Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A

Zapata Vásquez, Cristian Fernando

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

Ph.D. Lascano, Jorge Edison

27 de agosto del 2020

URKUND

Urkund Analysis Result

Analysed Document: TESIS CZAPATA Final cert.pdf [D79979759]
Submitted: 2020-09-27T00:01:00
Submitted By: jelascano@espe.edu.ec
Significance: 10%

Sources included in the report:

Documento: D77947409
Documento: D54656379
Documento: D25762727
TESIS BCP DANIEL URIBE.docx (D39020152)
TESIS BCP 05_04_2018.docx (D37511630)
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf
https://chaui20171701415019.wordpress.com/2018/02/01/auditoria-especifica-bcp/
https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo
https://repository.unad.edu.co/bitstream/handle/10596/2668/76323713.pdf?sequence=5&isAllowed=y
https://repositorio.upse.edu.ec/bitstream/46000/3978/1/UPSE-TIN-2017-0005.pdf
https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/8511/3/1124848759.pdf
https://contenido.bce.fin.ec/documentos/PublicacionesNotas/Notas/Inflacion/inf202005.pdf

Instances where selected sources appear:

73

Firma:

……

Lascano, Jorge Edison

DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A**" fue realizado por el señor **Zapata Vásquez, Cristian Fernando** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 31 de agosto de 2020

Firma:

Ing. .....

Lascano, Jorge Edison, Ph.D.

Director

C.C.: 1710893114

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo **Zapata Vásquez, Cristian Fernando**, con cédula de ciudadanía n° 1714751342, declaro que el contenido, ideas y criterios del trabajo de titulación*:* **Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A** es de mí autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 31 de agosto de 2020

Firma

.....

Zapata Vásquez, Cristian Fernando

C.C.: 1714751342

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Zapata Vásquez, Cristian Fernando** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Sangolquí, 31 de agosto de 2020

Firma

.....

Zapata Vásquez, Cristian Fernando

C.C.: 1714751342

Dedicatoria

A mi padre Marco F. Zapata.

Agradecimiento

Gracias a Laboratorios Bagó del Ecuador S.A., por facilitarme los insumos para la realización de este trabajo.

Agradezco de manera especial al mi tutor Edison Lascano por su acertada guía en este proyecto de titulación, ¡Gracias profe!

A mis docentes y compañeros de la maestría, con los cuales compartimos las aulas y fomentamos conocimientos.

A las personas que me incentivaron cursar esta maestría, que me dieron sus consejos, compañía y apoyo durante la colegiatura y durante el desarrollo de este proyecto.

También agradezco a mi familia y amigos.

Cristian F. Z.

Índice de contenido

Índice de tablas

Índice de figuras

Resumen

En la actualidad las empresas deben estar en la capacidad de reaccionar ante eventos inesperados que afecten sus operaciones y su imagen como organización. En Ecuador existen riesgos, como terremotos, incendios, inundaciones y erupciones volcánicas. Además, existen eventos inesperados relacionados con fallas humanas, como ciberataques y robo de datos. En el área de TI de las organizaciones, se ejecutan la mayoría de sus procesos críticos, por lo tanto, es indispensable contar con un plan que garantice que estos procesos continúen después de la ocurrencia de un desastre. El presente trabajo propone un plan de continuidad de negocio (BCP) para el departamento de tecnología de Laboratorios Bagó del Ecuador S.A., este BCP describe la preparación y capacidad de recuperación de la organización ante contingencias. El diseño de esta investigación se basa en el estándar ISO 22301, y en guías técnicas de instituciones especializadas en continuidad de negocio, como El Instituto Nacional de Ciberseguridad de España (INCIBE). El presente trabajo recopila información de la situación actual de la empresa, identifica activos y procesos críticos, realiza un análisis de impacto de negocio (BIA); y, hace un análisis de riesgos para identificar amenazas y vulnerabilidades con la metodología MAGERIT y con EAR/PILAR. Por consiguiente, define estrategias de recuperación que brindan la capacidad de resiliencia frente a eventos nos deseados. Por último, se presenta un costo referencial de la implementación del plan de continuidad, las conclusiones y recomendaciones.

PALABRAS CLAVE:

- **PLAN DE CONTINUIDAD DE NEGOCIO**
- **ANÁLISIS DE IMPACTO DE NEGOCIO**
- **ESTRATEGIAS DE RECUPERACIÓN**

Abstract

Nowadays, companies must react to unexpected events that affect their operations and their corporate image. In Ecuador, there are risks, such as earthquakes, fires, floods and volcanic eruptions. There are also unexpected events related to human failures, such as cyber-attacks and data theft. In IT departments, the most critical processes of the organizations are performed, therefore it is essential to have a plan that guarantees that these processes continue running after a disaster. The present work proposes a business continuity plan (BCP) for the information technology department of Laboratorios Bagó del Ecuador S.A., this BCP describes the organization and its recovery capacity in case of contingencies. The design of the present research is based on the ISO 22301 standard, and on technical guides of institutions recognized in business continuity, such as the Instituto Nacional de Ciberseguridad de España (INCIBE). This work collects information of the current status of the company, identifies critical assets and processes, performs a business impact analysis (BIA), and performs a risk analysis to identify threats and vulnerabilities by using the MAGERIT methodology and with EAR / PILAR tools, therefore it defines recovery strategies that provide resilience in case of unexpected events. Finally, a referential cost for implementing the continuity plan is computed, then conclusions and recommendations are set out.

KEY WORDS:

- **BUSSINES CONTINUITY PLAN**
- **BUSSINES IMPACT ANALISYS**
- **RECOVERY STRATEGIES**

Capítulo I. Generalidades

Introducción

En nuestro país existen riesgos latentes, terremotos, incendios, inundaciones y últimamente atentados terroristas, y las empresas en su mayoría no están preparadas para estas contingencias, además existen eventos inesperados que no necesariamente se relacionan con desastres naturales, también se relacionan con fallas humanas, interrupción de fluido eléctrico, ciberataques y pérdida de datos.

Tomando en cuenta todos estos posibles fallos, se debe contar con un BCP que ayude a recuperar la continuidad de las operaciones en las empresas. No se logrará levantar completamente todos los procesos del negocio, pero se debe contar con un mínimo necesario de procesos críticos para ejecutar sus operaciones y conservar la imagen corporativa de la empresa, minimizar el impacto y evitar grandes pérdidas monetarias.

La continuidad de negocio brinda valor a una organización, a la vez que establece una relación directa de la infraestructura con las vulnerabilidades que se puedan explotar. Así, se asegura la resiliencia empresarial, protegiendo la empresa de incidentes que provoquen una interrupción en la actividad con la gestión de riesgos, reduciendo la probabilidad de que se produzcan y garantizando su recuperación con una estrategia definida.

Planteamiento del problema

Laboratorios Bagó del Ecuador S.A. es una empresa farmacéutica de origen argentino con más de ochenta años de existencia y con veinte y siete años en el Ecuador, posee la fuerza de ventas más numerosa del sector, distribuida en todo el territorio nacional, su área tecnológica gestiona información de ventas, logística, inventarios, auditorias y talento humano. Su giro de negocio es la comercialización y

promoción de productos farmacéuticos con procesos que se apoyan en las Tecnologías de la Información y Comunicación (TIC) a lo largo de su cadena de valor, sin embargo, al igual que otras empresas su infraestructura tecnológica es susceptible a eventos no deseados o contingencias que pueden afectar su actividad económica, su información, su credibilidad y reputación. Por lo descrito, nos preguntamos:

- ¿Cómo reaccionar ante posibles fallas, eventos no deseados o desastres que puedan afectar a la continuidad de negocio del área de tecnología de la empresa?
- ¿Cuál es la estrategia de recuperación que se debe seleccionar de acuerdo al nivel de afectación de una contingencia, y permita recuperar las actividades en el departamento de tecnología?

Objetivo general

Proponer un BCP para el departamento de tecnología de Laboratorios Bagó del Ecuador S.A. que permita detectar amenazas y vulnerabilidades, minimizar riesgos e implementar controles para mejorar la capacidad de reacción ante posibles desastres aplicando una adecuada estrategia de recuperación.

Objetivos específicos

- Describir la situación actual de la infraestructura tecnológica de la empresa con respecto a estrategias y recursos para tratar riesgos, asegurar la información, resolver problemas de conexión y posibles amenazas que puedan explotar vulnerabilidades y que consigan interrumpir los servicios tecnológicos.
- Proponer un BCP para el departamento de tecnología de la organización basado en análisis de riesgos y en las buenas prácticas dictadas por instituciones de seguridad y por el estándar internacional ISO 22301.
- Manejar una herramienta que automatice los procesos de análisis de riesgos como EAR/PILAR con la metodología para gestión de riesgos MAGERIT.

- Recomendar estrategias de recuperación que se ajusten a cada tipo de incidente de acuerdo a niveles de criticidad en la organización.

Justificación e importancia

La no interrupción de los procesos de negocio es una condición importante en las empresas de la actualidad, las interrupciones causan efectos adversos en la economía y la imagen corporativa de una empresa. La continuidad de negocio es un factor fundamental que basado en estándares y buenas prácticas pueden minimizar los efectos adversos que se pueden presentar.

La presente propuesta surge de la necesidad de poseer estrategias que aseguren la continuidad del negocio en caso de contingencias o desastres como el terremoto de Manabí con magnitud de 7,8 grados *Mw* sufrido el 16 de abril del 2016 (Instituto Geofísico, 2016), en el cual debido al movimiento fallaron comunicaciones, edificios se quedaron sin suministro eléctrico y las vías terrestres se abrieron, al repetirse estos eventos de tales magnitudes pueden afectar a la infraestructura tecnológica la cual soporta los procesos esenciales del negocio.

Con la presente tesis se valorará el costo y el beneficio referencial que implica tener un plan adecuado de continuidad de negocio en el área tecnológica y que pueda ser implementado en toda la organización y sus diversas áreas, esta necesidad es requerida por los miembros del comité empresarial de Laboratorios Bagó del Ecuador S.A. para cumplir con las recomendaciones realizadas por la empresa de auditoria externa (PwC[1]) a su departamento de tecnologías de la información.

Adicionalmente, el presente trabajo se fundamentará en las mejores prácticas para proponer una guía de implantación de un plan de continuidad o contingencia en el área tecnológica ajustado a las necesidades

[1] PwC, ofrece servicios de Consultoría Tributaria y Consultoría Organizacional a empresas públicas y privadas.

de Laboratorios Bagó del Ecuador S.A. La guía se basará en análisis de riesgos, identificación de procesos críticos, detección de amenazas, vulnerabilidades, aplicación de estándares de continuidad y un presupuesto aproximado de la implementación de plan.

Esta propuesta investigativa dará la pauta para futuras implantaciones de planes de continuidad de negocio en otras empresas, además pretende concienciar y resaltar la importancia crítica de asegurar sus operaciones y reaccionar de manera proactiva frente a desastres.

Capítulo II. Marco teórico

Este capítulo incluye conceptos y fundamentos teóricos necesarios para llevar a cabo el presente proyecto. Inicia con un glosario de términos basado en definiciones de diferentes guías prácticas, continúa con normas y estándares referentes al BCP. Posteriormente, se presenta el BCP y sus tipos, finalmente se habla de su metodología y sus fases.

Glosario de términos

Ciberseguridad: También conocida como seguridad de tecnologías de la información, se enfoca en proteger los activos de información a través de estrategias y normas para tratar las amenazas que ponen en riesgo la información en sistemas interconectados.

Activos: Se consideran a los recursos que dan soporte a las actividades de negocio de una empresa. Son necesarios para que ésta funcione correctamente y alcance los objetivos planteados.

Procesos críticos: Conjunto de tareas o actividades esenciales para mantener el funcionamiento del negocio.

Contingencia: Evento o suceso no deseado que puede interrumpir las operaciones o actividades de una organización.

Alternativas de recuperación: Conjunto de actividades predefinidas que se las lleva a cabo ante la ocurrencia de un desastre o contingencia.

Incidente: Evento que esta fuera del funcionamiento normal de un proceso u operación, este evento provoca interrupción y baja la calidad de los servicios.

Vulnerabilidades: Falta de control o baja capacidad asociada a un recurso o proceso que puede ser explotada y provoca daño en dichos procesos.

Amenazas: Eventos que aprovechando una vulnerabilidad pueden desencadenar interrupción en las

actividades o procesos críticos, pueden provocar incidentes y pérdidas a la empresa.

MAGERIT: Metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica (Portal de Administración Electrónica, 2014) .

Disponibilidad: Cualidad o condición de un recurso, proceso y servicio que se encuentre a disposición cuando lo requiera la organización.

Plan de recuperación ante desastres o *Disaster Recovery Plan* (DRP): Se entiende como las actividades necesarias para recuperar las operaciones de TI. Se considera como parte esencial del BCP o como un plan de continuidad de negocio aplicado a los recursos tecnológicos.

Resiliencia: Capacidad para recuperarse luego de la ocurrencia de una calamidad o desastre.

Retorno de Inversión o *(Return on Investment)* ROI: valor que mide el retorno de inversión y determinar la viabilidad de un proyecto.

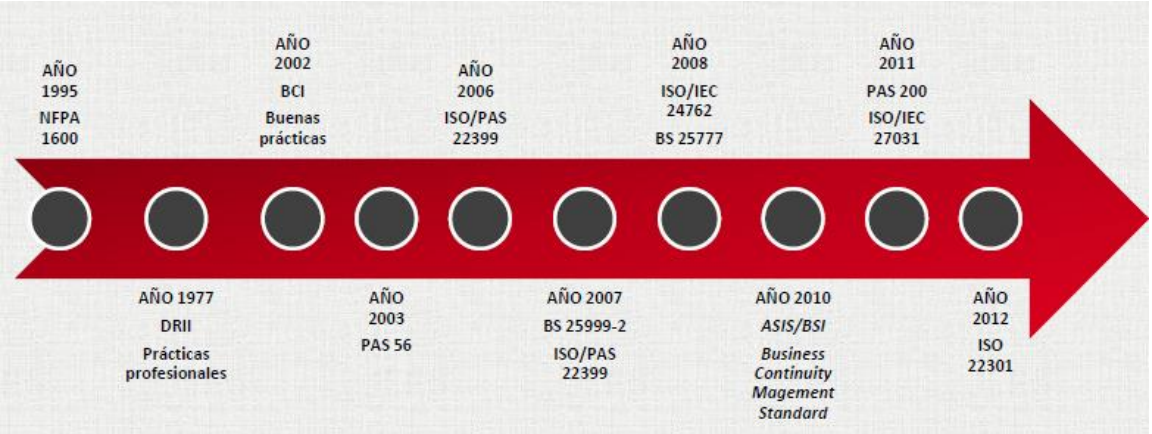
***Stakeholders*:** Referido a todos los sujetos o partes interesadas que se verán afectados por la organización.

Normas y Estándares

ISO 22301: (ISO 22301, 2012) Sistemas de Gestión de Continuidad de Negocio (SGCN). Es la norma internacional certificable para la Gestión de la Continuidad de Negocio y ha sido desarrollada para ayudar a las organizaciones a minimizar el riesgo de interrupciones en sus actividades. Sustituye a la norma Británica para la Gestión de Continuidad de Negocio BS25999, que estuvo vigente hasta 2007 como se puede ver en la Figura 1.

Figura 1

Evolución del estándar ISO 22301.



Nota. Tomado de *ISO 22301:2012 Antecedentes*, por International Dynamic Advisors, 2016, http://www.intedya.com/productos/riesgos%20y%20seguridad/ISO%2022301/07%202016%20ISO%2022301_%20PIC_%20ed00.pdf

La norma ISO 22301 se integra y se alinea con las normas: ISO 27001 (Gestión de Seguridad de la Información), ISO 9001 (Sistemas de la Gestión de la Calidad) e ISO 20000 (Gestión de servicios de TI), con el objetivo de facilitar la colaboración entre estándares y permitir la asociación en la implantación y operación del sistema de gestión de continuidad de negocio.

Esta norma adopta el ciclo *Plan-Do-Check-Act* (PDCA) como marco de referencia para el sistema de gestión de continuidad de negocio en todas sus etapas, lo cual hace ideal y ajustable a cualquier tipo y tamaño de empresa.

A continuación, la descripción de las actividades del ciclo.

***Plan*:** Establecimiento de políticas, objetivos, controles, procesos, y procedimientos relacionados a la continuidad de negocio, los cuales entregan valor al negocio.

***Do*:** Planificación de procesos de implementación y operación.

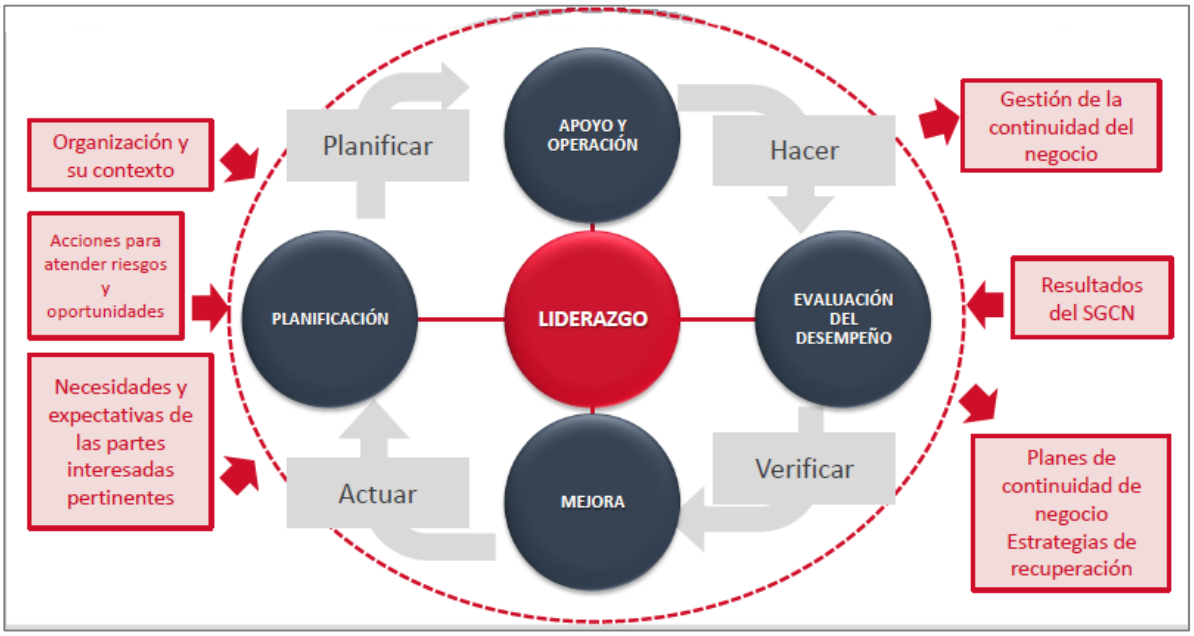
***Check*:** Monitoreo, medición, evaluación, y revisión de resultados que contrasten los objetivos y políticas de continuidad, por lo que se pueden determinar y autorizar acciones correctivas y de mejora.

***Act*:** La realización de acciones autorizadas para garantizar que el SGCN entregue sus resultados y mejore.

La Figura 2 ilustra los componentes del modelo PDCA aportan a un Sistema de Gestión de Continuidad de Negocio.

Figura 2

Ciclo PDCA aplicado a la continuidad de negocio.



Nota. Tomado de *ISO 22301:2012 Requisitos de la norma*, por International Dynamic Advisors, 2016, http://www.intedya.com/productos/riesgos%20y%20seguridad/ISO%2022301/07%202016%20ISO%2022301_%20PIC_%20ed00.pdf

Plan de Continuidad de Negocio - *Business Continuity Plan* (BCP)

Es un conjunto de prácticas, criterios, normas de actuación y herramientas organizativas que ante una contingencia que provocase la interrupción de alguna o de todas las áreas del negocio de una organización, permiten la recuperación de la operatividad de las mismas en el menor tiempo posible, de modo que las

pérdidas económicas ocasionadas sean menores, así como cuidar su reputación y posicionamiento en el mercado de una organización, en general, se tiene dos tipos de proyectos BCP.

Tipos de proyectos de continuidad de negocio

En términos generales, estos dos tipos de proyectos se los suelen enmarcar dentro del concepto de plan de continuidad de negocio, además se pueden integrar o ser parte del mismo, sin embargo, se los distingue como tipos de proyectos por su alcance o ámbito en el que se desarrollan.

- Plan de Continuidad TIC (PCTIC), forma parte del plan de continuidad de negocio de la organización, pero limitado al ámbito tecnológico. Por otro lado, un BCP sirve de disparador para los diferentes planes de contingencia. Por ejemplo, si se produce una inundación en un centro de cómputo, se ejecutaría el plan de continuidad necesario para recuperar los procesos afectados. En este caso los relacionados al área tecnológica.
- Plan de Recuperación ante Desastres (DRP), en este plan, el alcance del análisis es menos profundo y se enfoca en un ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe. Por ejemplo, si tenemos un plan de desastres para nuestro servidor proxy, el DRP contendrá todos los pasos necesarios para la recuperación de los servicios que brinda el equipo.

Es decir, un DRP está enfocado a los activos de la empresa, mientras que el PCTIC tiene un enfoque mayor en los procesos.

Metodología de un Plan de Continuidad de Negocio

El diseño de la presente propuesta se basará en las mejores prácticas del estándar de la norma ISO 22301:2012, y en guías técnicas de instituciones reconocidas en el campo de la continuidad de negocio

como El Instituto Nacional de Ciberseguridad de España (INCIBE)[2], las fases del siguiente apartado toman como marco de referencia el estándar ISO 22301 en pos de entregar a las empresas la capacidad de resiliencia y dar continuidad a sus actividades. Las guías se basan en experiencias y plasman modelos que se pueden ajustar a las realidades y complejidades de la organización.

Fases de un Plan de Continuidad de Negocio

Según el estándar ISO 22301:2012 (ISO 22301, 2012) y las guías prácticas (INCIBE, 2016) de implementación de un plan de continuidad, se definen las siguientes fases:

Fase 0. Determinación del alcance. Dependiendo de la complejidad organizativa de la empresa, se debe determinar las áreas o departamentos más importantes para empezar y definir el alcance del plan de continuidad, luego se pueden integrar de manera progresiva el resto de áreas, esto con el afán de no emplear recursos ni tiempo excesivo en el análisis de otras áreas. La determinación del alcance debe contar con el compromiso e inclusión de los directivos.

Fase 1. Análisis de la organización. En esta fase se recopila toda la información necesaria para establecer los procesos de negocio críticos, los activos que dan soporte a esos procesos y cuáles son las necesidades temporales y de recursos que se emplearan.

Fase 2. Determinación de la estrategia de continuidad. Conociendo los activos que soportan los procesos críticos, se debe determinar si cuando ocurre un desastre, la empresa será capaz de recuperar sus activos en el tiempo necesario. En los casos que no se llegue a recuperar en el tiempo establecido, se deberá establecer las diversas estrategias de recuperación.

[2] INCIBE, es una sociedad dependiente del Ministerio de Economía de España, y consolidada como entidad de referencia para el desarrollo de la Ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Fase 3. Respuesta a la contingencia. En esta fase se establecen las acciones e iniciativas necesarias con base a estrategias de recuperación, se documentará el Plan de Crisis y las respectivas actividades llevadas a cabo para recuperar la continuidad.

Fase 4. Prueba, mantenimiento y revisión. Con base a la infraestructura tecnológica de la empresa, se despliegan los planes de prueba y mantenimiento.

Fase 5. Concienciación. Esta fase fomenta la mejora continua del BCP, además del análisis e implantación del plan, es necesario que el personal técnico, así como los involucrados tengan todo el conocimiento, apliquen mejoras y recomendaciones al plan de continuidad.

A continuación, se detalla cada una de las fases con sus respectivas etapas o actividades:

Fase 0: Determinación del alcance. La ejecución de esta fase es imprescindible para poder determinar la magnitud y costo del proyecto que se va a desarrollar, además permite considerar su posible implementación. En esta fase también se determina los elementos críticos de la empresa que serán objeto de mejora en su continuidad. Se integra el personal, los activos, los sistemas informáticos, los procesos y otros servicios que, en caso de pérdida, impactarán a la organización. En nuestro caso nos centramos en el ámbito de la tecnología.

Otro elemento a considerar en el alcance de esta fase es, que durante el desarrollo del proyecto no sólo se implicarán a los activos tecnológicos, tales como servidores, dispositivos de red, equipos portátiles, base de datos y aplicaciones, sino también al personal de TI. Además, requerirá la colaboración de otras áreas.

Dado lo anterior, se puede plantear el enfoque del proyecto desde el punto de vista del activo, o del proceso. El enfoque por activo se relaciona con la mejora de la continuidad de un conjunto de activos, y a partir de estos se obtiene la información de los procesos que los usan. Este enfoque es más propio de un

DRP. Mientras que, el enfoque por proceso procura la mejora de la continuidad de un determinado proceso, independientemente de los activos que le den soporte. Este enfoque es más propio del negocio. La información documentada que se presenta en esta fase son el alcance y las políticas del BCP.

Fase 1: Análisis de la organización. Esta fase se relaciona con la obtención, elaboración y comprensión del ambiente tecnológico, de los procesos y de los recursos de la organización. Esto permite abordar las fases posteriores con una base sólida. Es transcendental que se involucre a todos los actores para que el resultado sea lo más cercano a la realidad. Según (ISO 22301, 2012), en esta fase se presenta el contexto de la organización a través de análisis de impactos en el negocio y la metodología de evaluación de riesgos que se van a aplicar.

En esta fase se realizan las siguientes actividades:

Mantener reuniones. La primera actividad es realizar reuniones con los usuarios finales de los procesos que se han seleccionado como alcance. De estas reuniones se debe obtener las dependencias tecnológicas de proveedores, personal implicado, las aplicaciones que se utilizan, y los datos sobre las necesidades de cada aplicación.

El paso siguiente es recolectar toda la información sobre las aplicaciones y servicios que presta el área tecnológica, el objetivo es obtener los detalles de su funcionamiento, instalación, proveedor, personal, etc. Esto se lo puede realizar a través de entrevistas y encuestas al personal de IT o revisando información que se disponga acerca de los descriptivos de cargo y documentación de recursos software / hardware de la empresa.

Con la realización de estos pasos previos, se obtendrá una visión general de todos los procesos de los cuales queremos mejorar su capacidad de reacción ante incidentes no deseados.

Análisis de Impacto sobre el Negocio (BIA). El siguiente paso es elaborar el Análisis de Impacto sobre el Negocio o BIA (Business Impact Analysis), a partir de la información que hemos recopilado. Este documento se debe realizar siempre desde el punto de vista del negocio, es decir con un enfoque organizacional.

BIA es uno de los principales ejes del BCP, al contener las necesidades de los procesos que se han definido como alcance. Así podremos clasificarlos según su criticidad y su dependencia de los activos tecnológicos; además contiene los requisitos temporales y de recursos de los procesos dentro del alcance, el cual unido al Análisis de Riesgos, define las iniciativas a implantar para recuperar los procesos en situaciones de contingencia (INCIBE, 2016).

La Figura 3 muestra los componentes del BIA para la clasificación de criticidad.

Figura 3

Componentes del BIA.

Nota. Tomado de *Análisis de impacto sobre el negocio* (p. 13), por INCIBE, 2016, https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Para cada proceso seleccionado, se debe obtener los siguientes datos:

- Tiempo de recuperación o RTO (*Recovery Time Objective*). Es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Este valor tiene un gran componente de subjetividad.
- Recursos humanos y tecnológicos empleados en el proceso. En este punto se debe determinar el personal, las aplicaciones, sistemas, equipamiento y elementos auxiliares (impresora, escáner, consumibles, etc.) que cada proceso necesita para su funcionamiento en una situación de contingencia, así como el tiempo de recuperación de cada uno de ellos.
    - En el caso de los recursos tecnológicos, se debe considerar las dependencias de infraestructura tecnológica proveída por terceros.
    - En el caso de los recursos humanos, se identifica el personal crítico que no puede ser reemplazado, ya sea por limitaciones de personal o por poseer el conocimiento específico sobre cada proceso.
- Tiempo máximo tolerable de caída o MTD (*Maximum Tolerable Downtime*). Es el periodo de tiempo máximo que un proceso puede estar caído antes de que se produzcan consecuencias desastrosas para la empresa. Se debe tener en cuenta la subjetividad de este tiempo en la mayoría de casos, ya que, incluso midiendo cuantitativamente el impacto de una contingencia, el determinar en qué momento dicho impacto pone en riesgo a la organización es una tarea compleja.

    El MTD está relacionado con el negocio, mientras que el RTO es determinado por personal técnico. En todo caso, el RTO debe ser inferior al MTD.

- Niveles mínimos de recuperación de servicio o ROL (*Revised Operating Level*). Es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada. Aunque el nivel de servicio no sea el óptimo o esté al ciento por ciento, debe tener en cuenta el público objetivo o destinatario de la actividad del servicio, cumplimiento de compromisos satisfechos con terceras partes, y porcentaje de la actividad habitual que es posible llevar a cabo con el nivel de recuperación alcanzado.
- Dependencias de otros procesos internos o proveedores externos. En función de la criticidad de las actividades en las que el proveedor esté implicado, se puede solicitar a éste que indique si dispone de un DRP y qué tiempos maneja. El propósito es validar que una situación de desastre en un proveedor crítico no traslade la contingencia a la empresa.
- Punto de Recuperación Objetivo o RPO (*Recovery Point Objective*). Este valor determina el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización.

Con la información obtenida, se evaluarán los impactos, se identificarán las operaciones críticas y se priorizará la recuperación de los procesos. Para esto se pueden utilizar los esquemas de valoración de las siguientes tablas:

Tabla 1

Valoración del impacto.

Nivel	Detalle
A	La operación es crítica para el negocio, al no contar con esta, el negocio no puede realizarse.
B	La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero no es crítica.
C	La operación no es una parte integral de las operaciones de negocio.

Tabla 2

Priorizar la recuperación del proceso.

Prioridad de recuperación	MTD en días	MTD en horas
1	0.5 - 1	12 - 24
2	1 - 2	24 - 48
3	2 - 3	48 - 72
4	3 - 4	72 - 96

La recopilación de datos de este análisis se realiza a través de tablas y categorizaciones, que pueden ser presentados en formato de hoja de cálculo.

Análisis de Riesgo. Se encarga de identificar las amenazas sobre los activos de una organización y su probabilidad de ocurrencia, las vulnerabilidades asociadas a cada activo y el grado de impacto que estas amenazas pueden provocar sobre la disponibilidad de los mismos. (INTECO, 2016).

En el análisis de riesgos de la presente investigación se usará la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), esta metodología es de carácter público, perteneciente al Ministerio de Política Territorial y Función Pública del Gobierno Español; su utilización no requiere autorización previa del mismo.

(Ministerio de Hacienda y Administraciones Públicas, 2012) MAGERIT, es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Esta metodología nace como respuesta a la percepción de que toda sociedad depende de manera creciente de los sistemas de información para la consecución de sus objetivos.

De acuerdo a MAGERIT, el proceso de gestión de riesgos está conformado por dos actividades:

- Análisis de Riesgos: Permite determinar qué tiene la organización y estimar que le podría pasar, para lo cual considera los siguientes elementos:
    - Activos, son los elementos del sistema de información que soportan la organización.
    - Amenazas, es todo aquello que puede afectar a los activos causando perjuicios a la organización.
    - Salvaguardas, medidas de protección que se despliegan en la organización para evitar que las amenazas causen un gran daño en la misma.
- Tratamiento del riesgo: permite organizar una defensa meticulosa y prudente que permita a la organización sobrevivir a los incidentes y seguir operando en las mejores condiciones.

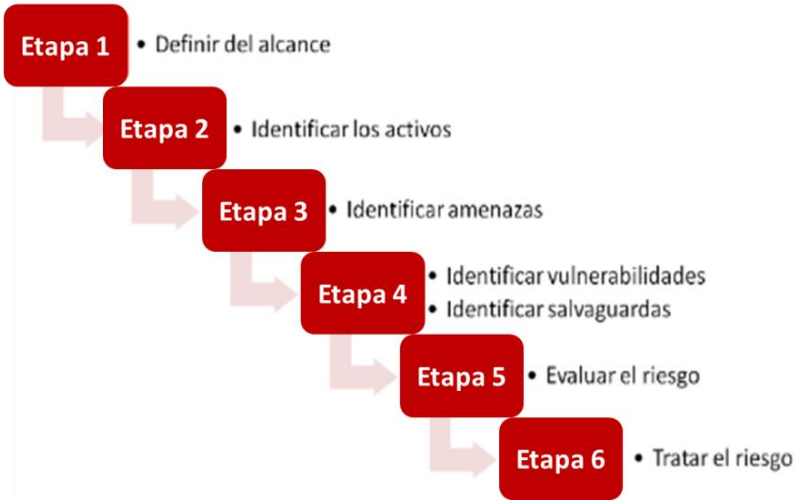
Entre los objetivos específicos del proyecto se consideró manejar una herramienta que automatice los procesos de análisis de riesgos como EAR/PILAR[3] con la metodología para gestión de riesgos MAGERIT. En el desarrollo del proyecto se presentarán los resultados obtenidos del Análisis de Riesgos con la herramienta EAR/PILAR.

A continuación, se describirá un conjunto de etapas que son comunes en la mayor parte de las metodologías para el análisis de riesgos.

Figura 4

Etapas para gestión de riesgos.

[3] EAR/PILAR, las herramientas EAR (Entorno de Análisis de Riesgos) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT y está desarrollada y financiada parcialmente por el CCN. (www.ccn-cert.cni.es).



Etapa 1. Definir el alcance

El primer paso para realizar el análisis de riesgos, es establecer el alcance del estudio. Vamos a seleccionar procesos o sistemas de las áreas estratégicas sobre las que debemos mejorar la seguridad y continuidad. En esta investigación se considerará los servicios y sistemas del departamento de TI de la empresa Laboratorios Bagó del Ecuador S.A.

Etapa 2. Identificar los activos

Habiendo definido el alcance, se debe identificar los activos más importantes que soportan el departamento, proceso, o sistema objeto del estudio. Realizar un inventario de activos como en la siguiente tabla:

Tabla 3

Ejemplo de inventario de activos.

Código	Nombre	Tipo	Descripción	Responsable	Ubicación	Crítico
S001	SERVIDOR_V1	Virtual	Servidor de base de datos	SISTEMAS	DATA CENTER	SI
W001	WIRELESS CONTROLER	Físico	Despliegue de configuraciones Wireless	SISTEMAS	DATA CENTER	NO
S002	SERVIDOR_V2	Virtual	Servidor e-learning	SISTEMAS	DATA CENTER	NO

Etapa 3. Identificar amenazas

Una vez identificados los activos principales, el paso siguiente consiste en identificar las amenazas a las que estos están expuestos. Conociendo la existencia de amenazas se debe realizar un enfoque práctico al tipo de amenaza que puede afectar uno o más activos. Las amenazas pueden ser de origen natural o humano, y podrán darse de forma accidental o deliberada.

Por ejemplo, para evaluar el riesgo de que corre un servidor de archivos, es recomendable, considerar las amenazas al que este es susceptible como: la posibilidad de daños por inundación o rotura de una cañería de agua, daño por incendio y por sobrecalentamiento.

Etapa 4. Identificar vulnerabilidades y salvaguardas

Esta etapa trata sobre el estudio de las características de los activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de computadores o servidores cuyos antivirus no están actualizados o una serie de activos para los que ya no existe soporte ni mantenimiento por parte del fabricante.

Por otra parte, también se analizará las medidas de seguridad implantadas en la organización. Por ejemplo, es posible que se haya instalado un sistema SAI (Sistema de Alimentación Ininterrumpida) con UPS para abastecer de electricidad a los equipos del centro de cómputo. Estas medidas de seguridad son conocidas también como salvaguardas y contribuyen a reducir el riesgo de las amenazas relacionadas con el corte de suministro eléctrico.

Etapa 5. Evaluar el riesgo

En esta etapa se cuenta con los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesto cada activo

- Conjunto de vulnerabilidades asociadas a cada activo
- Conjunto de medidas de seguridad o salvaguardas implantadas

Con estos conjuntos de información, se puede calcular el riesgo. Para cada par activo-amenaza, se estimará la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos, esto se puede observar en las siguientes tablas.

Tabla 4

Para el cálculo de la probabilidad de riesgo.

Cualitativa	Cuantitativa	Materialización De La Amenaza
Baja	1	Una vez al año
Media	2	Una vez al mes
Alta	3	Una vez a la semana

Tabla 5

Para el cálculo del impacto.

Cualitativo	Cuantitativo	Descripción Del Impacto
Bajo	1	El daño causado por la materialización de la amenaza no tiene consecuencias relevantes para la empresa.
Medio	2	El daño causado por la materialización de la amenaza tiene consecuencias relevantes para la empresa.
Alto	3	El daño causado por la materialización de la amenaza tiene consecuencias graves para la empresa.

- **Cálculo del riesgo**

Para calcular el riesgo, si puede optar por hacer un análisis cuantitativo, se calculará multiplicando los factores de probabilidad e impacto:

RIESGO = PROBABILIDAD x IMPACTO

Si se decide realizar el análisis cualitativo, se hará el uso de una matriz de riesgo como la que se muestra a continuación en la Figura 5.

Figura 5.

Matriz de riesgo.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Nota. Tomado de *Cálculo del riesgo*, por INCIBE, 2017, https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Como se mencionó en el apartado anterior, para estimar la probabilidad y el impacto se debe considerar las vulnerabilidades y salvaguardas existentes.

Por ejemplo, la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (Ej. Servidores redundantes), se puede considerar que el impacto será medio ya que estas medidas de preventivas harán que los procesos de negocio no se vean gravemente afectados por la caída del servidor.

Si por el contrario hemos identificado vulnerabilidades asociadas al activo, aplicaremos una penalización a la hora de estimar el impacto. Por ejemplo, si los equipos de climatización del centro de cómputo no han recibido el mantenimiento recomendado por el fabricante, se incrementa el impacto de amenazas como “condiciones ambientales inadecuadas” o “malfuncionamiento de los equipos debido a altas temperaturas”.

Etapa 6. Tratar el riesgo

Una vez hecho el cálculo del riesgo, se trata aquellos riesgos que superen un límite que se haya definido. Por ejemplo, se tratarán aquellos riesgos cuyo valor sea superior a 4 o superior al nivel medio en caso de que hayamos hecho el cálculo en términos cualitativos.

Para tratar el riesgo, existen cuatro estrategias principales:

- Transferir: Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- Eliminar: Eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico, se podría eliminar la red Wi-Fi de visitas para dar servicio si no es estrictamente necesario.
- Asumir: Siempre con justificación. Por ejemplo, el costo de instalar un generador eléctrico puede ser demasiado alto y, por tanto, la organización puede optar por asumir la compra.
- Mitigar: Por ejemplo, contratando un acceso a Internet de respaldo para poder acceder a los servicios en la nube en caso de que el enlace principal haya caído.

Cabe señalar que, llevar a cabo un análisis de riesgos y presentando el cuadro del plan de tratamiento de riesgos de continuidad del negocio, proporciona información de gran valor y contribuye en gran medida a mejorar la seguridad de una organización.

Fase 2. Determinación de la estrategia de continuidad. Para determinar las estrategias de recuperación a aplicar, se debe tener a la mano la siguiente información:

- Los procesos críticos de la organización, los tiempos de recuperación y los requisitos de pérdida de información de estos procesos.
- Los recursos implicados en cada proceso y los tiempos de recuperación de cada recurso que puede garantizar el personal técnico.

- Los riesgos a la que se encuentra sometida la infraestructura tecnológica.

A partir de la información obtenida anteriormente, se puede identificar si los recursos actuales y las estrategias de recuperación podrán cubrir el MTD establecido para cada uno de los procesos.

El objetivo es saber cómo recuperar un sistema para evitar que una contingencia lo degrade y le cause daños irreversibles que conllevan a perdidas en el negocio. Algunos elementos susceptibles a un evento de contingencia son: el personal, las dependencias de la organización, la infraestructura IT, la información y hasta los proveedores.

Como resultado de este proceso determinaremos las estrategias de recuperación adecuadas a cada caso, teniendo en cuenta que algunos procesos pueden necesitar varias estrategias de recuperación en función de su naturaleza y características. Para cada estrategia se debe valorar su costo y viabilidad de su implantación, mantenimiento, recursos necesarios, entre otros, de manera que se obtenga un conjunto de iniciativas a implantar para mejorar la continuidad del proceso; este documento contiene los apéndices donde se presentan las estrategias para cada actividad.

Fase 3. Respuesta a la contingencia. Esta fase es la encargada de implementar las estrategias propuestas para cada proceso crítico descritas en la fase anterior. Comienza con la implantación de las iniciativas identificadas en la anterior fase, y seguirá una fase de clasificación y priorización de medidas, en función del proceso afectado y la criticidad de éste.

Durante la implantación, se puede abordar la fase de documentación de la respuesta a la contingencia, y a partir de esto se debe enfocar en los elementos más relacionados con la tecnología, aunque son aplicables también a elementos que no sean tecnológicos.

Este proceso se lo organiza en torno a los siguientes elementos:

Plan de Crisis. Este documento es el elemento central en la gestión de la situación de crisis, cuyo objetivo es evitar que se tomen decisiones improvisadas que puedan empeorar la crisis o que, simplemente, no se tomen. Contiene todos los elementos necesarios para la gestión de los momentos iniciales de una crisis:

Tabla 6

Elementos de situación de crisis.

Elemento	Descripción
Condiciones de Disparo	Condiciones límite que deben darse para declarar una situación de crisis, se debe tomar en cuenta los MTDs de los proceso críticos.
Flujo	Flujo de toma de decisiones.
Medios	Para la declaración de una situación de crisis.
Personal	Recurso humano responsable de activar el Plan de Crisis y gestionarlo.
Contactos	Teléfonos, correos y datos de contacto del personal encargado de la gestión de la crisis.
Niveles	Niveles de prioridad para la recuperación de la infraestructura de la organización.
Requisitos	Requisitos temporales para la puesta en marcha del plan.
Planes Operativos	Planes Operativos existentes y el personal responsable de su activación.

Planes Operativos de Recuperación de Entornos. Luego de la ejecución del Plan de Crisis, se ponen en marcha todos los procesos necesarios para la recuperación de la infraestructura afectada a través de los Planes Operativos de Recuperación de Entornos. Dependiendo de la evaluación del alcance de la crisis y el entorno, se determina qué planes se ejecutan.

En estos documentos se puede describir uno o más entornos independientes y contienen información específica sobre el entorno al cual aplican. Por ejemplo, un entorno puede ser el servidor proxy, un ERP o el correo electrónico.

Procedimientos técnicos de trabajo o de Incidentes. Tras el disparo de los diferentes planes operativos, cada una de las infraestructuras afectadas comenzará su proceso de recuperación, tomando

como base para ello el último elemento de la ejecución de la estrategia de continuidad: los procedimientos técnicos de trabajo.

Toda esta documentación describe como se deben llevar las tareas necesarias para la gestión y recuperación de una aplicación, sistema, infraestructura o entorno. Aunque básicamente no son parte de la continuidad del negocio sino de la operación diaria de una organización, es en una situación de crisis cuando se los necesita de manera urgente.

Por lo tanto, estos documentos contienen gran cantidad de información específica de cada uno de los entornos: direcciones IP, versionado de programas, listado detallado de comandos, tablas de enrutamiento, recuperación de copias de base de datos, puesta en marcha de aplicaciones, etc. Esta documentación será apoyada por los manuales de procedimientos de levantamiento de servicios de la empresa.

Fase 4. Prueba, mantenimiento y revisión. Un BCP tiene como objetivo gestionar de manera efectiva el tiempo y una situación de crisis no deseada. Por lo tanto, es necesario que se lo mantenga actualizado en todo momento y que su vigencia sea evidenciada regularmente. Por ejemplo, debe actualizarse cuando hay movimientos de personal, cambios de versiones o de contactos del personal de crisis.

Para ello, es necesario llevar a cabo diferentes pruebas al menos una vez al año, sobre los entornos que hayamos definido en el alcance. De esta manera cubrir el conjunto de amenazas que hemos definido como potencialmente catastróficas, con diferentes grados de complejidad y elaboración.

Para la ejecución de las pruebas, es necesario llevar a cabo una planificación previa que tenga en cuenta los siguientes aspectos:

- Personal técnico implicado en la prueba.

- Usuario del aplicativo implicado.
- Personal externo: clientes, proveedores, etc.
- Descripción de la prueba a realizar.
- Descripción del resultado esperado luego de la ejecución de la prueba.
- Hora y fecha de realización.

Se debe tener en cuenta que siempre que la prueba pueda implicar una pérdida de servicio, ya sea ejecutada con éxito o no, se debe planificar en un horario extra laboral o de impacto mínimo.

Posteriormente a la prueba, se elabora un informe que recopile los resultados y describa las posibles incidencias surgidas durante ésta como son: los resultados no esperados, tiempos estimados superados, mala comunicación entre el personal, indisponibilidad de proveedores, etc. Cualquier incidencia que se haya producido debe analizarse para la aplicación de las medidas correctivas que sean necesarias.

Algunos ejemplos de posibles pruebas que pueden ejecutarse, siempre teniendo en cuenta la naturaleza de cada organización y que deben planificarse cuidadosamente, son las siguientes:

- Realizar la comprobación de que, ante una caída del suministro eléctrico, el sistema de alimentación ininterrumpida (UPS) y la central eléctrica de edificio funcionen.
- Verificar los tiempos de recuperación de los posibles repositorios documentales de la organización en una máquina de pruebas. Los permisos de los ficheros o archivos deben ser los mismos que cada uno tenía antes de la recuperación.
- Recuperación de las aplicaciones críticas del negocio y los datos asociados en máquinas instaladas durante la prueba.
- Acceso remoto a la infraestructura desde una ubicación externa.

Plan de mantenimiento. La intensión de este plan es mantener actualizada toda la documentación cada vez que se produzca un cambio significativo en la organización, a nivel de infraestructuras TIC, de personal, o de cualquier otro aspecto relacionado a los procesos críticos.

Esto permitirá que la documentación a utilizar en una situación de crisis refleje plenamente la información de los distintos involucrados en los procesos: infraestructura, personal, proveedores y terceras partes que deben tenerse en cuenta en una situación de contingencia.

Plan de Pruebas. El propósito es mostrar los distintos tipos de pruebas de contingencia que se debe llevar a cabo. A pesar de que el plan de mantenimiento contiene aquellos eventos que deben disparar una revisión o modificación del sistema (por ejemplo, el cambio de un proveedor), la ejecución de los planes de prueba es vital para garantizar la salud del BCP. Esto permite:

- Garantizar que la información del plan se mantiene actualizada.
- Garantizar que la organización podrá recuperarse en los tiempos establecidos, en situación contingencia, aspecto que puede determinar la continuidad de negocio de la organización.
- Incrementar la sinergia del personal implicado en una potencial contingencia.
- Mejorar el conocimiento de los usuarios en relación con las pruebas de continuidad.
- Incrementar la confianza de los usuarios en la organización.

Fase 5. Concientización. Como última fase de la implantación de un BCP, se debe llevar a cabo aquellas tareas que incrementen la concienciación del personal en relación con la continuidad. El público objetivo en este caso deberá ser tanto el personal técnico como el personal de negocio que tenga algún tipo de relación con los procesos críticos dentro del alcance.

En concreto, se debe plantear un proceso de concienciación que contemple la descripción de los elementos que se usan en la continuidad (análisis de impacto sobre el negocio, plan de crisis, estrategias

de recuperación, etc.). Además deben considerarse aspectos como por ejemplo, las responsabilidades o pruebas que se debe realizar con un documento de levantamiento de necesidades de capacitación (27001Academy, 2014).

El fundamento teórico antes descrito se usará para el diseño del plan de continuidad de negocio en el presente proyecto, cabe destacar que se utilizarán normas y estándares internacionales avalados por instituciones de tecnología como (ISO 22301, 2012) e INCIBE.

Los directivos de Laboratorios Bagó S.A son conscientes de la coyuntura actual con respecto a eventos inesperados que afecten las operaciones de la organización y este proyecto los podrá guiar para su toma de decisiones en la consecución e implementación de este plan de continuidad.

Según (27001Academy, 2014), recomienda veinte y cinco documentos para la certificación ISO 22301, a estos documentos, la norma los denomina como información documentada. Esta contiene registros, listas, alcance, políticas, procedimientos y metodologías. En el presente estudio se consideraran los documentos básicos para implementar el plan de continuidad propuesto según el alcance planteado como se ve en la

Tabla 7.

Tabla 7

Lista de documentación y registros que recomienda este proyecto.

Fases	Documentación	Descripción
FASE 0: Determinación del alcance	Alcance del BCP y explicación de las exclusiones.	Define claramente a qué partes de su organización se aplicará el BCP en base a las necesidades identificadas y a las pretensiones de la organización. También debe explicar los motivos por los que fueron excluidos del alcance algunas partes de su organización.
	Política y objetivos de la continuidad del negocio.	Documento central en el que la alta dirección debe indicar lo que quiere lograr con el BCP y cómo lo controlarán.
FASE 1:Análisis de la organización	Determinación del contexto de la organización.	Se determina a través de varios documentos; por ejemplo, el diagnóstico de la situación actual, el Marco legal, la Metodología de análisis de impactos en el negocio y la evaluación de riesgos.
	Análisis de impacto en el negocio y sus resultados.	Identificación de actividades de negocio y procesos, la recopilación de datos para dicho análisis se realiza a través de preguntas y encuestas, que pueden ser en un formato sencillo de hoja de cálculo.
	Análisis de riesgos y sus resultados.	Debe ser definida en una metodología antes de empezar a realizarla, en este caso MAGERIT. Los resultados de la evaluación de riesgos pueden ser documentados con la herramienta de análisis de riesgos EAR/PILAR y presentar el Plan de Tratamiento de Riesgos de Continuidad del Negocio.
FASE 2: Determinación de la estrategia de continuidad	Estrategia de la continuidad del negocio.	Es un documento de alto nivel que contiene estrategias para cada actividad bajo la forma de apéndices.

Fases	Documentación	Descripción
FASE 3: Respuesta a la contingencia	Procedimientos de respuesta ante incidentes y registros sobre un incidente.	Plan de crisis y plan de respuesta ante incidentes debe definir la forma de registrar los hechos del incidente; puede ser algo sencillo, como notas manuscritas en el plan junto a cada paso que se ejecuta.
FASE 4: Prueba, mantenimiento y revisión	Planes de pruebas y verificación e informes posteriores.	Cada plan debe definir los escenarios y objetivos que se deben cumplir; mientras que el informe debe indicar en qué nivel se han logrado esos objetivos.
	Programa de mantenimiento del BCP.	Como la documentación del BCP puede ser bastante amplia, y se puede convertir en obsoleta fácilmente, una buena práctica es definir exactamente cuándo se revisará cada documento. Esto puede ser una simple tabla que determine cuándo debe ser revisado cada documento y por quién.
FASE 5: Concienciación	Plan de capacitación y concienciación.	Contiene la descripción de las habilidades y necesidades de capacitación del personal.

La documentación anteriormente descrita puede ser demasiado extensa y confidencial, por lo cual en algunos casos se presentarán bosquejos y referencias de la documentación. Laboratorios Bagó del Ecuador S.A. a través de su gerente financiero, considera como entregable este proyecto de tesis finalizado para que les pueda servir como referencia en planes futuros.

Capítulo III. Plan de Continuidad de Negocio

En el presente capítulo se desarrollará el plan de continuidad de negocio propuesto en base a guías de implementación (INCIBE, 2016) y el estándar ISO 22301. Primero, se define el alcance del proyecto, luego se realiza el análisis de la organización, donde, se conoce el presente de la empresa en temas de continuidad, se identifican aplicaciones, servicios y procesos críticos; después se realiza el análisis de impacto en el negocio, así como también, el análisis de riesgos, identificación de amenazas y vulnerabilidades. Con todo lo anterior, se determinan las estrategias de continuidad, las cuales permitan la recuperación del negocio y disminuyan el impacto negativo de la materialización de eventos no deseados. Finalizando con un el plan de mantenimiento y concienciación del BCP.

Fase 0: Determinación del alcance

Alcance del BCP y explicación de las exclusiones

Objetivo, alcance y usuarios. El objetivo de este documento es definir claramente los límites del plan de Continuidad de negocio en Laboratorios Bagó del Ecuador S.A.

Los usuarios de este documento son los directivos de laboratorios Bagó, personal de Bagó IT y demás involucrados en el desarrollo del plan.

Definición del alcance del BCP. El alcance que se plantea en el presente proyecto es proponer un plan de continuidad de negocio para el área de Bagó IT, este plan tiene como objetivo obtener una óptima capacidad de reacción al producirse un incidente que afecte a las operaciones del área tecnológica de la empresa. Esto conlleva a disminuir pérdidas de información, monetarias y de imagen para la organización.

Procesos y servicios. Este plan considera los servicios que brinda Bagó IT a todas las áreas de la organización dentro de su cadena de valor. Además, se toma en consideración los procesos y activos

críticos asociados a cada actividad que se realizan en las diferentes áreas de la organización para mejorar su continuidad.

Unidades organizativas. Se considera al área de tecnología de Laboratorios Bagó del Ecuador S. A., porque es el área que estratégicamente apoya de manera transversal a todas las unidades de negocio de la organización, tales como Ventas, Logística, Marketing, Contabilidad, Departamento Técnico, Entrenamiento y Finanzas.

Ubicaciones. Las oficinas principales de Laboratorios Bagó del Ecuador S.A. están ubicadas en la calle Lizardo García E1080 y Av. 12 de octubre, esquina en Quito-Ecuador. Además, posee dos sucursales ubicadas en Guayaquil y Vía a la Mitad del Mundo. Toda la infraestructura tecnológica está instalada en sus oficinas principales.

Redes e infraestructura de TI. La **Tabla 8** muestra los servicios tecnológicos que brinda Bagó IT a la organización a través de su infraestructura para el desarrollo de las operaciones en sus diferentes áreas. La mayoría de servicios son entregados desde la sucursal principal, otros desde la nube y algunos son de proveedores con los que se posee una alianza estratégica.

Tabla 8

Servicios tecnológicos y aplicaciones.

Servicios Tecnológicos	Descripción	Módulos o Sistemas
Intranet Corporativa	Sitio web corporativo que brinda información y accesos a diferentes sistemas.	Fichero Médico (FICO), Ventas Propias, Muestra Médica, Reportes de ventas.
Gestión y administración de dispositivos móviles corporativos. MDM *(Mobile Device Management)*	SaaS que permite la gestión y control de los dispositivos móviles (*tablets* y *smartphones*) desplegados en la compañía.	MaaS360 Cloud Extender

Servicios Tecnológicos	Descripción	Módulos o Sistemas
Aplicaciones móviles	Desarrollos propios que ayudan a la gestión de actividades de las áreas desde su dispositivo móvil.	Sistema Bagó, Webservice, BagótoGo
Instalación de aplicaciones de proveedor	Aplicaciones de empresas proveedoras para apoyó al negocio.	Posso, NetOrder (Leterago), compiladores APK
Nube Privada	Repositorio de archivos y descarga de Literaturas (Presentaciones multimedia de productos).	oCloud, Owncloud
Ofimática	Herramientas de procesamiento de texto, presentaciones, hojas de cálculo.	Microsoft Office, Adobe Reader
DET	Sistema de gestión de procesos Financieros, de Comisiones, de Contabilidad e Inventarios.	Sistema de Comisiones, Facturación, Fichero Médico, Concep-Reporte, Ventas Ecuador, Asientos de ventas contabilidad, Sistema de activos fijos, Automatización de liquidaciones, Bagó New, CxP importaciones, Diarios Ecuador, Sistema de compras no productivas.
Administración de base de datos	Gestor y administrador de base de datos, Ejecución de consultas y reportes. Procesos ETL.	Oracle, Toad, SQL Developer, DbForge, Spoom
Correo electrónico	Envió y recepción de mensajes de correo.	PostFix, Thunderbird
Aplicaciones web	Aplicaciones propias para apoyo al negocio.	Sistema de Inversión por Médico, Facturación Electrónica, Sistema de Personal, DRS manager, Sistema de reembolso de gastos.
Repositorio de herramientas de diseño	Herramientas para diseño gráfico.	Creative Suit , KeyNote, I-Movie, Photoshop, Ilustrator, Acrobat Pro
e-learning	Aula virtual para capacitaciones.	Moodle, Vimeo, Camtasia
Internet y Navegación Web	Navegación para acceso a Internet y varias aplicaciones en líneas.	Ecuapass (Ventanilla Única Ecuatoriana), Portal ARCSA, Concep, Sisalem, Quipux, Web IESS, SAR Leterago, Asertec, AWS.
Transferencia de archivos	Transferencia para subida de archivos a entes regulatorios.	CuteFTP

Servicios Tecnológicos	Descripción	Módulos o Sistemas
Servidor de archivos	Acceso a sistemas y carpetas compartidas.	Samba
Página web	Alojamiento página web y Gestor de contenidos (CMS).	WordPress
Gestión Hipervisor vCenter	Plataforma para control de virtualización.	vSphere ESX, Wmware, SSH
Servicio de respaldos de información	Gestión de respaldos de información.	Veeam Backup, ArcServe
Inteligencia de negocios	Software de inteligencia empresarial.	MicroStrategy
Data Center	Centro de cómputo donde se concentran los diferentes sistemas de comunicaciones y servidores.	Sistemas de alimentación ininterrumpida para abastecimiento de energía eléctrica (UPS), aire acondicionado, equipos de comunicaciones, racks de servidores y sistemas de backups.
Servicio de telefonía IP	Telefonía por el protocolo IP que conecta todas las sucursales.	PBX Panasonic
Servicio de CCTV-NVR	Cámaras IP desplegadas en puntos estratégicos de las oficinas.	iVMS
Videoconferencia Fija y nube pública	Servicio de video conferencia para reuniones entre sucursales, la región y proveedores.	Webex, Zoom
Desarrollo de aplicaciones	Software para desarrollo de aplicaciones empresariales en base a los objetivos empresariales y de negocio.	Visual Basic 6.0, Visial .NET, Java, PHP, SQL, Android Studio, Ionic, Node JS, TomCat
Servicio de impresión	Impresoras desplegadas en las oficinas para impresión.	Solución Kyocera
Servidor de dominio	Servicio de libreta de direcciones, DNS, DHCP.	Samba, Ldap
Firewall	Servidor proxy de filtrado de navegación de Internet.	SuSEfirewall, squidProxy
AntiSpam	Filtrado de correo electrónico no deseado y malicioso.	Barracuda
Infraestructura de red	Redes LAN, Enlace de datos y redes WLAN.	Sistemas HP y Cisco

Servicios Tecnológicos	Descripción	Módulos o Sistemas
Gestión de plataforma de Antivirus	Servidor de actualización de base de datos de AV para alerta de amenazas y cliente antivirus.	ePo (McAfee antivirus ePolicy Orchestrator), McAfee End Point Security
Configuración de equipos de usuarios	Equipo de cómputo, desktops y laptops marca con sistema operativo.	Hardware HP, Windows 7/10

Exclusiones del alcance. El enfoque principal del proyecto es al área de tecnología de Laboratorios Bagó del Ecuador S.A., sin embargo, cabe recalcar que a futuro el BCP se puede extender a las demás áreas de la organización.

Política y objetivos de la continuidad del negocio

Objetivo, alcance y usuarios. El propósito de esta política es definir el objetivo, alcance y reglas básicas para la gestión de la continuidad del negocio.

Esta política se aplica a todo el Plan de Continuidad del Negocio (BCP).

Los usuarios de este documento son todos los empleados de Laboratorios Bagó del Ecuador S.A., como también todos los proveedores y socios que cumplen alguna función en el BCP.

Objetivo de la gestión de la continuidad del negocio. El objetivo del BCP es identificar potenciales amenazas en una organización y los impactos que esas amenazas podrían ocasionar sobre las operaciones; también sirve para proporcionar un marco de referencia para construir resiliencia organizacional con la capacidad de una respuesta efectiva.

Relación con los objetivos generales y otros documentos. Con la implementación del plan de continuidad de negocio, Laboratorios Bagó del Ecuador S.A. desea cumplir sus objetivos organizacionales en los ámbitos de cultura, recursos, prescripciones y ventas.

Establecer los objetivos de continuidad del negocio. Proponer la implementación de un BCP para el área de tecnología de Laboratorios Bagó del Ecuador S.A., donde se realice un análisis de impacto al negocio, un análisis de riesgos, se determinen las estrategias de continuidad y finalmente se establezcan planes de mantenimiento, pruebas y concientización.

Alcance del BCP. El plan de continuidad de negocio de Laboratorios Bagó del Ecuador S.A. será enfocado inicialmente al área de IT, luego con base a la experiencia podrá se extendido a las demás áreas del negocio en su cadena de valor.

A continuación en la Figura 6 se muestra la cadena de valor de Laboratorios Bagó.

Figura 6

Cadena de valor de Laboratorios Bagó del Ecuador S.A.

Productos y servicios clave. Los productos y servicios que son entregados por Bagó IT están en el documento de determinación del alcance en el apartado 0 Redes e infraestructura de TI.

Responsabilidades para la gestión de la continuidad del negocio. Responsabilidades generales:

- El personal de IT a cargo del plan de continuidad es el responsable de que sea implementado de acuerdo a esta política y proporcionará todos los recursos necesarios.
- El comité de crisis, será el encargado de declarar la situación de crisis y dará el paso a la ejecución del plan de continuidad.
- El comité paritario de la empresa será el responsable de la integridad física del personal.
- El comité directivo de la organización revisará, realizará cambios y aprobará esta política.

Medición. Se realizarán periódicamente pruebas y test de efectividad del plan de continuidad, usando como métricas los tiempos de recuperación resultantes de las pruebas.

Comunicación de la política. Esta política será publicada para en los diferentes medios de comunicación interna y externa a todo el personal del Laboratorios Bagó del Ecuador S.A.

El alcance y la política anteriormente descritos pueden ser trasladados a un formato específico para la firma de los directivos e involucrados.

Fase 1: Análisis de la organización

Determinación del contexto de la organización

En los siguientes apartados se presenta la información recabada y se realiza el análisis de los resultados obtenidos sobre el contexto de la organización.

Mantener reuniones. Se mantuvieron reuniones con el personal de diferentes departamentos de la empresa para realizar el levantamiento de información, se discutió respecto a los activos y los procesos

críticos que se apoyan en el departamento tecnológico. Además, se recolectó información sobre las aplicaciones y servicios que presta el área tecnológica, así como sus dependencias, recursos que utilizan y datos que manejan.

Adicionalmente se utilizó documentación disponible en la intranet de la empresa, los descriptivos de cargos, la página web corporativa y se emplearon métodos de investigación como la encuesta y la entrevista con el personal de IT.

Acerca de Laboratorios Bagó del Ecuador S.A. Tiene su origen en Argentina, se fundó en 1934 con el objetivo de construir una compañía farmacéutica de vanguardia y excelencia al servicio de la salud. A través de su desarrollado e investigación ha obtenido 85 patentes en el área terapéutica, tiene presencia en 50 países y posee 11 plantas industriales estratégicamente distribuidas en diferentes países.

Se expandió por Sudamérica y en nuestro país Laboratorios Bagó S.A. inició sus operaciones en junio de 1992, posee un portafolio de más de 100 productos que contribuyen a mejorar la salud y vida de los ecuatorianos. Además, el equipo de Bagó está conformado por más de 280 colaboradores entre comerciales y administrativos.

La empresa se destaca por su ágil crecimiento los últimos 10 años, en el 2019 se encuentra dentro de los tres primeros laboratorios (Del mercado farmacéutico total sin leches) de mayor preferencia por el médico a la hora de prescribir un producto y dentro de las diez mayores empresas farmacéuticas en un mercado de las más de 100 existentes en el país. Según datos proporcionados por IQVIA[4].

Laboratorios Bagó de Ecuador S.A. se enfoca en la promoción y comercialización de productos farmacéuticos a través de la visita médica, su fuerza de ventas está desplegada en todo el territorio

[4] IQVIA, compañía multinacional que provee información de los mercados de salud e investigación clínica.

nacional. La distribución de los productos la realiza su aliado estratégico Leterago del Ecuador S.A, empresa especializada en almacenamiento y distribución de productos farmacéuticos.

- **Misión**

Contribuir a mejorar la salud y vida de la población con productos farmacéuticos de la más alta calidad.

- **Visión**

Ubicarnos en el 2023, entre los tres primeros laboratorios*, trabajando con calidez y excelencia por la gente. *Del mercado farmacéutico total sin leches.

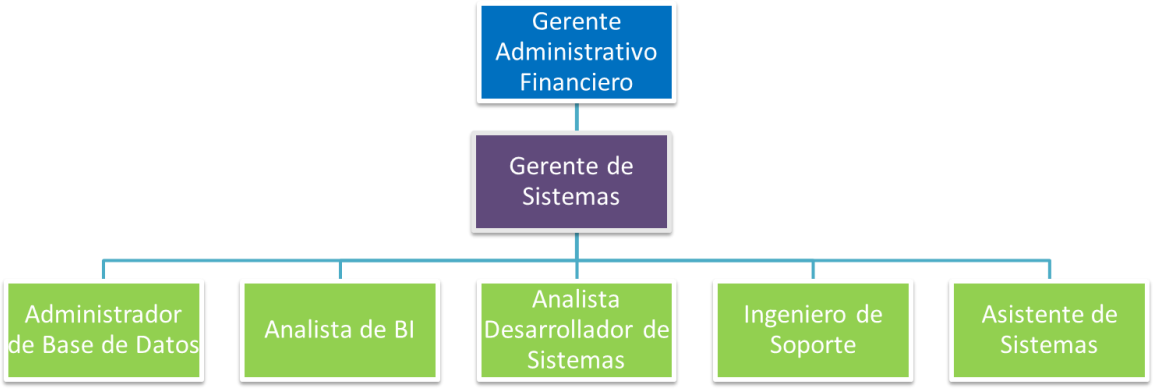
Departamento de Tecnologías de la Información. El área tecnológica de Laboratorios Bagó del Ecuador S.A. también denominado Bagó IT o Sistemas, gestiona información y procesos críticos para el giro de negocio, maneja información de ventas, mercadeo, logística, inventarios, auditorias y talento humano. Al igual que otras empresas su infraestructura tecnológica es susceptible a eventos no deseados o contingencias que pueden afectar su actividad económica, su información, su credibilidad y reputación. Sin embargo, a lo largo de su existencia no ha contado con un plan de continuidad de negocio que potencie su capacidad de reacción ante una situación de desastre que pueda ocurrir, es decir la empresa en la actualidad estaría con una desventaja competitiva si es víctima de una contingencia.

Por lo tanto, es indispensable contar con un proyecto de plan de continuidad que ayude al departamento Bagó IT a mantener sus actividades sin interrupciones, y como consecuencia a la empresa se mantenga como referente en el área farmacéutica.

A continuación en la Figura 7 se puede observar el organigrama correspondiente al departamento de tecnología de Bagó IT.

Figura 7

Organigrama del departamento de IT de Laboratorios Bagó del Ecuador S.A.



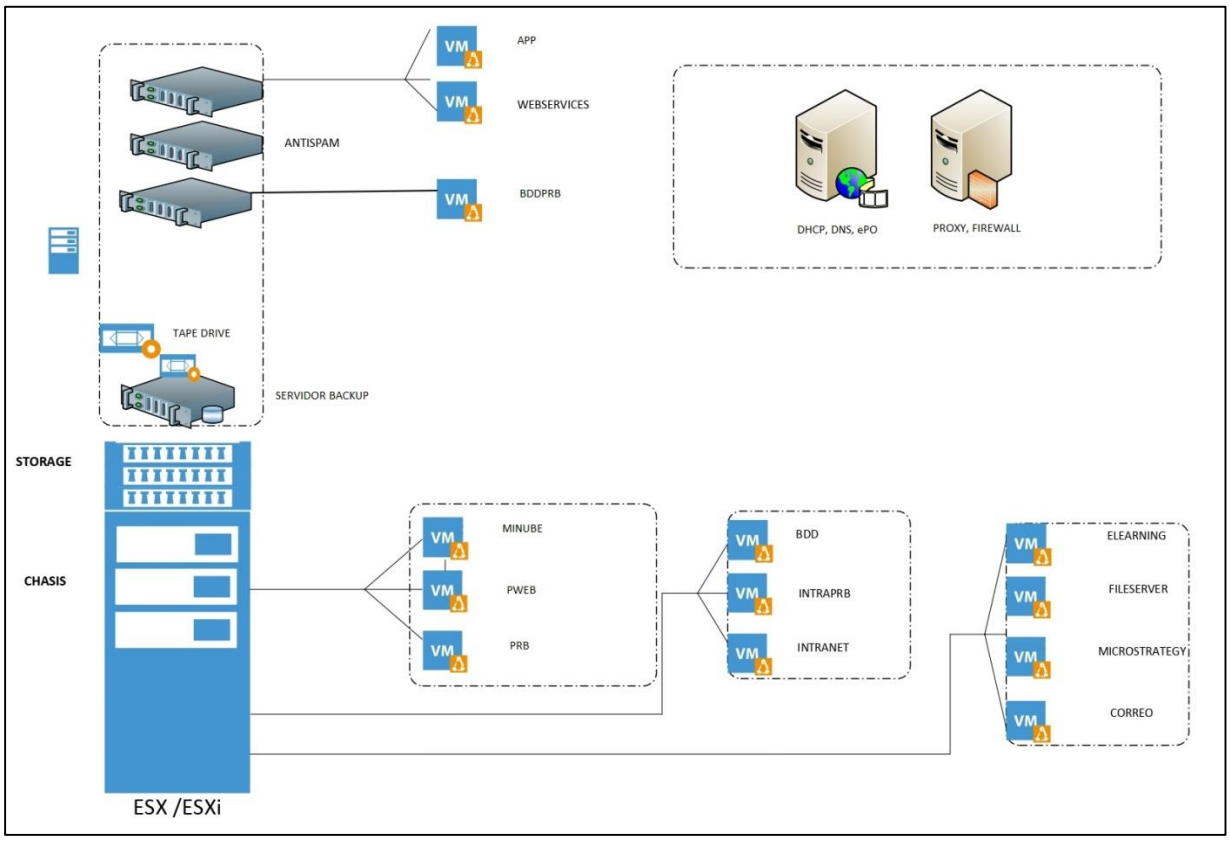
El departamento de tecnología Bagó IT está conformado por 8 profesionales, un gerente de Sistemas, un administrador de base de datos, un analista de inteligencia de negocios, tres programadores de sistemas, un ingeniero de soporte e infraestructura y un asistente de sistemas.

- **Diagrama de Servidores**

A continuación la Figura 8 muestra un esquema de la Infraestructura física y virtual de servidores de la organización, consta de seis servidores físicos de producción y dos de pruebas. Además, constan los servidores virtuales con servicios específicos que están alojados en un Chasis H IBM y un *Storage*.

Figura 8

Diagrama de servidores de Laboratorios Bagó del Ecuador S.A.

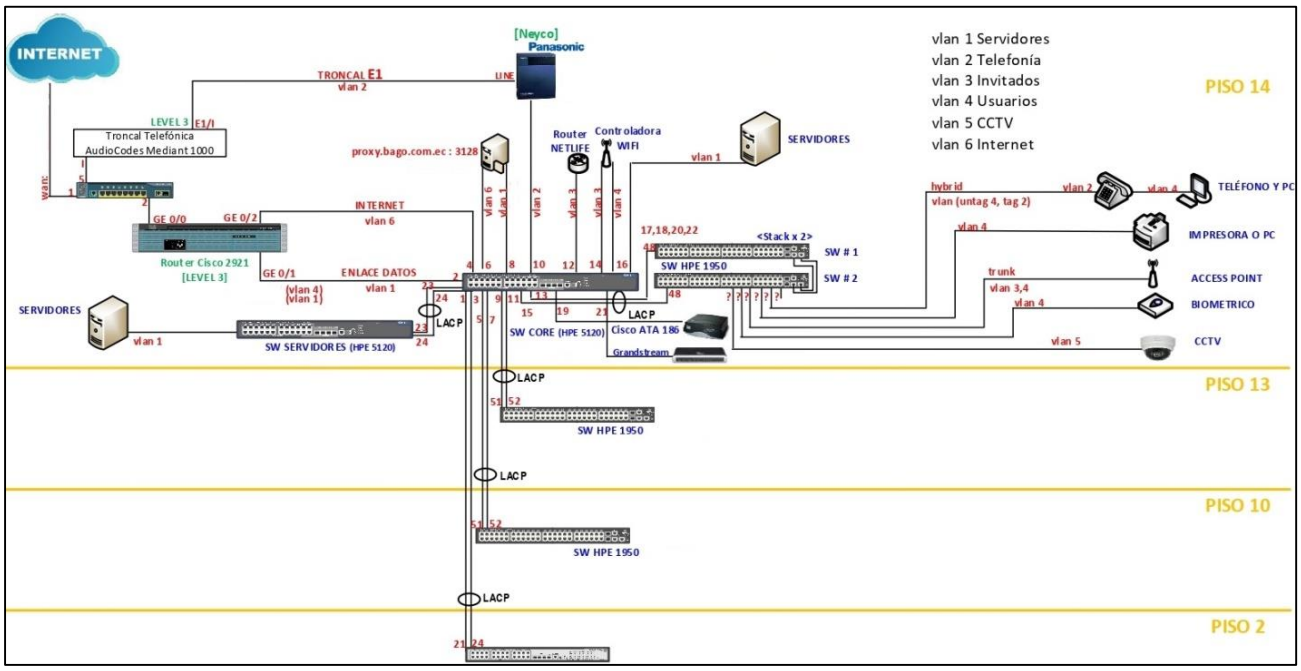


- **Diagrama de red**

El diagrama de red de la Figura 9 muestra los dispositivos de comunicaciones (Capa2, Capa3, PBX, servidores, equipos de cómputo, impresoras, controles de acceso, telefonía IP y CCTV) que posee la sede principal la cual brinda todos los servicios tecnológicos a las otras sedes, por tal razón en esta sede se enfocarán los esfuerzos por mejorar la continuidad de negocio. Además, la infraestructura de red organizacional de Laboratorios Bagó del Ecuador S. A consta de dos enlaces de datos WAN, uno a Guayaquil y otro a La Mitad del Mundo (Operador logístico Leterago) desde su sede principal en Quito.

Figura 9

Diagrama de red de Laboratorios Bagó del Ecuador S.A.



Además, Bagó IT posee documentación de procesos para levantamiento de servicios, así como de configuraciones de dispositivos para la restauración de equipos de comunicación. Esta documentación posee información confidencial por lo cual no es publicable en este estudio, sin embargo, la empresa internamente sabrá a cuál documento acudir cuando sea mencionado a lo largo de esta investigación.

Marco legal. En Ecuador, actualmente existe un marco legal que se aplica a instituciones financieras sobre continuidad de negocio y seguridad de la información, sin embargo, no ha sido publicado un marco legal que abarque a todas las industrias. A continuación se listan las resoluciones y acuerdos existentes en nuestro país con respecto a las instituciones financieras **(Advisera, 2017)**.

- Resolución JB-2012-2148: Seguridad de la información en canales electrónicos (aplica a todas las instituciones financieras).

- Resolución JB-2014-3066: Sistemas de Gestión de Seguridad de la Información basado en ISO 27001 and Sistemas de Gestión de Continuidad de Negocio basado en ISO 22301 (aplica a todas las instituciones financieras).
- Acuerdo Ministerial No. 166: Esquema Gubernamental de Seguridad de la Información basado en NTE ISO 27001 (ISO basado en ISO 27001:2005).
- Resolución de Gestión de Riesgo Operacional: nueva Resolución que es una mejora de la Resolución JB-2012-2148 y la Resolución JB-2014-3066, y requiere que todas las instituciones financieras definan e implementen un SGSI con un alcance limitado, seguridad de la información en los proyectos y Gestión de la seguridad de la información a terceras partes.

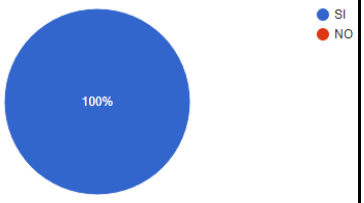
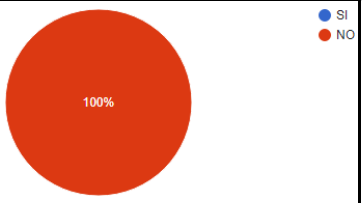
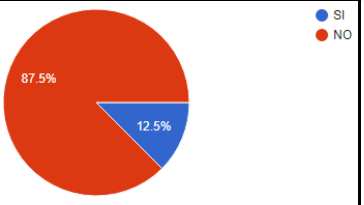
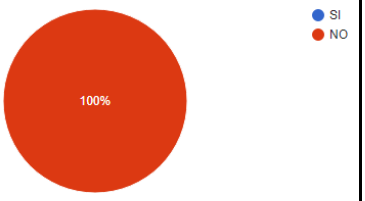
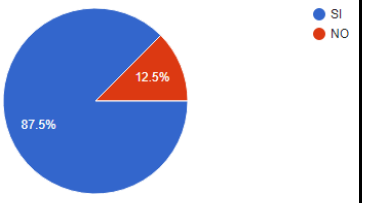
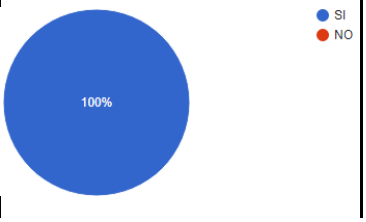
Diagnóstico de la situación actual de la Gestión de Continuidad de Negocio y Seguridad de la información. Para realizar el diagnóstico de la situación actual se empleó una encuesta (Anexo A), la cual se aplicó a todo el personal de Bagó IT. Según **(Cevallos, 2015)**, esta encuesta se compone de secciones basadas en lineamientos de la normas ISO 22301, con el objetivo de determinar si la organización cumple o no al 100% con las buenas prácticas determinadas en la norma, y conocer el estado actual para aplicar las mejoras correspondientes respecto a continuidad y seguridad de la información.

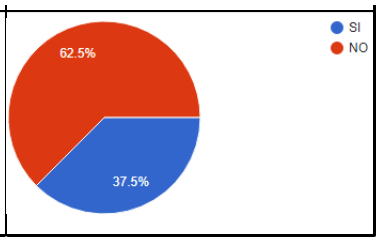
A continuación, en las figuras 10-13 se muestra la tabulación de resultados de manera gráfica y el análisis de las respuestas obtenidas en la encuesta:

Sección Plan de Continuidad de Negocio.

Figura 10

Resultados de encuesta, Sección Plan de Continuidad de Negocio.

a. Sección Plan de Continuidad de Negocio	% SI	% NO	GRÁFICO
1. ¿Conoce que es un Sistema de Gestión de Continuidad de Negocio o un Plan de continuidad de Negocio?	100.0	0.0	
2. ¿Si la continuidad de las operaciones de la empresa se ve afectada, existe un plan de continuidad de negocio o recuperación de desastres que seguir?	0.0	100.0	
3. ¿Se cuenta con un proceso documentado que declare situación de crisis en caso de incidentes?	12.5	87.5	
4. ¿Bagó IT cuenta con un sitio alterno para recuperación de actividades del data center en caso de desastre?	0.0	100.0	
5. ¿El comité empresarial de la organización ha demostrado interés y compromiso para garantizar la seguridad de información?	87.5	12.5	
6. ¿Usted conoce los riesgos a los cuales es susceptible el área tecnológica?	100.0	0.0	

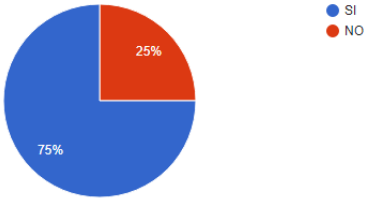
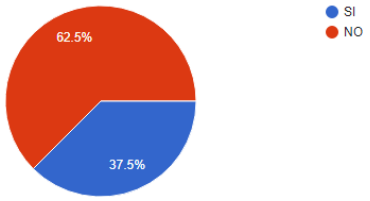
7. ¿Bagó IT cuenta con un análisis de impacto de negocio de sus activos y procesos?	37.5	52.5	

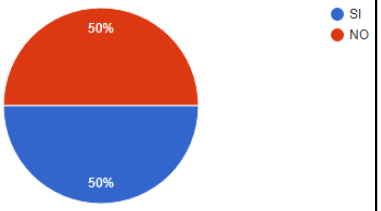
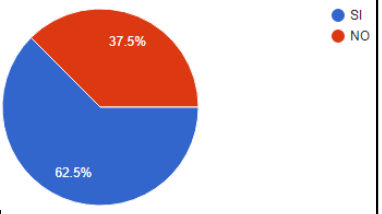
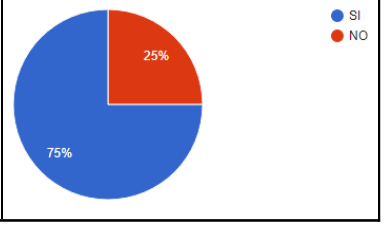
Como se puede evidenciar en la encuesta, todo el personal de área de tecnología está al tanto de lo que es un Plan de continuidad de negocio y de los riesgos a los que es susceptible la infraestructura tecnológica. Además, se puede constatar que actualmente existe interés por parte de los directivos de la empresa para implementar un Plan de continuidad, sin embargo, aún no existe un plan de continuidad implementado con el cual se puedan, declarar situaciones de crisis en caso de incidentes, definir un sitio alterno para alojar el Data center y conocer el impacto que ocasionaría la interrupción de actividades.

Sección Seguridad de la información.

Figura 11

Resultados de encuesta, Sección Seguridad de la información.

b. Sección Seguridad de la información	**% SI**	**% NO**	**GRÁFICO**
1. ¿Existe una política de respaldos documentada y formalizada para todos los tipos de respaldo de información?	75.0	25.0	
2. ¿Conoce cuál es el procedimiento y acciones seguir en el caso de falla de los servicios o aplicaciones que se brindan?	37.5	62.5	

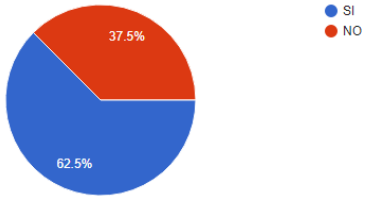
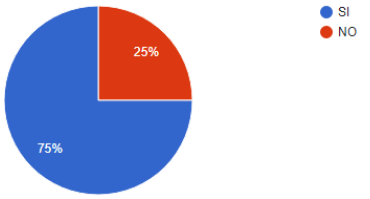
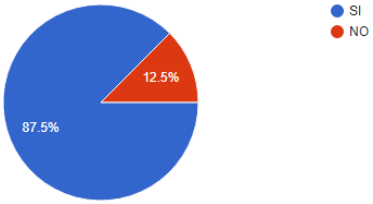
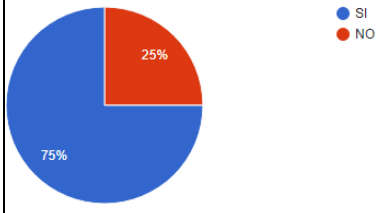
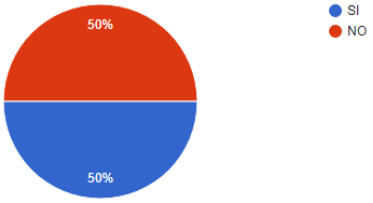
3. ¿Existe un procedimiento difundido sobre la descarga de archivos de fuentes desconocidas que puedan tener malware?	50.0	50.0	
4. ¿Se realizan revisiones periódicas del software y respaldo de equipos que manejen procesos críticos?	62.5	37.5	
5. ¿Existe un procedimiento o documentación para contención y resguardo de información de procesos críticos?	75.0	25.0	

Con respecto a la seguridad de la información, existen políticas, documentación y procedimientos de respaldos, sin embargo, no abarcan el 100% de la información disponible a ser respaldada. Además, el 62.5% del personal no conoce los procedimientos y acciones a seguir en caso de fallas en los servicios. Y en lo referente a las revisiones y respaldo de equipos, el 37.5% del personal no conoce que se realicen respaldos a todos los equipos que manejan procesos críticos.

Sección Gestión de activos.

Figura 12

Resultados de encuesta, Sección Gestión de Activos.

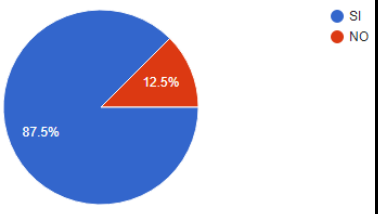
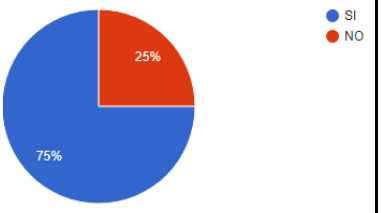
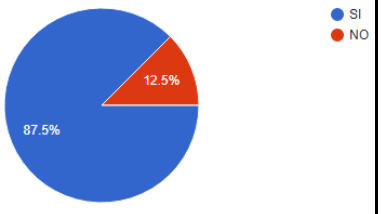
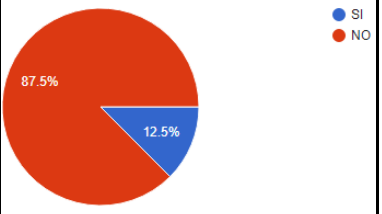
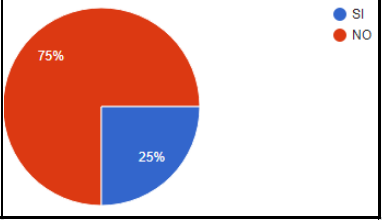
c. Sección Gestión de activos	% SI	% NO	GRÁFICO
1. ¿Se dispone de un inventario actualizado de todo el hardware y software?	62.2	37.5	
2. ¿Existen políticas del buen uso de los activos dentro de la empresa?	75.0	25.0	
3. ¿Se encuentra reglamentado el buen uso del correo electrónico?	87.5	12.5	
4. ¿Se encuentra reglamentado el uso de Internet?	75.0	25.0	
5. ¿Existe un procedimiento disciplinario para usuarios que incumplan políticas de resguardo de información?	50.0	50.0	

Sobre la gestión de activos tecnológicos, de acuerdo a las encuestas se puede deducir que, si existen políticas implementadas sobre el buen uso de los activos, del correo electrónico y del Internet. Sin embargo, estas políticas no son difundidas a todo el personal y no se conoce las condiciones de uso y sus penalizaciones. El 37.5% de los encuestados considera que no se lleva un inventario actualizado de hardware y Software, lo que hace suponer que el inventario actual de los activos no está completo.

Sección Seguridad física de la infraestructura.

Figura 13

Resultados de encuesta, Sección Seguridad física de la infraestructura.

d. Sección Seguridad física de la infraestructura	% SI	% NO	GRÁFICO
1. ¿El acceso al data center está controlado por un sistema de seguridad biométrico?	87.5	12.5	
2. ¿Existe una bitácora para registro de actividades y supervisión de terceros que visitan el data center?	75.0	25.0	
3. ¿El data center cuenta con un sistema de protección ante fallos de suministro eléctrico que permita brindar servicio de manera ininterrumpida?	87.5	12.5	
4. ¿Existe un sistema automático contra incendios en el data center?	12.5	87.5	
5. ¿El personal de IT está en capacidad de reaccionar en caso de una emergencia por un incendio?	25.0	75.0	

Con referencia a la seguridad de la infraestructura física del área, el 12.5% no conoce que para acceder al *Data center* se debe pasar por el control biométrico y el 25% dice que no existe una bitácora; además

no conocen que se cuenta con un sistema de UPS para protección en falla de suministro eléctrico, también el 12.5% no sabe que no existe un sistema automático contra incendios y el 75% del personal no está en la capacidad de reaccionar en caso de incendio.

Como resultado del promedio de las respuestas en cada sección, Bagó IT alcanza actualmente un nivel de cumplimiento de 57.96%; en conclusión, el área de tecnología de Laboratorios Bagó no aplica todas las buenas prácticas recomendadas por la norma ISO 22301 para continuidad de negocio y seguridad de información. Además, en la actualidad la empresa no posee un plan de continuidad de negocio que permita la continuidad de sus actividades ante un incidente o desastre en su área tecnológica.

Como resultado de esta investigación, se obtuvieron las impresiones de los directivos, en las cuales manifiestan su interés por la futura implementación de un plan de continuidad y por lo tanto este proyecto será de gran ayuda para implementar un BCP en la organización.

Análisis de impacto en el negocio (BIA)

Los objetivos de este análisis son: identificar los procesos críticos de la organización relacionados con Bagó IT ante eventos disruptivos, evaluar el impacto operacional que ocasionarían dichos eventos, además establecer los recursos y tiempos de recuperación del negocio. Esta metodología se basa en la norma ISO 22301.

Identificación de actividades de negocio y procesos. En este apartado se identifican las actividades de negocio así también como los procesos que aportan a la producción en la organización y la consecución de sus objetivos, se tomaron en cuenta todas las áreas dentro la cadena de valor de la empresa como se puede ver en la

Tabla **9**.

Tabla 9

Identificación de áreas, actividades de negocio y procesos.

Área	Actividad de Negocio	Procesos
Promoción y Ventas	Promoción de productos (Visita Médica)	Reporte de cumplimiento de visitas a través de los sistemas internos
		Visita Médica con dispositivo móvil (*Tablet*)
		Seguimiento de Prescripciones médicas y Zonales
		Consulta de Información estadística de farmacias
		Pedidos de productos
		Descarga de Literaturas
	Diseño de políticas de comercialización	Información de ventas
		Reporte de Muestra médica
		Control de la gestión de la fuerza de ventas
		Relacionamiento con los clientes y proveedores
	Diseño de estrategias para cumplimiento de cuotas	Proceso de cálculo de Comisiones (Cuotas y asignación de Líneas)
		Consulta de comisiones y cuotas
		Informe de rotación mensual y proyección de cuotas
	Análisis estratégico y Toma de decisiones	Reportes gerenciales de productos, especialidades, zonas y ventas

Área	Actividad de Negocio	Procesos
Marketing y Gestión Estratégica	Desarrollo y diseño de estrategias de marketing	Preparación de material promocional para *Tablets*
		Distribución de material audiovisual y multimedia
		Lanzamiento de nuevos productos
	Análisis de rentabilidad	Supervisión del margen de contribución CM4
	Controla y administración de Presupuestos	Asignación del presupuesto para médicos estratégicos
	Diseño Gráfico	Creación de representaciones gráficas de campañas de comunicación, eventos internos y material promocional
	Análisis y estadísticas de mercado	Gestión del fichero médico corporativo
		Generación y preparación de información estadística de proyección de ventas
		Desarrollo y preparación de información de archivos para zonales y participar en las reuniones
		Manejo de auditorías de mercado farmacéutico
		Generación de informes de inteligencia Competitiva y reportes
		Planificación mensual de muestra médica
		Ingresar pesos para el cálculo de comisiones

Área	Actividad de Negocio	Procesos
Gerencia General	Capacitación y Entrenamiento	Capacitación integral del Área Comercial
		Supervisión y actualización proyecto *e-learning*
	Dirección Médica	Farmacovigilancia y recepción de reportes de eventos adversos
		Supervisión de la documentación científica de los productos para obtención de registro sanitario
	Dirección Técnica	Gestión para la obtención y actualización de registros sanitarios
		Coordinación de actividades técnicas de control y normas emitidas por las autoridades sanitarias
		Renovación anual de los permisos de funcionamiento
		Gestión de la documentación técnica y legal de los productos
		Negociaciones estratégicas con las autoridades sanitarias
		Documentación técnica y legal para procesos regulatorios, obtención y aprobación de permisos productos controlados
		Aseguramiento de la Calidad
		Ingreso, recopilación y archivo de las contra muestras de cada lote de producto importado
		Desarrollo de artes de material de acondicionamiento de empaque
		Actualización de información técnica en la Intranet
	Contraloría y Auditoria	Creación de modelos de documentación para estandarizar procedimientos
		Identificación de procedimientos existentes y faltantes de los procesos *core* de la empresa
		Liquidación y control de planes promocionales con clientes
	Comunicación	Administración y actualización de página web
		Responsabilidad social RRS
		Comunicación e imagen corporativa externa con Medios

Área	Actividad de Negocio	Procesos
Recursos Humanos	Administración de personal	Ingreso de nuevo personal
		Control de ausencias (vacaciones, permisos médicos)
		Notificación de cambios en el personal
		Selección de personal
	Nómina	Política de remuneraciones y beneficios de los empleados a nivel general
		Control del proceso de nómina para el pago de sueldos y comisiones
		Reportes y pagos a organismos de control
	Capacitación y planes de desarrollo	Inducción a nuevos empleados
		Evaluación de Desempeño
		Coordinación de proceso de desarrollo organizacional
	Seguridad y Salud ocupacional	Atención médica – quirúrgica de nivel primario y de urgencia
		Registros médicos, atención diaria en consulta y hoja de evolución, de todo el personal
		Gestión de Seguridad y Salud ocupacional
	Comunicación Interna	Manejo de la Comunicación Interna
Administración y Finanzas	Contabilidad	Elaboración y presentación de los reportes contables de la compañía a Organismos de Control Local
		Revisión y envío de comprobantes de retención en la fuente
		Realización y preparación de declaraciones de impuestos y anexos tributarios
		Cierre mensual de ventas, cartera y cobranza

Área	Actividad de Negocio	Procesos
Administración y Finanzas	Contabilidad	Altas y bajas de activos fijos
		Generación de proveedores
		Reembolsos de gastos con todos los sustentos y registro
		Valoración y elaboración de costeo del producto PT y MM
		Registro contable de importaciones
		Baja de productos caducados en bodega de PT y MM
		Gestión de Inventarios
		Análisis y contabilización de facturas
	Compras y Logística	Gestión de los permisos de importación con las entidades regulatorias y control de vigencia
		Gestión del distribuidor (Leterago)
		Permisos de importación en las Entidades de Regulación del Comercio Exterior, INEN, MIPRO, SENAE
		Elaboración y el despacho oportuno de las muestras médicas
		Codificación de PVP de los productos arribados para la distribución o venta
		Pagos de importaciones y el ingreso de los productos a bodega
		Gestión de compras locales
		Control de inventarios, despachos, ingresos y devoluciones

Área	Actividad de Negocio	Procesos
Administración y Finanzas	Administración	Mantenimiento de edificio
		Cuadro de análisis de precios
		Diseño de estrategias, ejecución, dirección, control financiero, administrativo y contable del Laboratorio
		Facturación, notas de crédito y débito a clientes
		Control, seguimiento y análisis de flujo de caja
		Seguro de activos
		Planes telefonía celular
		Revisión del stock para pedidos especiales de cliente estratégico
	Sistemas (IT)	Administración de base de datos
		Gestión de funcionamiento de la infraestructura física y virtual de servidores (Base de datos, Almacenamiento, Aplicaciones (DET, Intranet, aplicaciones web), Proxy, Firewall, Antivirus, AntiSpam, Nube privada, Página web, BI, Respaldos, DHCP, Archivos, e-learning, Intranet, Correo, Dominio, DNS
		Gestión de respaldo de servidores virtuales
		Gestión de respaldo a cintas de información
		Administración de página web
		Administración de e-learning

Área	Actividad de Negocio	Procesos
Administración y Finanzas	Sistemas (IT)	Gestión y administración de dispositivos móviles corporativos
		Monitorear y garantizar la plataforma de *bussiness intelligence*
		Administración de la infraestructura de red cableada e inalámbrica
		Administración de la Intranet
		Supervisión de sistemas de respaldo de energía eléctrica
		Supervisión y mantenimiento de Data Center
		Conexión de enlaces de datos, telefónico e Internet corporativo
		Correo electrónico
		Central telefónica IP
		Cámaras IP
		Videoconferencia
		Análisis, desarrollo, programación, versionamiento y documentación la automatización de los sistemas de la organización
		Gestión de creación de usuarios y asignación de permisos a sistemas
		Asignación de permisos a carpetas

Con la identificación de estas actividades que se sustentan en recursos y activos tecnológicos, se procede a valorar el impacto que ocasionaría si una de las actividades se interrumpe, esto se analizará en el siguiente apartado.

Evaluación de Impactos operacionales. Tomando en cuenta las actividades de negocio que ayudan a cumplir la misión de la empresa es necesario evaluar el impacto que estas ocasionarían en caso de una interrupción. Este impacto operacional permite determinar el nivel de afectación de una interrupción en el negocio.

La Tabla 10 muestra a detalle el proceso o actividad de negocio y el servicio tecnológico, el módulo o sistema que soporta al proceso. Además, se muestra la valoración de impacto por cada actividad de negocio según la Tabla 1.

Tabla 10

Procesos con sus dependencias de recursos o servicios tecnológicos y nivel de impacto.

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Reporte de cumplimiento de visitas a través de los sistemas internos	Intranet	Fichero Médico (FICO)	B
Visita Médica con dispositivo móvil (Tablets)	Gestión y administración de dispositivos móviles corporativos MDM	MDM	B
Seguimiento de Prescripciones médicas y Zonales	Aplicaciones móviles	Sistema Bagó, Webservices	C
Consulta de Información estadística de farmacias	Instalación de aplicaciones de proveedor	Posso	C
Pedidos de productos	Instalación de aplicaciones de proveedor	NetOrder (Leterago)	A
Descarga de Literaturas	Nube Privada	oCloud	B

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Información de ventas	Intranet	Ventas Propias (DDD, Leterago)	B
Reporte de Muestra médica	Intranet	Muestra Médica	C
Control de la gestión de la fuerza de ventas	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Relacionamiento con los clientes y proveedores	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Proceso de cálculo de Comisiones (Cuotas y asignación de Líneas)	DET	Sistema de Comisiones	B
Consulta de comisiones y cuotas	DET, Intranet	Sistema de Comisiones, Reporte Intranet	C
Informe de rotación mensual y proyección de cuotas	Ofimática, Gestor Base de datos	Microsoft Office, Reportes BDD, SQL Developer	C
Reportes gerenciales de productos, especialidades, zonas y ventas	Intranet, Servidor de archivos	Microstrategy	B
Preparación de material promocional para Tablets	Instalación de aplicaciones de proveedor, Ofimática	Compilador APK, PowerPoint	C
Distribución de material audiovisual y multimedia	Nube Privada	Ocloud	B
Lanzamiento de nuevos productos	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Supervisión del margen de contribución CM4	Intranet, Ofimática	MicroStrategy, Microsoft Office	C
Asignación del presupuesto para médicos estratégicos	Aplicación web	Sistema de Inversión por Médico	B
Creación de representaciones gráficas de campañas de comunicación, eventos internos y material promocional	Ofimática, Creative Suit	KeyNote, PowerPoint, I-Movie, Photoshop, Ilustrator, Acrobat Pro	C
Gestión del fichero médico corporativo	DET	Fichero Médico (FICO)	A
Generación y preparación de información estadística de proyección de ventas	Ofimática, Gestor Base de datos	FoxPro, SQL, Farmatrack, Posso, Excel	B
Desarrollo y preparación de información para zonales y participar en las reuniones	Ofimática	Excel	C

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Manejo de auditorías de mercado farmacéutico	Datos de Auditorías externas	IMS Plus (PME-DDD), CloseUp, Pharma Mix	C
Generación de informes de inteligencia Competitiva y reportes	Intranet, Ofimática	MicroStrategy, Microsoft Office	C
Planificación mensual de muestra médica	Intranet	Muestra Médica	C
Ingresar pesos para el cálculo de comisiones	DET	Sistema de Comisiones	C
Capacitación integral del Área Comercial	Ofimática	Microsoft Office	B
Supervisión y actualización proyecto e-learning	Ofimática, e-learning, aplicaciones multimedia	Moodle, Vimeo, Camtasia	B
Farmacovigilancia de la empresa y recepción de reportes de eventos adversos	Correo electrónico, Servidor de archivos	Thunderbird	A
Supervisión de la documentación científica de los productos para obtención de registro sanitario	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Gestión para la obtención y actualización de registros sanitarios	Navegador, Ofimática, Correo electrónico	Ecuapass (Ventanilla Única Ecuatoriana), Microsoft Office, Thunderbird	A
Coordinación de actividades técnicas de control y normas emitidas por las autoridades sanitarias	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Renovación anual de los permisos de funcionamiento	Navegador, Ofimática, Correo electrónico	Portal ARCSA, Microsoft Office, Thunderbird, Adobe Reader	B
Gestión de la documentación técnica y legal de los productos	DET, Ofimática, Correo electrónico	Concep - Reporte Concep, Microsoft Office, Thunderbird	A
Negociaciones estratégicas con las autoridades sanitarias	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Documentación técnica y legal para procesos regulatorios hasta la obtención y aprobación de permisos productos controlados	Navegador, DET, Transferencia de archivos, , Servidor de archivos	Sisalem, CuteFTP, Quipux	A

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Aseguramiento de la Calidad	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Ingreso, recopilación y archivo de las contra muestras de cada lote de producto importado	DET, Servidor de archivos	Reporte de muestras	B
Desarrollo de artes de material de acondicionamiento de empaque	Ofimática	Microsoft Office, Adobe Reader	B
Actualización de información técnica en la Intranet	Intranet	Mantenimiento de registros sanitarios	C
Creación de modelos de documentación para estandarizar procedimientos	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Identificación de procedimientos existentes y faltantes de los procesos core de la empresa	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Liquidación y control de planes promocionales con clientes	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Administración y actualización de página web	Gestor de contenidos	WordPress	B
Responsabilidad social RRS	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Comunicación e imagen corporativa externa con Medios	Redes sociales	Facebook, instagram, twiter	B
Ingreso de nuevo personal	DET, Aplicación web	DRS manager, Sistema de Personal	C
Control de ausencias (vacaciones, permisos médicos)	DET, Intranet, Aplicaciones móviles	BagóToGo, reportes	C
Notificación de cambios en el personal	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Selección de personal	Ofimática, Correo electrónico, Software Perfil conductual	Microsoft Office, Thunderbird	C
Política de remuneraciones y beneficios de los empleados a nivel general	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Control del proceso de nómina para el pago de sueldos y comisiones	DET, Ofimática, Correo electrónico, Intranet	Sistema de Comisiones, Microsoft Office, Thunderbird, reportes	B

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Reportes y pagos a organismos de control	Navegador, Intranet	Web IESS, reportes	C
Inducción a nuevos empleados	Ofimática, Servidor de archivos	Microsoft Office	C
Evaluación de Desempeño	Software de Talento Humano	Acsendo	C
Coordinación de proceso de desarrollo organizacional	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Atención médica – quirúrgica de nivel primario y de urgencia	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Registros médicos, atención diaria en consulta y hoja de evolución, de todo el personal	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Gestión de Seguridad y Salud ocupacional	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Manejo de la Comunicación Interna	Ofimática, Correo electrónico, Navegador	Microsoft Office, Thunderbird, Herramientas web de diseño	C
Elaboración y presentación de los reportes contables de la compañía a Organismos de Control Local	Ofimática, Servidor de archivos	Microsoft Office	A
Revisión y envío de comprobantes de retención en la fuente	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Realización y preparación de declaraciones de impuestos y anexos tributarios	Ofimática, DIMM	Microsoft Office, ATS	A
Cierre mensual de ventas, cartera y cobranza	DET, Ofimática, Intranet	Ventas Ecuador, Asientos de ventas contabilidad, Excel, Consulta gerencial de ventas	B
Altas y bajas de activos fijos	Intranet, Ofimática	Sistema de activos fijos, Microsoft Office	C
Generación de proveedores	DET	Proveedores	C
Reembolsos de gastos con todos los sustentos y registro	DET, Intranet	Automatización de liquidaciones, Sistema de reembolso de gastos	C

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Valoración y elaboración de costeo del producto PT y MM	DET, Bagó New, Ofimática	Costo de producto MM, Reporte de producto MM costeado, Preliminar de costeo de PT, Excel	B
Registro contable de importaciones	DET	CxP importaciones, Diarios Ecuador	B
Baja de productos caducados en bodega de PT y MM	Bagó New	Logística e Inventario, Transacciones de inventario	B
Gestión de Inventarios	DET, Bagó New	Reportes&Informes - Inventarios	B
Análisis y contabilización de facturas	DET	CxP Facturas proveedores, CxP notas de crédito proveedores	B
Gestión de los permisos de importación con las entidades regulatorias y control de vigencia	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Gestión del distribuidor (Leterago)	Ofimática, Correo electrónico, Portal web	Microsoft Office, Thunderbird, SAR Leterago	A
Permisos de importación en las Entidades de Regulación del Comercio Exterior, INEN, MIPRO, SENAE	Portales web	Ecuapass	A
Elaboración y el despacho oportuno de las muestras médicas	DET, Ofimática, Correo electrónico	Boletas, Microsoft Office, Thunderbird	B
Codificación de PVP de los productos arribados para la distribución o venta	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Pagos de importaciones y el ingreso de los productos a bodega	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A
Gestión de compras locales	DET, Ofimática, Correo electrónico	Sistema de compras no productivas, Microsoft Office, Thunderbird	C
Control de inventarios, despachos, ingresos y devoluciones	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Mantenimiento de edificio	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Cuadro de análisis de precios	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Diseño de estrategias, ejecución, dirección, control financiero, administrativo y contable del Laboratorio	Intranet, Intranet Argentina, DET	Microstrategy, Sistema de Comisiones	B
Facturación, notas de crédito y débito a clientes	DET, Aplicación web de facturación electrónica	Facturación, edocs	A
Control, seguimiento y análisis de flujo de caja	DET, Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Seguro de activos	Ofimática, Correo electrónico, Portal web	Microsoft Office, Thunderbird, Asertec	C
Planes telefonía celular	DET, Ofimática, Correo electrónico	Microsoft Office, Thunderbird	C
Revisión del stock para pedidos especiales de cliente estratégico	DET, Ofimática, Correo electrónico	Microsoft Office, Thunderbird	B
Administración de base de datos	Software de administración de bases de datos	Oracle, Toad	A
Gestión de funcionamiento de la infraestructura física y virtual de servidores (Base de datos, Almacenamiento, Aplicaciones (DET, Intranet, aplicaciones web, etc.), Proxy, Firewall, Antivirus, Antispam, Nube privada, Página web, BI, Respaldos, DHCP, Archivos, e-learning, Intranet, Correo, Dominio, DNS	Gestión Hipervisor vCenter (Data Center)	vSphere ESX, Wmware, SSH	A
Gestión de respaldo de servidores virtuales	Servicio de respaldos de información	Veeam Backup	A
Gestión de respaldo a cintas de información	Servicio de respaldos de información	ArcServe	B
Administración de página web	Servidor página web, Gestor de contenidos	WordPress	B

Procesos	Servicios tecnológicos	Módulos o Sistemas	Nivel de impacto
Administración de e-learning	Servidor e-learning	Moodle	B
Gestión y administración de dispositivos móviles corporativos	MDM	MaaS360 Cloud Extender	B
Monitorear y garantizar la plataforma de bussiness intelligence	Software de inteligencia empresarial	MicroStrategy	B
Administración de la infraestructura de red cableada e inalámbrica	Software de monitoreo	MRTG, Nagios	A
Administración de la Intranet	Servidor Intranet	Joombla	A
Supervisión de sistemas de respaldo de energía eléctrica	UPS (Data Center)	Computer Power	A
Supervisión y mantenimiento de Data Center	Control de acceso biométrico, Aire acondicionado	ZKA access 3.5	B
Conexión de enlaces de datos, telefónico e Internet corporativo	Última milla, consola web (Data Center)	Century Link	B
Correo electrónico	Servicio de correo electrónico	Thunderbird	A
Central telefónica IP	Servicio de telefonía IP	Panasonic	C
Cámaras IP	Servicio de CCTV-NVR	iVMS	C
Videoconferencia	Videoconferencia Fija y nube pública	Webex, Zoom	C
Análisis, desarrollo, programación, versionamiento y documentación la automatización de los sistemas de la organización	Desarrollo de aplicaciones	Visual Basic 6.0, Visial .NET, Java, PHP, SQL, Android Studio, Ionic, Node JS, TomCat	B
Gestión de creación de usuarios y asignación de permisos a sistemas	Servidor samba, DET	Iom, DRS manager	B
Asignación de permisos a carpetas	Servidor de archivos	SSH	C

El nivel de impacto asignado a cada proceso y su dependencia tecnológica se realizó con base a el criterio de los usuarios involucrados en los procesos, la experiencia del área de Bagó IT y a los recursos esenciales que soportan los procesos principales de la organización, esta valoración se la obtuvo en las

reuniones mantenidas con los involucrados. Ver tabla y claves de evaluación el Anexo B. Por lo tanto, se asignó como nivel A, a las actividades que podrían afectar el cumplimiento de los objetivos corporativos en caso de interrupción.

Identificación de procesos críticos y establecimiento de tiempos de recuperación. Una vez valorizado el impacto operacional, se procede a identificar los procesos críticos en función al impacto que tendría en caso de una interrupción. La Tabla 11 muestra la identificación realizada con los procesos de nivel de impacto A.

En este apartado también se define el tiempo máximo de inactividad (MTD) que un proceso crítico puede estar detenido antes que se produzcan consecuencias irreversibles para el negocio, y se lo define en días. Además, a los procesos críticos se les asigna una ponderación de prioridad, es decir que proceso debe ser restaurado con mayor rapidez y en un orden específico, donde 1 es lo más prioritario y 4 lo menos prioritario según la Tabla 2. A continuación la Tabla 11 muestra lo descrito anteriormente.

Tabla 11

Procesos críticos, establecimiento de MTD y prioridad de recuperación.

Procesos críticos	Servicios tecnológicos	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Pedidos de productos	Instalación de aplicaciones de proveedor	NetOrder (Leterago)	A	1	3
Lanzamiento de nuevos productos	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	3	4
Gestión del fichero médico corporativo	DET	Fichero Médico (FICO)	A	1	2
Farmacovigilancia de la empresa y recepción de reportes de eventos adversos	Correo electrónico, Servidor de archivos	Thunderbird	A	2	2

Procesos críticos	Servicios tecnológicos	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Supervisión de la documentación científica de los productos para obtención de registro sanitario	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	2	2
Gestión para la obtención y actualización de registros sanitarios	Navegador, Ofimática, Correo electrónico	Ecuapass (Ventanilla Única Ecuatoriana), Microsoft Office, Thunderbird	A	2	3
Gestión de la documentación técnica y legal de los productos	DET, Ofimática, Correo electrónico	Concep-Reporte Concep, Microsoft Office, Thunderbird	A	3	3
Negociaciones estratégicas con las autoridades sanitarias	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	3	3
Documentación técnica y legal para procesos regulatorios hasta la obtención y aprobación de permisos productos controlados	Navegador, DET, Transferencia de archivos, Servidor de archivos	Sisalem, CuteFTP, Quipux	A	2	3
Aseguramiento de la Calidad	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	1	3
Elaboración y presentación de los reportes contables de la compañía a Organismos de Control Local	Ofimática, Servidor de archivos	Microsoft Office	A	2	2

Procesos críticos	Servicios tecnológicos	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Revisión y envío de comprobantes de retención en la fuente	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	2	4
Realización y preparación de declaraciones de impuestos y anexos tributarios	Ofimática, DIMM	Microsoft Office, ATS	A	2	4
Gestión de los permisos de importación con las entidades regulatorias y control de vigencia	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	2	3
Gestión del distribuidor (Leterago)	Ofimática, Correo electrónico, Portal web	Microsoft Office, Thunderbird, SAR Leterago	A	1	1
Permisos de importación en las Entidades de Regulación del Comercio Exterior, INEN, MIPRO, SENAE	Portales web	Ecuapass, Pudeleco, SOCE	A	2	2
Codificación de PVP de los productos arribados para la distribución o venta	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	2	3
Pagos de importaciones y el ingreso de los productos a bodega	Ofimática, Correo electrónico	Microsoft Office, Thunderbird	A	2	3
Facturación, notas de crédito y débito a clientes	DET, App web de facturación electrónica	Facturación, edocs	A	0.5	1

Procesos críticos	Servicios tecnológicos	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Administración de base de datos	Software de administración de bases de datos	Oracle, Toad	A	1	1
Gestión de funcionamiento de la infraestructura física y virtual de servidores (Base de datos, Almacenamiento, Aplicaciones (DET, Intranet, aplicaciones web, etc.), Proxy, Firewall, Antivirus, Antispam, Nube privada, Página web, BI, Respaldos, DHCP, Archivos, e-learning, Intranet, Correo, Dominio, DNS	Gestión Hipervisor vCenter	vSphere ESX, Wmware, SSH	A	0.5	1
Gestión de respaldo de servidores virtuales	Servicio de respaldos de información	Veeam Backup	A	1	2
Administración de la infraestructura de red cableada e inalámbrica	Software de monitoreo	MRTG, Nagios	A	0.5	1
Administración de la Intranet	Servidor Intranet	Joombla	A	1	1
Supervisión de sistemas de respaldo de energía eléctrica	UPS	Computer Power	A	0.5	1
Correo electrónico	Servicio de correo electrónico	Thunderbird	A	0.5	1

Como se puede apreciar en la tabla anterior, existe un rango MTD de 0,5 a 3 días, lo que quiere decir que se puede trabajar hasta 3 días sin que un proceso falle completamente y cause daños a la organización. Esta definición se la acordó con los usuarios involucrados en reuniones.

Como resultado de la ponderación establecida de MTD y prioridad en la Tabla 11, se pueden identificar los procesos que serán restaurados con mayor prioridad en el siguiente orden: Gestión de funcionamiento de la infraestructura física y virtual de servidores, Supervisión de respaldo de energía eléctrica, Infraestructura de red, Administración de base de datos, Facturación, Correo electrónico, Intranet y Gestión del distribuidor (Leterago). Con estos resultados se obtiene la pauta para enfocar esfuerzos en su gestión de continuidad y saber que procesos se deben restaurar primero.

Identificación de recursos. Este punto es clave para identificar los recursos (servicios, activos, aplicaciones, módulos o sistemas) de Bagó IT que apoyan a las actividades de negocio críticas. Así se puede dimensionar el impacto que provocaría la interrupción de los servicios tecnológicos en la organización, estos servicios son los que se requieren para que los usuarios realicen sus actividades.

En la Tabla 12 se muestran los principales servicios tecnológicos de Bagó IT que soportan de manera transversal a los procesos del negocio de la organización y su correspondiente categorización.

Tabla 12

Servicios tecnológicos de Bagó IT.

Servicios tecnológicos	Descripción	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Intranet Corporativa	Sitio web corporativo que brinda información y accesos a diferentes sistemas	Fichero Médico (FICO), Ventas Propias, Muestra Médica, Reportes	A	0.5	1

Servicios tecnológicos	Descripción	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Gestión y administración de dispositivos móviles corporativos. MDM (Mobile Device Management)	SaaS que permite la gestión y control de los dispositivos móviles (tablets y smartphones) desplegados en la compañía	MaaS360 Cloud Extender	B	1	2
Aplicaciones móviles	BagóToGo, Sistema Bagó, Webservices	Sistema Bagó, Webservices, BagóToGo	B	1	2
Instalación de aplicaciones de proveedor	Aplicaciones de empresas proveedoras para apoyó al negocio	Posso, NetOrder (Leterago), compiladores APK	B	1	3
Nube Privada	Para repositorio de archivos y descarga de Literaturas	Ocloud, Owncloud	B	1	2
Ofimática	Herramientas de procesamiento de texto, presentaciones, hojas de cálculo	Microsoft Office, Adobe Reader	C	2	3
DET	Sistema de gestión de procesos Financieros, Contables, Contabilidad e Inventarios.	Sistema de Comisiones, Facturación, Fichero Médico, Concep-Reporte, Ventas, Asientos de ventas, Sistema de activos fijos, Automatización de liquidaciones, Bagó New, CxP importaciones, Diarios, Sistema de compras no productivas	A	0.5	1
Administración de base de datos	Administrador de base de datos, Ejecución de consultas y reportes. ETL	Oracle, Toad, SQL Developer, DbForge, Spoom	A	0.5	1

Servicios tecnológicos	Descripción	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Correo electrónico	Envió y recepción de mensajes de correo	PostFix, Thunderbird	A	0.5	1
Aplicaciones web	Aplicaciones propias para apoyo al negocio	Sistema de Inversión por Médico, Facturación Electrónica, Sistema de Personal, DRS manager, Sistema de reembolso de gastos	A	0.5	1
Repositorio de herramientas de diseño	Herramientas para diseño	KeyNote, I-Movie, Photoshop, Ilustrator, Acrobat Pro	C	2	4
e-learning	Aulas virtual para capacitaciones	Moodle, Vimeo, Camtasia	B	1	3
Internet y Navegación Web	Navegación para acceso a Internet y varias aplicaciones en líneas	Ecuapass (Ventanilla Única Ecuatoriana), Portal ARCSA, Concep, Sisalem, Quipux, Web IESS, SAR Leterago, Asertec, AWS	B	1	3
Transferencia de archivos	Transferencia para subida de archivos a entes regulatorios	CuteFTP	C	2	4
Servidor de archivos	Acceso a sistemas y carpetas compartidas	Samba	B	1	2
Página web	Alojamiento página web y Gestor de contenidos CMS	WordPress	B	0.5	2
Gestión Hipervisor vCenter	Plataforma para control de virtualización	vSphere ESX, Wmware, SSH	A	0.5	1
Servicio de respaldos de información	Gestión de respaldos de información	Veeam Backup, ArcServe	B	0.5	2
Inteligencia de negocios	Software de inteligencia empresarial	MicroStrategy	B	1	3

Servicios tecnológicos	Descripción	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Data Center	Centro de computo donde se concentran los diferentes sistemas de comunicaciones y servidores	Sistemas de alimentación ininterrumpida para abastecimiento de energía eléctrica en caso de apagones UPS, aire acondicionado, equipos de comunicaciones, racks de servidores y sistemas de backups	A	0.5	1
Servicio de telefonía IP	Telefonía por el protocolo IP que conecta todas las sucursales	PBX Panasonic	B	1	2
Servicio de CCTV-NVR	Cámaras IP desplegadas en puntos estratégicos de las oficinas	iVMS	C	2	4
Videoconferencia Fija y nube pública	Servicio de video conferencia para reuniones entre sucursales, la región y proveedores	Webex, Zoom	C	2	4
Desarrollo de aplicaciones	Software para desarrollo de aplicaciones empresariales en base a los objetivos empresariales y de negocio	Visual Basic 6.0, Visial .NET, Java, PHP, SQL, Android Studio, Ionic, Node JS, TomCat	B	1	2
Servicio de impresión	Impresoras desplegadas en las oficinas para impresión	Solución Kyocera	C	1	4
Servidor de dominio	Servicio de libreta de direcciones, DNS, DHCP	Samba, Ldap	B	0.5	1

Servicios tecnológicos	Descripción	Módulos o sistemas	Nivel de impacto	MTD (días)	Prioridad de recuperación
Administración del servicio de Antivirus	Servidor de actualización de base de datos para alerta de amenazas	ePo (McAfee antivirus ePolicy Orchestrator)	A	1	2
AntiSpam	Filtrado de correo electrónico no deseado y malicioso	Barracuda	B	0.5	3
Firewall	Servidor proxy de filtrado de navegación de Internet	SuSEfirewall, squidProxy	A	0.5	1
Infraestructura de red	Redes LAN, Enlace de datos y redes WLAN	Sitemas HP y Cisco	A	0.5	1
Configuración de equipos de usuarios	Equipo de cómputo, sistema operativo, cliente antivirus	Hardware HP, Windows 7/10, Mcfee End Point Security	B	1	2

Así como con los procesos, se asignó el nivel de impacto, priorización y MTD a los recursos tecnológicos con base a su grado de importancia para el desarrollo del negocio, esto se determinó gracias a una mesa redonda realizada con el personal de Bagó IT; por otro lado, el MTD reflejado, evidencia que el área tecnológica tiene entre 0,5 y 2 días para restablecer sus servicios.

Cabe recalcar que existen procesos que dependen de aplicaciones de un tercero o proveedor como el sistema Posso y NetOrder de Leterago, en el análisis de impacto estas aplicaciones no son consideradas críticas para el negocio (nivel B), sin embargo, son parte del mismo, además se puede ver que se tiene un espacio de tiempo más amplio para su recuperación y ésta dependerá del proveedor previa negociación con la organización.

Asignación de los RTO y RPO a los recursos. Según la categorización anterior, en la Tabla 13 se muestran los recursos tecnológicos más importantes (nivel de impacto A) para el mejoramiento de su continuidad, también se muestra la asignación del RTO (Tiempo de recuperación objetivo) y el RPO (Punto de recuperación objetivo) a los recursos principales.

Tabla 13

Recursos tecnológicos más importantes con nivel de impacto A.

Servicios tecnológicos	Descripción	Nivel de impacto	MTD (días)	Prioridad de recuperación	RTO (h)	RPO (h)
Intranet Corporativa	Sitio web corporativo que brinda información y accesos a diferentes sistemas	A	0.5	1	4	12
DET	Sistema de gestión de procesos Financieros, Contables, Contabilidad e Inventarios.	A	0.5	1	4	8
Administración de base de datos	Gestor y administrador de base de datos, Ejecución de consultas y reportes. ETL	A	0.5	1	4	8
Correo electrónico	Envió y recepción de mensajes de correo	A	0.5	1	3	8
Aplicaciones web	Aplicaciones propias para apoyo al negocio	A	0.5	1	3	8
Gestión Hipervisor vCenter	Plataforma para control de virtualización	A	0.5	1	5	8
Data Center	Centro de computo donde se concentran los diferentes sistemas de comunicaciones y servidores	A	0.5	1	2	5
Firewall	Servidor proxy de filtrado de navegación de Internet	A	0.5	1	2	12
Infraestructura de red	Redes LAN, Enlace de datos y redes WLAN	A	0.5	1	2	12
Antivirus	Servidor de actualización de base de datos para alerta de amenazas	A	1	2	4	8

De la tabla anterior se puede concluir que para recuperar el negocio ante un evento disruptivo, se deben restaurar diez recursos o servicios tecnológicos, cada uno de estos recursos está asociado a uno o más procesos críticos de la organización (resultados Tabla 11), por ende se afirma una vez más, que mejorar la continuidad del departamento de tecnología de Laboratorios Bagó es esencial para mantener las actividades del negocio.

El tiempo máximo (RTO) en que el departamento de tecnología deberá levantar un procesó crítico es de 5 horas, esto corresponde al servicio de *Gestión Hipervisor vCenter*, ya que en este corren todos los servidores virtuales de la organización. Por otro lado, para el mismo servicio el tiempo máximo tolerable de pérdida de información (RPO) es de 8 horas, es decir se puede recurrir a un respaldo de 8 horas atrás para recuperar el servicio.

Análisis de Riesgos. Como sabemos nuestro país es altamente susceptible a eventos inesperados relacionados con amenazas de origen natural, por lo cual se deben tomar las medidas pertinentes para evitar, mitigar, transferir o asumir los riesgos que se presenten. En este apartado se identifican las amenazas que podrían afectar a los activos de la organización y su probabilidad de ocurrencia, las vulnerabilidades asociadas a los mismos y el impacto que las amenazas podrían provocar a la disponibilidad de los activos.

Según (Centro Criptológico Nacional, 2017), se realizará el análisis de riesgos basado en la metodología MAGERIT y con la ayuda de la herramienta de software EAR/PILAR[5], donde siguiendo la metodología mencionada, de forma cualitativa se identificarán y evaluarán los activos, así como las amenazas no solo

[5] EAR/PILAR, dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como ISO/IEC 27002 (2005, 2013) - Código de buenas prácticas para la Gestión de la Seguridad de la Información.

origen natural sino todas las que se asocian con el negocio y que afecten a los recursos críticos de la empresa. Las figuras mostradas en los siguientes apartados son los resultados brindados por EAR/PILAR.

Análisis de riesgos > activos > Identificación de activos. Una vez seleccionadas las actividades críticas de la organización en el BIA se va a identificar y valorar los activos asociados a estas actividades o procesos, además se evaluarán las amenazas sobre los activos identificados.

En la Tabla 14 se muestran los activos que soportan las actividades de negocio de la organización, los mismos que fueron ingresados en la herramienta EAR/PILAR.

Tabla 14

Identificación de activos de la empresa.

Código	Nombre	Tipo	Descripción y servicios	Responsable	Ubicación
S000	CHASIS H	Físico	VCENTER ESX/ESXi Gestor de máquinas virtuales	SISTEMAS (IT)	DATA CENTER
S001	DATABASE_V1	Virtual	Servidor de base de datos Oracle 12c	SISTEMAS (IT)	DATA CENTER
S002	ELEARNING_V2	Virtual	Servidor e-learning Moodle	SISTEMAS (IT)	DATA CENTER
S003	FILESERVER_V3	Virtual	Servidor de archivos y ejecutables sistema DET y aplicaciones	SISTEMAS (IT)	DATA CENTER
S004	STORAGE_F1	Físico	Servidor de Almacenamiento	SISTEMAS (IT)	DATA CENTER
S005	BACKUP_F2	Físico	Servidor de respaldos de información	SISTEMAS (IT)	DATA CENTER
S006	PROXY_F3	Físico	Servidor intermedio entre la red interna y externa, Firewall, navegación segura en Internet	SISTEMAS (IT)	DATA CENTER
S007	SERVIDOR_F4	Físico	DHCP, DNS, ePO (McAfee antivirus ePolicy Orchestrator)	SISTEMAS (IT)	DATA CENTER

Código	Nombre	Tipo	Descripción y servicios	Responsable	Ubicación
S008	MS_V12	Virtual	Servidor para inteligencia de negocios MicroStrategy	SISTEMAS (IT)	DATA CENTER
S009	INTRA_V4	Virtual	Servidor Intranet corporativa brinda acceso a varios sistemas	SISTEMAS (IT)	DATA CENTER
S010	APP_V5	Virtual	Servidor de aplicaciones Tomcat (varios sistemas y aplicaciones web)	SISTEMAS (IT)	DATA CENTER
S011	MINUBE_V6	Virtual	Servidor de repositorio de archivos, nube privada, owncloud	SISTEMAS (IT)	DATA CENTER
S012	WEBSERVICES_V7	Virtual	Servidor de webservices que soportan a las aplicaciones móviles	SISTEMAS (IT)	DATA CENTER
S013	BARRACUDA_F5	Físico	Applience de seguridad de correo, antiSpam	SISTEMAS (IT)	DATA CENTER
S014	PWEB_V8	Virtual	Servidor de página web, CMS WordPress	SISTEMAS (IT)	DATA CENTER
S015	MAIL_V9	Virtual	Servidor de correo electrónico	SISTEMAS (IT)	DATA CENTER
S016	SMB_V10	Virtual	Servidor de dominio Samba, LDAP	SISTEMAS (IT)	DATA CENTER
S017	PRB_V11	Virtual	Servidor de pruebas (aplicaciones, base de datos, servicios)	SISTEMAS (IT)	DATA CENTER
PC001	PC_1	Físico	Equipos de cómputo para usuarios	USUARIOS	OFICINAS
W001	WIRELESS CONTROLER	Físico	Controladora para desplegar configuraciones Wireless	SISTEMAS (IT)	DATA CENTER
W002	ACCESS POINT	Físico	Infraestructura inalámbrica	SISTEMAS (IT)	OFICINAS
IMP001	IMPRESORAS	Físico	Dispositivos de Impresión	SISTEMAS (IT)	OFICINAS
TB001	TABLETS	Físico	Dispositivos móviles	USUARIOS	CAMPO
DC001	DATA CENTER	Físico	Centro de computo	SISTEMAS (IT)	OFICINAS
SW001	SWITCH CORE	Físico	Dispositivos de comunicación capa 3	SISTEMAS (IT)	DATA CENTER

Código	Nombre	Tipo	Descripción y servicios	Responsable	Ubicación
SW002	SWITCHES	Físico	Dispositivos de comunicación capa 2	SISTEMAS (IT)	OFICINAS
R002	ROUTER	Físico	Conexión entre redes de las sucursales	PROVEEDOR	OFICINAS
T001	TAPE	Físico	Grabador de cintas LT0	SISTEMAS (IT)	DATA CENTER
N001	NVR	Físico	Monitoreo cámaras IP	SISTEMAS (IT)	DATA CENTER
PBX001	PBX	Físico	Central Telefónica IP	SISTEMAS (IT)	DATA CENTER

Así mismo, se consideran como activos al talento humano gracias al cual la empresa sale a flote realizando sus actividades en todas las áreas, los códigos serán U001 para Usuarios y PIT001 para el personal de IT. También se consideran a las instalaciones del edificio donde realizan las operaciones los usuarios con el código OF001. Además, cabe recalcar que el activo más importante, la información, está implícita en los activos que manejan datos.

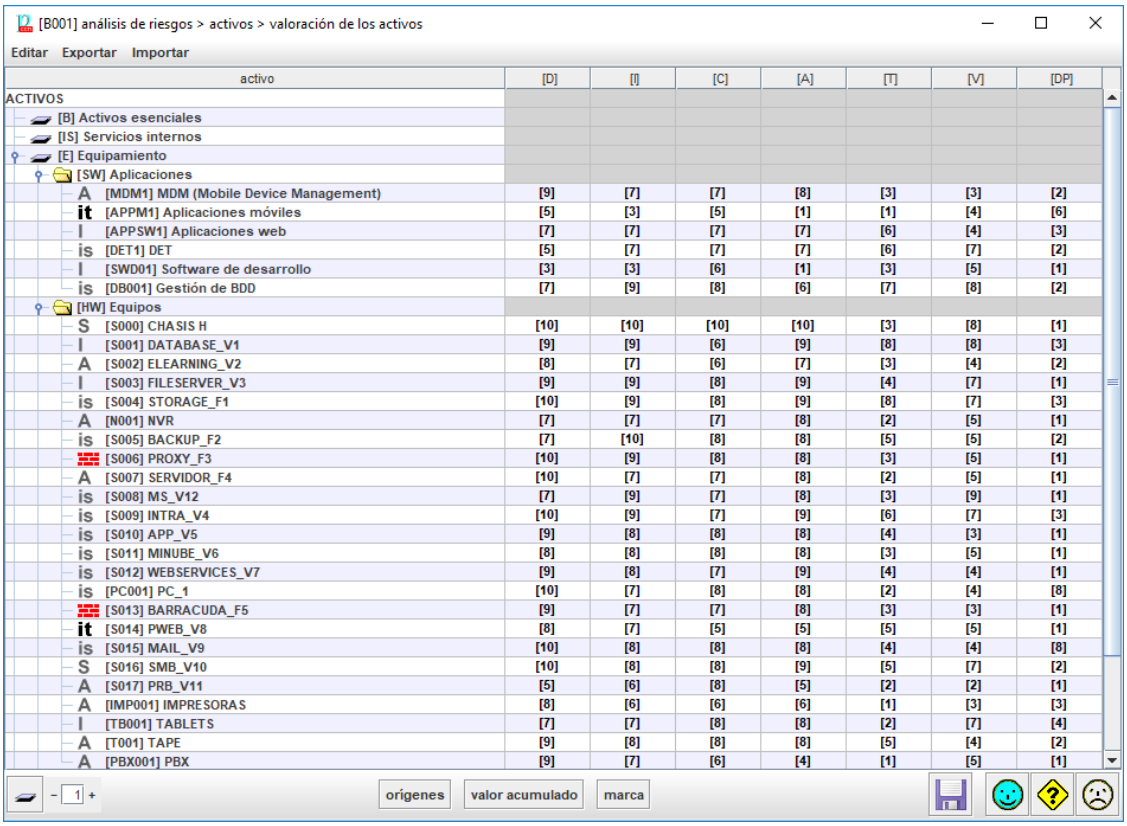
Análisis de riesgos > activos > valoración de activos. A continuación, en EAR/PILAR se valoran a los activos en siete dimensiones, disponibilidad [D], integridad [I], confidencialidad [C], autenticidad [A], trazabilidad [T], valor patrimonial o personal [V] y datos personales [DP], el rango usado va desde 0 a 10, siendo 0 el criterio de impacto despreciable y 10 el de mayor impacto, pasando por 5 de impacto medio. Además, si el activo no aplica en una dimensión se dejará en blanco. La valoración del activo va de acuerdo a su impacto para el negocio, es decir que tan importante es el activo para realizar un proceso esencial de la empresa.

La Figura 14 muestra la valoración de los activos de tipo [E] Equipamiento con respecto a [SW] Aplicaciones y [HW] Equipos.

La Figura 15 muestra la valoración de los activos de tipo [E] Equipamiento con respecto a [COM] Comunicaciones y [AUX] Elementos auxiliares, asimismo muestra la valoración de activos de tipo [L] Instalaciones.

Figura 14

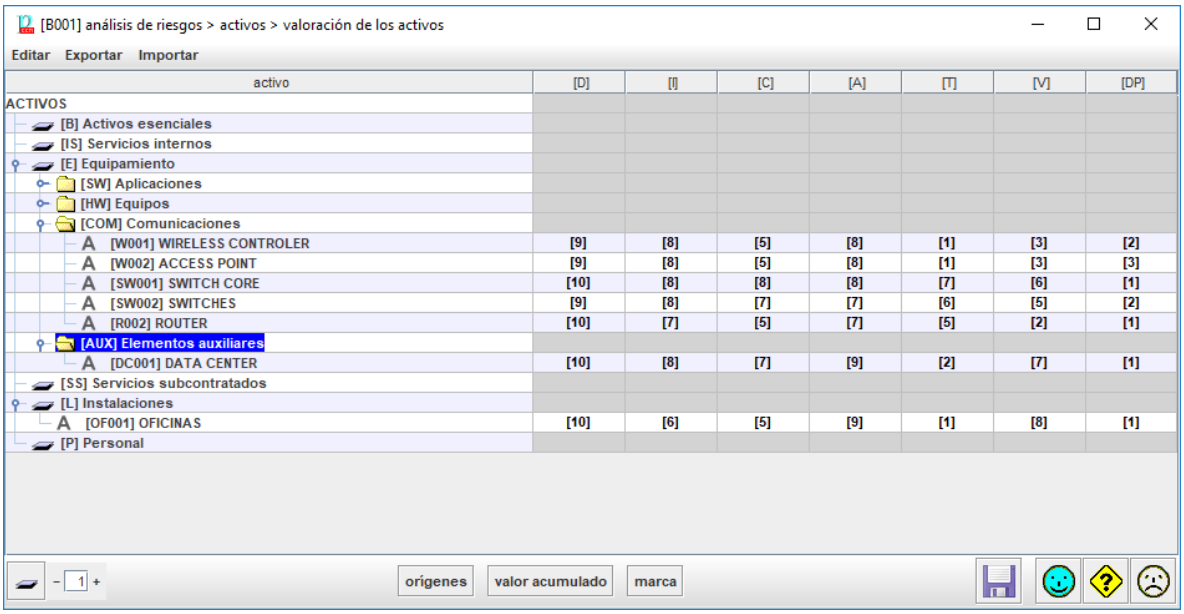
Equipamiento con respecto a software y equipos.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[MDM1] MDM (Mobile Device Management)	[9]	[7]	[7]	[8]	[3]	[3]	[2]
[APPM1] Aplicaciones móviles	[5]	[3]	[5]	[1]	[1]	[4]	[6]
[APPSW1] Aplicaciones web	[7]	[7]	[7]	[7]	[6]	[4]	[3]
[DET1] DET	[5]	[7]	[7]	[7]	[6]	[7]	[2]
[SWD01] Software de desarrollo	[3]	[3]	[6]	[1]	[3]	[5]	[1]
[DB001] Gestión de BDD	[7]	[9]	[8]	[6]	[7]	[8]	[2]
[HW] Equipos							
[S000] CHASIS H	[10]	[10]	[10]	[10]	[3]	[8]	[1]
[S001] DATABASE_V1	[9]	[9]	[6]	[9]	[8]	[8]	[3]
[S002] ELEARNING_V2	[8]	[7]	[6]	[7]	[3]	[4]	[2]
[S003] FILESERVER_V3	[9]	[9]	[8]	[9]	[4]	[7]	[1]
[S004] STORAGE_F1	[10]	[9]	[8]	[9]	[8]	[7]	[3]
[N001] NVR	[7]	[7]	[7]	[8]	[2]	[5]	[1]
[S005] BACKUP_F2	[7]	[10]	[8]	[8]	[5]	[5]	[2]
[S006] PROXY_F3	[10]	[9]	[8]	[8]	[3]	[5]	[1]
[S007] SERVIDOR_F4	[10]	[7]	[7]	[8]	[2]	[5]	[1]
[S008] MS_V12	[7]	[9]	[7]	[8]	[3]	[9]	[1]
[S009] INTRA_V4	[10]	[9]	[7]	[9]	[6]	[7]	[3]
[S010] APP_V5	[9]	[8]	[8]	[8]	[4]	[3]	[1]
[S011] MINUBE_V6	[8]	[8]	[8]	[8]	[3]	[5]	[1]
[S012] WEBSERVICES_V7	[9]	[8]	[7]	[9]	[4]	[4]	[1]
[PC001] PC_1	[10]	[7]	[8]	[8]	[2]	[4]	[8]
[S013] BARRACUDA_F5	[9]	[7]	[7]	[8]	[3]	[3]	[1]
[S014] PWEB_V8	[8]	[7]	[5]	[5]	[5]	[5]	[1]
[S015] MAIL_V9	[10]	[8]	[8]	[8]	[4]	[4]	[8]
[S016] SMB_V10	[10]	[8]	[8]	[9]	[5]	[7]	[2]
[S017] PRB_V11	[5]	[6]	[8]	[5]	[2]	[2]	[1]
[IMP001] IMPRESORAS	[8]	[6]	[6]	[6]	[1]	[3]	[3]
[TB001] TABLETS	[7]	[7]	[8]	[8]	[2]	[7]	[4]
[T001] TAPE	[9]	[8]	[8]	[8]	[5]	[4]	[2]
[PBX001] PBX	[9]	[7]	[6]	[4]	[1]	[5]	[1]

Figura 15

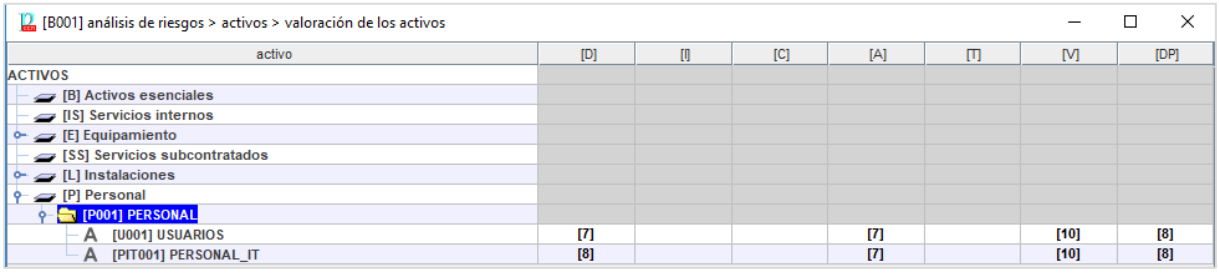
Equipamiento respecto a equipos de comunicaciones, elementos auxiliares e instalaciones.



La Figura 16 muestra la valoración de los activos dentro del tipo de activo [P] Personal.

Figura 16

Personal con respecto a usuarios y personal de tecnología.



En cada una de las figuras anteriores se puede apreciar el nivel de impacto de cada activo de la Tabla 14 en cada una de las dimensiones a la que aplica. Entonces se puede observar que los activos S000, S004, SS006, S007, S009, PC001, S015, S016, SW001, R002, DC001 y OF001 son los más críticos con relación a la disponibilidad (nivel 10), también se cataloga a los activos de tipo PERSONAL como los activos más valiosos dentro de la organización respecto a la dimensión [V].

Identificación de amenazas. Luego de la identificación y valoración de los activos se realiza la identificación de amenazas a las que es propenso cada activo de la organización. PILAR, de acuerdo a la naturaleza del activo realiza esta identificación automáticamente, correlaciona al activo con la amenaza gracias su catálogo. Las amenazas pueden ser de origen natural [N], industrial [I], humano (relacionado con errores no intencionados) [E], de origen intencionado relacionado con ataques [A] y también Riesgos de privacidad [PR].

Además, en esta valoración se incluye el porcentaje de consecuencias o efectos sobre las dimensiones al darse la materialización de la amenaza y la probabilidad en términos de frecuencia. Ver escalas en Figura 17 y Figura 18.

Figura 17

Tabla descriptiva de las consecuencias de la materialización de una amenaza.

nivel	porcentaje
T - total	100%
MA - muy alta	90%
A – alta	50%
M – media	10%
B – baja	1%

Nota. Tomado de *Cómo describir las consecuencias de la materialización de una amenaza* (p. 7), por Ayuda EAR/PILAR, 2018, https://www.pilar-tools.com/doc/v72/help_es_e_72.pdf

La Figura 18 indica las opciones de valoración de la probabilidad de materialización de amenazas, en este estudio se trabajará con la escala de *frecuencia* de ocurrencia, donde (0.01= cada cien años, 0.1 - 0.9= cada diez años, 1= una vez al año, 2 - 90= cada mes y 100= cada día).

Figura 18

Tabla descriptiva de la probabilidad de materialización de amenazas.

potencial	probabilidad	nivel	facilidad	frecuencia
XL extra grande	CS casi seguro	MA muy alto	F fácil	100
L grande	MA muy alta	A alto	M medio	10
M medio	P posible	M medio	D difícil	1
S pequeño	PP poco probable	B bajo	MD muy difícil	0,1
XS muy pequeño	MR muy rara	MB muy bajo	ED extremadamente difícil	0.01

Nota. Tomado de *Cómo describir la probabilidad de que se materialice una amenaza* (p. 6), por Ayuda EAR/PILAR, 2018, https://www.pilar-tools.com/doc/v72/help_es_e_72.pdf

A continuación, se presenta en las figuras el resultado de las amenazas asociadas con los activos críticos (nivel 10 en disponibilidad) determinados en el anterior apartado, el resto de activos están presentados en el Anexo C. En la Figura 19 se muestran las amenazas asociadas a los activos [S000] CHASIS H de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 19

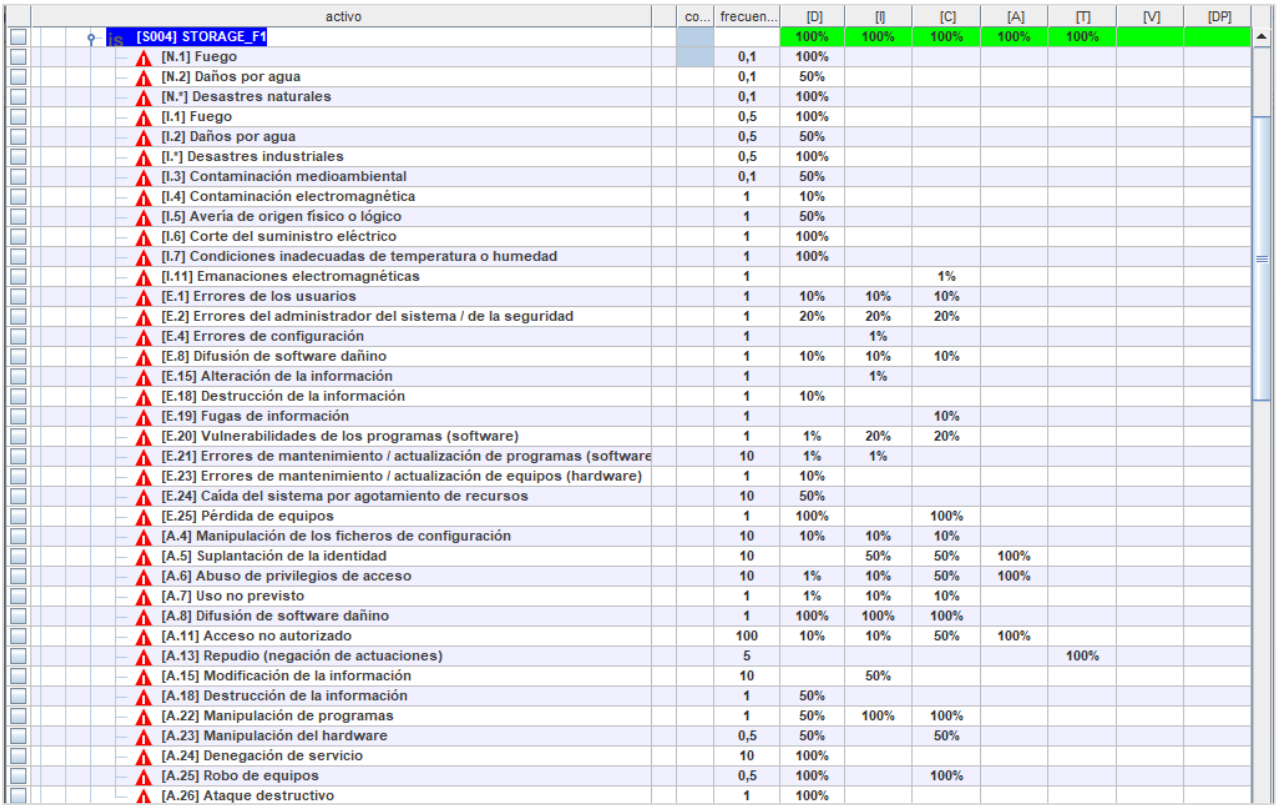
Amenazas asociadas a Equipamiento en Hardware Equipos, activo S000.

activo	co...	frecuencia	[D]	[I]	[C]	[A]
ACTIVOS						
[B] Activos esenciales						
[IS] Servicios internos						
[E] Equipamiento						
[SW] Aplicaciones						
[HW] Equipos						
[S000] CHASIS H			100%	100%	100%	
[N.1] Fuego		0,1	100%			
[N.2] Daños por agua		0,1	50%			
[N.*] Desastres naturales		0,1	100%			
[I.1] Fuego		0,5	100%			
[I.2] Daños por agua		0,5	50%			
[I.*] Desastres industriales		0,5	100%			
[I.3] Contaminación medioambiental		0,1	50%			
[I.4] Contaminación electromagnética		1	10%			
[I.5] Avería de origen físico o lógico		1	50%			
[I.6] Corte del suministro eléctrico		1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedac		1	100%			
[I.11] Emanaciones electromagnéticas		1			1%	
[E.8] Difusión de software dañino		1	10%	10%	10%	
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%	
[E.21] Errores de mantenimiento / actualización de progra		10	1%	1%		
[E.23] Errores de mantenimiento / actualización de equipo		1	10%			
[E.24] Caída del sistema por agotamiento de recursos		10	50%			
[E.25] Pérdida de equipos		0,1	100%		100%	
[A.7] Uso no previsto		1	1%	1%	10%	
[A.8] Difusión de software dañino		1	100%	100%	100%	
[A.11] Acceso no autorizado		1	10%	10%	50%	
[A.22] Manipulación de programas		1	50%	100%	100%	
[A.23] Manipulación del hardware		0,5	50%		50%	
[A.24] Denegación de servicio		2	100%			
[A.25] Robo de equipos		0,1	100%		100%	
[A.26] Ataque destructivo		1	100%			

En la Figura 20 se muestran las amenazas asociadas a los activos [S004] STORAGE_F1 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 20

Amenazas asociadas a Equipamiento en Hardware Equipos, activo S004.

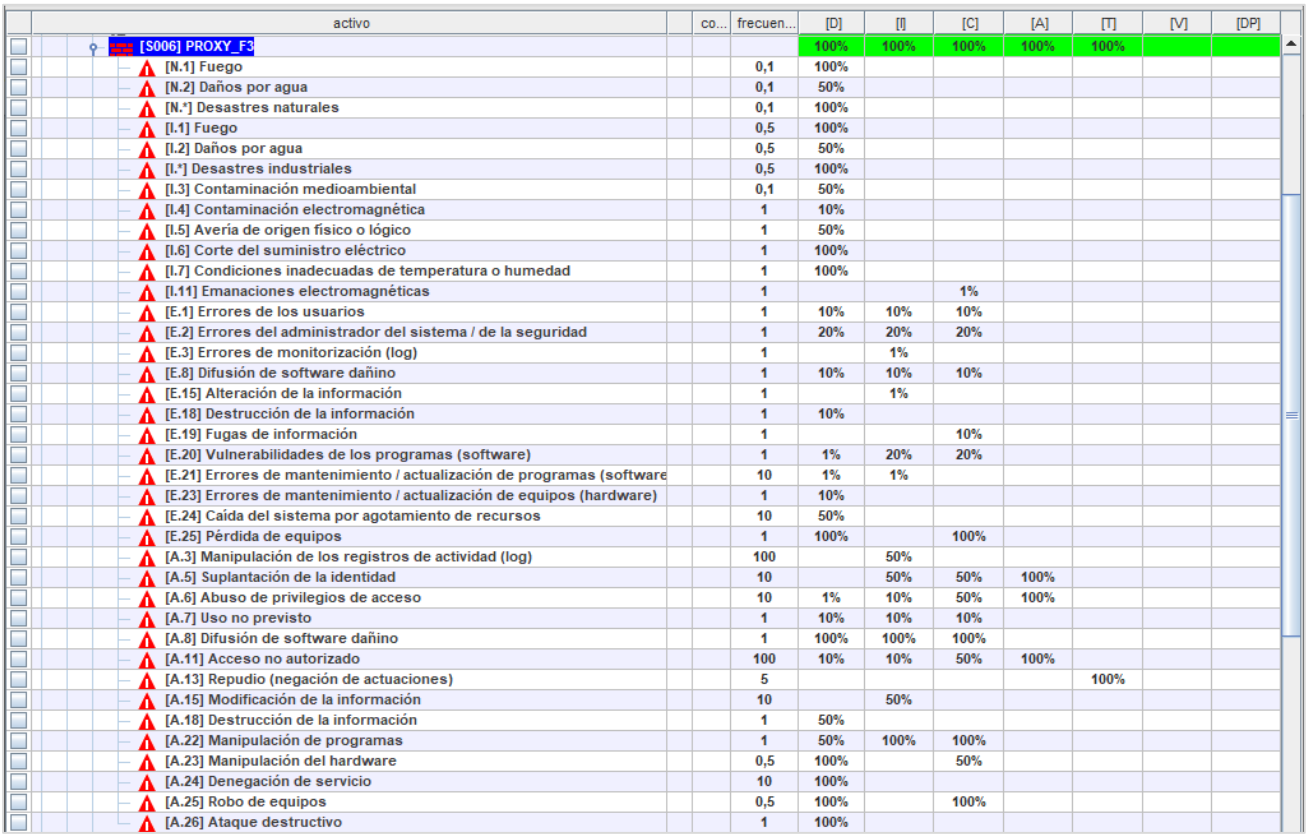


activo	co...	frecuen...	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[S004] STORAGE_F1			100%	100%	100%	100%	100%		
[N.1] Fuego		0,1	100%						
[N.2] Daños por agua		0,1	50%						
[N.*] Desastres naturales		0,1	100%						
[I.1] Fuego		0,5	100%						
[I.2] Daños por agua		0,5	50%						
[I.*] Desastres industriales		0,5	100%						
[I.3] Contaminación medioambiental		0,1	50%						
[I.4] Contaminación electromagnética		1	10%						
[I.5] Avería de origen físico o lógico		1	50%						
[I.6] Corte del suministro eléctrico		1	100%						
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%						
[I.11] Emanaciones electromagnéticas		1			1%				
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%				
[E.4] Errores de configuración		1		1%					
[E.8] Difusión de software dañino		1	10%	10%	10%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	10%						
[E.19] Fugas de información		1			10%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%				
[E.21] Errores de mantenimiento / actualización de programas (software		10	1%	1%					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%						
[E.24] Caída del sistema por agotamiento de recursos		10	50%						
[E.25] Pérdida de equipos		1	100%		100%				
[A.4] Manipulación de los ficheros de configuración		10	10%	10%	10%				
[A.5] Suplantación de la identidad		10		50%	50%	100%			
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	100%			
[A.7] Uso no previsto		1	1%	10%	10%				
[A.8] Difusión de software dañino		1	100%	100%	100%				
[A.11] Acceso no autorizado		100	10%	10%	50%	100%			
[A.13] Repudio (negación de actuaciones)		5					100%		
[A.15] Modificación de la información		10		50%					
[A.18] Destrucción de la información		1	50%						
[A.22] Manipulación de programas		1	50%	100%	100%				
[A.23] Manipulación del hardware		0,5	50%		50%				
[A.24] Denegación de servicio		10	100%						
[A.25] Robo de equipos		0,5	100%		100%				
[A.26] Ataque destructivo		1	100%						

En la Figura 21 se muestran las amenazas asociadas a los activos [S006] PROXY_F3 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 21

Amenazas asociadas a Equipamiento en Hardware Equipos, activo S006.

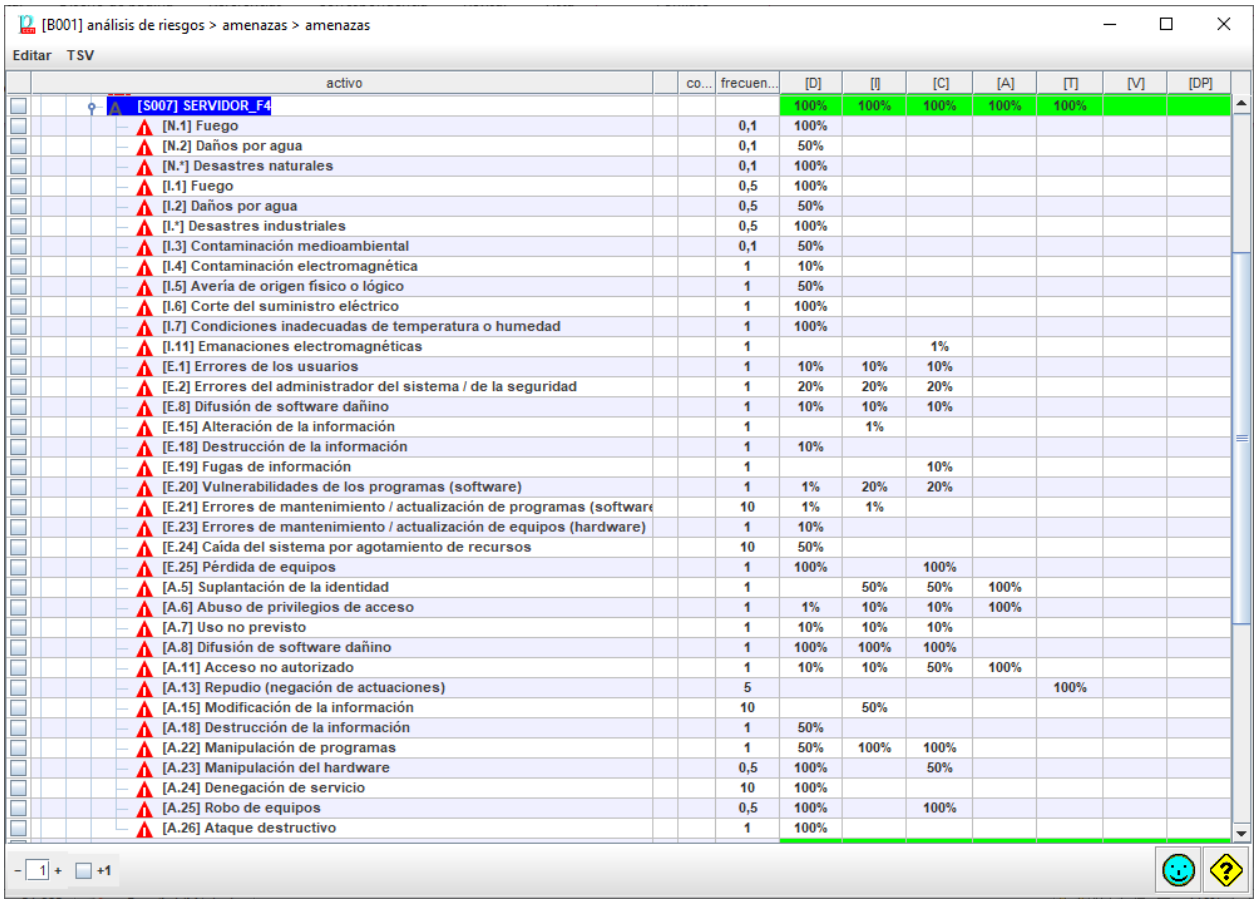


activo	co...	frecuen...	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[S006] PROXY_F3			100%	100%	100%	100%	100%		
[N.1] Fuego		0,1	100%						
[N.2] Daños por agua		0,1	50%						
[N.*] Desastres naturales		0,1	100%						
[I.1] Fuego		0,5	100%						
[I.2] Daños por agua		0,5	50%						
[I.*] Desastres industriales		0,5	100%						
[I.3] Contaminación medioambiental		0,1	50%						
[I.4] Contaminación electromagnética		1	10%						
[I.5] Avería de origen físico o lógico		1	50%						
[I.6] Corte del suministro eléctrico		1	100%						
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%						
[I.11] Emanaciones electromagnéticas		1			1%				
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%				
[E.3] Errores de monitorización (log)		1		1%					
[E.8] Difusión de software dañino		1	10%	10%	10%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	10%						
[E.19] Fugas de información		1			10%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%				
[E.21] Errores de mantenimiento / actualización de programas (software		10	1%	1%					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%						
[E.24] Caída del sistema por agotamiento de recursos		10	50%						
[E.25] Pérdida de equipos		1	100%		100%				
[A.3] Manipulación de los registros de actividad (log)		100		50%					
[A.5] Suplantación de la identidad		10		50%	50%	100%			
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	100%			
[A.7] Uso no previsto		1	10%	10%	10%				
[A.8] Difusión de software dañino		1	100%	100%	100%				
[A.11] Acceso no autorizado		100	10%	10%	50%	100%			
[A.13] Repudio (negación de actuaciones)		5					100%		
[A.15] Modificación de la información		10		50%					
[A.18] Destrucción de la información		1	50%						
[A.22] Manipulación de programas		1	50%	100%	100%				
[A.23] Manipulación del hardware		0,5	100%		50%				
[A.24] Denegación de servicio		10	100%						
[A.25] Robo de equipos		0,5	100%		100%				
[A.26] Ataque destructivo		1	100%						

En la Figura 22 se muestran las amenazas asociadas a los activos [S007] SERVIDOR_F4 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 22

Amenazas asociadas a Equipamiento en Hardware Equipos, activo S007.



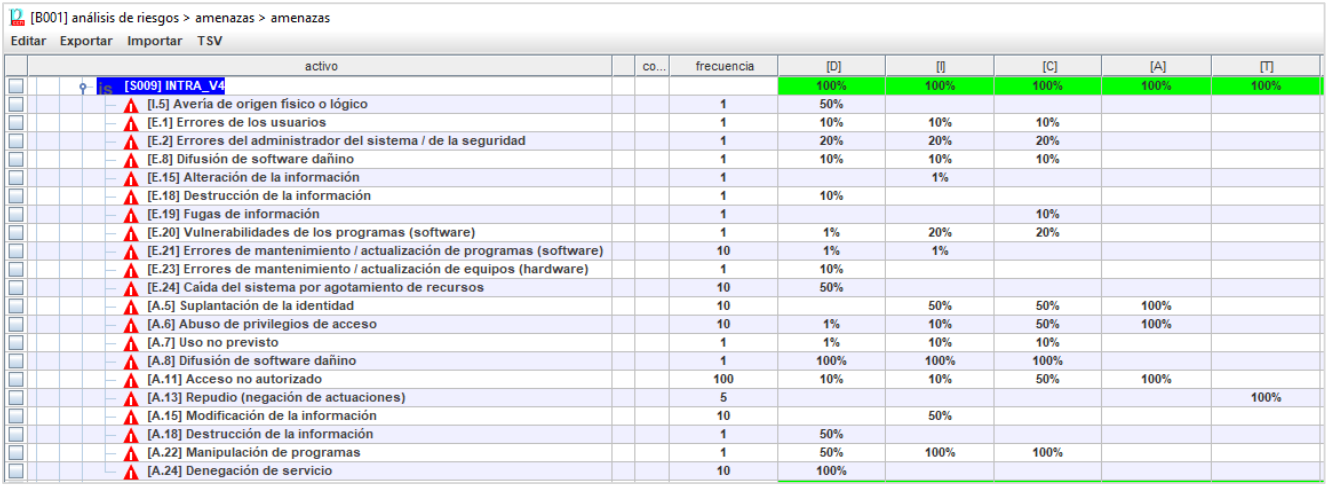
activo	co...	frecuen...	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[S007] SERVIDOR_F4			100%	100%	100%	100%	100%		
[N.1] Fuego		0,1	100%						
[N.2] Daños por agua		0,1	50%						
[N.*] Desastres naturales		0,1	100%						
[I.1] Fuego		0,5	100%						
[I.2] Daños por agua		0,5	50%						
[I.*] Desastres industriales		0,5	100%						
[I.3] Contaminación medioambiental		0,1	50%						
[I.4] Contaminación electromagnética		1	10%						
[I.5] Avería de origen físico o lógico		1	50%						
[I.6] Corte del suministro eléctrico		1	100%						
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%						
[I.11] Emanaciones electromagnéticas		1			1%				
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%				
[E.8] Difusión de software dañino		1	10%	10%	10%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	10%						
[E.19] Fugas de información		1			10%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%				
[E.21] Errores de mantenimiento / actualización de programas (software		10	1%	1%					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%						
[E.24] Caída del sistema por agotamiento de recursos		10	50%						
[E.25] Pérdida de equipos		1	100%		100%				
[A.5] Suplantación de la identidad		1		50%	50%	100%			
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%	100%			
[A.7] Uso no previsto		1	10%	10%	10%				
[A.8] Difusión de software dañino		1	100%	100%	100%				
[A.11] Acceso no autorizado		1	10%	10%	50%	100%			
[A.13] Repudio (negación de actuaciones)		5					100%		
[A.15] Modificación de la información		10		50%					
[A.18] Destrucción de la información		1	50%						
[A.22] Manipulación de programas		1	50%	100%	100%				
[A.23] Manipulación del hardware		0,5	100%		50%				
[A.24] Denegación de servicio		10	100%						
[A.25] Robo de equipos		0,5	100%		100%				
[A.26] Ataque destructivo		1	100%						

Como se puede ver en las figuras, de la 19 a la 22, los activos S000, S004, S006 y S007 son susceptibles a la materialización de amenazas que afectarían a su disponibilidad en mayor medida (frecuencia 1 con afectación a la disponibilidad de 100%) de: corte de suministro eléctrico, condiciones inadecuadas de temperatura y humedad, difusión de software dañino y ataque destructivo. También se puede apreciar que las amenazas de ataque [A.24] Denegación de servicio son las que con más frecuencia (10) se pueden dar y afectar en un 100% a la disponibilidad de los activos. Los activos analizados anteriormente también son propensos a sufrir amenazas de manipulación de programas que afecten a su integridad y confidencialidad en un 100%.

En la Figura 23 se muestran las amenazas asociadas a los activos [S009] INTRA_V4 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 23

Amenazas asociadas a Equipamiento en Hardware Equipos, activo S009.



[B001] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

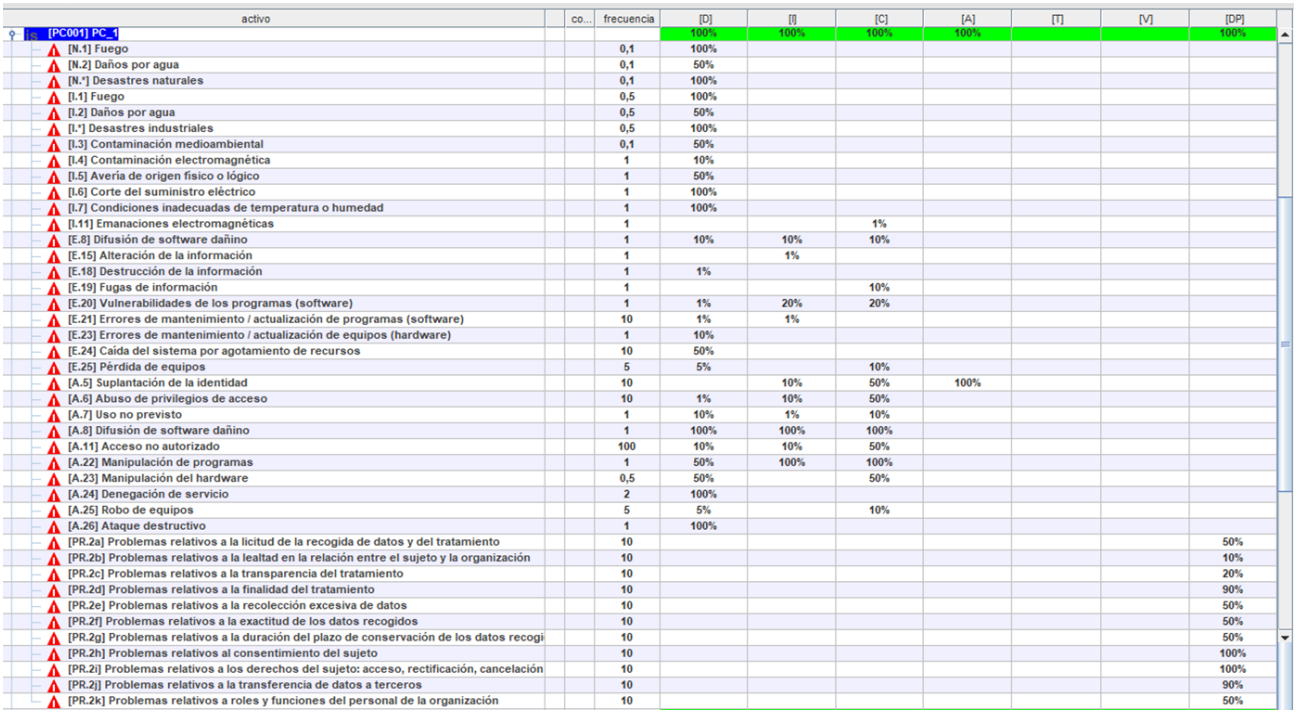
activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[S009] INTRA_V4			100%	100%	100%	100%	100%
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	10%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	10%				
[E.19] Fugas de información		1			10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.5] Suplantación de la identidad		10		50%	50%	100%	
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	100%	
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		100	10%	10%	50%	100%	
[A.13] Repudio (negación de actuaciones)		5					100%
[A.15] Modificación de la información		10		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%	100%		
[A.24] Denegación de servicio		10	100%				

El activo S009, es amenazado por suplantación de identidad y abuso de privilegios de acceso que afectaría a su autenticidad de manera mensual, también es susceptible a denegación de servicio y en mayor medida a accesos no autorizados con frecuencia de 100, es decir cada semana.

En la Figura 24 se muestran las amenazas asociadas a los activos [PC001] PC_01 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 24

Amenazas asociadas a Equipamiento en Hardware Equipos, activo PC001.



activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[PC001] PC_1			100%	100%	100%	100%			100%
[N.1] Fuego		0,1	100%						
[N.2] Daños por agua		0,1	50%						
[N.*] Desastres naturales		0,1	100%						
[I.1] Fuego		0,5	100%						
[I.2] Daños por agua		0,5	50%						
[I.*] Desastres industriales		0,5	100%						
[I.3] Contaminación medioambiental		0,1	50%						
[I.4] Contaminación electromagnética		1	10%						
[I.5] Avería de origen físico o lógico		1	50%						
[I.6] Corte del suministro eléctrico		1	100%						
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%						
[I.11] Emanaciones electromagnéticas		1			1%				
[E.8] Difusión de software dañino		1	10%	10%	10%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	1%						
[E.19] Fugas de información		1			10%				
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%				
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	1%					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%						
[E.24] Caída del sistema por agotamiento de recursos		10	50%						
[E.25] Pérdida de equipos		5	5%		10%				
[A.5] Suplantación de la identidad		10		10%	50%	100%			
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%				
[A.7] Uso no previsto		1	10%	1%	10%				
[A.8] Difusión de software dañino		1	100%	100%	100%				
[A.11] Acceso no autorizado		100	10%	10%	50%				
[A.22] Manipulación de programas		1	50%	100%	100%				
[A.23] Manipulación del hardware		0,5	50%		50%				
[A.24] Denegación de servicio		2	100%						
[A.25] Robo de equipos		5	5%		10%				
[A.26] Ataque destructivo		1	100%						
[PR.2a] Problemas relativos a la licitud de la recogida de datos y del tratamiento		10							50%
[PR.2b] Problemas relativos a la lealtad en la relación entre el sujeto y la organización		10							10%
[PR.2c] Problemas relativos a la transparencia del tratamiento		10							20%
[PR.2d] Problemas relativos a la finalidad del tratamiento		10							90%
[PR.2e] Problemas relativos a la recolección excesiva de datos		10							50%
[PR.2f] Problemas relativos a la exactitud de los datos recogidos		10							50%
[PR.2g] Problemas relativos a la duración del plazo de conservación de los datos recogi		10							50%
[PR.2h] Problemas relativos al consentimiento del sujeto		10							100%
[PR.2i] Problemas relativos a los derechos del sujeto: acceso, rectificación, cancelación		10							100%
[PR.2j] Problemas relativos a la transferencia de datos a terceros		10							90%
[PR.2k] Problemas relativos a roles y funciones del personal de la organización		10							50%

Las estaciones de trabajo PC001 son de los activos que más amenazas tienen, entre ellas amenazas de problemas relativos a la lealtad en la relación entre el sujeto y la organización, a los derechos del sujeto: acceso, rectificación, cancelación, y a la transferencia de datos a terceros.

En la Figura 25 se muestran las amenazas asociadas a los activos [S015] MAIL_V9 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 25

Amenazas asociadas a Equipamiento en Hardware Equipos, activo S015.

[B001] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[S010] APP_V5			100%	100%	100%	100%	
[S011] MINUBE_V6			100%	100%	100%	100%	100%
[S012] WEBSERVICES_V7			100%	100%	100%	100%	100%
[PC001] PC_1			100%	100%	100%	100%	
[S013] BARRACUDA_F5			100%	100%	100%	100%	100%
[S014] PWEB_V8			100%	100%	100%	100%	100%
[S015] MAIL_V9			100%	100%	100%	100%	100%
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	10%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	10%				
[E.19] Fugas de información		1			10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.5] Suplantación de la identidad		10		50%	50%	100%	
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	100%	
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		100	10%	10%	50%	100%	
[A.13] Repudio (negación de actuaciones)		5					100%
[A.15] Modificación de la información		10		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%	100%		
[A.24] Denegación de servicio		10	100%				

En la Figura 26 se muestran las amenazas asociadas a los activos [S016] SMB_V10 de tipo [E] Equipamiento con respecto a [HW] Equipos.

Figura 26

Amenazas asociadas a Equipamiento en Hardware Equipos, activo S016.

[B001] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

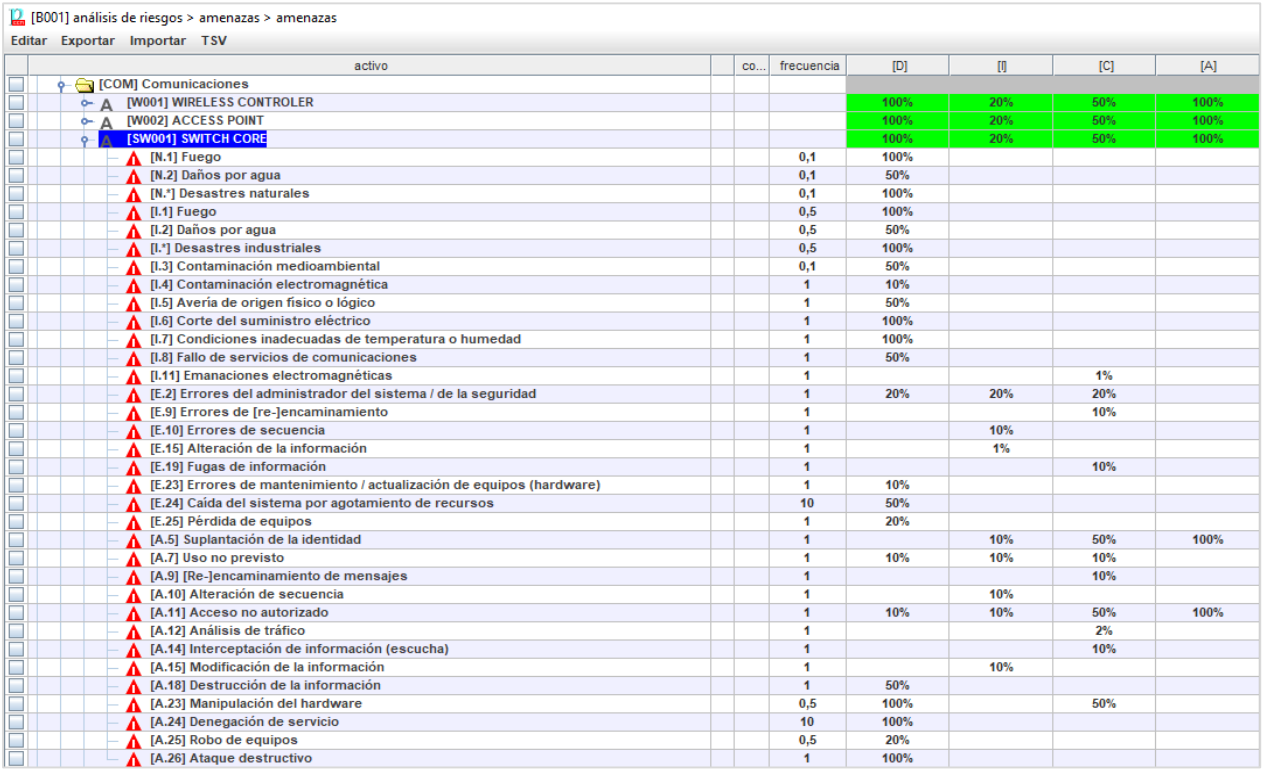
activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[S013] BARRACUDA_F5			100%	100%	100%	100%	100%
[S014] PWEB_V8			100%	100%	100%	100%	100%
[S015] MAIL_V9			100%	100%	100%	100%	100%
[S016] SMB_V10			100%	100%	100%	100%	100%
[I.5] Avería de origen físico o lógico		1	50%				
[E.1] Errores de los usuarios		1	10%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%		
[E.3] Errores de monitorización (log)		1		1%			
[E.4] Errores de configuración		1		1%			
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.15] Alteración de la información		1		1%			
[E.18] Destrucción de la información		1	10%				
[E.19] Fugas de información		1			10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.3] Manipulación de los registros de actividad (log)		100		50%			
[A.4] Manipulación de los ficheros de configuración		10	10%	10%	10%		
[A.5] Suplantación de la identidad		10		50%	50%	100%	
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	100%	
[A.7] Uso no previsto		1	1%	10%	10%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.11] Acceso no autorizado		100	10%	10%	50%	100%	
[A.13] Repudio (negación de actuaciones)		5					100%
[A.15] Modificación de la información		10		50%			
[A.18] Destrucción de la información		1	50%				
[A.22] Manipulación de programas		1	50%	100%	100%		
[A.24] Denegación de servicio		10	100%				

Los activos MAIL_V9 y SMB_V10 tienen frecuencia diaria de ataques de acceso no autorizado y mensualmente tiene riesgo de ataques de denegación de servicio, suplantación de identidad y abuso de privilegios de acceso.

En la Figura 27 se muestran las amenazas asociadas a los activos [SW001] SWITCH CORE de tipo [E] Equipamiento con respecto a [COM] Comunicaciones.

Figura 27

Amenazas asociadas a Equipamiento en Hardware Comunicaciones, activo SW001.



[B001] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

activo	co...	frecuencia	[D]	[I]	[C]	[A]
[COM] Comunicaciones						
[W001] WIRELESS CONTROLER			100%	20%	50%	100%
[W002] ACCESS POINT			100%	20%	50%	100%
[SW001] SWITCH CORE			100%	20%	50%	100%
[N.1] Fuego		0,1	100%			
[N.2] Daños por agua		0,1	50%			
[N.*] Desastres naturales		0,1	100%			
[I.1] Fuego		0,5	100%			
[I.2] Daños por agua		0,5	50%			
[I.*] Desastres industriales		0,5	100%			
[I.3] Contaminación medioambiental		0,1	50%			
[I.4] Contaminación electromagnética		1	10%			
[I.5] Avería de origen físico o lógico		1	50%			
[I.6] Corte del suministro eléctrico		1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%			
[I.8] Fallo de servicios de comunicaciones		1	50%			
[I.11] Emanaciones electromagnéticas		1			1%	
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%	
[E.9] Errores de [re-]encaminamiento		1			10%	
[E.10] Errores de secuencia		1		10%		
[E.15] Alteración de la información		1		1%		
[E.19] Fugas de información		1			10%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%			
[E.24] Caída del sistema por agotamiento de recursos		10	50%			
[E.25] Pérdida de equipos		1	20%			
[A.5] Suplantación de la identidad		1		10%	50%	100%
[A.7] Uso no previsto		1	10%	10%	10%	
[A.9] [Re-]encaminamiento de mensajes		1			10%	
[A.10] Alteración de secuencia		1		10%		
[A.11] Acceso no autorizado		1	10%	10%	50%	100%
[A.12] Análisis de tráfico		1			2%	
[A.14] Interceptación de información (escucha)		1			10%	
[A.15] Modificación de la información		1		10%		
[A.18] Destrucción de la información		1	50%			
[A.23] Manipulación del hardware		0,5	100%		50%	
[A.24] Denegación de servicio		10	100%			
[A.25] Robo de equipos		0,5	20%			
[A.26] Ataque destructivo		1	100%			

En la Figura 28 se muestran las amenazas asociadas a los activos [R002] ROUTER de tipo [E] Equipamiento con respecto a [COM] Comunicaciones.

Figura 28

Amenazas asociadas a Equipamiento en Hardware Comunicaciones, activo R002.

[B001] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

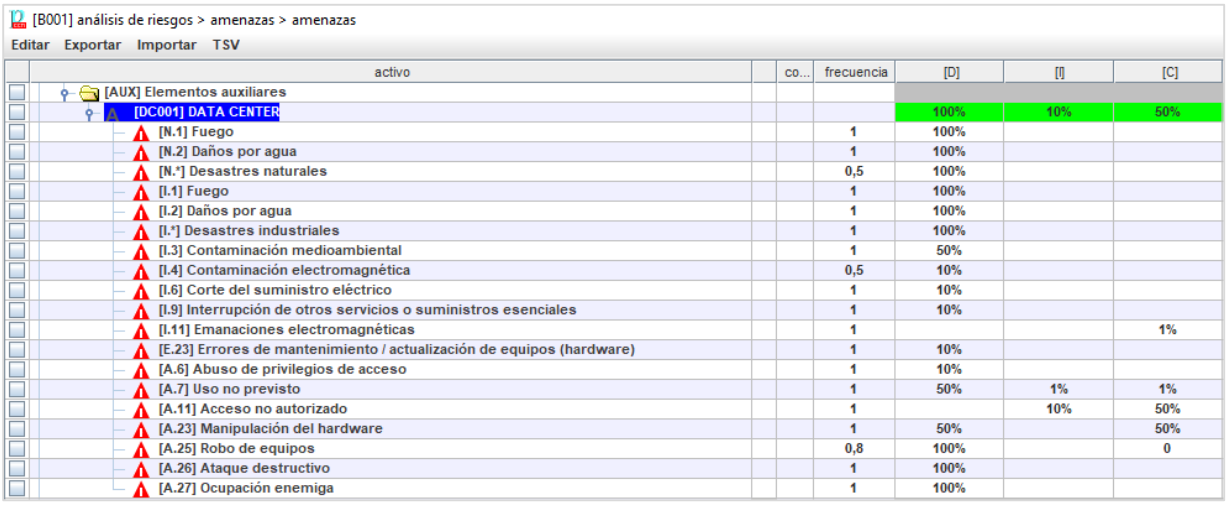
activo	co...	frecuencia	[D]	[I]	[C]	[A]
[R002] ROUTER			100%	20%	50%	100%
[N.1] Fuego		0,1	100%			
[N.2] Daños por agua		0,1	50%			
[N.*] Desastres naturales		0,1	100%			
[I.1] Fuego		0,5	100%			
[I.2] Daños por agua		0,5	50%			
[I.*] Desastres industriales		0,5	100%			
[I.3] Contaminación medioambiental		0,1	50%			
[I.4] Contaminación electromagnética		1	10%			
[I.5] Avería de origen físico o lógico		1	50%			
[I.6] Corte del suministro eléctrico		1	100%			
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%			
[I.8] Fallo de servicios de comunicaciones		1	50%			
[I.11] Emanaciones electromagnéticas		1			1%	
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%	
[E.9] Errores de [re-]encaminamiento		1			10%	
[E.10] Errores de secuencia		1		10%		
[E.15] Alteración de la información		1		1%		
[E.19] Fugas de información		1			10%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%			
[E.24] Caída del sistema por agotamiento de recursos		10	50%			
[E.25] Pérdida de equipos		1	20%			
[A.5] Suplantación de la identidad		1		10%	50%	100%
[A.7] Uso no previsto		1	10%	10%	10%	
[A.9] [Re-]encaminamiento de mensajes		1			10%	
[A.10] Alteración de secuencia		1		10%		
[A.11] Acceso no autorizado		1	10%	10%	50%	100%
[A.12] Análisis de tráfico		1			2%	
[A.14] Interceptación de información (escucha)		1			10%	
[A.15] Modificación de la información		1		10%		
[A.18] Destrucción de la información		1	50%			
[A.23] Manipulación del hardware		0,5	100%		50%	
[A.24] Denegación de servicio		10	100%			
[A.25] Robo de equipos		0,5	20%			
[A.26] Ataque destructivo		1	100%			

Los principales activos para comunicaciones SW001 y R002 tienen como amenazas más frecuentes, corte de suministro eléctrico, condiciones inadecuadas de humedad, suplantación de identidad, acceso no autorizado, denegación de servicio y ataque destructivo.

En la Figura 29 se muestran las amenazas asociadas a los activos [DC001] DATA CENTER de tipo [E] Equipamiento con respecto a [AUX] Elementos auxiliares.

Figura 29

Amenazas asociadas a Equipamiento en Hardware Elementos Auxiliares, activo DC001.

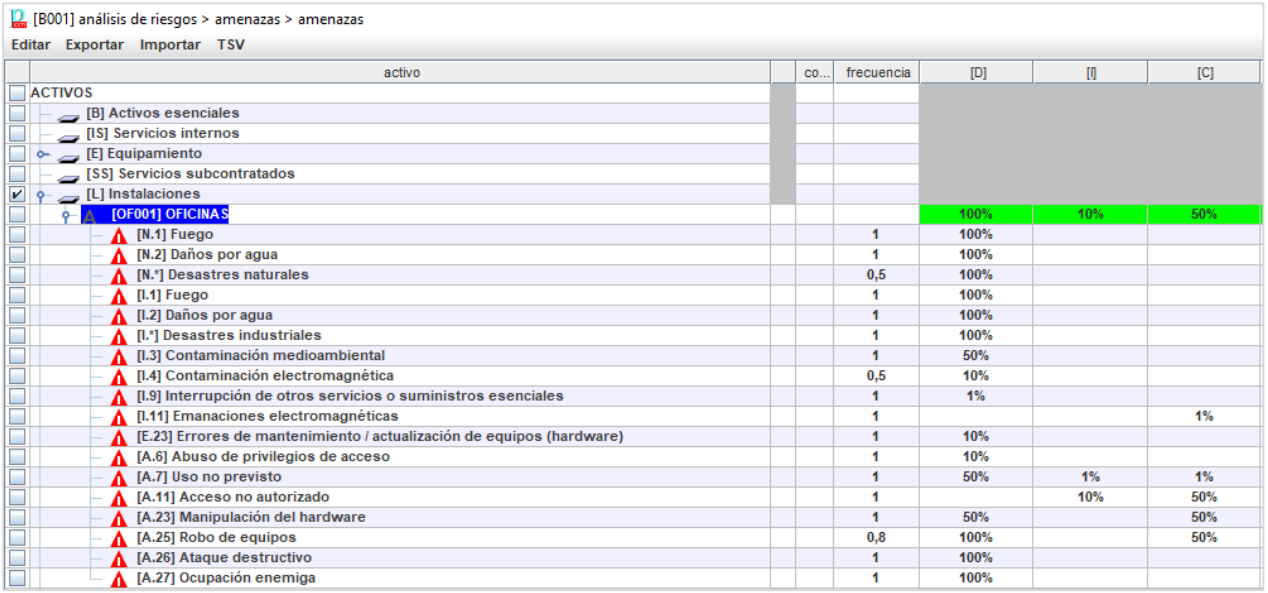


activo	co...	frecuencia	[D]	[I]	[C]
[AUX] Elementos auxiliares					
[DC001] DATA CENTER			100%	10%	50%
[N.1] Fuego		1	100%		
[N.2] Daños por agua		1	100%		
[N.*] Desastres naturales		0,5	100%		
[I.1] Fuego		1	100%		
[I.2] Daños por agua		1	100%		
[I.*] Desastres industriales		1	100%		
[I.3] Contaminación medioambiental		1	50%		
[I.4] Contaminación electromagnética		0,5	10%		
[I.6] Corte del suministro eléctrico		1	10%		
[I.9] Interrupción de otros servicios o suministros esenciales		1	10%		
[I.11] Emanaciones electromagnéticas		1			1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%		
[A.6] Abuso de privilegios de acceso		1	10%		
[A.7] Uso no previsto		1	50%	1%	1%
[A.11] Acceso no autorizado		1		10%	50%
[A.23] Manipulación del hardware		1	50%		50%
[A.25] Robo de equipos		0,8	100%		0
[A.26] Ataque destructivo		1	100%		
[A.27] Ocupación enemiga		1	100%		

En la Figura 30 se muestran las amenazas asociadas a los activos [OF001] OFICINAS de tipo [L] Instalaciones.

Figura 30

Amenazas asociadas Instalaciones, activo OF001.



activo	co...	frecuencia	[D]	[I]	[C]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SS] Servicios subcontratados					
[L] Instalaciones					
[OF001] OFICINAS			100%	10%	50%
[N.1] Fuego		1	100%		
[N.2] Daños por agua		1	100%		
[N.*] Desastres naturales		0,5	100%		
[I.1] Fuego		1	100%		
[I.2] Daños por agua		1	100%		
[I.*] Desastres industriales		1	100%		
[I.3] Contaminación medioambiental		1	50%		
[I.4] Contaminación electromagnética		0,5	10%		
[I.9] Interrupción de otros servicios o suministros esenciales		1	1%		
[I.11] Emanaciones electromagnéticas		1			1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%		
[A.6] Abuso de privilegios de acceso		1	10%		
[A.7] Uso no previsto		1	50%	1%	1%
[A.11] Acceso no autorizado		1		10%	50%
[A.23] Manipulación del hardware		1	50%		50%
[A.25] Robo de equipos		0,8	100%		50%
[A.26] Ataque destructivo		1	100%		
[A.27] Ocupación enemiga		1	100%		

Con respecto a las OFICINAS y DATA CENTER, las oficinas al contener al centro de cómputo comparten las mismas amenazas: fuego, daños por agua, desastres naturales e industriales, ataque destructivo y ocupación enemiga.

En la Figura 31 se muestran las amenazas asociadas a los activos [U001] USUARIOS y [PIT001] PERSONAL_IT de tipo [P] Personal.

Figura 31

Amenazas asociadas a Personal en activos U001 y PIT001.

[B001] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

activo	co...	frecuencia	[D]	[I]	[C]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					
[P001] PERSONAL					
[U001] USUARIOS			50%	100%	100%
[PIT001] PERSONAL_IT			50%	100%	100%
[E.15] Alteración de la información		1		10%	
[E.18] Destrucción de la información		1	1%		
[E.19] Fugas de información		1			10%
[E.28] Indisponibilidad del personal		1	20%		
[A.15] Modificación de la información		1		50%	
[A.18] Destrucción de la información		1	10%		
[A.19] Revelación de información		10			50%
[A.28] Indisponibilidad del personal		0,5	50%		
[A.29] Extorsión		0,9	50%	100%	100%
[A.30] Ingeniería social (picaresca)		1	50%	100%	100%

En lo referente al personal en la Figura 31 se puede observar que entre los ataques más frecuentes que afectan la integridad y confidencialidad se tiene, extorsión e ingeniería social con frecuencia anual.

Como se evidencia en las imágenes anteriores, EAR/PILAR realiza la correlación de las amenazas asociadas con los activos, esta correlación la realiza gracias a su catálogo que contiene información respecto a la naturaleza del activo y la asocia con la amenaza correspondiente.

Como resultado se tiene que las amenazas más recurrentes relacionadas a los activos físicos son: fuego, daños por agua, corte del suministro eléctrico y desastres naturales. En esta investigación se logró recabar

que a lo largo del funcionamiento de Laboratorios Bagó del Ecuador S. A. en sus nuevas instalaciones desde el año 2014, si se han materializado amenazas de inundaciones, corte de suministro eléctrico y sismos, sin embargo, el centro de cómputo no se ha visto perjudicado, lo que afortunadamente no ha afectado al desempeño de sus actividades, no obstante, los activos son susceptibles a interrupciones.

Ahora, como ejemplo se interpretan las amenazas a las que es susceptible el activo DATABASE_V2 (ver Anexo C), este activo está expuesto a la materialización de amenazas por fuego, daños por agua y desastres naturales cada 10 años, la ocurrencia de estas amenazas provocaría fallas al 100% de la disponibilidad, por otro lado es susceptible a caídas del sistema por agotamiento de recursos cada mes, esto significa que se puede llenar un disco duro durante ese período y no estar disponible, también es susceptible cada día a accesos no autorizados lo cual implicaría un 100% de afectación a la disponibilidad, integridad y confidencialidad de los datos.

Salvaguardas. Las salvaguardas son medidas técnicas y organizativas relacionadas a la seguridad de la información para hacerle frente a una amenaza. Para cada amenaza se va a aplicar una salvaguarda con el objetivo de minimizar la materialización de las mismas. Según (Ayuda EAR/PILAR, 2018), las métricas de las salvaguardas se catalogan en función de:

- Aspecto del que trata la salvaguarda (aspecto).
    - G para Gestión
    - T para Técnico
    - F para seguridad Física
    - P para gestión del Personal
- Tipo de protección (tdp) que proporciona la salvaguarda.
    - PR – prevención

  - DR – disuasión
  - EL – eliminación
  - IM – minimización del impacto
  - CR – corrección
  - RC – recuperación
  - AD – administrativa
  - AW – concienciación
  - DC – detección
  - MN – monitorización
  - std – norma
  - proc – procedimiento
  - cert – certificación o acreditación
- Nivel de madurez
  - L0 inexistente
  - L1 iniciado
  - L2 parcialmente realizado
  - L3 en funcionamiento
  - L4 monitorizado
  - L5 mejora continua
- Recomendación: Es una valoración en el rango de 0 a 10 estimada por PILAR, teniendo en cuenta el tipo de activos y su valoración en cada dimensión.
- Peso relativo de criticidad.

Figura 32

Peso relativo de criticidad.

3	máximo peso	crítica
2	peso alto	muy importante
1	peso normal	importante
0	peso bajo	interesante
✓	aseguramiento: componentes certificados	

Nota. Tomado de *Peso relativo* (p. 90), por Ayuda EAR/PILAR, 2018, https://www.pilar-tools.com/doc/v72/help_es_e_72.pdf

A continuación en la Figura 33 y Figura 34 se muestran las salvaguardas sugeridas por EAR/PILAR en función de: aspecto, tdp, recomendación, la criticidad para aplicar a los activos, la valoración de la recomendación, los niveles de madurez actual (columna *current*), nivel objetivo (columna *target*), y también rangos de niveles de madurez recomendados por la herramienta (columna PILAR).

El semáforo de la columna cuatro en las figuras muestra en un color si la madurez de la salvaguarda elegida es suficiente o no, y así poder tomar las acciones necesarias para aumentar el nivel de madurez en la organización. Los colores del semáforo se calculan usando 2 referencias.

VERDE: la madurez objetivo

- Clic derecho en la cabecera de la fase que desea usar como objetivo, la cabecera de la columna seleccionada se pinta en VERDE.

ROJA: la madurez evaluada

- Clic en la cabecera de la fase que se desea, la cabecera de la fase seleccionada se pinta en ROJO.

Usando esta información, PILAR asigna un color a la columna cuatro:

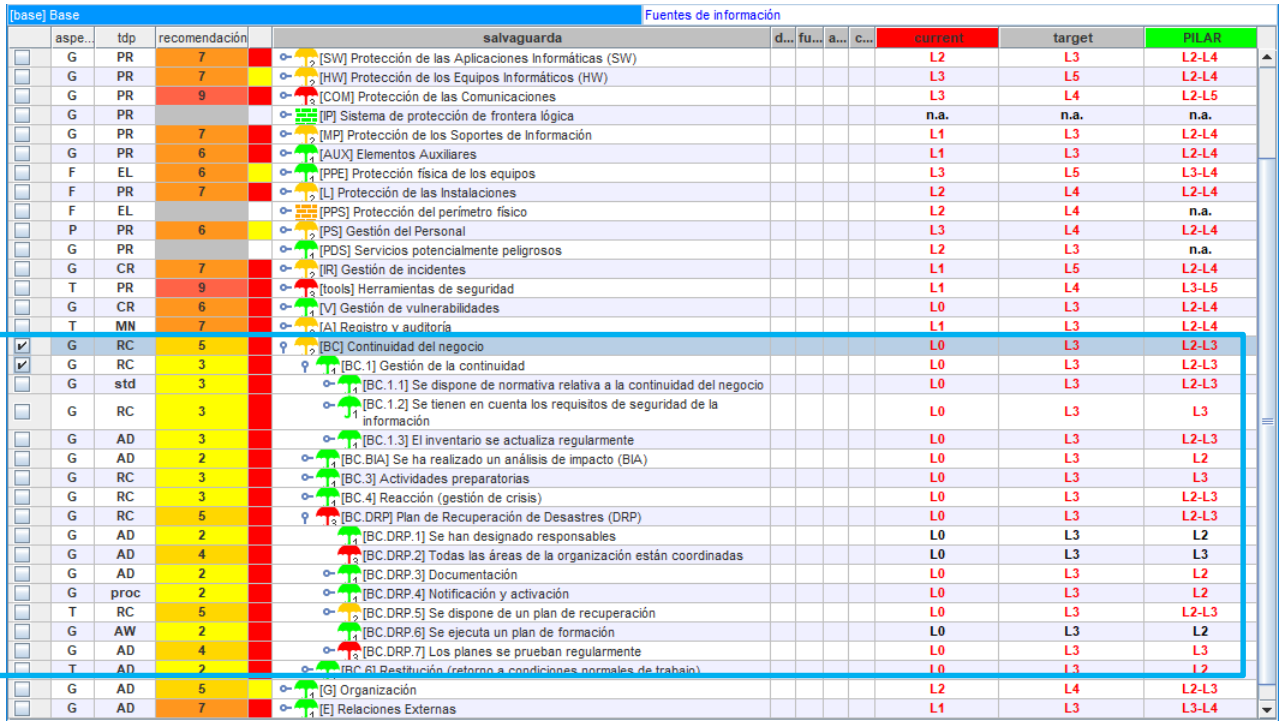
- AZUL si la madurez actual (ROJA) está por encima del objetivo(VERDE)

- VERDE si la madurez actual (ROJA) está a la altura del objetivo (VERDE)
- AMARILLO si la madurez actual (ROJA) está por debajo del objetivo (VERDE)
- ROJA si la madurez actual (ROJA) está muy por debajo del objetivo (VERDE)
- GRIS si la salvaguarda no es aplicable

En la Figura 33 se resalta la salvaguarda Continuidad de Negocio en su estado actual (*current*), con el aspecto G (para gestión), como tipo de protección RC (recuperación), el semáforo en la cuarta columna indica que tiene nivel de madurez actual es ROJA la cual está muy por debajo del objetivo que muestra la columna PILAR, y el nivel de criticidad es muy importante. Entonces, el nivel de madurez actual es L0 (inexistente) y se recomienda que se deba llegar a un nivel de madurez objetivo (*target*) de L3.

Figura 33

Salvaguardas con estado de madurez actual (columna roja current).

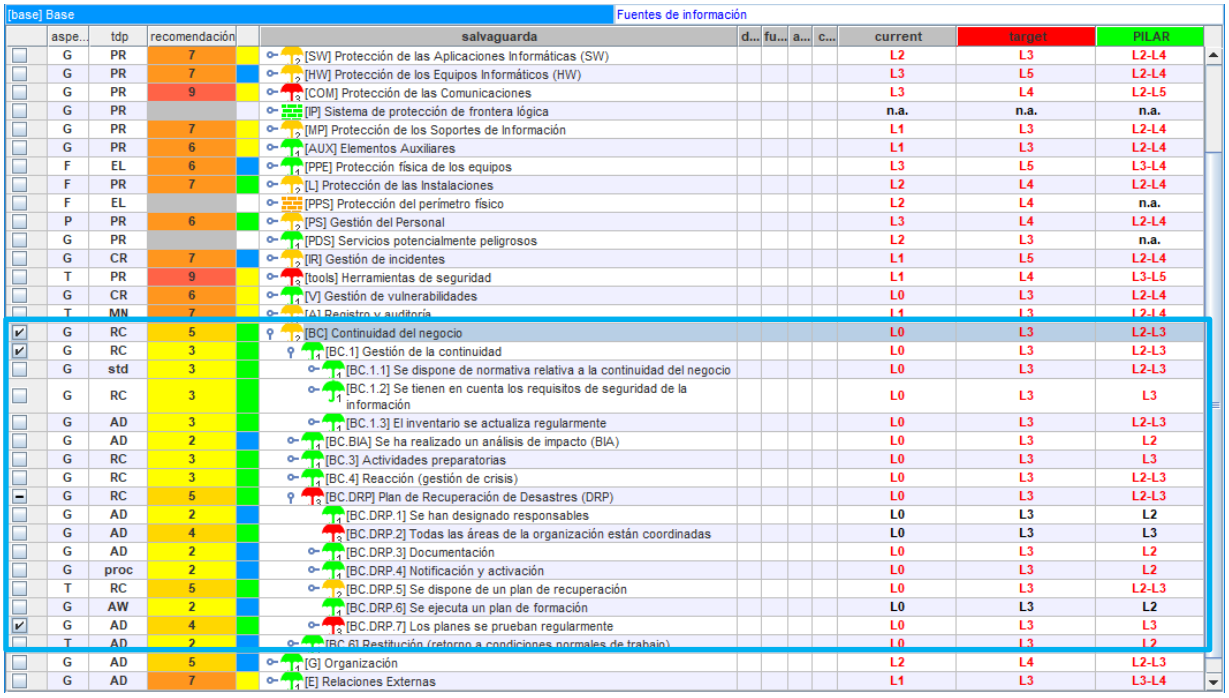


	aspe...	tdp	recomendación	salvaguarda	d...	fu...	a...	c...	current	target	PILAR
☐	G	PR	7	[SW] Protección de las Aplicaciones Informáticas (SW)					L2	L3	L2-L4
☐	G	PR	7	[HW] Protección de los Equipos Informáticos (HW)					L3	L5	L2-L4
☐	G	PR	9	[COM] Protección de las Comunicaciones					L3	L4	L2-L5
☐	G	PR		[IP] Sistema de protección de frontera lógica					n.a.	n.a.	n.a.
☐	G	PR	7	[MP] Protección de los Soportes de Información					L1	L3	L2-L4
☐	G	PR	6	[AUX] Elementos Auxiliares					L1	L3	L2-L4
☐	F	EL	6	[PPE] Protección física de los equipos					L3	L5	L3-L4
☐	F	PR	7	[L] Protección de las Instalaciones					L2	L4	L2-L4
☐	F	EL		[PPS] Protección del perímetro físico					L2	L4	n.a.
☐	P	PR	6	[PS] Gestión del Personal					L3	L4	L2-L4
☐	G	PR		[PDS] Servicios potencialmente peligrosos					L2	L3	n.a.
☐	G	CR	7	[IR] Gestión de incidentes					L1	L5	L2-L4
☐	T	PR	9	[tools] Herramientas de seguridad					L1	L4	L3-L5
☐	G	CR	6	[V] Gestión de vulnerabilidades					L0	L3	L2-L4
☐	T	MN	7	[A] Registro y auditoría					L1	L3	L2-L4
☑	G	RC	5	[BC] Continuidad del negocio					L0	L3	L2-L3
☑	G	RC	3	[BC.1] Gestión de la continuidad					L0	L3	L2-L3
☐	G	std	3	[BC.1.1] Se dispone de normativa relativa a la continuidad del negocio					L0	L3	L2-L3
☐	G	RC	3	[BC.1.2] Se tienen en cuenta los requisitos de seguridad de la información					L0	L3	L3
☐	G	AD	3	[BC.1.3] El inventario se actualiza regularmente					L0	L3	L2-L3
☐	G	AD	2	[BC.BIA] Se ha realizado un análisis de impacto (BIA)					L0	L3	L2
☐	G	RC	3	[BC.3] Actividades preparatorias					L0	L3	L3
☐	G	RC	3	[BC.4] Reacción (gestión de crisis)					L0	L3	L2-L3
☐	G	RC	5	[BC.DRP] Plan de Recuperación de Desastres (DRP)					L0	L3	L2-L3
☐	G	AD	2	[BC.DRP.1] Se han designado responsables					L0	L3	L2
☐	G	AD	4	[BC.DRP.2] Todas las áreas de la organización están coordinadas					L0	L3	L3
☐	G	AD	2	[BC.DRP.3] Documentación					L0	L3	L2
☐	G	proc	2	[BC.DRP.4] Notificación y activación					L0	L3	L2
☐	T	RC	5	[BC.DRP.5] Se dispone de un plan de recuperación					L0	L3	L2-L3
☐	G	AW	2	[BC.DRP.6] Se ejecuta un plan de formación					L0	L3	L2
☐	G	AD	4	[BC.DRP.7] Los planes se prueban regularmente					L0	L3	L3
☐	T	AD	2	[BC.6] Restitución (retorno a condiciones normales de trabajo)					L0	L3	L2
☐	G	AD	5	[G] Organización					L2	L4	L2-L3
☐	G	AD	7	[E] Relaciones Externas					L1	L3	L3-L4

La Figura 34 muestra la salvaguarda Continuidad de Negocio objetivo (*target*) con el semáforo en la cuarta columna de color VERDE el cual indica la madurez objetiva está a la altura de la recomendación en la columna PILAR. Es decir que aplicando las salvaguardas necesarias sobre las amenazas se logrará tener un nivel de madurez L3.

Figura 34

Salvaguardas con estado de madurez objetivo (columna roja target).



[base] Base — Fuentes de información

	aspe...	tdp	recomendación	salvaguarda	d...	fu...	a...	c...	current	target	PILAR
☐	G	PR	7	[SW] Protección de las Aplicaciones Informáticas (SW)					L2	L3	L2-L4
☐	G	PR	7	[HW] Protección de los Equipos Informáticos (HW)					L3	L5	L2-L4
☐	G	PR	9	[COM] Protección de las Comunicaciones					L3	L4	L2-L5
☐	G	PR		[IP] Sistema de protección de frontera lógica					n.a.	n.a.	n.a.
☐	G	PR	7	[MP] Protección de los Soportes de Información					L1	L3	L2-L4
☐	G	PR	6	[AUX] Elementos Auxiliares					L1	L3	L2-L4
☐	F	EL	6	[PPE] Protección física de los equipos					L3	L5	L3-L4
☐	F	PR	7	[L] Protección de las Instalaciones					L2	L4	L2-L4
☐	F	EL		[PPS] Protección del perímetro físico					L2	L4	n.a.
☐	P	PR	6	[PS] Gestión del Personal					L3	L4	L2-L4
☐	G	PR		[PDS] Servicios potencialmente peligrosos					L2	L3	n.a.
☐	G	CR	7	[IR] Gestión de incidentes					L1	L5	L2-L4
☐	T	PR	9	[tools] Herramientas de seguridad					L1	L4	L3-L5
☐	G	CR	6	[V] Gestión de vulnerabilidades					L0	L3	L2-L4
☐	T	MN	7	[A] Registro y auditoría					L1	L3	L2-L4
☑	G	RC	5	[BC] Continuidad del negocio					L0	L3	L2-L3
☑	G	RC	3	[BC.1] Gestión de la continuidad					L0	L3	L2-L3
☐	G	std	3	[BC.1.1] Se dispone de normativa relativa a la continuidad del negocio					L0	L3	L2-L3
☐	G	RC	3	[BC.1.2] Se tienen en cuenta los requisitos de seguridad de la información					L0	L3	L3
☐	G	AD	3	[BC.1.3] El inventario se actualiza regularmente					L0	L3	L2-L3
☐	G	AD	2	[BC.BIA] Se ha realizado un análisis de impacto (BIA)					L0	L3	L2
☐	G	RC	3	[BC.3] Actividades preparatorias					L0	L3	L3
☐	G	RC	3	[BC.4] Reacción (gestión de crisis)					L0	L3	L2-L3
☐	G	RC	5	[BC.DRP] Plan de Recuperación de Desastres (DRP)					L0	L3	L2-L3
☐	G	AD	2	[BC.DRP.1] Se han designado responsables					L0	L3	L2
☐	G	AD	4	[BC.DRP.2] Todas las áreas de la organización están coordinadas					L0	L3	L3
☐	G	AD	2	[BC.DRP.3] Documentación					L0	L3	L2
☐	G	proc	2	[BC.DRP.4] Notificación y activación					L0	L3	L2
☐	T	RC	5	[BC.DRP.5] Se dispone de un plan de recuperación					L0	L3	L2-L3
☐	G	AW	2	[BC.DRP.6] Se ejecuta un plan de formación					L0	L3	L2
☑	G	AD	4	[BC.DRP.7] Los planes se prueban regularmente					L0	L3	L3
☐	T	AD	2	[BC.6] Restitución (retorno a condiciones normales de trabajo)					L0	L3	L2
☐	G	AD	5	[G] Organización					L2	L4	L2-L3
☐	G	AD	7	[E] Relaciones Externas					L1	L3	L3-L4

Como resultado de este el análisis de riesgos y las salvaguardas en las figuras anteriores, se puede evidenciar que el estado actual de madurez con respecto a la continuidad del negocio es inexistente (L0), además indica que: el aspecto es de gestión, tipo de protección recuperación, con recomendación 5 y semáforo en color rojo, lo que quiere decir que está por debajo de los niveles de las recomendaciones ideales. Asimismo, se puede observar que dentro de la salvaguarda de continuidad de negocio tiene un

peso crítico el Plan de Recuperación de Desastres (DRP), el cual ayuda a mantener y coordinar actividades para recuperar la infraestructura tecnológica.

Por lo tanto, la implementación del plan de continuidad para Laboratorios Bagó del Ecuador S.A. ayudará a que se aumente el nivel de madurez a L3 (en funcionamiento) y a semáforo verde, y así estar por encima de los niveles recomendables con respecto a la salvaguarda de continuidad de negocio. Ver más salvaguardas en Anexo D.

Impacto y Riesgo. En esta etapa se verá el resultado del impacto y el riesgo acumulados que afectan a cada grupo de activos. El impacto se define como la medida del daño sobre un activo cuando se materializa una amenaza. Por otro lado, el riesgo es la medida de un daño probable sobre un activo o sistema. El riesgo crece con el impacto y la probabilidad de ocurrencia.

La Figura 35 y Nota. Tomado de *Escala nominal del impacto*, por EAR/PILAR, 2018, Software µPILAR.

Figura 36 indican las escalas nominales de impacto y riesgo respectivamente. Las escalas son extraídas de (Ayuda EAR/PILAR, 2018).

Figura 35

Escala nominal del impacto.

Nota. Tomado de *Escala nominal del impacto*, por EAR/PILAR, 2018, Software µPILAR.

Figura 36

Escala nominal del riesgo. Niveles de criticidad.

Nota. Tomado de *Niveles de criticidad – Código de colores* (p. 109), por Ayuda EAR/PILAR, 2018, https://www.pilar-tools.com/doc/v72/help_es_e_72.pdf

- Impacto acumulado

Este impacto se calcula tomando en cuenta el valor acumulado, es decir el valor del activo más el valor de los activos que dependen de él, además se consideran las amenazas a las que está expuesto.

A continuación en las Figura 37 y Figura 38 se muestran los resultados del nivel de impacto para los activos de la organización calculados por PILAR.

Figura 37

Impacto acumulado: Equipamiento, Aplicaciones y Equipos.

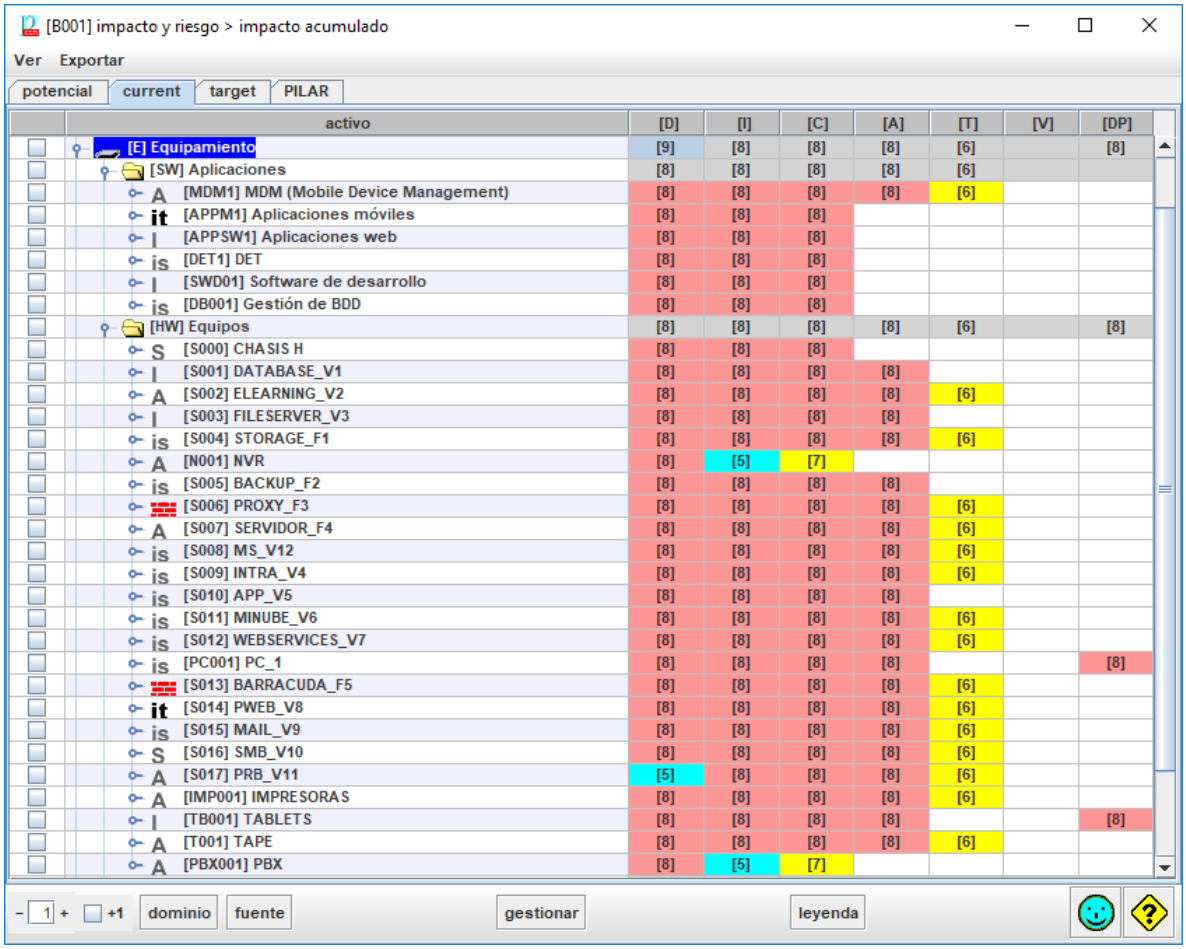
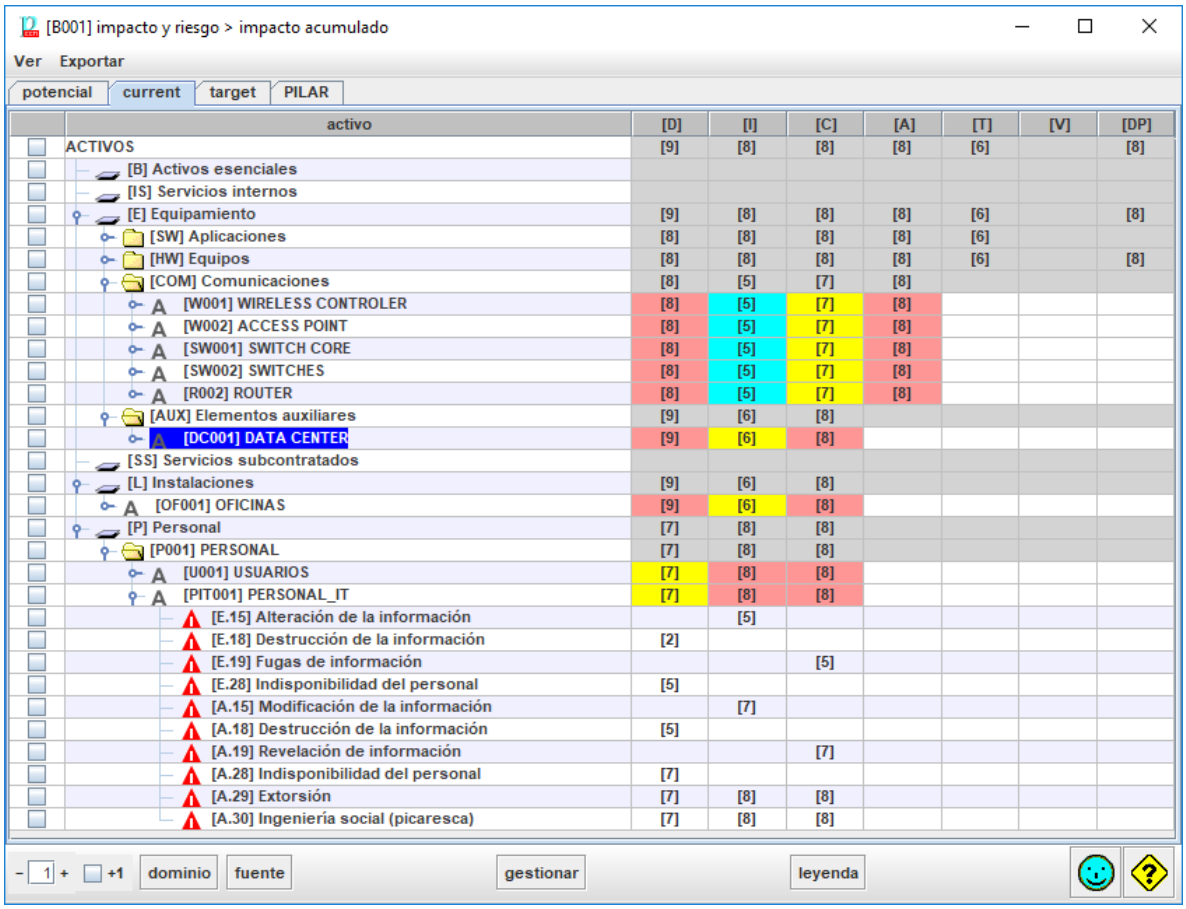


Figura 38

Impacto acumulado: Equipamiento, Comunicaciones, Elementos auxiliares y Personal.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[9]	[8]	[8]	[8]	[6]		[8]
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	[9]	[8]	[8]	[8]	[6]		[8]
[SW] Aplicaciones	[8]	[8]	[8]	[8]	[6]		
[HW] Equipos	[8]	[8]	[8]	[8]	[6]		[8]
[COM] Comunicaciones	[8]	[5]	[7]	[8]			
[W001] WIRELESS CONTROLER	[8]	[5]	[7]	[8]			
[W002] ACCESS POINT	[8]	[5]	[7]	[8]			
[SW001] SWITCH CORE	[8]	[5]	[7]	[8]			
[SW002] SWITCHES	[8]	[5]	[7]	[8]			
[R002] ROUTER	[8]	[5]	[7]	[8]			
[AUX] Elementos auxiliares	[9]	[6]	[8]				
[DC001] DATA CENTER	[9]	[6]	[8]				
[SS] Servicios subcontratados							
[L] Instalaciones	[9]	[6]	[8]				
[OF001] OFICINAS	[9]	[6]	[8]				
[P] Personal	[7]	[8]	[8]				
[P001] PERSONAL	[7]	[8]	[8]				
[U001] USUARIOS	[7]	[8]	[8]				
[PIT001] PERSONAL_IT	[7]	[8]	[8]				
[E.15] Alteración de la información		[5]					
[E.18] Destrucción de la información	[2]						
[E.19] Fugas de información			[5]				
[E.28] Indisponibilidad del personal	[5]						
[A.15] Modificación de la información		[7]					
[A.18] Destrucción de la información	[5]						
[A.19] Revelación de información			[7]				
[A.28] Indisponibilidad del personal	[7]						
[A.29] Extorsión	[7]	[8]	[8]				
[A.30] Ingeniería social (picaresca)	[7]	[8]	[8]				

Como resultado del análisis podemos observar en las figuras anteriores que el nivel de impacto predominante en los activos es el 8, es decir que el nivel actual de impacto al materializarse una amenaza es alto.

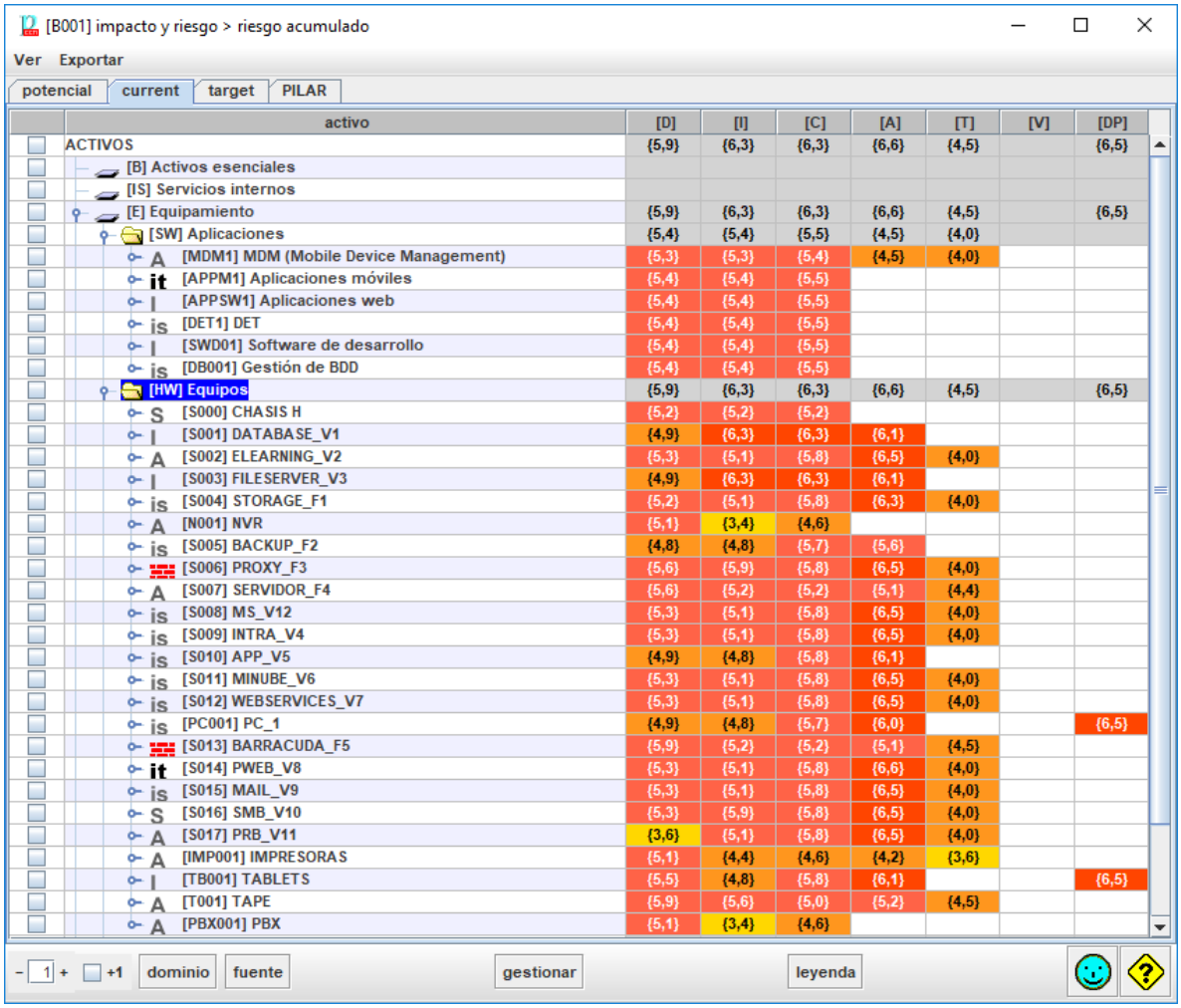
- Riesgo acumulado

Este riesgo es calculado sobre un activo teniendo en cuenta el impacto acumulado debido a una amenaza y a la probabilidad de ocurrencia de la misma. La

Figura 39 y Figura 40 muestran el resultado del riesgo acumulado de los activos de la organización calculados por PILAR.

Figura 39

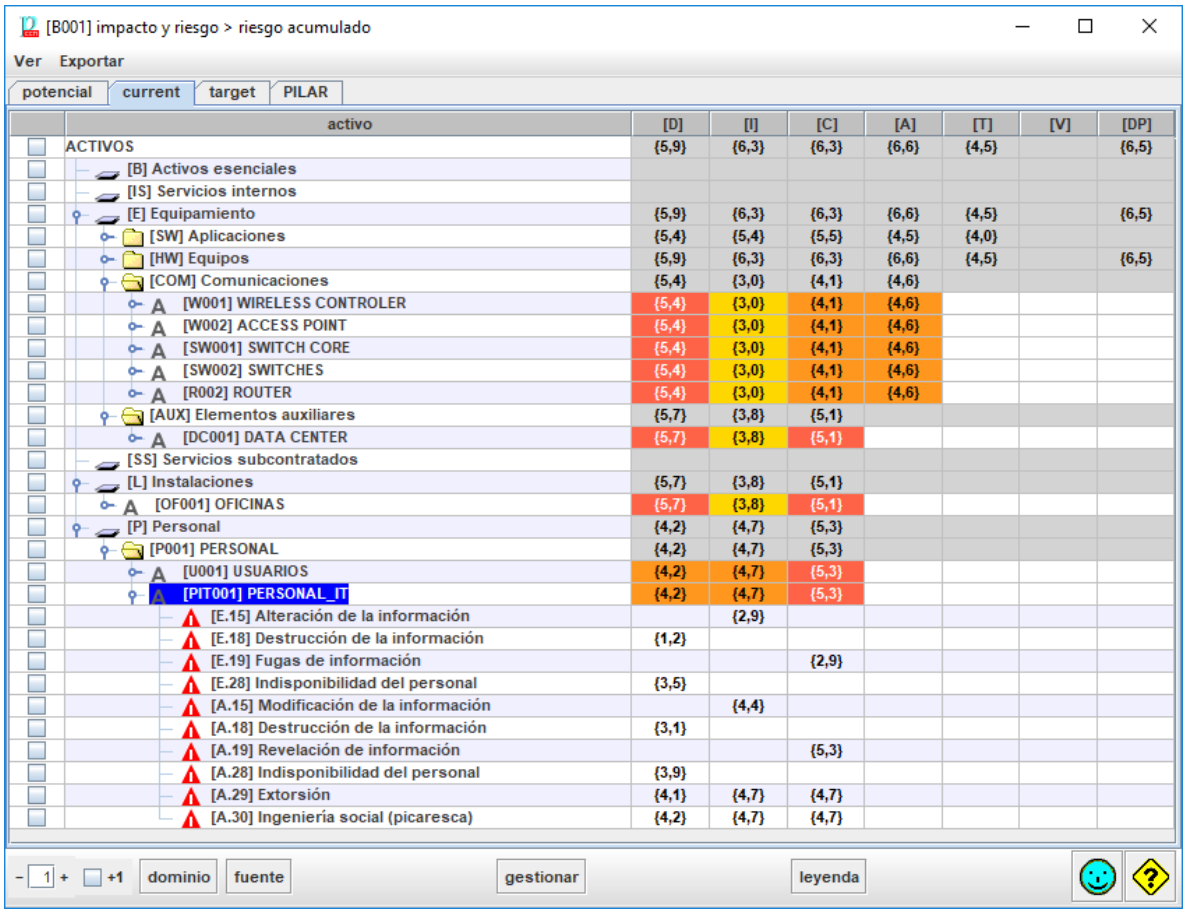
Riesgo acumulado: Equipamiento, Aplicaciones y Equipos.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{5,9}	{6,3}	{6,3}	{6,6}	{4,5}		{6,5}
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	{5,9}	{6,3}	{6,3}	{6,6}	{4,5}		{6,5}
[SW] Aplicaciones	{5,4}	{5,4}	{5,5}	{4,5}	{4,0}		
[MDM1] MDM (Mobile Device Management)	{5,3}	{5,3}	{5,4}	{4,5}	{4,0}		
[APPM1] Aplicaciones móviles	{5,4}	{5,4}	{5,5}				
[APPSW1] Aplicaciones web	{5,4}	{5,4}	{5,5}				
[DET1] DET	{5,4}	{5,4}	{5,5}				
[SWD01] Software de desarrollo	{5,4}	{5,4}	{5,5}				
[DB001] Gestión de BDD	{5,4}	{5,4}	{5,5}				
[HW] Equipos	{5,9}	{6,3}	{6,3}	{6,6}	{4,5}		{6,5}
[S000] CHASIS H	{5,2}	{5,2}	{5,2}				
[S001] DATABASE_V1	{4,9}	{6,3}	{6,3}	{6,1}			
[S002] ELEARNING_V2	{5,3}	{5,1}	{5,8}	{6,5}	{4,0}		
[S003] FILESERVER_V3	{4,9}	{6,3}	{6,3}	{6,1}			
[S004] STORAGE_F1	{5,2}	{5,1}	{5,8}	{6,3}	{4,0}		
[N001] NVR	{5,1}	{3,4}	{4,6}				
[S005] BACKUP_F2	{4,8}	{4,8}	{5,7}	{5,6}			
[S006] PROXY_F3	{5,6}	{5,9}	{5,8}	{6,5}	{4,0}		
[S007] SERVIDOR_F4	{5,6}	{5,2}	{5,2}	{5,1}	{4,4}		
[S008] MS_V12	{5,3}	{5,1}	{5,8}	{6,5}	{4,0}		
[S009] INTRA_V4	{5,3}	{5,1}	{5,8}	{6,5}	{4,0}		
[S010] APP_V5	{4,9}	{4,8}	{5,8}	{6,1}			
[S011] MINUBE_V6	{5,3}	{5,1}	{5,8}	{6,5}	{4,0}		
[S012] WEBSERVICES_V7	{5,3}	{5,1}	{5,8}	{6,5}	{4,0}		
[PC001] PC_1	{4,9}	{4,8}	{5,7}	{6,0}			{6,5}
[S013] BARRACUDA_F5	{5,9}	{5,2}	{5,2}	{5,1}	{4,5}		
[S014] PWEB_V8	{5,3}	{5,1}	{5,8}	{6,6}	{4,0}		
[S015] MAIL_V9	{5,3}	{5,1}	{5,8}	{6,5}	{4,0}		
[S016] SMB_V10	{5,3}	{5,9}	{5,8}	{6,5}	{4,0}		
[S017] PRB_V11	{3,6}	{5,1}	{5,8}	{6,5}	{4,0}		
[IMP001] IMPRESORAS	{5,1}	{4,4}	{4,6}	{4,2}	{3,6}		
[TB001] TABLETS	{5,5}	{4,8}	{5,8}	{6,1}			{6,5}
[T001] TAPE	{5,9}	{5,6}	{5,0}	{5,2}	{4,5}		
[PBX001] PBX	{5,1}	{3,4}	{4,6}				

Figura 40

Riesgo acumulado: Equipamiento, Comunicaciones, Elementos auxiliares y Personal.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{5,9}	{6,3}	{6,3}	{6,6}	{4,5}		{6,5}
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento	{5,9}	{6,3}	{6,3}	{6,6}	{4,5}		{6,5}
[SW] Aplicaciones	{5,4}	{5,4}	{5,5}	{4,5}	{4,0}		
[HW] Equipos	{5,9}	{6,3}	{6,3}	{6,6}	{4,5}		{6,5}
[COM] Comunicaciones	{5,4}	{3,0}	{4,1}	{4,6}			
[W001] WIRELESS CONTROLER	{5,4}	{3,0}	{4,1}	{4,6}			
[W002] ACCESS POINT	{5,4}	{3,0}	{4,1}	{4,6}			
[SW001] SWITCH CORE	{5,4}	{3,0}	{4,1}	{4,6}			
[SW002] SWITCHES	{5,4}	{3,0}	{4,1}	{4,6}			
[R002] ROUTER	{5,4}	{3,0}	{4,1}	{4,6}			
[AUX] Elementos auxiliares	{5,7}	{3,8}	{5,1}				
[DC001] DATA CENTER	{5,7}	{3,8}	{5,1}				
[SS] Servicios subcontratados							
[L] Instalaciones	{5,7}	{3,8}	{5,1}				
[OF001] OFICINAS	{5,7}	{3,8}	{5,1}				
[P] Personal	{4,2}	{4,7}	{5,3}				
[P001] PERSONAL	{4,2}	{4,7}	{5,3}				
[U001] USUARIOS	{4,2}	{4,7}	{5,3}				
[PIT001] PERSONAL_IT	{4,2}	{4,7}	{5,3}				
[E.15] Alteración de la información		{2,9}					
[E.18] Destrucción de la información	{1,2}						
[E.19] Fugas de información			{2,9}				
[E.28] Indisponibilidad del personal	{3,5}						
[A.15] Modificación de la información		{4,4}					
[A.18] Destrucción de la información	{3,1}						
[A.19] Revelación de información			{5,3}				
[A.28] Indisponibilidad del personal	{3,9}						
[A.29] Extorsión	{4,1}	{4,7}	{4,7}				
[A.30] Ingeniería social (picaresca)	{4,2}	{4,7}	{4,7}				

Como resultado de la observación de las figuras anteriores tenemos que, el riesgo acumulado actual en los activos va de muy alto {4,2} a crítico {5,9} en la dimensión de disponibilidad. Lo que nos da la alerta para minimizar las amenazas y bajar el nivel de riesgo acumulado, esto se consigue aplicando las salvaguardas recomendadas por PILAR en el apartado 3.2.3.4 Salvaguardas. El Anexo E muestra la evaluación y el tratamiento del riesgo de los activos críticos.

Fase 2: Determinación de la estrategia de continuidad

En esta fase se determinarán las estrategias idóneas que se utilizarán para recuperar las actividades de negocio críticas, mismas que están asociadas a los principales recursos o servicios tecnológicos en caso de una interrupción. Esta asignación se basa en la información que se logró recabar en el BIA y en el análisis

de riesgos asociados a los activos críticos. Además, se trabaja en función a los recursos organizacionales que son susceptibles a contingencias tales como: personal, dependencias de la organización, infraestructura IT, información y proveedores.

Objetivo, alcance y usuarios

Definir cómo Laboratorios Bagó del Ecuador S.A. garantizará que se cumplan todas las condiciones para reanudar las actividades de negocio ante el caso de un desastre o un incidente disruptivo.

Este documento se aplica a todo el alcance del BCP, según se define en la Política de la gestión de continuidad del negocio. Los usuarios de este documento son miembros de la alta dirección y personas que implementan el proyecto de gestión de la continuidad del negocio. En caso de desastres que imposibiliten el acceso a las oficinas principales, se contrataran oficinas equipadas (conexión a Internet, estaciones de trabajo, sala de reuniones, red LAN y WLAN) para la reunión de comité de crisis, el cual gestionará el traslado de los usuarios de los procesos clave del negocio para la recuperación.

Datos de la estrategia

Los datos de la estrategia están redactados con base a los resultados del Análisis del impacto en el negocio y el análisis de riesgos. Se puede ver la tabla resumen en el Anexo E. Para el tratamiento de las actividades consideradas no críticas, en el caso de una contingencia se recurrirá a los procesos internos de la organización, estos procesos ya están definidos en una bitácora de errores y soluciones de Bagó IT.

Análisis de impacto en el negocio (BIA). Del análisis del impacto en el negocio realizado, se establece que ocho actividades (nivel de impacto A y prioridad de recuperación 1) sostienen a los productos y servicios clave de la organización. A continuación en la Tabla 15 se listan las actividades mencionadas con sus dependencias de servicios, sistemas y activos, los períodos máximos tolerables de

interrupción, los objetivos de tiempo de recuperación y el orden sugerido de recuperación para cada actividad en Laboratorios Bagó del Ecuador S.A.

Tabla 15

Lista de actividades críticas con sus dependencias, MTD y RTO.

Actividades	Servicios Tecnológicos	Módulos o Sistemas	Activos	MTD (Días)	RTO (H)	Orden
Gestión de funcionamiento de la infraestructura física y virtual de servidores (Base de datos, Almacenamiento, Aplicaciones (DET, Intranet, aplicaciones web, etc.), Proxy, Firewall, Antivirus, Antispam, Nube privada, Página web, BI, Respaldos, DHCP, Archivos, e-learning, Intranet, Correo, Dominio, DNS	Gestión Hipervisor vCenter, Data Center, Vmware	vSphere ESX, Wmware, SSH	DATA CENTER CHASIS H STORAGE_F1	1	7	1
Supervisión de sistemas de respaldo de energía eléctrica	Data Center, UPS	Computer Power	DATA CENTER INSTALACIONES	0.5	2	2
Administración de la infraestructura de red cableada e inalámbrica	Infraestructura de red, Software de monitoreo, Consola de Administración	MRTG, Nagios	PROXY_F3 SERVIDOR_F4 SMB_V10 SWITCH CORE ROUTER	2	8	3
Administración de base de datos	Base de datos, Software de administración de base de datos	Oracle, Toad	STORAGE_F1 DATABASE_V1	0.5	4	4
Facturación, notas de crédito y débito a clientes	DET, Aplicación web de facturación electrónica	Facturación, edocs	FILESERVER_V3 PC_1	0.5	4	5

Actividades	Servicios Tecnológicos	Módulos o Sistemas	Activos	MTD (Días)	RTO (H)	Orden
Correo electrónico	Servicio de correo electrónico	Thunderbird	MAIL_V9	0.5	3	6
Administración de la Intranet	Servidor Intranet, Aplicaciones web	Joomla	INTRA_V4	1	7	7
Gestión del distribuidor (Leterago)	Ofimática, Correo electrónico, Portal web del proveedor	Microsoft Office, Thunderbird, SAR Leterago	PC_1 MAIL_V9 INTRA_V4	3	18	9

Como se puede observar en la tabla anterior, ante un evento disruptivo, el departamento de Bagó IT tiene como prioridad restaurar las actividades críticas relacionadas a su infraestructura tecnológica para luego así, dar soporte a las actividades principales del negocio de la organización y que esta siga operando.

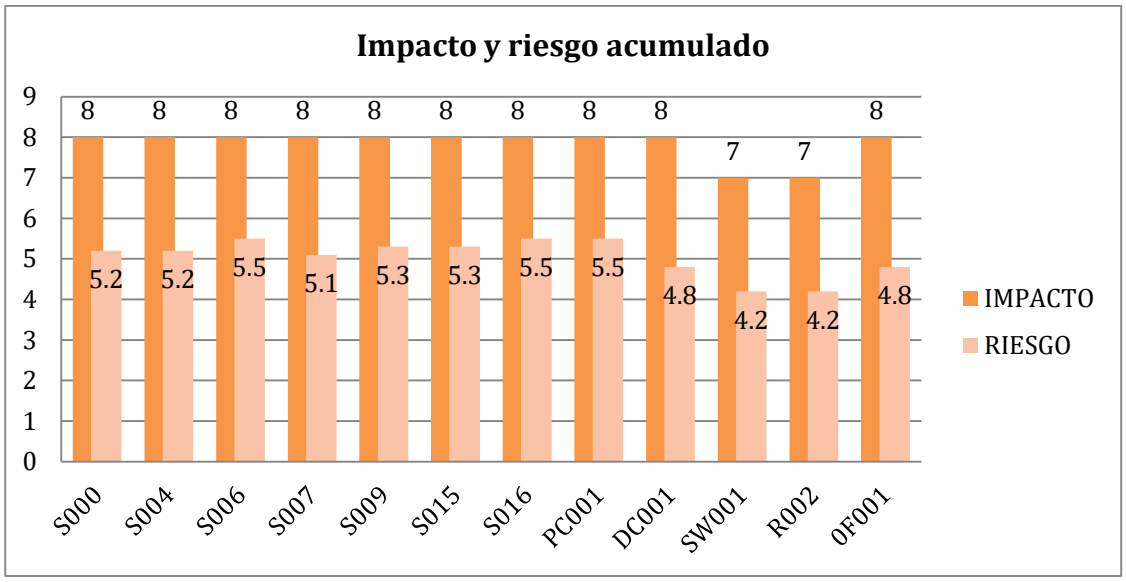
Evaluación de riesgos. A continuación, en este apartado se presenta: el resultado de la evaluación de riesgos, los mayores riesgos que podrían producir un incidente disruptivo, el impacto y el riesgo al que son susceptibles los activos, las amenazas y sus respectivas salvaguardas para tratar los riesgos.

El resultado de la evaluación de riesgos que pueden afectar la continuidad del negocio se lo generó gracias a la ayuda de la herramienta EAR/PILAR, la cual se detalla en el apartado 3.2.3.5; además se puede apreciar el tratamiento de riesgos en el Anexo F.

La Figura 41 describe el impacto y riesgo acumulado que actualmente pueden sufrir los activos críticos del departamento de tecnología de la organización.

Figura 41

Impacto y riesgo acumulado en los activos principales.



En la figura anterior se puede observar que el impacto en la mayoría de activos es de 8 es decir muy alto y el riesgo es de 5.5 lo que en la escala nominal significa estado crítico.

Según la evaluación de riesgos y el impacto al que son susceptibles los activos, se listan las amenazas más recurrentes que podrían producir un incidente disruptivo, es decir, una interrupción del negocio y se les aplicará su respectiva salvaguarda a manera de recomendación para disminuir el nivel de riesgo; la Tabla 16 muestra lo antes mencionado.

Tabla 16

Lista de amenazas con su respectiva salvaguarda y tratamiento para disminuir el riesgo.

Amenazas	Salvaguardas	Aspecto	Tipo de Protección
Abuso de privilegios de acceso	Se debe utilizar un número limitado y controlado de actividades de ejecución: las que requieren sus privilegios especiales	[G] gestión	[AD] administrativa
Acceso no autorizado	Comprobación de datos no autorizados o inconsistentes	[G] gestión	[DC] detección
Ataque destructivo	Copias de seguridad fuera de las instalaciones, alquiler de equipos para caso de emergencia, copias impresas de procedimientos y restauración de sistemas	[F] física	[IM] minimización del impacto

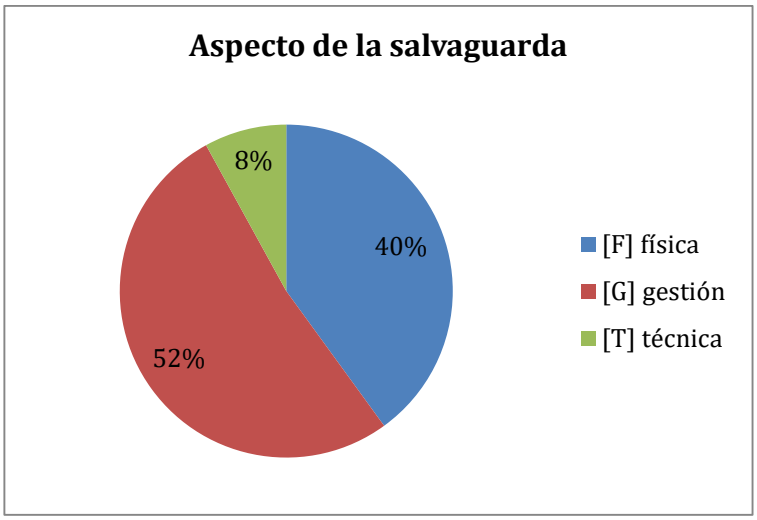
Amenazas	Salvaguardas	Aspecto	Tipo de Protección
Caída del sistema por agotamiento de recursos	Implementar mecanismos de detección, monitorización y registro de uso de recursos de equipos	[G] gestión	[EL] eliminación
Condiciones inadecuadas de temperatura y humedad	Alarma en tiempo real cuando el sistema se sale de especificaciones	[F] física	[MN] monitorización
Corte de suministro eléctrico	Contar con un Sistema de alimentación redundante que garantiza el funcionamiento de los equipos críticos, y la continuidad de las operaciones	[F] física	[CR] corrección
Daños por agua	Sistema de detección de inundación	[F] física	[DC] detección
Denegación de servicio	Sistema de protección frente a ataques de denegación de servicio (DoS)	[G] gestión	[IM] minimización del impacto
Desastres industriales	Plan de continuidad de negocio, sitios alternos, respaldos en la nube, póliza de seguro	[F] física	[RC] recuperación
Desastres naturales	Plan de continuidad de negocio, sitios alternos, respaldos en la nube, póliza de seguro	[F] física	[RC] recuperación
Difusión de software dañino	La base de datos de virus se debe actualizar regularmente	[T] técnica	[PR] prevención
Fallo de servicios de telecomunicaciones	Enlaces de datos e Internet redundantes con reemplazos de equipos	[F] física	[EL] eliminación
Fuego	Sistema automático de detección de incendios	[F] física	[DC] detección
Manipulación de hardware	Sistemas de recuperación con equipos redundantes, copia exacta de los datos y configuraciones.	[F] física	[IM] minimización del impacto
Manipulación de los registros de actividad (log)	Aseguramiento de la integridad, estableciendo políticas para la manipulación de la información.	[G] gestión	[PR] prevención
Manipulación de programas	Protección de aplicaciones, procedimiento de uso de aplicaciones, perfiles de seguridad	[T] técnica	[EL] eliminación
Modificación de la información	Aseguramiento de la integridad, estableciendo políticas para la manipulación de la información.	[G] gestión	[IM] minimización del impacto

Amenazas	Salvaguardas	Aspecto	Tipo de Protección
Ocupación enemiga	Copias de seguridad fuera de las instalaciones, alquiler de equipos para caso de emergencia y copias impresas de procedimientos y restauración de sistemas	[F] física	[IM] minimización del impacto
Pérdida de equipos	Se deben implementar medidas frente a posibles robos	[G] gestión	[PR] prevención
Problemas relativos a la transferencia de datos a terceros	Políticas de confidencialidad de información	[G] gestión	[IM] minimización del impacto
Problemas relativos al consentimiento del sujeto	Impedir el uso de equipos a terceros	[G] gestión	[IM] minimización del impacto
Repudio (negación de actuaciones)	Servicio de no repudio, empleo de firmas digitales	[G] gestión	[IM] minimización del impacto
Robo de equipos	Sistema de anclaje de equipos, alarmas antirrobo y técnicas de criptografía.	[G] gestión	[PR] prevención
Suplantación de identidad	Sistema que comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador	[G] gestión	[EL] eliminación
Uso no previsto	Impedir el desarrollo de eventos no autorizados con políticas de uso	[G] gestión	[PR] prevención

La Figura 42 muestra el resumen de los aspectos de las salvaguardas que se deben tomar en cuenta para aumentar el nivel de madurez de la organización en términos de seguridad y así disminuir el riesgo de afectación en los activos más importantes.

Figura 42

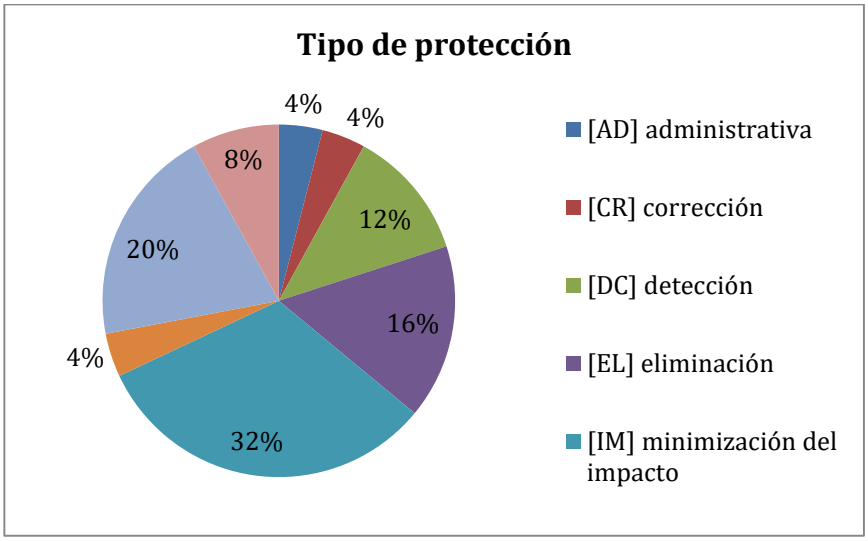
Porcentaje de aspectos con relación a las salvaguardas.



La Figura 43 muestra el resumen de tipo de protección (tdp) que proporciona la salvaguarda al aplicarla en los activos analizados.

Figura 43

Porcentajes de tipo de protección (tdp).



Para todos los riesgos o amenazas que podrían causar incidentes es necesario:

Aplicar medidas correctivas o preventivas que minimicen el riesgo de ocurrencia, a estas medidas las llamamos salvaguardas y se la puede observar en Tabla 16. Además, con la aplicación de estas medidas

aumentará el nivel de madurez con respecto a la continuidad del negocio revisada en el apartado 3.2.3 Análisis de Riesgos.

Estrategia de recuperación de actividad. En los siguientes apartados se describen las estrategias de recuperación con el procedimiento interno a aplicar para cada actividad considerada clave. Los datos de las actividades se las puede observar en la Tabla 15. Además, se codificarán las actividades y estrategias para mejor ubicación y mención en este estudio**.**

Algo importante que destacar al momento de definir o ejecutar una estrategia es, precautelar la integridad física del personal, especialmente ante eventos como desastres naturales, fuego, desastres industriales, daños por agua y ataque destructivo. Para esto se debe apoyar en el comité paritario de la empresa y en el técnico de seguridad y salud ocupacional.

Gestión de funcionamiento de la infraestructura física y virtual de servidores (A). Objetivo: Comprender el entorno tecnológico de la infraestructura de servidores virtuales y físicos que soporta las actividades críticas y tener la capacidad para replicarlo o recuperarlo en caso de desastre. El RTO para esta actividad es de 7 horas.

Recursos:

- El Gerente de recuperación; es decir, la persona responsable para la recuperación de esta actividad es el Administrador de Base de Datos.

Servicios:

- Gestión Hipervisor vCenter y Vmware

Activos:

- [S001] CHASIS H - VCENTER ESX/ESXi - Gestor de máquinas virtuales. Impacto 8, Riesgo 5.2
- [S004] STORAGE_F1 - Servidor de Almacenamiento. Impacto 8, Riesgo 5.2

- [DC001] DATA CENTER - Centro de cómputo. Impacto 8, Riesgo 4.8

La actividad A se recuperará de la siguiente forma:

Para casos como: desastres naturales, fuego, desastres industriales, daños por agua y ataque destructivo, tenemos:

- Recuperación de la actividad en una ubicación alternativa física o en la nube (AE1)

  Conmutación de los servicios principales (Base de datos, DET, Intranet, aplicaciones web, correo, proxy, firewall, DHCP y DNS) a un sitio alterno físico ubicado en las dependencias de Laboratorios Bagó del Ecuador S.A en la ciudad de Guayaquil. Si el sitio alterno es en la nube, aplicar la conmutación virtual de los servicios principales al sitio (Base de datos, correo, aplicaciones, almacenamiento y servicios), para hacer efectiva esta estrategia se debe contar con una contratación de servicio tipo IaaS.

Para casos como: difusión de software dañino y caída del sistema por agotamiento de recursos, tenemos la siguiente estrategia:

- Procedimientos de recuperación para restaurar los servicios (AE2)

  Recurrir a la documentación interna de procedimientos para levantamiento de servicios en caso de interrupción por infección de malware o por problemas con el hardware (avería de equipos, espacio insuficiente en discos y falta de memoria o procesador). En este caso se aplicaría entre los procedimientos el de errores y soluciones del servidor de archivos.

Supervisión de sistemas de respaldo de energía eléctrica (B). Objetivo: Reducir el impacto que genera la falta de disponibilidad de energía eléctrica para el funcionamiento de los equipos. El RTO para esta actividad es de 2 horas.

Recursos:

- El Gerente de recuperación de esta actividad es el Ingeniero de soporte e infraestructura.

Servicios:

- Data Center y UPS

Activos:

- [DC001] DATA CENTER - Centro de cómputo. Impacto 8, Riesgo 4.8. Se encuentra el UPS.
- [OF001] Instalaciones - Oficinas donde se desempeñan las actividades. Impacto 8, Riesgo 4.8. Se cuenta con una central eléctrica.

La actividad B se recuperará de la siguiente forma:

Para eventos como: corte de suministro eléctrico, robo de equipos y uso no previsto. La estrategia es la siguiente:

- Sistema redundante de suministro de energía eléctrica (BE1)

  Además del sistema interno de UPS que posee el Data Center con su respectivo plan de mantenimiento, se cuenta con el procedimiento de conmutación a la central eléctrica del edificio. Sin embargo, en caso de evento disruptivo de corte de energía eléctrica y que afecte a las fuentes de alimentación antes mencionadas, la estrategia de recuperación es hacer uso de una planta eléctrica propia o contratada con la carga suficiente para mantener a los equipos en funcionamiento. También se puede contar un contrato de respaldo de suministro de energía eléctrica con el edificio, para hacerlo efectivo cuando se presente una contingencia, y abastecerse de energía desde la central eléctrica del mismo, este contrato debe garantizar la disponibilidad de la central del edificio con mantenimientos habituales, combustible disponible y realización de

pruebas periódicas con alta y baja carga. Se deberá levantar un procedimiento llamado recuperación de suministro externo de energía para la ejecución de esta estrategia.

Administración de la infraestructura de red cableada e inalámbrica (C). Objetivo: Garantizar la conectividad de equipos y sucursales de la empresa tanto en red WAN como LAN. El RTO para esta actividad es de 8 horas.

Recursos:

- Los gerentes de recuperación de esta actividad son el Ingeniero de soporte e infraestructura y el Administrador de Base de Datos.

Sistemas:

- Infraestructura de red - Redes LAN, enlace de datos y redes WLAN.

Activos:

- [S007] SERVIDOR_F4 - DHCP, DNS, ePO (McAfee antivirus ePolicy Orchestrator). Impacto 8, Riesgo 5.1
- [S006] PROXY_F3 - Servidor intermedio entre la red interna y externa, Firewall, navegación segura en Internet. Impacto 8, Riesgo 5.5
- [S016] SMB_V10 - Servidor de dominio Samba, LDAP. Impacto 8, Riesgo 5.5
- [R002] ROUTER - Conexión entre redes de las sucursales. Impacto 7, Riesgo 4.2
- [SW001] SWITCH CORE - Dispositivos de comunicación capa 3. Impacto 7, Riesgo 4.2

La actividad C se recuperará de la siguiente forma:

Para casos como: fallo de servicios de telecomunicaciones, acceso no autorizado y manipulación de hardware.

- Sistema redundante de conexión a Internet y enlaces de datos (CE1)

Disponer de enlaces redundantes de conexión de datos e Internet con otro proveedor para conectarse en caso de falla del proveedor principal de telecomunicaciones, es importante que se considere una acometida o última milla diferente a la contratada actualmente. Acudir al procedimiento de interrupción de servicio de internet.

- Sistemas de recuperación con equipos redundantes, copia exacta de los datos y configuraciones (CE2)

Recurrir a reemplazo inmediato de equipos en caso de averías y falla de configuraciones por parte del proveedor de telecomunicaciones y proveedor de mantenimiento de equipos de conectividad. Además, se debe contar con equipos de contingencia como servidores, *appliance*, tarjetas de red y *access point* disponibles en el departamento de IT con su respectiva copia de configuración para su inmediato reemplazo y levantamiento. Se debe contar con un repositorio de configuraciones de equipos de comunicaciones y de seguridad perimetral.

Administración de Base de datos (D). Objetivo: Garantizar la integridad, confiabilidad y disponibilidad de los datos con un proceso de recuperación de la información vital para la empresa. El RTO para esta actividad es de 4 horas.

Recursos:

- El Gerente de recuperación de esta actividad es el Administrador de Base de Datos.

Servicios:

- Software gestor y administrador de base de datos, Ejecución de consultas y reportes.

Activos:

- [S001] DATABASE_V1 - Servidor de base de datos Oracle 12c. Impacto 8, Riesgo 4.9
- [S004] STORAGE_F1 - Servidor de Almacenamiento. Impacto 8, Riesgo 5.2

- [T001] TAPE – Librería de quema de cintas magnéticas. Impacto 8, Riesgo 5.9

La actividad D se recuperará de la siguiente forma:

Para casos como: acceso no autorizado, difusión de software dañino y suplantación de identidad.

- Copias de seguridad y procedimientos de recuperación (DE1)

  Recurrir a las copias de seguridad realizadas por las diferentes estrategias de respaldos como son: cintas magnéticas, NAS (almacenamiento conectado en red) y las alojadas en los discos luego de un trabajo programado de respaldo. Luego aplicar el proceso de recuperación correspondiente a cada estrategia de respaldo; por ejemplo, para recuperación de cintas tener disponible, en buenas condiciones y actualizada la librería de respaldos TAPE. También se puede disponer de *backups* encriptados del proveedor en la nube y de una aplicación que restaure los datos de forma manual y automática, la misma debe tener estándares de RTO y RPO cuando se detecte un evento disruptivo. Por último, se debe contar un sistema gestor de credenciales con encriptación para que estén protegidas, y con procesos previos de autenticación las credenciales deben estar disponibles al momento de requerirlas.

Facturación, notas de crédito y débito a clientes (E). Objetivo: Reducir el impacto que genera la falta de disponibilidad de las aplicaciones. El RTO para esta actividad es de 4 horas.

Recursos:

- El Gerente de recuperación de esta actividad es el Gerente de Sistemas.

Servicios:

- DET - Sistema de gestión de procesos Financieros, Contables, Contabilidad e Inventarios.

Activos:

- [S003] FILESERVER_V3 - Servidor de archivos y ejecutables del sistema DET y aplicaciones. Impacto 8, Riesgo 4.9.
- [PC001] PC_1 - Equipos de cómputo para usuarios. Impacto 8, Riesgo 5.5.

La actividad E se recuperará de la siguiente forma:

Para casos como: desastres naturales, fuego, desastres industriales y daños por agua, tenemos lo siguiente:

- Traslado de los usuarios y reemplazar los equipos de los usuarios (EE1)

  Si el caso lo amerita se debe trasladar los usuarios a oficinas contratadas en otras dependencias o recurrir al teletrabajo habilitando las aplicaciones en sus equipos. Y contar con equipos de contingencia, en los cuales estén instalados el software y las aplicaciones necesarias para su trabajo.

- Coordinación para la conexión con el servidor de archivos, ubicados en sitio alterno o nube tipo SaaS (EE2)

  Realizar la conmutación para habilitar el servicio de facturación desde un sitio alterno configurado en las instalaciones de la ciudad de Guayaquil. Por otro lado, si la estrategia es tener servicio en la nube tipo SaaS realizar las configuraciones necesarias de conexión en la infraestructura y equipos de los usuarios.

Para eventos como: difusión de software dañino, abuso de privilegios de acceso, manipulación de programas y robo de equipos.

- Restaurar los archivos de datos del software de los sistemas/aplicaciones (EE3)

  Acudir al procedimiento de respaldos para realizar la restauración de los archivos ejecutables para la ejecución de las aplicaciones, recurriendo a las copias o respaldos de información. Probar y verificar las funciones del sistema operativo y software de aplicaciones de acuerdo a lo requerido. Además, verificar la coherencia de los datos.

Correo electrónico (F). Objetivo: Garantizar que la organización este comunicada ante un evento disruptivo que afecte al envío y recepción de correos electrónicos. El RTO para esta actividad es de 3 horas.

Recursos:

- Los gerentes de recuperación de esta actividad son el Ingeniero de soporte e infraestructura y el Administrador de Base de Datos.

Servicios:

- Correo electrónico.

Activos:

- [S015] MAIL_V9 - Servidor de correo electrónico. Impacto 8, Riesgo 5.3.

La actividad F se recuperará de la siguiente forma:

Para casos como: abuso de privilegios de acceso y modificación de la información.

- Copias de seguridad y procedimientos de recuperación (FE1)

  Recurrir a las copias de seguridad realizadas por las diferentes estrategias de respaldos como son: cintas magnéticas y respaldo de la máquina virtual en nube o en sitio alterno. Luego aplicar el proceso de recuperación correspondiente a cada estrategia de respaldo, por ejemplo, para recuperación se debe realizar la conmutación a la réplica de la máquina virtual en la nube con

software de replicación Veeam Backup, esta actividad consta en un procedimiento interno de conmutación de máquinas virtuales.

Para eventos como: difusión de software dañino y denegación de servicio

- Detección de malware y ejecutar métodos de recuperación en caliente (FE2)

  Aplicar un escaneo de los correos, liberar espacio en el disco duro por logs creados de manera deliberada, liberar la cola de correo saturado que puede impedir en el envío y recepción de correos, solicitar la desafiliación del dominio en las listas negras de los servidores de internet previo un escaneo de virus. Las bases de datos de los antivirus deben estar actualizadas. Aplicar procedimiento de errores y soluciones de servidor de correo electrónico.

Administración de la Intranet (G). Objetivo: Recuperar los servicios y aplicaciones que brinda la intranet a los procesos de negocio. El RTO para esta actividad es de 7 horas.

Recursos:

- El Gerente de recuperación de esta actividad es el Administrador de Base de Datos.

Servicios:

- Intranet Corporativa - Sitio web corporativo que brinda información y accesos a diferentes sistemas.
- Aplicaciones web - Aplicaciones propias para apoyo al negocio.

Activos:

- [S009] INTRA_V4 - Servidor Intranet corporativa brinda acceso a varios sistemas. Impacto 8, Riesgo 5.3.

La actividad G se recuperará de la siguiente forma:

Para casos como: difusión de software dañino, abuso de privilegios de acceso, denegación de servicio y suplantación de identidad.

- Copias de seguridad y procedimientos de recuperación (GE1)

  Al igual que con el servicio de correo electrónico, se debe recurrir a las copias de seguridad realizadas por las diferentes estrategias de respaldos, cintas magnéticas y respaldo de la máquina virtual en nube o en sitio alterno. Inmediatamente aplicar el proceso de recuperación correspondiente a cada estrategia de respaldo, para este caso la recuperación además del servidor debe ser hacia los servicios internos que presta la intranet, como aplicaciones web y accesos a diferentes sistemas. Estos procesos requieren confirmación de parte de los usuarios.

Gestión del distribuidor Leterago (H). Objetivo: Recuperar de manera inmediata los procesos de distribución y adecuación de mercadería (producto terminado y muestra médicas). El RTO para esta actividad es de 18 horas, es el máximo RTO para una actividad crítica ya que no depende solo del departamento de Bagó IT sino también de terceros.

Recursos:

- Los gerentes de recuperación de esta actividad son el Ingeniero de soporte e infraestructura y el Administrador de Base de Datos.
- Navegador y Ofimática

Servicios:

- Correo electrónico.
- Aplicaciones web - Aplicaciones propias para apoyo al negocio (FE).

- Instalación de aplicaciones de proveedor - Aplicaciones de empresas proveedoras para apoyó al negocio *NetOrder*.
- DET Sistema de gestión de procesos Financieros, Contables, Contabilidad e Inventarios (boletas).

Activos:

- [S015] MAIL_V9 - Servidor de correo electrónico. Impacto 8, Riesgo 5.3
- [S009] INTRA_V4 - Servidor Intranet corporativa brinda acceso a varios sistemas. Impacto 8, Riesgo 5.3
- [PC001] PC_1 - Equipos de cómputo para usuarios. Impacto 8, Riesgo 5.5

La actividad H se recuperará de la siguiente forma:

Para eventos como: difusión de software dañino, abuso de privilegios de acceso, denegación de servicio, modificación de la información, manipulación de programas y ataque destructivo.

- Copias de seguridad y procedimientos de recuperación (HE1)

  Solicitar las copias de seguridad realizadas por las diferentes estrategias de respaldos, cintas magnéticas y respaldo de la máquina virtual en nube o en sitio alterno de la intranet, correo y servidor de archivos. Luego aplicar el proceso de recuperación correspondiente a cada estrategia de respaldo, para este caso la recuperación además del servidor debe ser hacia los servicios internos que presta la intranet, como aplicaciones web y accesos a diferentes sistemas. Estos procesos requieren confirmación de parte de los usuarios.

Para eventos en el proveedor como: denegación de servicio y ataque destructivo.

- Contrato de alta disponibilidad de servicio con el proveedor y Sistema redúndate de creación de pedidos (HE2)

Hacer efectivo contrato de disponibilidad y acuerdos de niveles de servicio con el proveedor para que garantice la adecuación, almacenamiento y distribución de los productos. Además, contar con acceso redundante a la aplicación de pedidos, además de acceso por aplicación para *tablet* y garantizar el acceso por computador de parte del proveedor.

Fase 3: Respuesta a la contingencia

Comité de Crisis

Ante un evento disruptivo, el encargado de activar el plan de continuidad de negocio y dirigir las acciones durante la contingencia es el comité de crisis, el mismo que está conformado por:

- Gerente General (Líder de la organización)
- Gerente Administrativo y Financiero (Informe financiero para la aplicación del plan)
- Gerente de Sistemas (Líder del área de IT)
- Administrador de Base de Datos (Responsable de las copias de seguridad e infraestructura)
- Técnico de Seguridad y Salud Ocupacional (Encargado de velar por seguridad física del personal)
- Ingeniero de infraestructura y soporte.

Como miembros de apoyo del comité de crisis estará, el personal de Bagó IT que serán responsables de analizar y demarcar el impacto de la incidencia, además realizar el papel de gerente de recuperación del proceso a cargo, el asistente administrativo a cargo de la logística en caso de ir a un sitio alterno, la coordinadora de compras quien se encargara de las adquisiciones y la coordinadora de comunicaciones quien se encarga de informar a los clientes, proveedores y usuarios sobre la situación.

El comité de crisis es dirigido por el Gerente de crisis, en este caso será el Gerente de Sistemas, la función del gerente de crisis es llamar a reunión al comité, notificar la materialización de un evento

disruptivo, informar de las condiciones y definir en conjunto si se dispara el plan de recuperación. En el caso de inasistencia de algún miembro del comité, este debe designar un reemplazo.

Para declarar una situación de crisis se debe basar en el MTD de cada proceso crítico, por ejemplo, si el proceso E (Facturación, notas de crédito y débito a clientes) con MTD de 0.5 días se llega a interrumpir, se deben ejecutar los procedimientos habituales para restablecer el servicio, de no ser suficientes estos procedimientos, quiere decir que podría superar el MTD para ese proceso, entonces se convoca el comité de crisis para posteriormente ejecutar el plan de continuidad.

Planes Operativos de Recuperación de Entornos

Este plan contiene la información sobre que recursos intervienen en la recuperación de entornos o procesos críticos. Es decir que recursos, servicios o activos del cual depende un proceso se deben recuperar. Para la recuperación, dependiendo del evento, en primer lugar, se debe acudir a los procesos de recuperación internos de la organización, si no son suficientes aplicar el plan de continuidad. Para poner en marcha del plan operativo de recuperación se deben ejecutar las siguientes acciones:

- Analizar, quién, cómo y bajo qué circunstancias debe ser activado.
- Realizar el árbol de llamadas para informar a las personas involucradas sobre la activación del plan.
- Ubicar a las personas que intervienen en el plan.
- Realizar una evaluación de los servicios disponibles (se incluyen servicios de terceros).
- Comunicación de fondo y forma de la ejecución del plan de comunidad a los empleados, usuarios clave y demás departamentos.

Una vez realizadas las acciones previas se aplica la estrategia de recuperación. A continuación, un ejemplo:

- Proceso Crítico

Facturación, notas de crédito y débito a clientes (E)

- Plan operativo de recuperación de entornos para la actividad E

Este proceso depende de los siguientes recursos y se deben ejecutar las acciones de recuperación para:

  - Recurso humano: gerente de sistemas, usuario final a cargo de este proceso y asistente de facturación.
  - DET - Sistema de gestión de procesos Financieros, Contables, Contabilidad e Inventarios.
  - [S003] FILESERVER_V3 - Servidor de archivos y ejecutables del sistema DET y aplicaciones
  - [PC001] PC_1 - Equipos de cómputo para usuarios

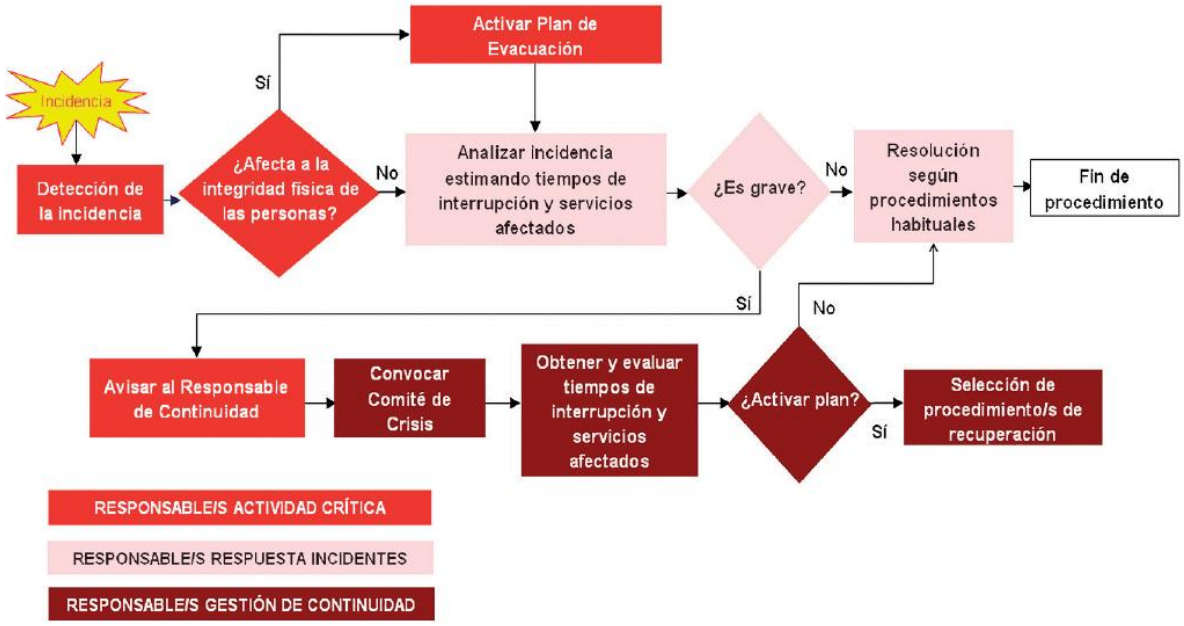
Procedimientos técnicos de trabajo o de Incidentes

Continuando con el ejemplo, como respuesta a la crisis se recurren a los procedimientos técnicos de trabajo de carácter interno que posee la organización y se ejecuta el flujo de la Figura 44 en caso de interrupción; estos procedimientos internos tienen información de direcciones IP, puesta en marca de aplicaciones, listado de comandos, levantamiento de aplicaciones y configuraciones. Todos estos procesos técnicos se alinean con la estrategia de recuperación escogida para recuperar las operaciones dependiendo de la incidencia. Los procedimientos internos son confidenciales por contener información privada y no se los puede mostrar, sin embargo, con este estudio los responsables de las actividades sabrán cuando aplicarlos.

A continuación, la Figura 44 muestra el flujo en caso de interrupción de una actividad de negocio el cual se recomienda seguir.

Figura 44

Diagrama de flujo en caso de interrupción de una actividad de negocio.



Nota. Tomado de *Ejemplo de secuencia de tareas a realizar en caso de paralización de la actividad* (p. 58), INTECO, 2016, https://opinit.files.wordpress.com/2010/11/guia_practica_para_pymes_como_implantar_un_plan_de_continuidad_de_negocio.pdf

El ejemplo y el flujo de interrupción anterior se pueden aplicar a todos los procesos o actividades críticas mencionadas en la estrategia de recuperación.

Se debe activar el procedimiento o plan operativo de recuperación una vez hecha la evaluación de la indisponibilidad del recurso crítico por comité de crisis y se debe aplicar la estrategia para retornar a las actividades normales definida para dicha indisponibilidad. En el ejemplo anterior se aplican las estrategias de recuperación de la actividad E.

Fase 4: Prueba, mantenimiento y revisión

Objetivo, alcance y usuarios

El objetivo de este plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los convenios para la gestión de la continuidad del negocio, como también para establecer las acciones correctivas necesarias.

Este Plan se aplica a todos los elementos que se encuentran dentro del alcance del BCP.

Los usuarios de este documento son todas las personas que cumplen una función en el BCP.

Plan de mantenimiento y revisión del BCP

Elementos del BCP. A continuación, la lista.

- Análisis de Impacto sobre el Negocio (BIA)
- Análisis de Riesgos
- Cambios organizativos y de negocio
    - Revisión periódica en busca de cambios en la estructura de la organización, cambio de personal, de procesos y de tecnología.
- Contratos con proveedores
    - Mantener actualizados los contratos con los proveedores que son aliados del BCP.
- Contactos y responsabilidades
    - Deben mantenerse actualizados ante movimientos de personal o cambio de funciones.
- Capacitaciones
    - Los responsables deben ser adecuadamente formados y concienciados acerca de los diferentes conceptos que contempla la continuidad de negocio.
- Comunicación del BCP
    - Inculcar y promocionar una cultura de continuidad de negocio en la organización.

- Auditorías internas y externas
    - De todos y cada uno de los componentes del plan de continuidad de negocio
- Pruebas de estrategias de recuperación
    - Revisión de los resultados de las pruebas realizadas y de que las mejoras identificadas en las mismas han sido aplicadas.
- Actualización del BCP
    - Esto permitirá que la documentación que tengamos que utilizar en una situación de crisis refleje fielmente la información de los distintos actores involucrados en los procesos.

Para mantener la exactitud y utilidad de todos los elementos del BCP, es necesario revisarlos y actualizarlos de acuerdo a las siguientes frecuencias mostradas en la siguiente tabla.

Tabla 17

Cuadro de frecuencia de ejecución de mantenimiento de los elementos del BCP.

Elemento Del BCP	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
BIA	X											
Análisis de Riesgos	X											
Cambios organizativos y de negocio	X						X					
Contratos con proveedores		X						X				
Contactos y responsabilidades	X			X			X			X		
Capacitaciones	X			X			X			X		
Comunicación del BCP	X		X		X		X		X		X	
Pruebas de estrategias de recuperación						X						
Auditorías internas y externas											X	
Actualización del BCP						X						X

El Gerente de crisis será el responsable de este plan, debe cumplir y hacer cumplir las tareas en los meses designados. Además, puede asignar a responsables para cada tarea e ir verificando que se cumpla con la revisión y la actualización de las mismas. La vigencia de este plan es anual.

Implementación de pruebas y verificaciones

La prueba y verificación de continuidad del negocio se implementará en Laboratorios Bagó del Ecuador S.A de la siguiente manera:

- Plazo: desde enero hasta diciembre de manera anual.
- Personal responsable de la coordinación e implementación de la prueba y verificación: Personal IT (Administrador de Base de datos, ingeniero de infraestructura, analista desarrollador, analista BI y gerente de sistemas), usuario del aplicativo o proceso y proveedores.
- Los objetivos de la prueba y verificación son los siguientes:
    - Implementar planes de recuperación para cada actividad.
    - Garantizar que, en situación de contingencia, la organización podrá recuperarse en los tiempos establecidos.
    - Verificar si el personal a cargo está familiarizado con el plan de continuidad.
    - Incrementar la confianza de los usuarios en la organización.
    - Asegurar que todos los recursos necesarios del plan estén disponibles.
    - Garantizar que la información del plan se mantiene actualizada.
- Alcance de la prueba y verificación:
    - El alcance de las pruebas tiene su base en la lista de actividades críticas de la organización descritas en la Tabla 15.
- Método de prueba y verificación:

- Planificar las pruebas en horarios fuera de oficina y con procesos que no afecten al trabajo productivo de la organización.
- Simular el ambiente de un evento o desastre no deseado.
- Aplicar la respuesta a la contingencia.
- Seguir el Diagrama de flujo en caso de interrupción de una actividad de negocio.
- Convocar al comité de crisis de ser necesario.
- Disparar el plan de continuidad de negocio.
- Seleccionar la estrategia de recuperación a aplicar según el evento disruptivo.
- Evaluar y revisar los resultados obtenidos.
- Realizar las recomendaciones de mejora.
- Llenar el formulario del Anexo G (Formulario de revisión post incidente)

Informe de pruebas y verificaciones

A continuación, se presenta un informe de las pruebas realizadas en Laboratorios Bagó del Ecuador S.A. para la actividad o proceso B (Supervisión de sistemas de respaldo de energía eléctrica). Esta prueba se la realizó en un ambiente controlado, simulando un corte de energía eléctrica, luego del horario de oficina y teniendo como estrategia de recuperación un contrato de respaldo de suministro de energía eléctrica con el edificio, esto esta descrito en la estrategia de continuidad BE1. Esta prueba se la realizó cuando se dio mantenimiento a los equipos UPS.

La prueba y verificación se realizó usando el siguiente esquema:

- Fecha: 8 de agosto del 2019
- Persona responsable de la coordinación e implementación de la prueba y verificación: Ingeniero de soporte e infraestructura y el Administrador de Base de datos.

- Alcance de la prueba y verificación: con esta prueba se obtendrá tiempos de respuesta o de entrada en funcionamiento de los equipos UPS y del generador eléctrico del edificio, participaran el ingeniero de infraestructura y la empresa proveedora del servicio de mantenimiento de UPS con 2 técnicos.
- Procesos de prueba y verificación:
    - Como primer paso, se realiza la notificación vía correo electrónico al personal que se va realizar un mantenimiento del Sistemas de alimentación ininterrumpida. En la realidad ante un apagón no se realiza este paso.
    - Luego, se comunica a la administración del edificio que se va a realizar el apagado del UPS. Este paso fuera de pruebas no se lo realiza ya que ellos garantizan en caso de apagón proveer energía, en esta ocasión por ser un ambiente controlado sí.
    - Una vez hecho el mantenimiento, con la presencia de los técnicos y el ingeniero de soporte, se procede a realizar la simulación de un corte de energía eléctrica bajando el interruptor que provee energía al Data center.
    - Proceso de verificación donde se procede a tomar tiempos de respuesta o de funcionamiento tanto de los UPS como de la central o generador del edificio.
    - Declarar situación de crisis o no, apoyados en esta guía.
    - Registro de cumplimiento de los objetivos de la prueba.
    - Por último, mencionar acciones o medidas correctivas y recomendaciones.
- Datos recolectados
    - Tiempo de respuesta del UPS: menos de 1 segundo, entró en funcionamiento inmediatamente.

- Tiempo de respuesta del generador del edificio: 6 segundos

Tabla 18

Logro de objetivos de la prueba.

Objetivos de la prueba	**Logro de objetivos (1: No alcanzado; 2: Alcanzado parcialmente; 3: Alcanzado)**
Simular ambiente controlado de corte de energía	3
Verificar y tomar tiempos de respuesta	3
Objetivos de la prueba	**Logro de objetivos (1: No alcanzado; 2: Alcanzado parcialmente; 3: Alcanzado)**
Comprobar funcionamiento de UPS	3
Comprobar funcionamiento del generador eléctrico	3
Verificar la validez de la estrategia BE1	3

Con base a los resultados de la prueba, se concluye que:

- No ameritó declaración de situación de crisis, la prueba cumplió con el RTO de 2 horas propuesto.

Recomendaciones:

- Para cuando el logro de objetivos sea 1 o 2 se deben aplicar medidas preventivas y correctivas en la estrategia.
- En caso de apagón con daño del UPS el generador debe entrar en funcionamiento inmediatamente, se debe solicitar a la administración del edificio que funcione de esa manera.

Esta prueba debe ser registrada para llevar el control de pruebas realizadas, la fecha y sus resultados para gestión interna del departamento de Bagó IT.

Fase 5: Concienciación

El personal de Bagó IT, así como el personal a cargo de los procesos críticos será el público objetivo de la fase de concienciación. Las necesidades formativas o de concienciación para público objetivo serán temas que tengan que ver con continuidad de negocio (riesgos, medidas preventivas y seguimiento de

procesos) y seguridad de la información. La organización puede hacer uso de diferentes medios para difundir los temas de concienciación mencionados.

La primera opción es difundir a través de la Intranet corporativa, además se enviarán correos electrónicos y también charlas de concientización para lograr la asimilación y adopción del mensaje que se quiere transmitir. Incluso se puede extender la fase de concienciación a terceros o proveedores los cuales sean aliados estratégicos de la empresa. Todo lo anterior mencionado es con el objetivo de lograr una comunicación efectiva con los involucrados y que sean conscientes de la importancia de un plan de continuidad de negocio en todas sus fases.

Plan y métodos de concienciación

Para que el personal comprenda la importancia de la continuidad de negocio y de su propio aporte al mismo, y para que acepte las políticas y comprenda las consecuencias para la empresa, se deben aplicar los métodos de concienciación que se muestran en la Tabla 19 :

Tabla 19

Métodos de concienciación.

Métodos de concienciación	**ene**	**feb**	**mar**	**abr**	**may**	**jun**	**jul**	**ago**	**sep**	**oct**	**nov**	**dic**
Día informativo	X											
Capacitaciones		X					X					
Artículos en la Intranet			X					X				
Reuniones conjuntas			X						X			
Mensajes de correo electrónico interno	X			X			X			X		
Videos informativos				X				X				X
Encuestas de satisfacción						X						X

El cronograma anterior puede variar dependiendo de las estrategias que le convengan a la empresa para no afectar su normal desempeño.

Capítulo IV. Presupuesto referencial del BCP IT propuesto

En este capítulo se presentará un presupuesto referencial de la implementación el plan de continuidad de negocio para Laboratorios Bagó del Ecuador S.A. usando una de las estrategias principales planteadas en el capítulo 3. Según (Leon, 2019).

La estrategia a ser utilizada en la estimación del presupuesto es la Recuperación de la actividad en una ubicación alternativa física o nube (AE1), la opción investigada es la de sitio alterno en la nube. Esta estrategia fue escogida porque responde a la continuidad de una de las actividades más importantes del área tecnológica Bagó IT. Esta actividad es la de Gestión de funcionamiento de la infraestructura física y virtual de servidores (A).

Para implementar el presente proyecto se analizarán los recursos humanos, técnico materiales, financieros y de tiempo que se relacionen con la ejecución de las estrategias que conformarían el plan de continuidad.

Recursos humanos

Los participantes como recursos humanos del proyecto pueden ser internos o de otras compañías que presten servicios a la empresa ejecutora. En este caso los participantes solo serán externos al departamento de tecnología de Laboratorios Bagó del Ecuador S.A.

En la Tabla 20 se mencionan todos los participantes en el proyecto por año, su salario mensual y su salario anual de acuerdo al porcentaje de participación durante la implementación de proyecto y el periodo de soporte y mantenimiento.

Tabla 20

Recursos humanos del proyecto.

Cargo participante	Etapa	% de participación	Salario mensual	Salario anual por participación
Administrador de Base de datos/ Ing. Infraestructura externo	Implementación (3 meses) AÑO 0 [6]	50% (4 horas/día)	$1,700.00	$2,250.00
Administrador de Base de datos/ Ing. Infraestructura externo	Soporte/Mantenimiento (12 meses) AÑO 1	10% (0.8 horas/día)	$1,700.00	$2,040.00

El salario anual por participación después del año de implementación se calcula tomando el salario de $1,700 por la participación del 10% y por 12 meses, lo que da como resultado $2,040. Este valor se considerará en el presupuesto total de recursos humanos externos para el resto de años del contrato, los valores descritos de implementación, soporte y mantenimiento son propuestos por un proveedor del servicio consultado.

Recursos técnicos materiales

En esta sección se describen los recursos materiales técnicos tales como pagos de licencias, transferencia de conocimientos, subcontrataciones y honorarios profesionales por asesoría e implementación. Se logró obtener una propuesta económica de un proveedor mayorista de telecomunicaciones con el cual se dimensionó los requerimientos para un sitio alterno en la nube. Ver propuesta en el Anexo H.

[6] AÑO 0, momento en el tiempo donde se realizan las inversiones fijas de un proyecto de inversión, su duración depende el tempo de implementación.

El dimensionamiento se basó en cantidad de servidores y en las características principales de estos servidores como procesadores, memoria RAM y demanda de almacenamiento. Los servidores escogidos fueron Base de datos, correo, aplicaciones, almacenamiento y servicios, los mismos considerados como activos críticos para dar continuidad a la actividad A en este estudio. La duración del contrato en la oferta es de 36 meses (3 años) y el tiempo de implementación una vez acordado con el proveedor será de 3 meses. Además, se consideró un RTO de 4 horas el cual está dentro de las recomendaciones de este estudio (7 horas).

La Tabla 21 muestra los recursos técnicos materiales necesarios para la implementación del plan de continuidad de negocio.

Tabla 21

Recursos técnico materiales.

Recursos necesarios	Costo mensual	Costo año 0	Costo anual
Sitio alterno en la nube	$1,754.33	$0	$21,051.96
Implementación Sitio (un solo pago año uno)	$1,280.00	$1,280.00	$0
Enlace Dedicado de 30 MB desde la Sucursal Quito hacia el Data Center de proveedor	$750.00	$0	$,9000.00
Implementación enlace de datos (un solo pago año uno)	$200.00	$200.00	$0
Total		**$1,480.00**	**$30,051.96**

Presupuesto estimado del proyecto

El presupuesto total es proyectado a tres años, tiempo en el cual estará vigente el contrato con el proveedor y por ende el plan de continuidad con la actual tecnología, pasado este tiempo se considera renovar el contrato con tecnología a la fecha, lo que puede mejorar el servicio y el costo, esto se puede ver en la Tabla 22.

Tabla 22

Proyección de la inversión de recursos.

Elementos de gastos	Año 0	Año 1	Año 2	Año 3	Total
Recursos Humanos externos Salario participantes en el proyecto	$2,250.00	$2,040.00	$2,040.00	$2,040.00	$8,370.00
Recursos técnicos materiales Sitio alterno en la nube, enlace de datos e implementaciones	$1,480	$30,051.96	$30,051.96	$30,051.96	$91,635.88
Total Costos BCP Bagó IT	**$3,730.00**	**$32,091.96**	**$32,091.96**	**$32,091.96**	**$100,005.88**

Como se puede apreciar en la tabla anterior, se proyecta una inversión importante, el año 0 es menor porque se solo se consideran los costos de implementación y no del servicio, para los siguientes años los costos son mayores y constantes durante el tiempo de contrato. Esta inversión se la justificará en el siguiente apartado.

Relación Costo - Beneficio

Según (ISACA, 2012). Para valorar el costo y benéfico de la implementación del proyecto, se calculará el ROI que es uno de los indicadores financieros para calcular los resultados financieros de las inversiones de una empresa. También, para tener un panorama más preciso de las consecuencias financieras de este proyecto, se calcularán otros indicadores financieros como: Flujo de fondos, valor presente neto y tasa interna de retorno.

Para el año 0, se dimensionaron costos de RRHH, mercadería y costo de contacto de 3 meses, tiempo que dura la implementación de la estrategia de BCP. Es decir, en el año 0 se dividieron para 3 los rubros

correspondientes del año 1. Para los años posteriores se consideró la inflación de 2019 que fue de 0.19%[7]. La inversión se realizará con fondos propios (Tasa de descuento 0%).

Costo en personal de RRHH, se tienen 260 trabajadores, 180 pertenecen al área de ventas y 80 al área administrativa, entre todos al año se paga por nómina de $5,760,000.00; y los sueldos tienen un aumento anual se de la inflación del anterior año (0.19%).

Con respecto a la adquisición de mercadería o productos para su promoción y venta, la empresa los adquiere a un costo de $ 20,000,000.00 por año, aplicado la inflación para los próximos años.

La fuerza de ventas de Laboratorios Bagó del Ecuador S.A. realiza 32,400 contactos al mes (180 visitadores, realizando 9 contactos por día, mes de 20 días laborables), se denomina contacto a la visita que se realiza a un médico. El costo por contacto es de $20, este valor implica todo los que se invierte para que un representante médico realice una visita, donde se incluye, costo de muestras médicas, desplazamientos, desarrollo de estrategias de marketing multimedia, acceso a la tecnología y promociones comerciales.

Entonces, realizando el cálculo del costo total de contactos al mes sería de $648,000. Este valor dividido para el número de días trabajados al mes (20) da un valor de $32,400 por día. Al año el costo es de $7,776,000.00; también para el cálculo al resto de años se aplica la misma inflación.

Los datos anteriores fueron proporcionados por diferentes departamentos de la empresa, entre ellos el Departamento de Gestión Estratégica y son aproximados, no se muestran datos exactos por acuerdos de confidencialidad. La Tabla 23 muestra los valores de costos, ingresos y flujo de fondos de la compañía en los próximos 3 años, se enlista elementos de costos como recursos humanos (RRHH), adquisición de

[7] Banco Central del Ecuador (BCE), la inflación 2019 es de 0.19% según publicación del su página web: https://contenido.bce.fin.ec/documentos/PublicacionesNotas/Notas/Inflacion/inf202005.pdf

mercadería, costo del contacto y se incluye el costo del plan de continuidad de negocio de Bagó IT. Por último, se incluyen los ingresos constantes por ventas anuales (ventas en el 2018).

Tabla 23

Flujo de fondos de la compañía.

Elementos	0	1	2	3
RRHH	$ 1,920,000.00	$ 5,760,000.00	$ 5,770,944.00	$ 5,781,908.79
Mercadería	$ 6,666,666.67	$ 20,000,000.00	$20,038,000.00	$20,076,072.20
Costo Contacto	$ 2,592,000.00	$ 7,776,000.00	$ 7,790,774.40	$ 7,805,576.87
BCP Bagó IT	$ 3,730.00	$ 32,091.96	$ 32,091.96	$ 32,091.96
Total costos	$ 11,182,396.67	$ 33,568,091.96	$33,631,810.36	$33,695,649.82
Total ingresos		$ 48,000,000.00	$48,000,000.00	$48,000,000.00
Flujo de fondos (FNE)	**$ (11,182,396.67)**	**$ 14,431,908.04**	**$14,368,189.64**	**$14,304,350.18**

La Tabla 24 muestra los indicadores financiaros que ayudan a la toma de decisiones para saber si se procede con la inversión.

Tabla 24

Indicadores financieros de rentabilidad.

Indicador	Sigla	Valor
Valor Presente Neto	VPN	$ 31,922,051.19
Tasa Interna de Retorno	TIR	116%
Beneficio	B	$144,000,000.00
Costo	C	$112,077,948.81
Relación Costo-Beneficio	B/C	1.28
Retorno de Inversión	ROI	28%

Según la tabla anterior, la TIR nos da 116% lo que indica que nos conviene realizar la inversión, además, la relación Costo-Beneficio es bastante aceptable con 1.28, para finalizar el ROI nos muestra una rentabilidad del 28% lo cual nos indica que se debe realizar la inversión.

Análisis de beneficios

Como se observa se necesita una importante inversión para la implementación de este plan de continuidad de negocio, sin embargo, es justificable por las pérdidas económicas que se generarían por la falta del plan. Al presente plan, haciendo una analogía, se lo considera como un seguro de vida, el cual se lo paga para estar protegidos financieramente si ocurre algún evento inesperado.

A continuación, un análisis de las pérdidas de la empresa en caso de ocurrir un evento disruptivo o contingencia.

El costo de interrupción de los servicios tecnológicos ocasiona pérdidas monetarias y de imagen, esto basado en que se puede interrumpir por completo la gestión de la infraestructura física y virtual de servidores, donde corren procesos críticos como el de facturación o el de correo electrónico.

En el 2018 la empresa facturó 48 millones de dólares, esto dividido para el número de días laborados al año (260), resulta que se factura $184,615.38 al día, este valor por hora laborable (8) da $23,076.92; este cálculo muestra el costo de interrupción por horas si se deja de laborar de manera normal.

Por ejemplo, si la empresa interrumpe sus operaciones por algún incidente o evento inesperado por 4 horas, puede llegar a perder $92,307.69.

Como se puede apreciar el contar con el plan de continuidad de negocio para el área tecnológicas puede evitar grandes pérdidas monetarias a la empresa.

Capítulo V. Conclusiones y recomendaciones

Conclusiones

- Del diagnóstico realizado sobre la situación actual de la empresa con respecto a continuidad de negocio, seguridad de información, gestión de activos, y seguridad física; se concluye que, Laboratorios Bagó del Ecuador S.A no cuenta con un BCP y no se aplican medidas para la seguridad de la información, la identificación de amenazas y la aplicación de salvaguardas para tratar riesgos que afecten a la continuidad de operaciones en casos de desastre o de interrupción de actividades.
- Del estudio realizado en este trabajo, se corrobora que Bagó IT dentro de la cadena de valor de la empresa apoya a toda la organización a través de su infraestructura tecnológica, además sus servicios aportan al desarrollo de las operaciones en sus diferentes áreas, como son: Ventas, Logística, Marketing, Contabilidad, Departamento Técnico, Entrenamiento y Finanzas. Por lo tanto, es un área fundamental para aplicar un BPC.
- La presente investigación propone un BCP para el departamento de Bagó IT fundamentada en las buenas prácticas dictadas por instituciones avaladas en temas de ciberseguridad y en el estándar ISO 22301, donde se incluyen, el estudio de la situación actual, análisis de impacto del negocio, análisis de riesgos y se determinan estrategias de recuperación en base a los recursos tecnológicos analizados. Asimismo, esta investigación sirve como soporte para la creación de un BCP integral el cual vincule a todos los departamentos de la empresa.
- La actividad que debe ser restaurada con mayor prioridad en Bagó IT es la de Gestión de funcionamiento de la infraestructura física y virtual de servidores, puesto que en esta actividad están concentrados todos los servicios que Bagó IT brinda a la organización, por lo tanto, se deben enfocar todos los esfuerzos en minimizar riesgos y mejorar su gestión de continuidad y así

disminuir el impacto que pueda causar la interrupción de esta actividad.

- De la aplicación de la herramienta EAR/PILAR, se concluye que, las amenazas más recurrentes relacionadas a los activos físicos de Laboratorios Bagó del Ecuador S. A. son: fuego, daños por agua o inundaciones, corte del suministro eléctrico y desastres naturales.
- De acuerdo al análisis de riesgos y las salvaguardas, se evidenció que el estado actual de madurez con respecto a la continuidad del negocio es inexistente (L0) en la empresa, además se pudo observar que el Plan de Recuperación de Desastres (DRP) tiene un peso crítico, este DRP ayuda a mantener y coordinar actividades para recuperar la infraestructura tecnológica. Por lo tanto, según los resultados la implementación de un BCP para Laboratorios Bagó del Ecuador S.A. ayudará a que incremente su nivel de madurez a L3 (en funcionamiento) y aumentar la capacidad de recuperación de las actividades de la organización.
- La inversión en un plan de continuidad para el departamento de IT del Laboratorios Bagó del Ecuador S.A es justificable, por el resultado positivo de los indicadores financieros, desde el punto de vista organizacional mejora su nivel de madurez en términos de seguridad informática y desde el monetario protege a la empresa de pérdidas económicas.
- Esta propuesta investigativa dará la pauta para futuras implantaciones de planes de continuidad de negocio en otras empresas, además pretende concienciar y resaltar la importancia de asegurar las operaciones de un negocio y reaccionar de manera proactiva frente a desastres.

Recomendaciones

- Se recomienda el levantamiento de la documentación de todos los procesos internos de Bagó IT para restaurar los servicios críticos que se puedan ver perjudicados y así poder recuperar las actividades a su estado normal.

- Para el éxito del plan de continuidad de negocio es esencial involucrar a todo el personal de la empresa: directivos, personal de IT, jefaturas, recursos humanos y el usuario final.
- En esta investigación se identificó que en el año 2014 las instalaciones de Laboratorios Bagó del Ecuador S.A sufrieron eventos no deseados como: inundaciones, sismos y corte de suministro eléctrico, por esta razón se recomienda adoptar las salvaguardas aplicables a dichos eventos para minimizar el riesgo y en caso de producirse alguna interrupción se deben aplicar las estrategias de recuperación acordes a estos eventos disruptivos, estas estrategias son: AE1 (Recuperación de la actividad en una ubicación alternativa física o en la nube) y BE1 (Sistema redundante de suministro de energía eléctrica).
- Para aumentar el nivel de madurez de la organización con respecto a la continuidad de negocio y seguridad, se recomienda aplicar medidas correctivas o preventivas que minimicen el riesgo de ocurrencia e impacto, estas medidas son las salvaguardas descritas en el apartado 3.2.3.4 de este documento y se las puede aplicar dependiendo de la naturaleza de la amenaza.
- Uno de los activos más importantes es el personal o recurso humano de la empresa, por lo que se recomienda vincular en el plan de continuidad al comité paritario y al técnico de seguridad y salud ocupacional, para precautelar la integridad de las personas a través de sus brigadas: evacuación, primeros auxilios, incendios y comunicación.
- También se recomienda un plan de gestión del conocimiento, esto permitirá que exista el reemplazo correspondiente del desarrollo de las funciones en caso de la ausencia de algún miembro del personal de Bagó IT, y así esta persona tenga todo el conocimiento de los procesos del plan de continuidad de negocio.

- Las pruebas del plan de continuidad deben realizarse en entornos controlados y con la previa notificación a los usuarios de la realización de mantenimiento a la infraestructura, puesto que existe personal que trabaja fuera de horarios de oficina y requiere de los servicios tecnológicos.
- De acuerdo a los resultados de esta investigación, se recomienda la implementación de este plan de continuidad de negocio para el departamento de tecnología de la organización. Además, se enfatiza iniciar por este departamento, porque según los resultados es el que más procesos de negocio críticos apoya, y en la actualidad según las nuevas tendencias tecnológicas como la transformación digital, las TICs ya son consideradas como pieza estratégica para el desarrollo del negocio en las empresas.

Referencias

27001Academy. (2014). *Lista de documentación requerida para ISO 22301.* https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/ES/Checklist_of_ISO_22301_Mandatory_Documentation_ES.pdf

Advisera. (2017). *27001/ISO 22301 Knowledge base*. 27001 Academy. https://advisera.com/27001academy/knowledgebase/laws-regulations-information-security-business-continuity/

Ayuda EAR/PILAR, C. (2018). *PILAR Análisis y Gestión de Riesgos Ayuda.* https://www.pilar-tools.com/doc/v72/help_es_e_72.pdf

Centro Criptológico Nacional. (abril de 2017). *Guía de Seguridad de las TIC.* https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/2142-ccn-stic-472f-manual-de-usuario-pilar-basic-6-2/file.html

Cevallos, J. (2015). *Plan de continuidad de negocio aplicado al centro de datos de la fiscalización del proyecto hidroeléctrico Coca Codo Sinclair.* [Tesis de maestria]. Universidad de las Fuerzas Armadas ESPE.

INCIBE. (2016). *Plan de Contingencia y Continuidad de Negocio.* https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

INCIBE. (16 de enero de 2017). *Análisis de riesgos en 6 pasos.* https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Instituto Geofísico, E. (2016). *Informe Sísmico Especial N.13.* Escuela Politécnica Nacional. https://www.igepn.edu.ec/servicios/noticias/1317-informe-sismico-especial-n-13-2016

INTECO. (2016). *Guía práctica para PYMES: Cómo implantar un Plan de Continuidad de Negocio.* https://opinit.files.wordpress.com/2010/11/guia_practica_para_pymes_como_implantar_un_plan_de_continuidad_de_negocio.pdf

International Dynamic Advisors, I. (Julio de 2016). *Sistemas de Continuidad del Negocio.* http://www.intedya.com/productos/riesgos%20y%20seguridad/ISO%2022301/07%202016%20ISO%2022301_%20PIC_%20ed00.pdf

ISACA. (julio de 2012). *Calcular el ROI de la nube: Desde la perspectiva del cliente*. https://www.isaca.org/

ISO 22301. (2012). *Seguridad de la Sociedad: Sistemas de continuidad de Negocio- Requisitos*. https://www.iso.org/standard/75106.html

Leon, F. M. (11 de 2019). *Guía metodológica para elaborar la propuesta de proyecto de innovación.* https://docplayer.es/25631262-Guia-metodologica-para-elaborar-la-propuesta-de-proyecto-de-innovacion.html.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

MINTIC. (2015). *Guía para realizar el Análisis de Impacto de Negocios BIA*. https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

Portal de Administración Electrónica. (2014). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XNDbq6R7ncc

Anexos