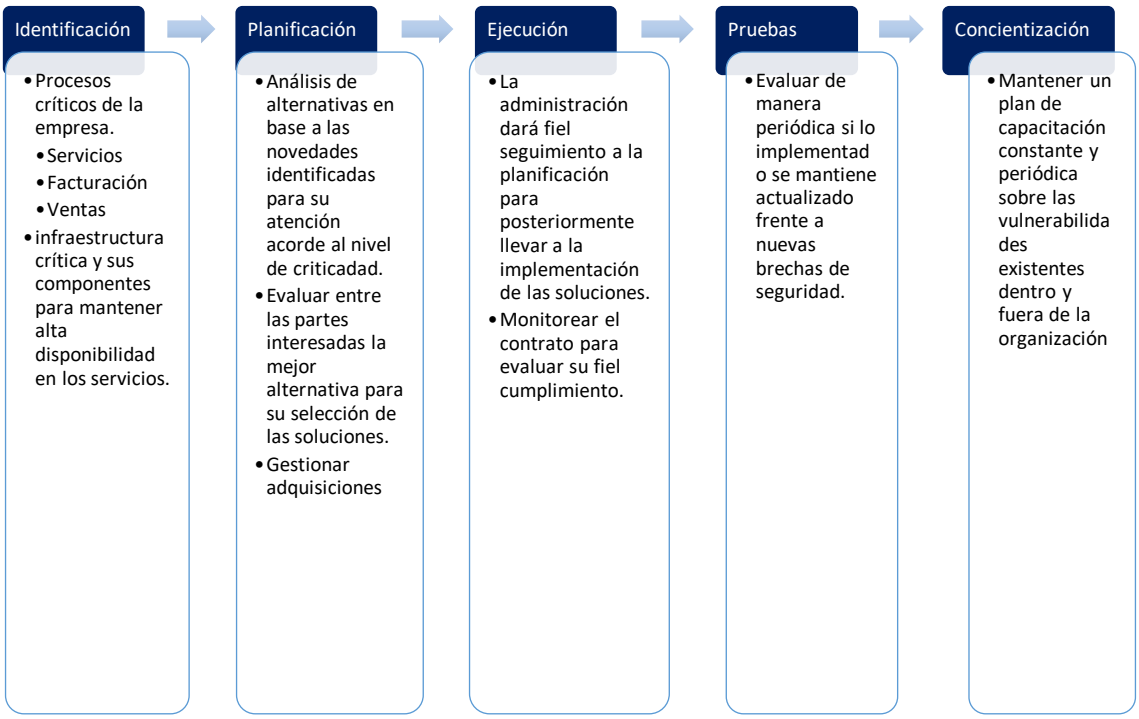
Tabla 5. Plan de Acción

Problema	Causas del problema	Acciones propuestas	Responsables	Plazo
Plan de continuidad del negocio frente a eventos de vulnerabilidad y/o ataques cibernéticos	Falta de un área responsable en terminos de tecnología de la información	Contratar un experto que lidere el área de tecnología	Gerente y mandos medios	Q1-2022
	Ausencia de definición de responsabilidades	Elaborar la matriz RACI y en cuanto a la operación del negocio, en ella se deben especificar quienes son los responsables..	Gerente y experto hacer contratado	Q1-2022
	Desconocimiento frente a fallos, eventos de vulnerabilidad o ataques cibernéticos	Capacitar al personal de manera periódica. Definición de roles y privilegios de usuarios con máximos privilegios.	Gerente y mandos medios	Q1-2022
	Tiempos de recuperación no definidos	Implementar soluciones en la nube que permitan restablecer los servicios en tiempos adecuados a la operación.	Gerente y experto hacer contratado	Q4-2022
	Falta de identificación de activos y servicios críticos dentro de la organización	Identificar la realidad del negocio en cuanto a los activos crítico y facilita la toma de	Gerente y experto hacer contratado	Q4-2022

		decisiones frente a incidentes de ciberseguridad. .		
	Ausencia de políticas, procedimientos y cumplimiento de normativas Legales en seguridad.	Desarrollar políticas y procedimientos en términos de seguridad de la información. Aplicación de mejoras preventivas para garantizar las operaciones del negocio	Gerente y experto hacer contratado	Q2-2022
	Ausencia de un plan de continuidad de negocio	Implementar y darle seguimiento de manera periódica. Contratación de seguros para contener el impacto en casos de eventos no deseados.	Gerente y experto hacer contratado	2022

Elaborado por: Gutiérrez, 2021

Como complemento al plan de acción se elabora este esquema metodológico para su aplicación:



Elaborado por: Gutiérrez, 2021

4.2.1. Premisas o supuestos

- Para implementar los planes de acción y aplicar estrategias, se requiere contratar a un experto que pueda mantener y administrar el plan de continuidad de negocio aplicado a seguridad de la información.
- Concientizar a todos los miembros de la organización para que cuenten con una cultura de prevención frente a vulnerabilidades a las que se pueden ver expuestos..
- Se necesita de un seguimiento en base a una peridicidad definida para evaluar el cumplimiento y sua actualización en caso de requerirlo.
- La adquisición de cortafuegos para previnir ataques externos en los diversos niveles de la arquitectura de la red.

4.2.2. Objetivo de la propuesta metodológica

Diseñar un plan de continuidad de negocio aplicado a la seguridad de la información en la empresa Intervisión de la ciudad Guayaquil ver tabla 6.

Tabla 6. Objetivo de la propuesta metodológica

Actividad Tecnológica	Acción
Tecnología de proceso	Contratar un experto que lidere el área de tecnología
	Elaborar la matriz RACI y en cuanto a la operación del negocio, en ella se deben especificar quienes son los responsables..
	Capacitar al personal de manera periódica. Definición de roles e identificación de usuarios con máximos privilegios.
Tecnología de producto	Implementar soluciones en la nube que permitan restablecer los servicios en tiempos adecuados a la operación.
Tecnología de operación	Identificar la realidad del negocio en cuanto a los activos críticos y facilita la toma de decisiones frente a incidentes de ciberseguridad. .
	Desarrollar políticas y procedimientos en términos de seguridad de la información. Aplicación de mejoras preventivas para garantizar las operaciones del negocio
	Implementar y darle seguimiento de manera periódica al plan. Contratación de seguros para contener el impacto en casos de eventos no deseados.

Elaborado por: Gutiérrez, 2021

4.2.3. Objeto de la propuesta

Se busca implementar la propuesta metodológica es en el área de tecnología de la información.

Inicialmente se requiere contratar un experto técnico que tenga la visibilidad para poder llevar a cabo y liderar el proyecto relacionado al diseño del plan de recuperación del negocio.

Posteriormente definir las responsabilidades que van a llevar a cabo y medir los niveles de servicios en caso de contar con el apoyo de un tercero al momento de darle un seguimiento a sus actividades a llevar a cabo.

Adicionalmente que la organización mantenga una identificación de los activos y servicios críticos para poder contar con una visibilidad integral que le permita conocer cuáles serían los riesgos de mayor impacto y probabilidad. Con ello se establecerían prioridades sobre aquellos de que requieren mayor atención para analizar su mitigación.

Evaluar de los resultados, para implementar mejoras o reforzar aspectos débiles en las medidas de seguridad.

Generar una visión de prevención en la organización integrando a todas las personas que la forman.

Facilitar el cumplimiento de las normativas legales en cuestión de seguridad.

Finalmente se requiere contar un centro de respaldo de los servicios críticos de la organización para poder rehabilitar la operación del negocio en el menor tiempo posible.

4.2.4. Responsables de la implementación y control

Tabla 7. Responsables de la implementación y control

Cargos	Funciones
Gerente General	Velar por que la organización mantenga un estrategia de servicio y la continuidad de las operaciones. Ademas del fiel cumplimiento con los entes de control, exposición de indicadores mensuales y los estados financieros a los accionistas.

	Proponer mejoras a la organización para su operación.
Esperto Técnico	Experto técnico realice la identificación de mejoras, controles e identificación de amenazas internas y externas para la organización. Supervisa las implementaciones de contrataciones con terceros.
Proveedores de servicios	Entregar servicios de calidad para los cuales fueron requeridos, incluyendo los tiempos de entrega, calidad y la garantía de sus entregables. Proporcionar planes de contingencia que se adecuen a nuestra organización para la continuidad del negocio

Elaborado por: Gutiérrez, 2021

4.3. Fases para su puesta en práctica

Tabla 8. Diagrama de Gantt

	Q1 - 2022	Q2 - 2022	Q3 - 2022	Q4 - 2022
Definir responsabilidades				
Establecer una política de comunicación para culturizar al equipo interno y externos				
Concientizar a personal sobre las vulnerabilidades existentes				
Ejecutar el plan de continuidad de negocio				
Detallar los procedimientos y controles específicos				
Seguimiento y actualización del plan de continuidad de negocio				
Implantación de un centro de respaldo.				
Actividades para verificar, revisar y evaluar las estrategias de recuperación				

Elaborado por: Gutiérrez, 2021

4.4. Indicadores de evaluación

Tabla 9. Indicadores de evaluación

No.	Dimensión	Indicador	Unidad de medida	Frecuencia	2021 Actualidad	2022 Esperado
1	Identificar	Evaluar los activos críticos de la organización	%	Trimestral	29%	19%
2		Período Máximo Tolerable de Interrupción	Horas	Mensual	No definido	< 4 horas
3		Tiempo de Recuperación	Horas	Mensual	No definido	< 4 horas
4	Detectar	Métodos de respaldo	Horas	Mensual	No definido	Diaria Semanal
5		Pruebas para evaluar el plan	%	Trimestral	No definido	Escenarios definidos para ejecución y % de efectividad
6	Responder	Metodos de respuesta frente a incidentes	Horas	Mensual	No controlado	Automatizado diariamente

Elaborado por: Gutiérrez, 2021

En la tabla 9 se describe los indicadores que se van a medir acorde a las dimensiones basadas en NIST, a continuación, describimos el análisis de cada indicador y lo esperado:

1. Activos críticos: Actualmente tenemos una evaluación inicial de los activos y servicios de la organización que se están viendo afectados por su criticidad en un 29% y lo esperado es ir midiendo de manera trimestral los avances de las mejoras para el periodo 2022.
2. Tiempo Interrupción: Conocemos de la debilidad actual de no conocer el tiempo máximo que puede estar el negocio sin operar, sin embargo, nuestra meta para el 2022 es que este tiempo de interrupción se encuentre por debajo de las 4 horas.

3. Tiempo de recuperación: Lo esperado frente alguna interrupción que se presentes es activar los métodos de recuperación basados en una lista de chequeo que permita estar operativos en un rango no mayor a 4 horas.

4.5. Niveles de Madurez

Tabla 10. Niveles de Madurez (Incibe, Incibe, 2020)

Niveles de madurez	
Los siguientes niveles de madurez serán utilizados para indicar los valores de cada métrica:	
L0	**INEXISTENTE**: esta medida o medidas no están siendo aplicadas en este momento.
L1	**INICIAL / AD-HOC**: cuando la organización no proporciona un entorno estable para aplicar estas medidas. El éxito o fracaso de las mismas depende de la competencia y buena voluntad de las personas; aunque, es difícil prever su reacción ante una situación de emergencia. Pese a su naturaleza caótica, es más que no tener nada.
L2	**REPETIBLE, pero INTUITIVO**: cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.
L3	**PROCESO DEFINIDO**: se dispone un catálogo de procesos para abordar este aspecto de la ciberresiliencia que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general.
L4	**GESTIONADO Y MEDIBLE**: cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos para abordar este aspecto de la ciberresiliencia. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.
L5	**OPTIMIZADO**: en este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos para abordar este aspecto de la ciberresiliencia basada en los resultados de las medidas e indicadores.

5. CONCLUSIONES

La Propuesta metodológica del diseño del plan de continuidad de negocio enfocado en términos de seguridad de la información para la empresa INTERVISION cuenta con las siguientes conclusiones:

Las PYMES a nivel mundial hoy en día son víctimas de interrupciones debido a su baja atención y protección en términos de continuidad de las operaciones. Lo cual ha conllevado a que ciertas empresas hayan sido víctimas de ataques por mantener brechas de seguridad en sus sistemas de información, entornos de red, sistemas operativos vulnerables, entre otros; lo cual impide seguir operando con normalidad y en casos verse afectados por secuestros de información hasta llegar a pedir cuantiosas sumas de dinero para su restablecimiento de información.

La empresa INTERVISIÓN actualmente se encuentra con un nivel de madurez inicial y nuestra propuesta es llevarla que alcance un nivel de madurez gestionado y medible dentro de los dos siguientes años.

Para lo cual incluimos dentro de nuestra propuesta de identificación de activos, servicios, responsables y el análisis de impacto del negocio por proceso van a contribuir a la organización a tener una visibilidad más clara de la situación actual, para poder prevenir ataques externos, errores humanos, situaciones extraordinarias como la pandemia COVID-19, la cual se presta para que ciberdelincuentes se aprovechen usando esquemas maliciosos.

El plan de continuidad de negocios incluye la matriz de riesgos, siendo un factor determinante para evitar que se materialicen los riesgos o minimizar su impacto en caso de que se lleguen a presentar.

6. RECOMENDACIONES

En base al análisis realizado en cuanto al diseño del plan de continuidad de negocio enfocado en términos de seguridad de la información para la empresa INTERVISION describimos las siguientes recomendaciones:

Recomendamos llevar de la mano esta propuesta con un experto en terminos de tecnología de la información para que el plan llegue al nivel de madurez gestionado y medible. Adicionalmente definir los responsables por procesos para que se involucren como dueños del proceso y puedan liderar y proponer acciones de mejora. También sugerimos implementar el centro de respaldo en la nube y mantener sus principales sistemas de gestión del negocio en servidores de alta disponibilidad. Inclusive desarrollar políticas, procedimientos y controles específicos a ejecutar ante la aparición de una amenaza.

Se recomienda iniciar un plan de concientización a los empleados y clientes claves en terminos de seguridad de la información y las formas de prevención, ya que en la

actualidad según estudios a nivel mundial demuestran que el personal no capacitado en términos de seguridad de la información es el eslabón mas debil en cuanto a los vectores de ataque ya sea por ingeniería social, suplantación de identidad, entre otros.

Revisar la factibilidad de implementar un monitoreo permanente que integre la medición de los indicadores acorde a su periodicidad para evaluar los avances de los resultados obtenidos a corto y mediano plazo.

7. REFERENCIAS BIBLIOGRÁFICAS

Andrés Cárdenas Pallo,Mario Ron Egas ,Víctor Paliz, 2013, Desarrollo del plan de continuidad del negocio para la empresa EQUIVIDA S.A para el periodo 2012-2015, Universidad ESPE, http://repositorio.espe.edu.ec/handle/21000/7362, Ecuador

Botha, J., and R. Von Solms.(2004) "A Cyclic Approach to Business Continuity Planning." Information Management & Computer Security 12 (4): 328–337

Christian Camilo Urcuqui, Melisa García Peña, José Luis Osorio Quintero, Andrés Navarro Cadavid,2018, Ciberseguridad un enfoque desde la ciencia de los datos, Editorial Universidad Icesi, Colombia

Christian Camilo Urcuqui, Melisa García Peña, José Luis Osorio Quintero, Andrés Navarro Cadavid,2018, Ciberseguridad un enfoque desde la ciencia de los datos, Editorial Universidad Icesi,Colombia

Clark, P., and Philip.(2010) "Contingency Planning and Strategies", in 2010 Information Security Curriculum Development Conference on - InfoSecCD '10, New York, USA: ACM Press. p. 131.

Cyril Onwubiko, Focusing on the Recovery Aspects of Cyber Resilience, Research Series, London, UK

Eduardo Hernan Amaya Guzmán, 2015, La seguridad informática en el contexto de los planes de continuación del negocio, Universidad Piloto de Colombia,

Franklin Faried Freire Fajardo, 2017, Plan de contingencia ante ciberataques, Universidad Politécnica del Ecuador, Ecuador

Gustavo Adolfo Castillo Gonzalez, 2017, Plan de continuidad del negocio basado en servicios en la nube para el área de tecnología, Universidad Galileo, Guatemala.

Incibe, https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Incibe, https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

Incibe, https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

Incibe, https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf

Jairo David Rojas Bustamante, 2017, Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del Ecuador, Universidad Udla, http://dspace.udla.edu.ec/handle/33000/7531

Janusz ZAWIŁA-NIEDŹWIECKI, 2010, BUSINESS CONTINUITY, Foundations of Management, Vol. 2, No. 2 (2010), ISSN 2080-7279

Lehan Nur Fadzlina Aini M., Razak Khamarrul Azahari y Kamarudin Khairul Hisyam, 2020, Planificación de la continuidad y la resiliencia del negocio en caso de desastre, Volumen No. 13 (7), Páginas 1-80, Julio (2020)

Lidia Sánchez Guerra,2017, Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031, Escuela Técnica Superior de Ingeniería de la Universidad de Santiago de Compostela, España.

Lidia Sánchez Guerra,2017, Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031, Escuela Técnica Superior de Ingeniería de la Universidad de Santiago de Compostela, España.

Marco de Trabajo, Cobit 5 – Implementación, ISACA

Marco de Trabajo, Cobit 5 – Procesos Catalizadores, ISACA

Marco de Trabajo, Cobit 5, ISACA

Marco de Trabajo, Cobit 5, ISACA

Martínez Díaz, Camilo Andrés, EL NIVEL DE DESARROLLO DE LA GESTIÓN DE RIESGO CIBERNÉTICO EN LAS INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD (IPS): UN ANÁLISIS BAJO EL CONTEXTO DE GOBIERNO CORPORATIVO, Colegio de Estudios Superiores de Administración – CESA, Bogotá - Colombia

Moh Heng, G. (1996) "Developing a Suitable Business Continuity Planning Methodology." Information Management & Computer Security 4 (2): 11–13.

Montoya, B. (2017). ¿Cómo minimizar el riesgo de afectación de un ataque cibernético en los blancos estratégicos nacionales? Recuperado de: http://hdl.handle.net/10654/15693.

Navid Sahebjamnia , S. Ali Torabi , S. Afshin Mansour, 2017 , Building organizational resilience in the face of multiple disruptions, International Journal of Production Economics 197 (2018) 63–83

NIST – Marco de Trabajo - Mejoramiento de Infraestructura crítica en Ciberseguridad

NIST SP 800 – 160 (2019), "Developing Cyber Resilient System - A System Security Engineering Approach", NIST Systems Special Publication 800-160 Volume 2. September 2019

S.A. Torabi, H. Rezaei Soufi, Navid Sahebjamnia, 2014, A new framework for business impact analysis in business continuity management (with a case study), Procedia Computer Science 161 (2019) 275–282

Silmie Vidiya Fani, Apol Pribadi Subriadi, 2019, Business Continuity Plan: Examining of Multi-Usable Framework, Procedia Computer Science 161 (2019) 275–282

Susan Snedaker, MBA, CISM, CPHIMS, CHCIO, Information Technology Executive, United States, 2020, Business Continuity–Pandemic Preparation, ISACA BLog

8. ANEXOS

Anexo N° 1 Entrevistas y Conclusiones de la entrevista a los jefe y Gerente.

Entrevista a Gerente General #1

1. **¿La Organización cuenta con métodos de recuperación en caso de ataques por amenazas internas y externas ?**

   En la actualidad no contamos con ningun método.

2. **¿Mantiene la Organización identificado los activos criticos y los servicios que estos ofrecen en la organización?**

   No contamos con un inventario de activos criticos ni la clasificación de su servicio.

3. **¿Se realizan copias de seguridad y se conservan los activos de clasificación mas sencible ?**

   No contamos con está buena practica.

4. **¿Se ha estimado el tiempo maximo aceptable de una interrupcion del servicio critico?**

   No se ha determinado estimar el tiempoo máximo.

5. **¿La Organización conoce cómo actuar y a dónde acudir cuando ha sido victima de un ataque?**

   Actualmente lo que se hace es contactar a un expeerto externo para identificar la causa /problema del ataque.

6. **¿Estaria de acuerdo en implementar el plan de contigencia y Coninuidad de negocio el cual consiste en marcar las prioridades los responsables y los recursos que se van a emplear para mejorar el nivel de ciberseguridad en la organización?**

   Si, considerando que podemos ser vulnerables frente a cualquier amenaza que se pueda presentar dentro de la organización seria importante poder implementar el plan.

7. **¿En qué tiempo considera usted implementar esta mejora dentro de su organización?**

   Frente a cualquier amenza como a la Covid-19 sería primordial implementarlo en el primer trimestre de 2022.

Entrevista a Jefaturas #2

1. **La Organización cuenta con métodos de recuperación en caso de ataques por amenazas internas y externas?**

   No cuenta.

2. **¿ Cre usted que el personal a su cargo está preparado para reactivar las operaciones dentro de la organización frente alguna vulnerabilidad explotada?**

   No existe ningún procedimiento ni metodología a seguir para reactivar las operaciones que hayan sido afectada

3. **¿Se ha definido y puesto en marcha un plan de formación de continuidad de negocio destinados al personal de la organización?**

   No se ha establecido un plan de continuidad a la actualidad.

4. **¿Estaria usted de acuerdo en concientizar e implementar mejoras para contar con un plan de continuidad de negocios ?**

   Si estaria de acuerdo.

5. **Cre usted que el personal a su cargo está preparado para reactivar las operaciones dentro de la organización frente alguna vulnerabilidad explotada?**

   No existe ningun procedimiento ni metodologia a seguir para reactivar las operaciones que hayan sido afectada.

Anexo N° 2 Análisis de impacto del negocio (BIA)

ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)							
ACTIVIDAD O	ÁREA O	DEPENDENCIA	REQUISITOS NEGOCIO		CAPACIDAD SISTEMAS		¿LA CAPACIDAD DE SISTEMAS CUBRE LOS REQUISITOS DEL NEGOCIO?
PROCESO	DEPARTAMENTO	SERVICIOS TIC	RTO	RPO	RTO	RPO	
Gestión nómina	Administración	Herramienta de pago de nómina	2	2	2	5	No. La capacidad actual de sistemas no permite cubrir los requisitos de negocio en lo que respecta el tiempo de recuperación (RPO).
Gestión stock	Inventario	Herramienta de inventario de activos	1	2	3	5	No. La capacidad actual de sistemas no permite cubrir los requisitos de negocio en lo que respecta el tiempo de recuperación (RTO).
Pago Proveedores	Contabilidad	Herramienta de pago a proveedores	3	4	3	5	No. La capacidad actual de sistemas no permite cubrir los requisitos de negocio en lo que respecta el tiempo de recuperación (RTO y RPO).
Compras de insumos	Contabilidad	Herramienta de compras locales	2	2	2	5	No. La capacidad actual de sistemas no permite cubrir los requisitos de negocio en lo que respecta el tiempo de recuperación (RPO).
Ventas	Servicio al Cliente	Generación de comprobantes eletrónicos. Cierres diarios de ventas.	1	2	2	5	No. La capacidad actual de sistemas no permite cubrir los requisitos de negocio en lo que respecta el tiempo de recuperación (RPO).
Gestión cobros	Contabilidad	Reportes de cartera desde el sistema	1	2	2	5	No. La capacidad actual de sistemas no permite cubrir los requisitos de negocio en lo que respecta el tiempo de recuperación (RPO).

Elaborado por: Gutiérrez, (2021)

Fuente: Adaptado (Incibe, Incibe, s.f.)

Anexo N° 3 Tablas de estimación (RTO, RPO) y la capacidad de los sistemas (RTO, RPO).

1. TABLA PARA ESTIMAR EL RTO (Tiempo de recuperación)	
VALOR	**DESCRIPCIÓN**
1	La actividad o el proceso requiere alta disponibilidad (100%).
2	La actividad o el proceso no puede estar interrumpida más de 8 horas.
3	La actividad o el proceso no puede estar interrumpida más de 24 horas.
4	La actividad o el proceso no puede estar interrumpida más de 72 horas.
5	Otros requisitos menos restrictivos que los indicados previamente.

2. TABLA PARA ESTIMAR EL RPO (Dependencia de Datos)	
VALOR	**DESCRIPCIÓN**
1	La actividad o el proceso requiere disponer del 100% de los datos.
2	La actividad o el proceso tolera la pérdida de los datos generados o modificados en las últimas 4 horas.
3	La actividad o el proceso tolera la pérdida de los datos generados o modificados en las últimas 8 horas.
4	La actividad o el proceso tolera la pérdida de los datos generados o modificados en las últimas 24 horas.
5	Otros requisitos menos restrictivos que los indicados previamente.

3. TABLA PARA ESTIMAR LA CAPACIDAD DE SISTEMAS EN TÉRMINOS DE RTO	
VALOR	**DESCRIPCIÓN**
1	Los servicios y herramientas TIC de los que dependen la actividad o el proceso disponen de una configuración de alta disponibilidad (100%).
2	Es posible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 8h.
3	Es posible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 24h.
4	Es posible recuperar los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a 72h.
5	No existen medios que garanticen la recuperación de los servicios y herramientas TIC de los que dependen la actividad o el proceso en un tiempo inferior a los indicados y/o el tiempo de recuperación no está acotado.

4. TABLA PARA ESTIMAR LA CAPACIDAD DE SISTEMAS EN TÉRMINOS DE RPO	
VALOR	**DESCRIPCIÓN**
1	Los servicios y herramientas TIC de los que dependen la actividad o el proceso disponen de una configuración de alta disponibilidad de datos (100%).
2	La solución y política de copias existente garantiza que a lo sumo, se perderán los datos generados o modificados en las últimas 4 h.
3	La solución y política de copias existente garantiza que a lo sumo, se perderán los datos generados o modificados en las últimas 8 h.
4	La solución y política de copias existente garantiza que a lo sumo, se perderán los datos generados o modificados en las últimas 24 h.
5	No se realizan copias de seguridad.

Fuente: (Incibe, Incibe, s.f.)

Anexo N° 4 Matriz Riesgos

ANÁLISIS DE RIESGOS				
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor 01 (Aplicaciones)	Desastres naturales	Bajo (1)	Medio (2)	2
Servidor 01 (Aplicaciones)	Fuga de información	Medio (2)	Alto (3)	6
Servidor 01 (Aplicaciones)	Alteración de la información	Bajo (1)	Alto (3)	3
Servidor 01 (Aplicaciones)	Degradación de los soportes de almacenamiento de la información	Bajo (1)	Medio (2)	2
Servidor 01 (Aplicaciones)	Errores de mantenimiento / actualización de programas (software)	Medio (2)	Medio (2)	4
Servidor 01 (Aplicaciones)	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	Alto (3)	6
Servidor 01 (Aplicaciones)	Caída del sistema por sobrecarga	Medio (2)	Medio (2)	4
Servidor 01 (Aplicaciones)	Acceso no autorizado	Medio (2)	Medio (2)	4
Servidor 01 (Aplicaciones)	Errores del administrador	Medio (2)	Alto (3)	6
Servidor 01 (Aplicaciones)	Errores de configuración	Medio (2)	Alto (3)	6
Servidor 01 (Aplicaciones)	Denegación de servicio	Medio (2)	Bajo (1)	2
Switch 01	Fallo de servicios de comunicaciones	Medio (2)	Medio (2)	4
Switch 01	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	Alto (3)	3
Switch 01	Errores de mantenimiento / actualización de equipos (hardware)	Bajo (1)	Alto (3)	3
Switch 01	Caída del sistema por sobrecarga	Medio (2)	Medio (2)	4
Switch 01	Abuso de privilegios de acceso	Bajo (1)	Alto (3)	3
Switch 01	Acceso no autorizado	Bajo (1)	Alto (3)	3
Switch 01	Errores del administrador	Medio (2)	Medio (2)	4
Switch 01	Errores de configuración	Medio (2)	Medio (2)	4
Switch 01	Denegación de servicio	Medio (2)	Alto (3)	6
Equipos de Computación	Alteración de la información	Medio (2)	Medio (2)	4
Equipos de Computación	Destrucción de información	Medio (2)	Alto (3)	6
Equipos de Computación	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	Medio (2)	2
Equipos de Computación	Difusión de software dañino	Medio (2)	Medio (2)	4
Equipos de Computación	Abuso de privilegios de acceso	Medio (2)	Medio (2)	4
Router Wifi	Fallo de servicios de comunicaciones	Medio (2)	Medio (2)	4
Router Wifi	Errores de mantenimiento / actualización de programas (software)	Medio (2)	Medio (2)	4
Router Wifi	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	Medio (2)	4
Router Wifi	Caída del sistema por sobrecarga	Medio (2)	Alto (3)	6
Router Wifi	Errores del administrador	Medio (2)	Medio (2)	4
Router Wifi	Errores de configuración	Medio (2)	Alto (3)	6
Router Wifi	Denegación de servicio	Bajo (1)	Alto (3)	3

Servidor web - Sitio web alojado y gestionada por un proveedor externo	Desastres naturales	Bajo (1)	Alto (3)	3
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Fuga de información	Medio (2)	Medio (2)	4
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Alteración de la información	Medio (2)	Alto (3)	6
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Destrucción de información	Medio (2)	Alto (3)	6
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Interrupción de otros servicios y suministros esenciales	Bajo (1)	Alto (3)	3
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Degradación de los soportes de almacenamiento de la información	Bajo (1)	Medio (2)	2
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Errores de mantenimiento / actualización de programas (software)	Medio (2)	Medio (2)	4
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Acceso no autorizado	Medio (2)	Medio (2)	4
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Errores del administrador	Medio (2)	Alto (3)	6
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Denegación de servicio	Medio (2)	Alto (3)	6
Servidor web - Sitio web alojado y gestionada por un proveedor externo	Extorsión	Bajo (1)	Alto (3)	3
Dispositivos móviles para telefonía y datos	Desastres naturales	Bajo (1)	Medio (2)	2
Dispositivos móviles para telefonía y datos	Interceptación de información (escucha)	Medio (2)	Alto (3)	6
Dispositivos móviles para telefonía y datos	Corte del suministro eléctrico	Bajo (1)	Medio (2)	2
Dispositivos móviles para telefonía y datos	Caída del sistema por sobrecarga	Bajo (1)	Alto (3)	3
Dispositivos móviles para telefonía y datos	Errores de configuración	Medio (2)	Alto (3)	6

Elaborado por: Gutiérrez, (2021)

Fuente: Adaptado (Incibe, Incibe, 2020)

Anexo N° 5 Clasificación de probabilidad e impacto

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Fuente: Plantilla Incibe

Anexo N° 6 Matriz RACI – Dominios APO 13 -COBIT5

Matriz RACI APO13																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO13.01 Establecer y mantener un SGSI.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Supervisar y revisar el SGSI.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Fuente: (ISACA, Cobit 5 - Marco de Trabajo - Procesos Catalizadores)

Anexo N° 7 Matriz RACI – Dominios DSS04 -COBIT5

Matriz RACI DSS04																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Mantener una estrategia de continuidad.				A	C	R					I					C	C	R	R	C	R				R	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.					I	R									I	C	C	R	C	C	R				A	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.					I	R									I		R	R		C	R				A	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.				A	I	R					I							R		C	R				R	
DSS04.06 Proporcionar formación en el plan de continuidad.					I	R												R		R	R	R			A	
DSS04.07 Gestionar acuerdos derespaldo.																				C	A				R	
DSS04.08 Ejecutar revisiones post-reanudación.					C	R					I							R	C	C	R	R			A	

A continuación, describimos el resultado del análisis para la propuesta planteada en base a las metodologías estudiadas y sugerimos su aplicación como parte del trabajo de investigación desarrollado.

Anexo N° 8 Mapeo de marcos de trabajo NIST, COBIT5 e INCIBE

Función	Categoría	Subcategoría	COBIT / NIST Referencias	INCIBE (Plan Director Seguridad)

IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-6:** Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	· **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11	CONOCER LA SITUACIÓN ACTUAL
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética	**ID.BE-5:** Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	· **COBIT 5** BAI03.02, DSS04.02 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14	CONOCER LA ESTRATEGIA DE LA ORGANIZACIÓN
	Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	**ID.GV-1:** Se establece y se comunica la política de seguridad cibernética organizacional.	· **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families	
		ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	· **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2	

		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-4:** Se identifican los impactos y las probabilidades del negocio.	· **COBIT 5** DSS04.02 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11	CLASIFICACIÓN Y PRIORIZACIÓN
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	· **COBIT 5** APO12.05, APO13.02 · **NIST SP 800-53 Rev. 4** PM-4, PM-9	
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **NIST SP 800-53 Rev. 4** PM-9	APROBACIÓN POR LA DIRECCIÓN
	Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e	**ID.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	· **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, **APO13.02,** BAI01.03, BAI02.03, BAI04.02 · **NIST SP 800-53 Rev.** 4 SA-9, SA-12, PM-9	
		ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01,	

	implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03	
			· **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9	
		ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	· **COBIT 5** DSS04.04	
			· **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9	
PROTECT (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-3:** Se gestiona el acceso remoto.	· **COBIT 5** APO13.01, DSS01.04, DSS05.03	
			· **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15	
	Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos.	· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06	
			· **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28	
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	· **COBIT 5** APO13.01, BAI04.04	
			· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5	

	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-2:** Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	· **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03	
			· **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17	
		PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información	· **COBIT 5** APO13.01, DSS01.01, DSS04.07	
			· **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9	
		PR.IP-7: Se mejoran los procesos de protección.	· **COBIT 5** APO11.06, APO12.06, DSS04.05	
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6	
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	· **COBIT 5** APO12.06, DSS04.03	
			· **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	· **COBIT 5** DSS04.04	
			· **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14	
	Tecnología de protección (PR.PT): **L**as soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas,	**PR.PT-2:** Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	· **COBIT 5** APO13.01, DSS05.02, DSS05.06	
			· **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	

	procedimientos y acuerdos relacionados.	**PR.PT-4:** Las redes de comunicaciones y control están protegidas.	· **COBIT 5** DSS05.02, APO13.01	
			· **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	
DETECTAR (DE)	**Procesos de Detección (DE.DP):** Los procesos de detección y el mantenimiento de los procedimientos son probados para garantizar la prevención de elementos aómalos.	**DE.DP-3:** Se prueban los procesos de detección.	· **COBIT 5** APO13.02, DSS05.02	
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14	
		DE.DP-5: los procesos de detección se mejoran continuamente.	· **COBIT 5** APO11.06, APO12.06, DSS04.05	
			· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	
RESPONDER (RS)	**Mejoras (RS.IM):** Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas.	**RS.IM-2:** Se actualizan las estrategias de respuesta.	· **COBIT 5** BAI01.13, DSS04.08	DEFINIR PROYECTOS E INICIATIVAS
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	
RECUPERAR (RC)	**Mejoras (RC.IM):** La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Incorpora planes de recuperación y lecciones aprendidas.	· **COBIT 5** APO12.06, BAI05.07, DSS04.08	
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	