DISEÑO DEL PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA, ALINEADO CON LA POLÍTICA DE GOBIERNO DIGITAL DEL MINISTERIO DE LAS TIC

JHONATAN CASTILLO PALLARES
JULIETH PAOLA SUÁREZ MOGOLLÓN

UNIVERSIDAD POPULAR DEL CESAR
FACULTAD DE INGENIERÍA Y TECNOLOGÍAS
PROGRAMA INGENIERÍA DE SISTEMAS
LINEA DE INVESTIGACIÓN EN INGENIERÍA DEL SOFTWARE
AGUACHICA, CESAR
2025

DISEÑO DEL PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA, ALINEADO CON LA POLÍTICA DE GOBIERNO DIGITAL DEL MINISTERIO DE LAS TIC

JHONATAN CASTILLO PALLARES
JULIETH PAOLA SUÁREZ MOGOLLÓN

Proyecto de grado para optar el título de Ingeniera de sistemas, modalidad presencial.

Director
Ing. Erney Alberto Ramírez Camargo

Co-director
Ing. Didier Fernando Guerrero Sumalave

UNIVERSIDAD POPULAR DEL CESAR
FACULTAD DE INGENIERÍA Y TECNOLOGÍAS
PROGRAMA INGENIERÍA DE SISTEMAS
LINEA DE INVESTIGACIÓN EN INGENIERÍA DEL SOFTWARE
AGUACHICA, CESAR
2025

DEDICATORIA

A mi madre Sandra Mogollón Zambrano, a mi padre Eduvin Suárez Carballo, por ser mi bastón, por ser mis guías, por la confianza y por darme la oportunidad de lograr y vivir este momento que tanto han anhelado, por no rendirse a pesar de las adversidades porque este logro es más suyo que mío, por ustedes y para ustedes.

A mis hermanos Andrés Mauricio Suárez Mogollón, Oscar Humberto Suárez Mogollón, José Alfredo Suárez Mogollón, por creer en mí, por su apoyo y por ser mi otro motivo para lograr este propósito de vida.

Para ese corazón que en su momento relució y palpito lleno de vida y ahora es un ángel danzando en el firmamento, ese ser que inicio este camino conmigo y ahora tengo la bendición de terminar por las dos, tu presencia deja un eco armonioso que perdurara hasta el fin de los días, en tu memoria Bresly Seleny Ojeda Ramírez…

Julieth Paola Suárez Mogollón.

A mi madre Rosalba Pallares Sánchez, por ser mi sostén, mi apoyo, por ser quien me da la fuerza para continuar y lograr cada uno de mis objetivos.

Jhonatan Castillo Pallares.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos principalmente a Dios por otorgarnos la oportunidad de despertar cada día, vivir con salud, amor, felicidad al lado de los nuestros, por guiarnos por el camino del bien y la prosperidad.

Al Ingeniero Erney Alberto Ramírez Camargo, director de proyecto, por ser un excelente guía y apoyo, por su dedicación, su tiempo, su comprensión en la realización de este proyecto y cumplimiento de este logro.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

1. PROBLEMA DE INVESTIGACIÓN

De acuerdo a Gordillo (2017), la información es uno de los activos más importantes dentro en una organización, ya sea por seguridad y protección de dicha información manejada, además; se ha convertido en un activo indispensable, debido a que con esto se busca salvaguardar y proteger la información y los procesos ante riesgos y amenazas. Anteriormente las empresas hacían uso de redes intranet para proteger la información, pero han modificado su modus operandi debido a la expansión generada por los negocios, es por eso que el autor expresa que con la apertura de internet se perdió la idea de las redes internas.

A nivel mundial hay un incremento considerable en el número de organizaciones que se plantean de forma empírica, es decir, se forman a través de la experiencia, y esto conlleva a una mala organización de la información, y que a su vez haya pérdida de información muy fácilmente. Toda esta falta de organización en las instituciones ha llevado al ministerio de las TIC a regular iniciativas que normalicen los Planes de Gestión de Continuidad del Negocio en las instituciones, debido a que es indispensable tener un plan de contingencia, para que asegure el correcto funcionamiento de las operaciones de las empresas relacionadas (MinTIC, 2010a).

La seguridad en las organizaciones es uno de principales recursos de la información, por lo tanto, se protege por medio de políticas de seguridad, controles, que se han de implementar con base a los recursos humanos, hardware y software disponible, por lo tanto, el incumplimiento de alguna de estas políticas puede llevar a sanciones graves para la empresa (Vega Velasco Walter, 2008) por lo anterior en el contexto particular, se encuentra que la UPC no cuenta con un plan o norma que regule el respaldo de la información manejada por la entidad.

La falta de interés por parte de algunas empresas de proteger bien la información, las hace más vulnerables contra ataques y robos de información, además de no contar con planes que aseguren la continuidad operativa (Delgado, 2015). En una entrevista realizada a la persona responsable de gestión de calidad se evidenció que la Universidad Popular del Cesar, Seccional Aguachica no cuenta un con plan de contingencia o continuidad en caso de fallas eléctricas, naturales, incendios, entre otras. No se cuenta con estrategias para responder ante estos incidentes ya que todo se maneja desde la sede central, no se han evaluado los riesgos para determinar el impacto de dichas interrupciones tanto en términos de magnitud de daños como de periodo de recuperación además en caso de que ocurra una catástrofe ya sea natural o causada por el hombre dentro de la universidad se presentarían daños y destrucción de la infraestructura (Ojeda Ramirez & Suárez Mogollón, 2021).

1.1. FORMULACIÓN DEL PROBLEMA

Con base en la problemática mencionada anteriormente, se plantea la siguiente pregunta de investigación: ¿Cómo el diseño de un Plan de Gestión de Continuidad del Negocio permite reducir el impacto de eventos disruptivos y de igual manera garantizar la continuidad de los procesos críticos de la Universidad Popular del Cesar, Seccional Aguachica?

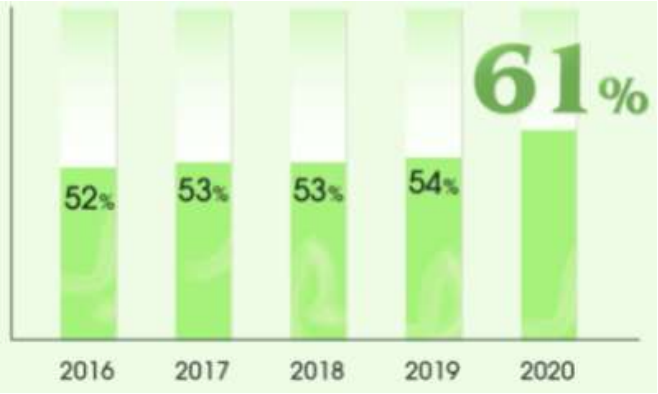
1.2. JUSTIFICACIÓN

Ati Guillen (2018), en su investigación resalta el desarrollar procesos y procedimientos en caso de presentarse diversas eventualidades anormales o sorpresivos que puedan interrumpir los servicios prestados y la pérdida de información alojada en el lugar del siniestro. Por todo esto, para las instituciones es de vital importancia estar prevenidos para posibles situaciones de riesgo contra la seguridad de la información, con la cual se puedan determinar las funciones más críticas de la empresa y reforzarlas para cuestiones de emergencias no previstas (Montserrath Range, 2017), es por eso que la implementación y regulación de estos planes de contingencia en casos de desastre o pérdida de la información alojada en las instituciones, todo esto con el fin de minimizar pérdidas de tipo económica, como también minimizar interrupciones en el servicio y la disponibilidad de la información. El tener un Plan de Gestión de Continuidad de Negocio es una gran ventaja, debido a que los usuarios van a tener un respaldo ante las posibles situaciones mencionadas anteriormente.

Las instituciones que no prevén estos tipos de imprevistos y no están preparados contra posibles desastres, estarían propensas a desaparecer debido a que además que se les dificultará operar, sus ingresos se verán seriamente afectados (Torchio, 2020). Para la Universidad Popular del Cesar, Seccional Aguachica es de suma importancia, un plan de gestión que proteja la operatividad de la información almacenada en las instalaciones de la UPC, Seccional Aguachica por docentes, estudiantes y personal administrativo en caso de presentarse desastres naturales, robo de información, fallas en los sistemas hardware y software, entre otras posibles eventualidades.

Un estudio realizado por la firma Data Health Check en el 2019 un 54% de las organizaciones contaban con un plan de este tipo y para el año 2020 aumento hasta el 61%, a consecuencia del coronavirus.

Figura 1. Crecimiento de implementación de un plan de continuidad



Fuente: Data Health Check

En su informe se destaca que actualmente el 61% de las organizaciones cuenta con un Plan de Continuidad del Negocio actualizado, antes de la pandemia el 66% no tenía un plan de respuesta frente a situaciones como las que ha provocado el coronavirus, ahora el 85% ya cuenta con un plan de recuperación de desastres TI dentro de su estrategia de Plan de Continuidad del Negocio y el 65% de ellos lo ha usado en los últimos 12 meses. Finalmente, la encuesta refleja que el 89% de los encuestados tiene plena confianza en sus planes de recuperación ante desastres (Rodríguez, 2020).

1.3. OBJETIVO GENERAL.

Diseñar el Plan de Gestión de Continuidad del Negocio para la Universidad Popular del Cesar, Seccional Aguachica, alineado con la política de Gobierno Digital del Ministerio de las TIC.

1.3.1. Objetivos específicos.

1. Realizar un diagnóstico sobre la situación actual de la Universidad en cuanto a la aplicación de la estrategia de Gobierno Digital.

2. Analizar los componentes del modelo gestión de continuidad del negocio con base en los requerimientos normativos.

3. Elaborar una guía para gestión de continuidad del negocio orientada a la Universidad Popular del Cesar, Seccional Aguachica.

4. Construir el cronograma de implementación, evaluación, seguimiento y mejora continua del plan de gestión de continuidad del negocio para la Universidad Popular del Cesar.

1.4. DELIMITACION.

1.4.1 Temporal. El desarrollo de este proyecto de investigación se llevará a cabo en un lapso de 6 meses a partir de la aprobación del formato dos (2).

1.4.2 Espacial. El desarrollo de este proyecto de investigación se realizará en la Universidad Popular del Cesar, en el municipio de Aguachica, al sur del departamento del Cesar, en la carrera 40, vía al mar.

1.4.3 Contextual. Aguachica segunda ciudad del Departamento del Cesar, está ubicada al sur del departamento del Cesar, a los 8º 18’ 45” de latitud norte y 73º 37´37” de longitud oeste del meridiano de Greenwich, entre la cordillera oriental y el valle del río Magdalena, a una distancia de 301 kilómetro de Valledupar, la capital del Cesar. Su extensión territorial es de 876.26 kilómetros cuadrados que ocupa el 3,8% de la superficie del 24 departamento. Limita por el norte con el municipio de La Gloria (Cesar), El Carmen (Norte Santander), por el este con Rio de Oro (Cesar), por el sur con San Martín (Cesar) y Puerto Wilches (Santander), por el oeste con Gamarra (Cesar) y Morales (Bolívar).

El territorio de Aguachica tiene una zona montañosa al norte, representadas por las estibaciones noroccidentales de la cordillera oriental con elevaciones entre los 200 y 2.150 metros sobre el nivel del mar (msnm); al sur una zona de planicie o llanura regada por los ríos Lebrija y Magdalena y sus numerosas quebradas y arroyos hoy disminuidos drásticamente por la deforestación, su fisiografía oscila entre los 50 y los 200 msnm. Presenta un clima con temperatura promedio de 28 ºC y precipitación media anual de 1.835 mm, con dos periodos de lluvias al año (Web, 2020).

Figura 2. Mapa geográfico de Aguachica

Fuente: Google Maps

2. MARCO REFERENCIAL

En este capítulo se describe la base conceptual y teórica que sustenta el proyecto de investigación. En la sección 2.1 se describe los trabajos existentes relacionados con el proyecto. La sección 2.2 se presenta la base teórica de la política de Gobierno Digital: concepto, propósitos y elementos. La sección 2.3 presenta el marco legal del proyecto. La sección 2.4 se presentan los conceptos relacionados con el Plan de Gestión de Continuidad del Negocio.

2.1. ESTADO DEL ARTE

A nivel internacional se encuentran diversos referentes teóricos que han propuesto y diseñado un Plan de Gestión de Continuidad del Negocio que permite la continuidad de las operaciones antes, durante y después de una interrupción en una organización.

Matos (2021) presenta un trabajo de investigación que tuvo como objetivo proponer un Plan de Continuidad de Negocio en el área de producción de una empresa cosmética peruana, como ventaja competitiva para afrontar eventos disruptivos (incidente que puede causar una desviación negativa no planificada de la entrega esperada de productos o servicios de una organización) que se presenten en el trascurso del tiempo y que pueda comprometer la resiliencia de la organización. La metodología consistió en realizar el análisis situacional de la empresa identificando tres procesos críticos que son fabricación, envasado y acondicionado. Seguidamente se realizó la evaluación de riesgo iniciando con la identificación de las amenazas externas a las que está expuesta la empresa y posteriormente se identificó las amenazas internas a las que están expuestas los procesos críticos, se analizó la vulnerabilidad y la probabilidad de ocurrencia. Finalmente se asignó un valor al riesgo para ser evaluado en el Análisis de Impacto en el Negocio (BIA). Se concluyó con la propuesta de un Plan de Continuidad de Negocio en el área de producción que permitirá adoptar estrategias para salvaguardar el proceso operativo y seguir produciendo a un mínimo aceptable durante un evento disruptivo para cumplir con las expectativas de las partes interesadas.

Del corral & Pinargote (2019) presentan una propuesta de Diseño de un Plan de Continuidad de Negocio para las operaciones alineado a COBIT 5 para CORPQSF S.A, se desarrolló con el fin de brindar a la empresa una forma de precautelar que sus servicios estén disponibles de forma ininterrumpida y de esta manera poder continuar con sus operaciones de forma total o parcial, hasta poder resolver la eventualidad presentada, consiguiendo así el objetivo de estar

operativo 24x7 y de esta manera brindar a sus clientes un servicio que les permita la continuidad de sus operaciones. También se evaluaron condiciones financieras para determinar la factibilidad de la propuesta que permita a la empresa obtener el mayor beneficio posible.

Segura (2019) presentó un estudio que se llevó a cabo en la planta de la empresa Irex de Costa Rica S.A, ubicada en Concepción de Tres Ríos, ésta se dedica a la comercialización de productos de limpieza. Las operaciones de esta industria química implican que sus colaboradores y la comunidad vecina se expongan a fallas tecnológicas en los mecanismos de producción, tales como: fuga de gas cloro, fuga de ácido sulfónico, explosión de calderas, derrames de sustancias químicas e incendios. Actualmente, los peligros se mantienen latentes y en caso de no intervenir, la continuidad del negocio estaría en juego. Debido a esto, se plantea como objetivo general proponer un Plan de Continuidad del Negocio ante desastres tecnológicos. Ahora bien, con el fin de lograr el objetivo, inicialmente se aplicó una lista de verificación para medir el cumplimiento con los parámetros de la INTE/ISO 22301:2015, se identificaron los procesos de soporte, operativos y de apoyo mediante entrevistas y grupos focales. Igualmente, se determinó periodos máximos tolerables de interrupción. Por último, se evaluó cada uno de los riesgos tecnológicos. Concluyendo que la gestión de la empresa Irex de Costa Rica S.A., no cuenta con una estrategia en la prevención y recuperación de procesos críticos. Por lo que se desarrolla documentalmente un Plan de Continuidad de Negocio de acuerdo a los requisitos de la norma. Incluyendo responsables, tareas por ejecutar, protocolos de emergencia, procedimientos de gestión y otros aspectos.

A nivel nacional también se encuentran diferentes referentes teóricos que han diseñado e implementado un Plan de Gestión de Continuidad del Negocio.

Para Sánchez (2015) el principal objetivo de este trabajo es la realización del Plan de Continuidad del Negocio para la E.S.E Hospital Emiro Quintero Cañizares, determinándose la necesidad de evaluar los riesgos tecnológicos, para cual se realizó una serie de encuestas y visitas donde se evaluó y valoró la situación actual en la que se encuentra la empresa, para el logro de objetivos, se planteó el diseño de formatos.

Tellez (2015) fundamenta su proyecto en aplicar la norma ISO 22301 para el diseño del Plan de Gestión de Continuidad del Negocio en la oficina de informática y telemática de la alcaldía de Cali con el fin de lograr y mejorar la disponibilidad de los servicios que esta presenta hacia otras dependencias y la ciudadanía. Se realizó el Plan de Continuidad de Negocio para los 5 servicios críticos de la asesoría (canal internet, intranet, portal municipal, plan de gestión documental y el correo) con base a la metodología establecida por la norma. Se inicia con un Análisis de Impacto del Negoció para la determinación de los servicios y tiempos críticos de recuperación, es decir, determinar el tiempo máximo tolerable en el cual se debe recuperar un servicio sin que este cause un

impacto significativo en la organización; una vez concluida esta parte se procede a la realización del Análisis de Riesgo para la identificación y tratamiento de los riesgos bajo la metodología impuesta por el departamento de la función pública; con base a los tiempos obtenidos por el BIA1∗ y la sugerencia de los controles identificados gracias al Análisis de Riesgos, se procede a la búsqueda de una estrategia de respaldo tanto interna como externa , que asegure, la disponibilidad de la información, aun cuando sea de gran dificultad el acceso o se presente un incidente que deje de manera inoperante la torre de la alcaldía y finalmente realizamos los procedimientos preventivos y correctivos que sirvan de constancia para los demás funcionarios sobre el cómo realizar una recuperación de un determinado servicio, y el Plan de Continuidad en el cual se establece el procedimiento que se debe manejar cuando se presente algún incidente.

Malaver (2020) presenta su estudio el cual se realizó en Bancompartir, con sede principal ubicada en Bogotá, consistió en el análisis de la información suministrada por líderes de los procesos del Banco y observaciones tomadas en el sitio con el fin de generar el marco de conocimientos necesario al tema en estudio: "Diseño de un Plan de Continuidad del Negocio". A partir del análisis realizado se puede concluir que los procesos que presentan mayor criticidad son los clasificados como misionales que son los que sostienen la operación del negocio. Se estableció una estrategia de Continuidad del Negocio basada en los procesos críticos y en los recursos como personal, aplicativos, costos y tecnología que son necesarios para que puedan operar, todo enfocado a mantener el servicio en caso de un evento de indisponibilidad.

A nivel local en el departamento del Cesar se encuentra como referente una investigación desarrollada por los especialistas Karen Lorena León y Danny Jhoan Ríos quienes plantean de forma clara y precisa la necesidad de diseñar el Plan de Continuidad del Negocio en el área de Tecnologías de la Información del proyecto Ruta del Sol - Sector 2, siendo este, el objeto a investigar en este proyecto. Se realizó un análisis de los posibles riesgos potenciales y las vulnerabilidades a las cuales están expuestos los equipos de cómputo y sistemas de información, con el fin de elaborar un diagnóstico que permita evaluar y valorarlos para la toma de decisiones y/o estrategias técnicas y sistemáticas que ayude a mitigarlos. Para el desarrollo del Plan de Continuidad del Negocio se tomó como referencia el análisis y la comparación de las normativas existentes conocidas como ISO/IEC 27001:2005, ISO/IEC 27002:2007, NTC 5722, NIST 800-34, NFPA1600:2010 Y ASIS SPC.1:2009 que permitirá a la empresa establecerlo como un instrumento en la continuidad de las actividades y operaciones tecnológicas,, garantizando las posibilidades de supervivencia y disminuyendo el impacto en las pérdidas que podría afectar la credibilidad de la empresa (León & Rios, 2017).

2.2. MARCO TEÓRICO

En esta sección se describe la fundamentación teórica de este proyecto, divida de la siguiente manera a saber: (i) Política de Gobierno Digital; (ii) propósito de la política y, (iii) estructura de la política.

2.2.1 ¿Qué es la política de Gobierno Digital? De acuerdo a MinTIC (2018) Gobierno Digital es la política pública que tiene como finalidad "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".

2.2.2 Propósito de la política. Impactar positivamente la calidad de vida de los ciudadanos y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado (MinTIC, 2022b).

2.2.3 Estructura de la política. La Política de Gobierno Digital se lleva a cabo mediante un esquema que articula los elementos que la componen, con la finalidad de lograr su objetivo, entendidos de la siguiente manera:

Gobernanza: Es uno de los elementos transversales de la política que se relaciona con la implementación de la Política de Gobierno Digital basada en el relacionamiento de orden nacional y territorial y el nivel central y descentralizado, involucrando a los grupos de interés en la toma de decisiones, la definición de focos estratégicos y en la distribución eficiente de los recursos.

Innovación Pública Digital: Es el segundo componente transversal, se basa en la implementación de la política a través del relacionamiento con los Grupos de Interés (sector privado, academia civil, ciudadanos, sociedad civil y entidades públicas), que genere valor público a través de la introducción de soluciones novedosas y creativas y que hagan uso de las Tecnologías de la Información y las Comunicaciones y de metodologías de innovación, para resolver problemáticas públicas desde una perspectiva centrada en los habitantes del territorio nacional.

Habilitadores: Son los encargados de generar capacidades para ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores:

(i) *Arquitectura:* Busca el fortalecimiento institucional a través del enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de proyectos con componentes de TI, los cuales deberán estar articulados con su orientación estratégica, su modelo de gestión, su plan de transformación digital y su estrategia de TIC.

(ii) *Seguridad y Privacidad de la Información:* Su objetivo es desarrollar capacidades en la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

(iii) *Cultura y Apropiación:* Busca desarrollar las capacidades requeridas para el acceso, uso, aprovechamiento y apropiación de las TIC entre las personas en situación de discapacidad y fomentando su inclusión con enfoque diferencial.

(iv) *Servicios Ciudadanos Digitales:* Busca mejorar la interacción con la ciudadanía y garantizar su derecho a la utilización de medios digitales ante la administración pública.

Líneas de Acción: Son acciones orientadas a: desarrollar servicios y procesos inteligentes, tomar decisiones basadas en datos y consolidar un Estado abierto. Estas acciones tienen como objetivo articular las Iniciativas Dinamizadoras de la Política de Gobierno Digital. Hacen parte de las Líneas de Acción las siguientes:

(i) *Servicios y Procesos Inteligentes:* Busca el desarrollo de servicios y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad, a partir del entendimiento de las necesidades del usuario y su experiencia con esquemas de atención proactiva y el uso de tecnologías emergentes.

(ii) *Decisiones Basadas en Datos:* Busca el desarrollo económico y social del país impulsado por datos, con mecanismos de gobernanza para el acceso, intercambio, reutilización y explotación de los datos, que den cumplimiento a las normas de protección y tratamiento de datos personales y permitan mejorar la toma de decisiones y la prestación de servicios.

(iii) *Estado Abierto:* Busca la transparencia en la gestión pública con un enfoque de apertura por defecto, confianza social e institucional, colaboración y participación efectiva de los Grupos de Interés, para fortalecer la democracia y dar soluciones a problemas de interés público a través de prácticas innovadoras con TIC.

Iniciativas Dinamizadoras: Son los elementos que materializan las Líneas de Acción y permiten dar cumplimiento al objetivo de la Política de Gobierno Digital. Entre las iniciativas dinamizadoras se encuentran:

(i) *Proyectos de Transformación Digital:* Son Proyectos que generan valor público mediante el uso y la apropiación de las TIC para el logro de los objetivos estratégicos institucionales.

(ii) *Estrategias de Ciudades y Territorios Inteligentes:* Las entidades territoriales podrán desarrollar estrategias de ciudades y territorios inteligentes, a través del uso de TIC como herramientas de transformación social, económica y ambiental de los territorios (Mineducación, 2022, pp. 9–11).

Figura 3. Elementos que componen la estructura de la política de gobierno digital

Fuente: MinTIC

2.3. MARCO LEGAL

En esta sección se muestran diferentes normas, leyes y decretos que van de la mano con este proyecto de investigación.

Constitución Política de Colombia de 1991, En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece que "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades

correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas" (Perez, 1991).

Ley 1273 DE 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Andrade Serrano et al., 2009).

Decreto 767 de 2022 Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (Valderrama Rojas et al., 2022).

NTC/ISO 22301:2019 Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio, especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para protegerse, reducir la probabilidad de ocurrencia de, prepararse, responder y recuperarse de las interrupciones cuando estas surjan. Los requisitos que se especifican en este documento son genéricos y están destinados para ser aplicados en todas las organizaciones, o partes de estas, sin tener en cuenta el tipo, tamaño o naturaleza de la organización. El grado de aplicación de estos requisitos depende del ambiente operativo y la complejidad de la organización (ISO, 2019).

LEY 44 DE 1993 Por la cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal. LEY 44 DE 1993 (febrero 5) por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. "Los derechos consagrados a favor de los artistas intérpretes o ejecutantes, de los productores de fonogramas y de los organismos de radiodifusión tendrán la siguiente duración: Cuando el titular sea persona natural, la protección se dispensará durante su vida y ochenta años más a partir de su muerte (Gaviria Trujillo & Villegas Ramirez, 1993).

DECRETO 3942 DE 2010 Por el cual se reglamentan las Leyes 23 de 1982, 44 de 1993 y el artículo 2°, literal c) de la Ley 232 de 1995, en relación con las sociedades de gestión colectiva de derecho de autor o de derechos conexos y la entidad recaudadora y se dictan otras disposiciones (Santos Calderón & Vargas Lleras, 2010).

DECRETO 2573 DE 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones (Santos Calderon et al., 2014).

LEY 1915 DE 2018 Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos (Rivera Florez et al., 2018).

Proyecto de Ley 062 de 2019 Por medio de la cual se modifica y adiciona la ley estatutaria 1266 de 2008 y se dictan disposiciones generales de habeas data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones "habeas data"(Velasco Chaves et al., 2019).

2.4. MARCO CONCEPTUAL

En esta sección se muestran diferentes términos de gran valor para este proyecto de investigación.

Conforme con la norma ISO 22301 Continuidad de Negocio es el término que se acuña para referirse a las estrategias y planificación mediante las cuales las organizaciones se preparan para dar respuesta a eventos catastróficos tales como incendios, inundaciones, ataques cibernéticos, accidentes o errores humanos (ISOTools, 2022a).

La Gestión de Continuidad de Negocio (BCM sus siglas en inglés, por *Business Continuity Management*) es un proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor (MinTIC, 2010b).

Según MINTIC (2010) cuando se habla de Plan de Continuidad de Negocio se hace referencia a procedimientos documentados que guían, orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada/tras la interrupción.

El Análisis de Impacto del Negocio (BIA sus siglas en inglés, por *Bussiness Impact Analysis*), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio (MinTIC, 2010b).

Un Plan de Recuperación de Desastres (DRP sus siglas en inglés, por *Disaster Recovery Plan*) es un documento creado por una empresa que contiene instrucciones detalladas acerca de cómo responder a incidentes no planificados como desastres naturales, cortes de electricidad, ataques cibernéticos y cualquier otro evento disruptivo. El plan incluye estrategias para minimizar los efectos de un desastre y permitir que una organización continúe operando o reanude rápidamente las operaciones importantes (IBM, 2022).

Tiempo de Recuperación Objetivo (RTO sus siglas en inglés, por *Recovery Time Objective*) Definido por la organización. El RTO es el retraso máximo aceptable entre la interrupción del servicio y la restauración del servicio. Esto determina qué se considera un periodo de tiempo aceptable cuando un servicio no está disponible (Amazon, 2022).

Punto de Recuperación Objetivo (RPO sus siglas en inglés, por *Recovery Point Objective*) es el tiempo máximo de pérdida de información, por lo tanto, hace referencia al volumen de datos que se encuentran en riesgo de pérdida dentro de un tiempo considerado por la organización como tolerable (ISOTools, 2022b).

El Análisis de Riesgo es el proceso de comprender la naturaleza del riesgo y sus características, incluido el nivel de riesgo, si lo hubiera. El análisis de riesgos implica una consideración detallada de las incertidumbres, las fuentes de riesgo, las consecuencias, la probabilidad, los eventos, los escenarios, los medios de control y su eficacia, proporciona datos para evaluar el riesgo, tomar la decisión de tratarlo o no y cómo, y elegir la estrategia y los métodos de tratamiento más efectivos (ISO, 2018).

Gobierno en línea (GEL) es una estrategia definida por el Gobierno Nacional que pretende lograr un salto en la inclusión social y en la competitividad del país a través de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones. Esta estrategia pretende contribuir a mejorar la eficiencia y transparencia del Estado Colombiano a través de la construcción gradual de un gobierno electrónico, además de promover la actuación del gobierno como usuario modelo y motor de la utilización de las TIC (MinTIC, 2022a).

De acuerdo con la Gobernación de Guaviare (2020) Información en línea es la fase inicial de la estrategia Gobierno en Línea, en la cual las entidades habilitan sus sitios Web para proveer en línea información, junto con esquemas de búsqueda básica. La información, en su mayoría, se mantiene estática y no existe interacción en línea sino una relación unidireccional. Adicionalmente, se crea un portal de Gobierno que ofrece el acceso a través de un solo punto a la información que publican las entidades en sus sitios Web.

3. DISEÑO METODOLOGICO

Este proyecto estuvo enmarcado en un tipo de investigación descriptiva con un enfoque cualitativo.

3.1. TIPO Y ENFOQUE DE INVESTIGACIÓN

Investigación descriptiva porque se buscó especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis y el enfoque cualitativo porque se utilizó la recolección y análisis de datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación (Hernández Sampieri et al., 2014).

3.2. POBLACIÓN DE LA INVESTIGACION

Considerando que la población objeto de la investigación, es cuantitativamente reducida, compuesta por los directores de la Oficina de Admisiones, Registro y Control Académico, Oficina de Bienestar Institucional, Dirección Académica y los directores pertenecientes a los distintos departamentos de programas de la Universidad Popular del Cesar, Seccional Aguachica, se trabajó con el total de la población.

3.3. TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

(Ramos Montiel et al., 2018) precisan que las técnicas e instrumentos de recolección de información, representa la manera en la cual se recolecta información necesaria de la población objeto, se aplica en un determinado momento con el propósito de dar respuesta al problema o pregunta de investigación además de cumplir con los objetivos plateados en el presente proyecto. En base a lo anterior las encuestas, entrevistas no estructuradas y listas de verificación son las técnicas a ser aplicadas al personal administrativo entre los que se encuentra la líder del programa de Ingeniería de Sistemas de la Universidad Popular del Cesar, Seccional Aguachica.

El Profesor García Ferrando (1993) define la encuesta como "una investigación realizada sobre una muestra de sujetos representativa de un colectivo más amplio, utilizando procedimientos estandarizados de interrogación a fin de

obtener mediciones cuantitativas de una gran variedad de características objetivas y subjetivas de la población.

La entrevista no estructurada es un instrumento que permite la aproximación de manera natural a los sujetos de una población de estudio, tiene como rasgo significativo abordar temas de interés para el investigador desde la espontaneidad la cual proporciona riqueza informativa (Schettini et al., 2016).

Por otra parte, Mendez (2001) destaca la observación directa como "el proceso mediante el cual se perciben deliberadamente ciertos rasgos existentes en la realidad por medio de un esquema conceptual previo y con base en ciertos propósitos definidos generalmente por una conjetura que se quiere investigar", siendo este método al cual se recurrirá mediante una lista de verificación para el cumplimiento de los objetivos del presente proyecto de investigación.

3.4. ANALISIS DE LOS RESULTADOS

Después de efectuadas la encuesta, entrevista y la lista de verificación se procedió a realizar el análisis de los datos en base al método de triangulación de datos recomendado por Sampieri (Hernández Sampieri et al., 2014), con la finalidad de contemplar la situación actual en cuanto a la aplicación de la estrategia de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

3.5. METODOLOGIA DE INVESTIGACIÓN

La metodología de investigación que se usó se compone de cuatro (4) fases a saber: Diagnostico, Planificación, Implementación y Gestión, las cuales fueron tomadas del ciclo del Modelo de Seguridad y Privacidad de la Información (MSPI) emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Figura 4. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Fuente: MinTIC

Diagnóstico: En esta fase se identificó el estado actual de la Universidad Popular del Cesar, Seccional Aguachica con respecto a la aplicación de la estrategia de Gobierno Digital.

Planificación: En esta fase se definió la estrategia metodológica a seguir, que permita establecer políticas, objetivos, procesos y procedimientos, pertinentes que le permitan a la Universidad, la preparación para la continuidad del negocio.

Implementación: Esta fase le permitirá a la Universidad llevar a cabo la implementación de la planificación realizada en la fase anterior, teniendo en cuenta los aspectos más relevantes en los procesos de implementación de la estrategia para la continuidad del negocio, las cuales deberán ser puestas en práctica después de la aprobación de la alta dirección.

Gestión: Esta fase le permitirá a la Universidad valorar el desempeño y la eficacia de la implementación, a través de un instrumento que permita determinar la efectividad de dicha implementación (MinTIC, 2010b).

4. RESULTADOS

Los resultados del presente proyecto se detallan a continuación.

4.1. DIAGNOSTICO DEL ESTADO ACTUAL DE LA UNIVERSIDAD EN CUANTO A LA APLICACIÓN DE LA ESTRATEGIA DE GOBIERNO DIGITAL.

La estrategia de Gobierno Digital es una política del Gobierno Nacional liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que propende por la transformación digital pública y ofrecer acompañamiento en la implementación de iniciativas que solventen problemáticas a través del uso de las TIC logrando así que las entidades mejoren en la prestación de servicios y por consecuencia crear valor público, lo cual es de mucho valor para la Universidad Popular del Cesar como entidad de orden nacional.

Para la identificación del estado actual de la Universidad Popular del Cesar, Seccional Aguachica en relación a la aplicación de la política de Gobierno Digital se empleó una entrevista con el propósito de obtener información de gran interés de igual forma se utilizó la encuesta y lista de verificación, las cuales fueron aplicadas a los representantes de cada dependencia para efectuar el objetivo específico número uno (1) y el buen desarrollo de la presente investigación.

Aunado a lo anterior, en este capítulo se describen los elementos institucionales de la Universidad Popular del Cesar, Seccional Aguachica. En la sección 4.1.1. se describe el contexto del claustro educativo. En la sección 4.1.2. se muestran los objetivos institucionales. La sección 4.1.3. presenta la misión y visión de la institución. La sección 4.1.4. presenta como se estructura la universidad. La sección 4.1.5. detalla las funciones del Vicerrector. La sección 4.1.6. detalla las funciones del jefe de la oficina asesora de informática y sistemas. Finalmente, en la sección 4.1.7. se presenta el análisis de los instrumentos de recolección de la información.

4.1.1. Contexto de la organización.

La Universidad Popular del Cesar, se crea en el año 1976 en el cual el Instituto Tecnológico Universitario del Cesar, se transforma en Universidad como establecimiento público con personería jurídica, teniendo como sede principal la ciudad de Valledupar, cuyo objetivo principal será la investigación y la docencia a través de programas que han de conducir a la obtención de licenciaturas, grados profesionales y títulos académicos.

Por iniciativa del representante de los ex – rectores de la Universidad Popular del Cesar en el Consejo Superior Universitario, Dr. Vicente Vaños Galvis, se presentó el proyecto de acuerdo, en el mes de septiembre de 1995, para que funcionaran, en extensión, los programas Administración de Empresas y Contaduría Pública en el Municipio de Aguachica. Esta iniciativa sostenía que el Municipio de Aguachica presentaba las mejores condiciones básicas para el funcionamiento de la Universidad basándose en un estudio de factibilidad realizado en 1992 por los profesores Simón Martínez Guarnes y la profesora Carmen Patricia Guerrero a los habitantes de los Municipios del Sur del Departamento del Cesar.

Con la aprobación del Acuerdo N° 033 el 22 de diciembre del año 1995 por parte del Consejo Superior Universitario se dio vía libre para que empezaran a funcionar en Aguachica los programas anteriormente citados en extensión, para concretar y fortalecer esta decisión el 21 de enero de 1996 se firmó en Aguachica un Convenio Interinstitucional Tripartita entre la Gobernación del Cesar, Dr. Mauricio Pimiento Barrera; la Alcaldía de Aguachica, Dr. Luís Fernando Rincón López (q.e.p.d.) y la Universidad Popular del Cesar, Dr. José Antonio Murgas. Este convenio definió los compromisos económicos que cada institución aportaría para el funcionamiento en extensión del Alma Mater en el Municipio de Aguachica. Es de anotar que sólo la Gobernación cumplió con los recursos comprometidos en el convenio, que en los dos años (1996 – 1997) sumaron aproximadamente $140.000.000 millones; el Municipio de Aguachica cumplió en el primer año de 1996 aportando $15.000.000 millones y la Universidad Popular del Cesar, bajo la rectoría del Dr. José Antonio Murgas, hizo que los primeros recursos recibidos por concepto de matrícula durante la vigencia 1996 fueran transferidos a la Universidad Popular del Cesar – Valledupar y sólo a partir de la vigencia de 1997, por presión del Consejo Superior Universitario, se logró que los recursos captados por matrícula en Aguachica hicieran parte de su propio presupuesto (Rincón Páez, 2020).

4.1.2. Objetivos institucionales.

La Universidad Popular del Cesar (2016) mediante su Proyecto Educativo Institucional (PEI) regula sus actividades a partir de los siguientes objetivos institucionales:

- Garantizar a la sociedad el cumplimiento de su misión y visión en cuanto a la calidad de la educación, mediante la implementación de procesos de autoevaluación, acreditación de sus programas y autorregulación en procura de asegurar la calidad y la excelencia.

- Cumplir las funciones de docencia, con el fin de generar y transmitir el conocimiento a través de metodologías que interrelacionen lo humanístico y lo tecnológico en los estudios propios de cada profesión; en el marco de una educación general, propiciando un escenario para la actividad inter, multi y transdiciplinaria.

- Fortalecer la competitividad, fomentando procesos de innovación, coordinación y supervisión de los proyectos de investigación; asegurando una estrecha interacción entre el Sistema Nacional de Ciencia, Tecnología e Innovación, la Universidad Popular del Cesar y el sector productivo.

- Propender por un conocimiento de la sociedad colombiana a través del fortalecimiento de la comunidad de investigadores de las Ciencias Básicas, Aplicadas, Sociales y Humanas.

- Realizar labores de extensión científica, cultural y de servicio social hacia la comunidad.

- Brindar formación científica, pedagógica, técnica y tecnológica de alto nivel al personal docente e investigadores, como respuesta a garantizar una educación de calidad en sus diferentes niveles y modalidades de formación.

- Promover la conformación de comunidades académicas y científicas, en redes altamente especializadas de conocimiento en el contexto de la educación superior, con la respectiva incorporación de las nuevas tecnologías de la información y la comunicación.

- Extender los programas académicos en el contexto regional para satisfacer las necesidades sociales, culturales, económicas, políticas y educativas de las comunidades interesadas.

- Consolidar y dinamizar el sostenimiento de la comunidad académica Upecista, fortaleciendo las capacidades individuales y colectivas para producir conocimientos educativos, científicos, sociales, económicos y culturales pertinentes.

- Además de los objetivos en comento, la Universidad Popular del Cesar cumplirá aquellos que regulan la Educación Superior en Colombia expresados en la Constitución y la Ley.

- Profundizar en la formación integral de los colombianos dentro de las modalidades y calidades de la Educación Superior, capacitándolos para cumplir las funciones profesionales, investigativas y de servicio social que requiere el país.

- Trabajar por la creación, el desarrollo, la transmisión del conocimiento en todas sus formas y expresiones, promoviendo su utilización en todos los campos para solucionar las necesidades del país.

- Prestar a la comunidad un servicio con calidad, el cual hace referencia a los resultados académicos, a los medios y procesos empleados, a la infraestructura institucional, a las dimensiones cualitativas y cuantitativas del mismo y a las condiciones en que se desarrolla cada institución.

- Ser factor de desarrollo científico, cultural, económico, político y ético a nivel nacional y regional, actuando armónicamente entre sí con las demás estructuras educativas y formativas.

- Contribuir al desarrollo de los niveles educativos que le preceden para facilitar el logro de sus correspondientes fines.

- Promover la formación y la consolidación de comunidades académicas y la articulación con sus homólogas a nivel regional, nacional e internacional.

- Promover la preservación de un medio ambiente sano y fomentar la educación y cultura ecológica.

- Conservar y fomentar, el patrimonio cultural del país.

4.1.3. Misión y visión.

Misión. La Universidad Popular del Cesar, como institución de educación superior oficial del orden nacional, forma personas responsables social y culturalmente; con una educación de calidad, integral e inclusiva, rigor científico y tecnológico; mediante las diferentes modalidades y metodologías de educación, a través de programas pertinentes al contexto, dentro de la diversidad de campos disciplinares, en un marco de libertad de pensamiento; que consolide la construcción de saberes, para contribuir a la solución de problemas y conflictos, en un ambiente sostenible, con visibilidad nacional e internacional.

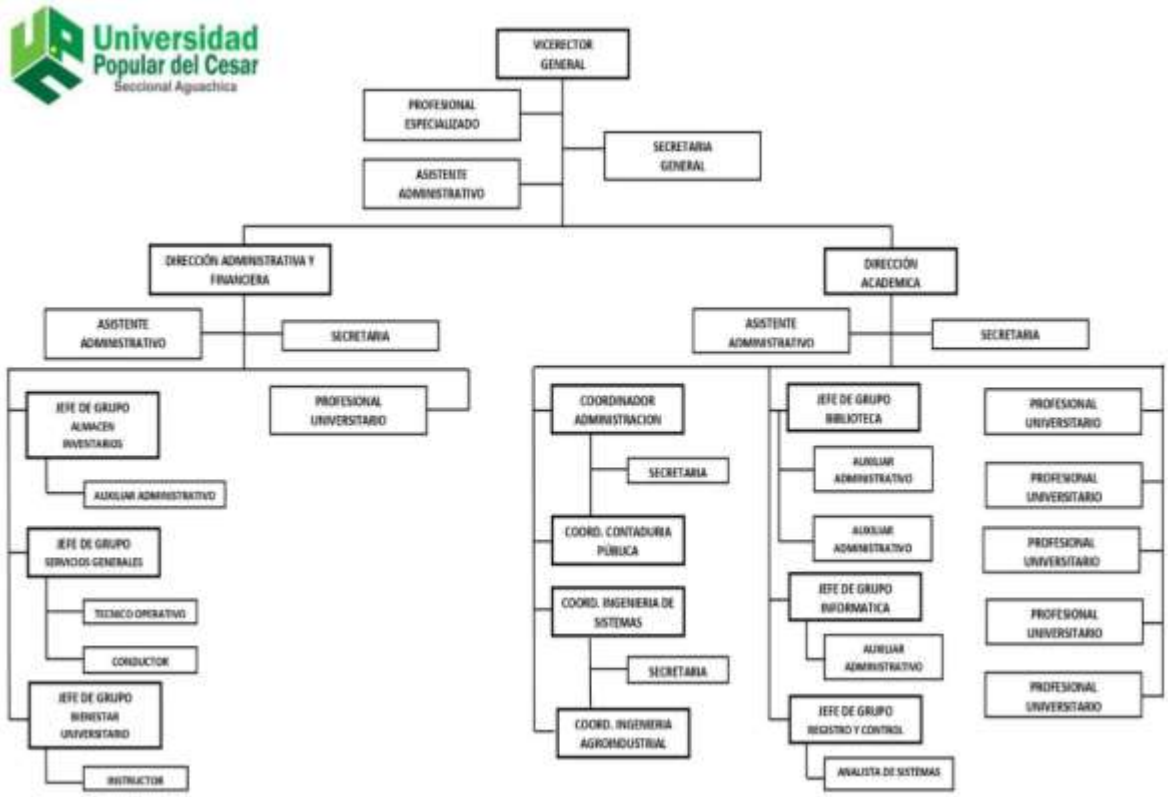
Visión. En el año 2025, la Universidad Popular del Cesar será una Institución de Educación Superior de alta calidad, incluyente y transformadora; comprometida en el desarrollo sustentable de la Región, con visibilidad nacional y alcance internacional (Consejo Superior Universitario de la Universidad Popular del Cesar, 2016b).

4.1.4. Estructura.

4.1.4.1. Organigrama general.

La estructura general de la Universidad Popular del Cesar, Seccional Aguachica es jerárquica, el nivel más alto lo comprende la Vicerrectoría General, de la cual se desprenden dos grandes direcciones, la Dirección administrativa y financiera y la Dirección Académica, las cuales lideran las demás áreas de la institución.

Figura 5. Organigrama de la Universidad Popular del Cesar, Seccional Aguachica.

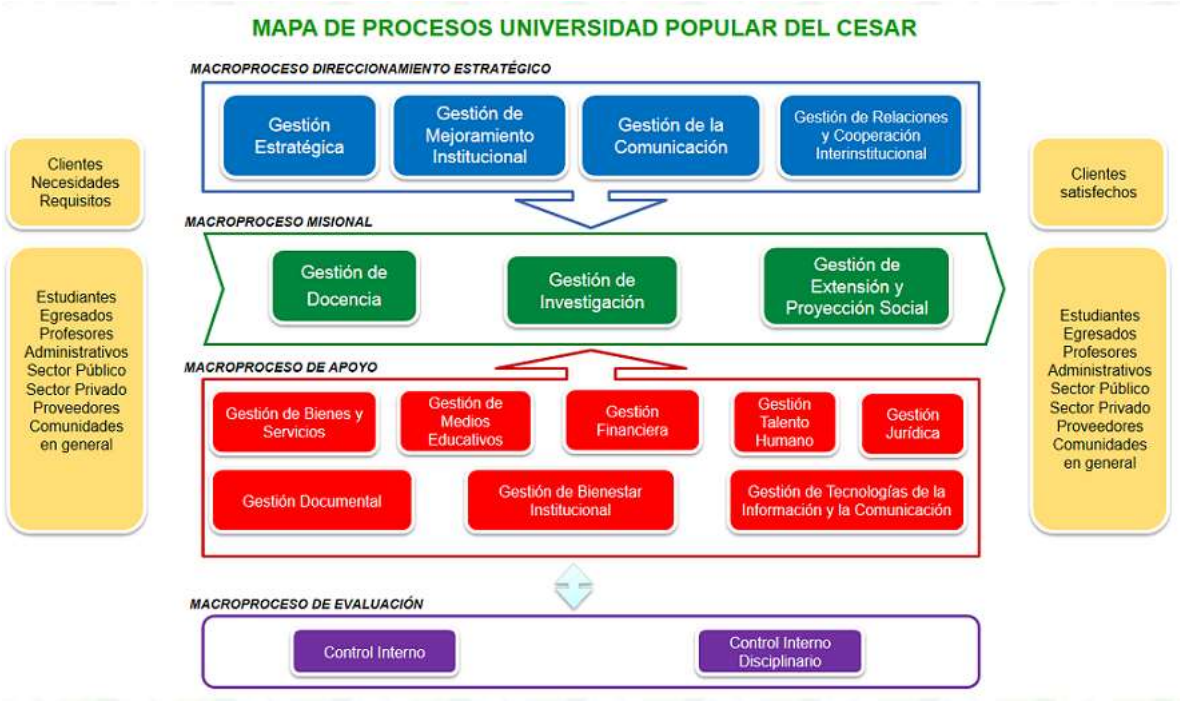


Fuente: Universidad Popular del Cesar, Seccional Aguachica.

4.1.4.2. Mapa de procesos.

La Universidad Popular del Cesar, Seccional Aguachica obra conforme a los siguientes macro procesos: Macroproceso de Direccionamiento Estratégico, Macroproceso Misional, Macroproceso de Apoyo y Macroproceso de Evaluación.

Figura 6. Mapa de procesos de la Universidad Popular del Cesar, Seccional Aguachica



Fuente: Universidad Popular del Cesar, Seccional Aguachica.

4.1.5. Funciones del vicerrector.

El Rector de la Universidad Popular del Cesar (Meza Daza, 2018) mediante la Resolución 022 de 16 de enero de 2018 dictamina las funciones del Vicerrector General de la Seccional Aguachica de la siguiente manera:

4.1.5.1. Propósito principal.

Bajo la dirección del Rector, planear, organizar, dirigir y controlar las actividades propias de su dependencia verificando el cumplimiento de los objetivos trazados. Proponer a la alta dirección universitaria, políticas y estrategias de desarrollo según el área de su especialidad a fin de apoyar el desarrollo de las actividades básicas de la institución, actuar siguiendo los principios de servicio a lo académico, desarrollando iniciativa y liderazgo para permitir la excelencia en las

actividades académicas, administrativas o de investigación que le sean encomendadas.

4.1.5.2. Funciones esenciales.

1. Organizar, coordinar y orientar la prestación de los servicios propios de su Vicerrectoría a fin de garantizar el cumplimiento de la misión y los objetivos de la Universidad.

2. Contribuir a la formulación de las políticas generales sobre aspectos específicos de su área y velar por su correcta aplicación en la Universidad.

3. Gestionar la consecución de recursos financieros adicionales para el desarrollo de los programas y proyectos de su área y promover su realización con otras entidades tanto del sector público como privados, nacionales e internacionales

4. Velar por la organización, dirección, y control de las funciones de las distintas dependencias adscritas a su Vicerrectoria.

5. Participar en la elaboración del Plan de Desarrollo de la Universidad y presentar las recomendaciones para la ejecución del mismo en las áreas afines con su especialidad.

6. Evaluar el desempeño y logro de objetivos de las distintas dependencias a su cargo y presentar los respectivos informes al Rector u órganos directivos de la Universidad cuando estos lo requieran.

7. Presidir o asistir a los Comités o Consejos que en función de su cargo le corresponda y en aquellos que por delegación expresa de autoridad competente le corresponda actuar.

8. Asesorar a los Consejos Superior y Académico y al Rector en lo relacionado con las políticas propias de su Vicerrectoria.

9. Expedir los actos administrativos que sean necesarios para garantizar el buen funcionamiento de su dependencia.

10. Participar en la elaboración del Presupuesto anual de Ingresos, gastos e inversiones de la Universidad promoviendo su relación con los lineamientos del Plan de Desarrollo de la Universidad.

11. Estudiar los proyectos de su área y someterlos a consideración de las respectivas instancias.

12. Presidir, coordinar y supervisar el funcionamiento de los comités que le sean asignados en razón de su cargo.

13. Promover aquellas actividades que permitan una proyección externa de las actividades de la Vicerrectoria mediante la aplicación y/o divulgación de resultados.

14. Las demás que se señalen en los actos administrativos que expidan los Consejos Superior y Académico, la Rectoría y los organismos gubernamentales.

4.1.6. Funciones del jefe oficina asesora informática y sistemas.

El Rector de la Universidad Popular del Cesar (Guevara Gomez, 2020) en ejercicio de sus facultades legales y estatutarias decreta mediante la Resolución 0090 de 24 de enero de 2020 las funciones y competencias laborales del jefe de oficina asesora informática y sistemas como se muestra a continuación:

4.1.6.1. Propósito principal.

Diseñar, dirigir, desarrollar y evaluar los procesos informáticos y de comunicaciones de la entidad de tal manera que garanticen el logro de la misión y objetivos de la Universidad Popular del Cesar.

4.1.6.2. Funciones esenciales.

1. Asesorar y aconsejar a la dirección universitaria en la formulación, coordinación y ejecución de las políticas y planes generales de la entidad.

2. Absolver consultas, prestar asistencia técnica, emitir conceptos y aportar elementos de juicio para la toma de decisiones relacionadas con la adopción, la ejecución y el control de los programas propios del organismo.

3. Proponer y realizar estudios e investigaciones relacionados con la misión institucional y los propósitos y objetivos de la entidad que le sean confiados por la administración.

4. Asistir y participar, en representación del organismo o entidad, en reuniones, consejos, juntas o comités de carácter oficial, cuando sea convocado o delegado.

5. Preparar y presentar los informes sobre las actividades desarrolladas, con la oportunidad y periodicidad requeridas.

6. Las demás que les sean asignadas por autoridad competente, de acuerdo con el área de desempeño y la naturaleza del empleo.

4.1.6.3. Funciones esenciales jefe oficina asesora informática y sistemas.

1. Dirigir institucionalmente los temas relacionados con la informática para garantizar el logro de los objetivos de la entidad.

2. Proponer al Rector la formulación y adopción de las políticas y estrategias informáticas y de comunicaciones de la entidad para el cumplimiento de la misión institucional.

3. Diseñar, desarrollar y evaluar, en conjunto con los Directivos y demás jefes de Oficina, el Plan Maestro Informático de la Entidad con el fin de atender eficientemente a los usuarios internos y externos.

4. Formular y adoptar las políticas de administración, seguridad y control, necesarias para garantizar la eficacia, eficiencia y confiabilidad de los recursos informáticos de la Universidad.

5. Diseñar los sistemas de información de la Universidad, soportados por tecnologías de información y comunicaciones para mantener un estricto control sobre su adecuado uso.

6. Coordinar la planeación, para el uso y evaluación de los sistemas de información, soportados por tecnologías de información y comunicaciones de la Universidad.

7. Adelantar estudios de mercado y de costos en materia de tecnologías de información y comunicaciones, requeridas por la Oficina de Planeación, para la formulación, preparación e inscripción de los proyectos de inversión de la Universidad ante los organismos competentes.

8. Definir y elaborar los términos de referencia en los temas de tecnologías de información y comunicaciones, requeridas por la Entidad para adelantar los procesos de adquisición de bienes y servicios.

9. Diseñar los planes de capacitación en informática dirigido al personal de sistemas y usuarios sobre los servicios y recursos informáticos e informar a la Oficina del Grupo de Gestión de Desarrollo Humano para su ejecución. Prestar el servicio de soporte técnico de hardware y software que requieran las dependencias de la Universidad.

10. Coordinar la elaboración e implementación del Plan de Acción Anual de la dependencia acorde con el Plan de Desarrollo Institucional, el presupuesto y las funciones de las mismas.

11. Preparar el Plan anual de compras de la dependencia a su cargo en las fechas estipuladas para ello.

12. Responder por la adopción, desarrollo, implementación, mantenimiento, revisión y perfeccionamiento del Sistema de Gestión de la Calidad de la Entidad con el propósito de mejorar el desempeño institucional y la capacidad de proporcionar servicios que respondan a las necesidades y expectativas de los usuarios.

13. Preparar y presentar los informes sobre las actividades desarrolladas con la oportunidad y periodicidad requeridas para permitir evaluar la gestión de la dependencia.

14. Las demás funciones que le sean asignadas por el jefe inmediato y que correspondan a la naturaleza del cargo.

4.1.7. Instrumentos de recolección de información.

La recolección de información se efectuó a través de una encuesta, una entrevista y una lista de chequeo (ver anexo D, E, F), las cuales fueron aplicadas a los líderes de las áreas de Dirección Académica, Dirección Administrativa y Financiera, la Oficina de Admisiones, Registro y Control Académico, la Oficina de Bienestar Institucional y a los distintos departamentos de programa. El objetivo de estos instrumentos es identificar el estado actual de la Universidad Popular del Cesar, Seccional Aguachica en cuanto a la aplicación de la estrategia de Gobierno Digital.

4.1.7.1. Análisis de los resultados de las encuestas.

Figura 7. Backups.

Fuente: Encuesta anexo (D)

Se observa que el 81,8% de la población encuestada realiza copias de seguridad para respaldar la información esencial que se produce, procesa y gestiona en sus respectivas oficinas y el 18,2% no lo hace, lo cual representa un riesgo latente de una probable pérdida parcial o total de la información ante la ocurrencia de un evento no deseado, generando así daños tanto en las dependencias como para la universidad.

Figura 8. Frecuencia de realización de backups.

Fuente: Encuesta anexo (D)

Se evidencia que el 36,4% y el 45,5% de la población de estudio realiza frecuentemente y con poca frecuencia respectivamente, backups de la

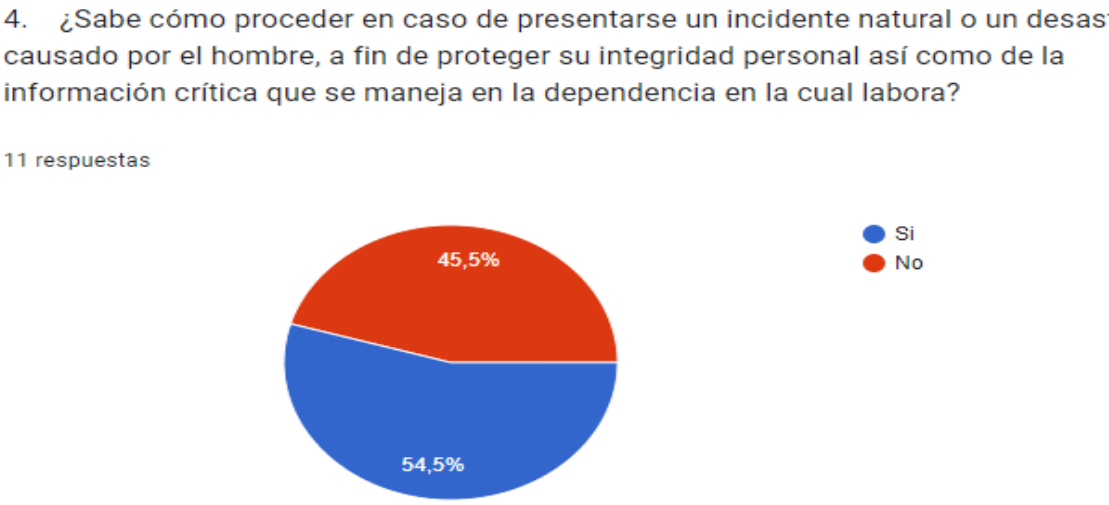
información relevante y pertinente a sus correspondientes áreas de trabajo, contrario a esto el 18,2% demuestra una vez mas no realizar backups siendo inexistente la prevención de la materialización de riesgos para la seguridad de la información.

Figura 9. Capacitación para las buenas prácticas de la información.

Fuente: Encuesta anexo (D)

Solo el 18,2% de la población afirma recibir a menudo capacitación respecto a buenas prácticas de gestión eficiente de la información frente al 63,6% que manifiesta casi nunca recibir capacitación y al 18,2% que asegura nunca recibir capacitación existiendo así una vulnerabilidad y en consecuencia una posible brecha de seguridad que afecte a la universidad.

Figura 10. Actuación en casos de incidentes o desastres.



Fuente: Encuesta anexo (D)

Se observa que el 54,5% de los encuestados sabe cómo proceder ante un posible incidente o desastre durante la ejecución de sus funciones, sin embargo, el 45,5% no sabe reaccionar ante la posibilidad de ocurrencia de estos eventos reflejando su desconocimiento en cuanto a la adopción y ejecución de las medidas necesarias para prevenir y/o afrontar riesgos y daños que se generen.

Figura 11. Ejecución de controles.

Fuente: Encuesta anexo (D)

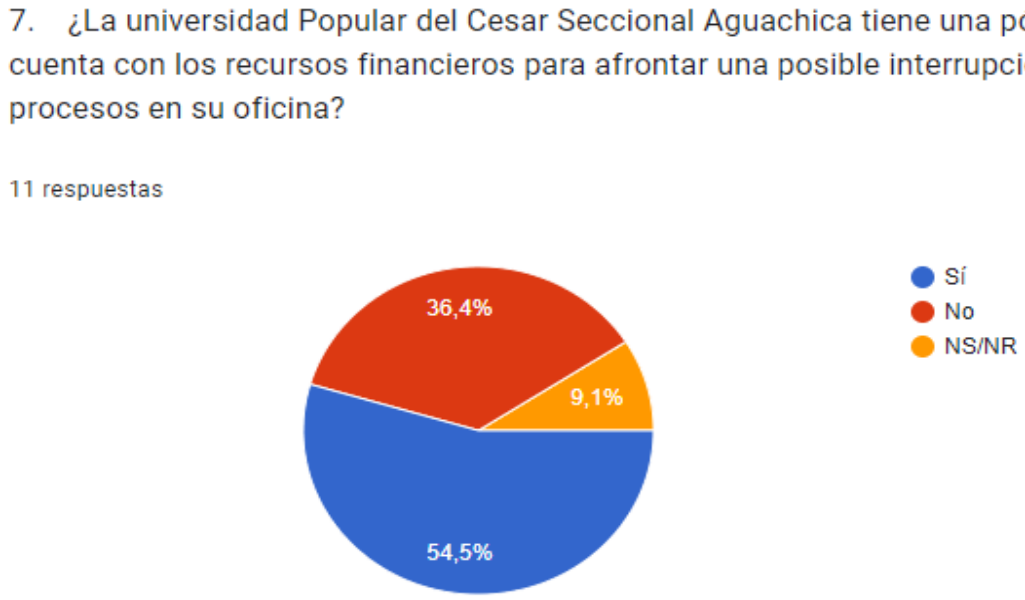
El 45,5% de los encuestados afirma que se aplican controles a fin de proteger los equipos de cómputo e información contra software malicioso, el otro 45,5% manifiesta que no se aplican y el 9.1% desconoce si estos controles se ejecutan, lo que representa una vulnerabilidad para la seguridad de la información, así como también la carencia de cultura de seguridad organizacional.

Figura 12. Estrategias para la mitigación de riesgos.

Fuente: Encuesta anexo (D)

El 27,3% de la población encuestada asegura que se implementan estrategias para mitigar riesgos digitales que podrían presentarse en sus respectivas dependencias contrario al 72,7% que afirma no efectuarse dichas estrategias en sus dependencias evidenciando no estar preparados para afrontar situaciones de riesgo como tampoco para reducir el impacto de estos en la continuidad del negocio lo que provocaría afectaciones graves para la universidad.

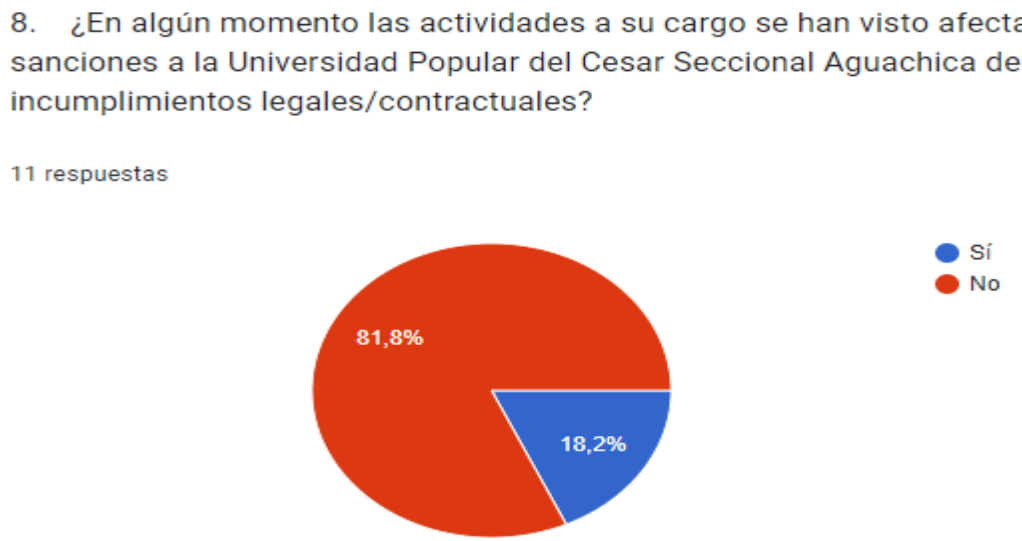
Figura 13. Póliza contra posibles interrupciones de los procesos.



Fuente: Encuesta anexo (D)

Se observa que el 54,5% de los encuestados sostiene que la universidad cuenta con una póliza para afrontar y respaldar una posible interrupción de los procesos, el 36,4% expresa lo contrario y el 9,1% desconoce si se cuenta con dicha póliza o con los recursos financieros que le permita a las dependencias y/o a la universidad proteger los activos así como evitar la pérdida de productividad y asegurar la continuidad operativa.

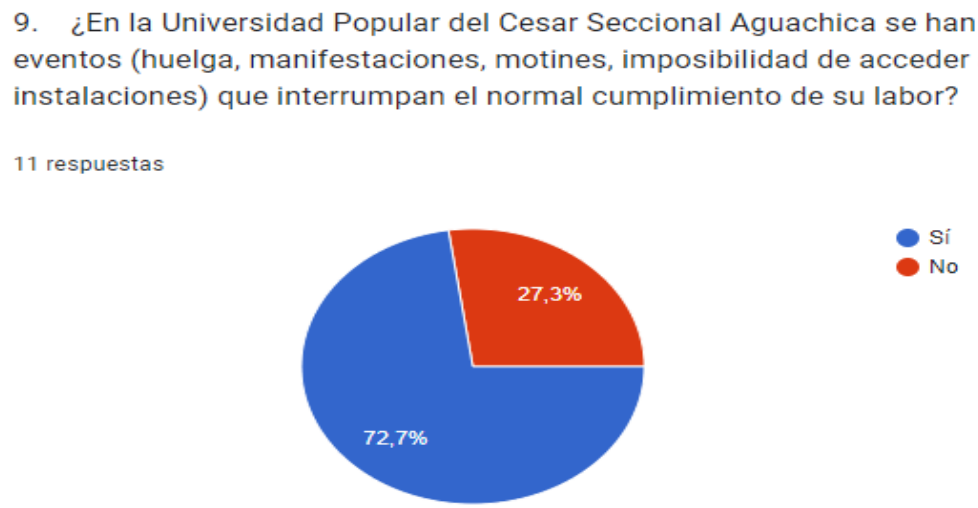
Figura 14. Actividades afectadas por sanciones.



Fuente: Encuesta anexo (D)

El 81,8% de los encuestados niega que sus actividades administrativas se hayan visto afectadas debido a una sanción, por el contrario, el 18,2% lo afirma, por consecuencia esto podría generar riesgos financieros, acciones disciplinarias e interrupción en la prestación de los servicios ofrecidos por alguna de las dependencias u oficinas afectadas considerando la naturaleza y la gravedad de la sanción.

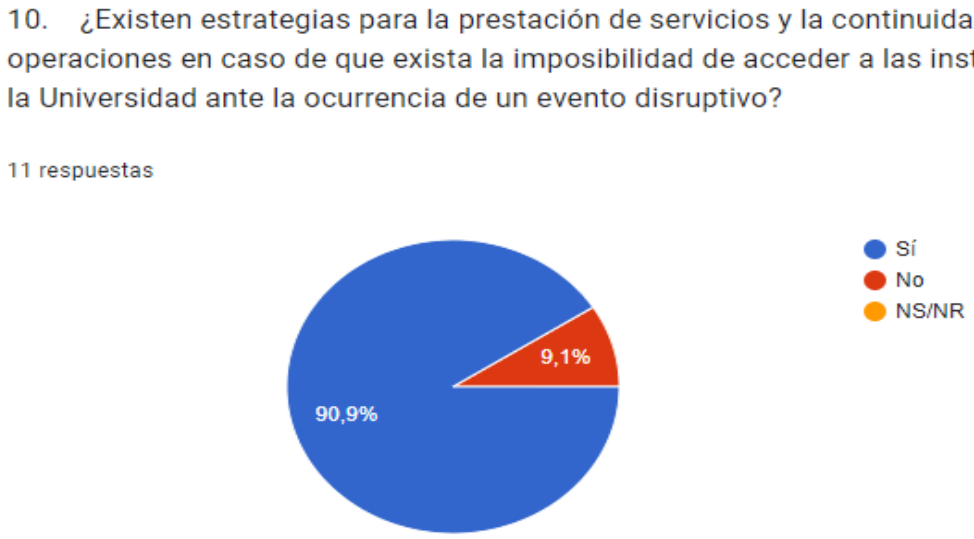
Figura 15. Eventos que impiden el cumplimiento de las actividades de los administrativos.



Fuente: Encuesta anexo (D)

Se observa que el 72,7% de los administrativos encuestados tiene la certeza de que se han presentado eventos que impiden el normal desarrollo de las actividades/funciones críticas de los distintos departamentos, así como de toda la universidad y que conllevan riesgos significativos para la misma, contrario a esto el 27,3% de los encuestados niegan la ocurrencia de eventos de este tipo durante la ejecución de sus labores.

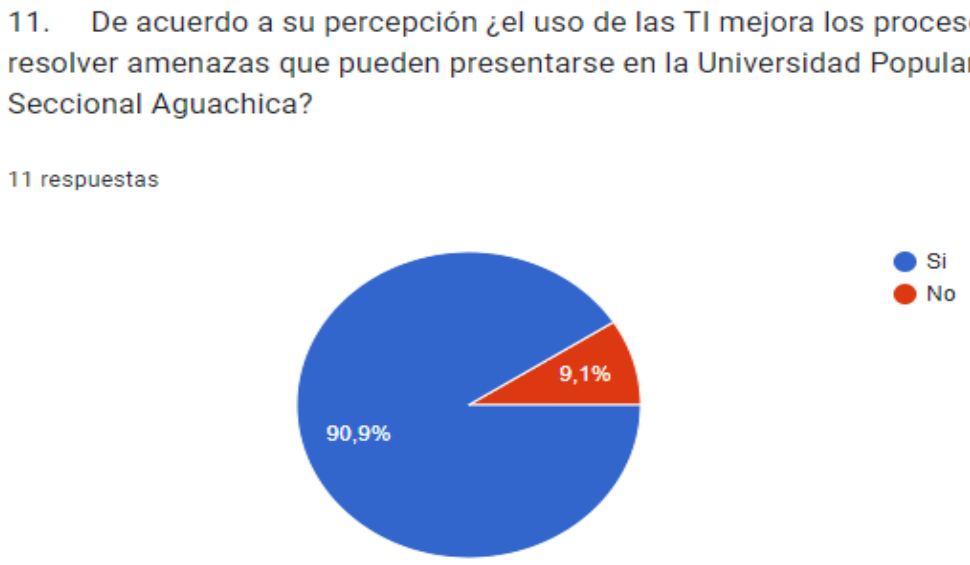
Figura 16. Estrategias para prestación de servicios y continuidad de las operaciones de la UPC.



Fuente: Encuesta anexo (D)

Para el 90,9% de la población encuestada la universidad cuenta con las estrategias necesarias que les permite continuar operando ante la ocurrencia de un evento disruptivo que impida el acceso a las instalaciones, diferente al 9,1% que afirma la inexistencia de las estrategias, las cuales son imprescindibles ya que permiten minimizar los daños sobre los activos, responder efectiva y rápidamente a una interrupción de los servicios y operaciones esenciales de la universidad así como también evitar pérdidas financieras.

Figura 17. Uso de TI.



Fuente: Encuesta anexo (D)

Se observa que el 90,9% de los encuestados coincide en que el uso de las TI (Tecnología de la Información) mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la universidad, cabe resaltar que la relevancia de las TI se encuentra en los beneficios que se obtienen tras su aplicación como lo es la obtención y respaldo de los datos, el procesamiento y la disponibilidad de la información, la toma de decisiones, resolución de problemas, aumento en la productividad además de garantizar la seguridad de la información; sin embargo el 9,1% difiere, ya que consideran que la optimización y mejora de los procesos y solución de amenazas no se relaciona con el uso de la TI.

Figura 18. Apropiación de proyectos de TI.

Fuente: Encuesta anexo (D)

El 54,5% de los encuestados asegura que se ejecutan en los distintos departamentos donde laboran, iniciativas de uso y apropiación de proyectos de TI que se elaboran en la universidad, el 27,7% afirman lo contario, el 18,2% desconoce si lo anterior se lleva a cabo evidenciando la desinformación y la necesidad de integrar proyectos de TI que fomenten mejorar la cultura organizacional por parte de la población administrativa y que además favorecen la competitividad y productividad de los diferentes dependencias de la Universidad Popular del Cesar, Seccional Aguachica.

4.1.7.2. Análisis de los resultados de las entrevistas.

Conforme a las entrevistas dirigidas al personal administrativo de las áreas anteriormente mencionadas (ver anexo Q, R, S, T, U, V, W, X, Y, Z, AA) se observa que en su mayoría los procesos de mayor criticidad son aquellos propios del macroproceso de gestión docencia involucrados con la planeación académica tales como, plan de acción, asignación académica, horarios, así como también la inscripción, admisión, grado de estudiantes, contratación y renovación de registro calificado.

La información manejada por cada uno de los funcionarios en sus respectivas oficinas es preferentemente almacenada en Discos Duros y Google Drive un

servicio en la nube que ofrece seguridad y accesibilidad a la información, sin embargo, una minoría de la población entrevistada elige el equipo portátil, así como desistir del uso de herramientas que permitan tener un respaldo o algún tipo de medida para salvaguardar la información lo que implica un alto riesgo para los activos y en consecuencia para la universidad.

Por otra parte, no hay claridad con respecto a la existencia de una directriz en materia de seguridad de la información que oriente al personal administrativo ante incidentes de seguridad, aunado a lo anterior, una parte de los entrevistados afirma recibir capacitaciones semestrales y/o anuales, la otra parte difiere, expresando que no reciben una formación que les permita obtener las habilidades y los conocimientos para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades, así como tampoco se realizan simulacros para determinar los tiempos de respuesta y recuperación ante una posible eventualidad como la mencionada anteriormente.

Poniendo en contexto, la materialización de un evento imprevisto tal como una falla eléctrica, es una situación que provocaría la suspensión de actividades laborales, además se observa que los administrativos no están preparados para enfrentarse o gestionar de forma idónea tal eventualidad, lo que afectaría los procesos críticos de cada área, la comunicación interna, proyectos en curso, datos e información, reafirmando lo expuesto en el párrafo anterior.

Al presentarse un evento catastrófico que ponga en riesgo las instalaciones de la Universidad Popular del Cesar, Seccional Aguachica y su productividad afectaría no solo a los procesos o a la sede en si misma sino también, en cierta medida a la sede central, además de ello la mayor parte de la población entrevistada considera las pérdidas financieras como consecuencia de lo anterior en ese sentido declaran que la universidad cuenta con una póliza o con los recursos financieros necesarios para afrontar la interrupción de los procesos críticos que se manejan en cada una de las dependencias.

4.1.7.3. Análisis de los resultados de las listas de chequeo.

De acuerdo con las listas de chequeo aplicadas al personal administrativo de los distintos departamentos de la Universidad Popular del Cesar, Seccional Aguachica (ver anexos BB, CC, DD, EE, FF, GG, HH, II, JJ, KK, LL) la población administrativa afirma que se garantiza la protección de los datos personales a través del Acuerdo N° 019 del 5 de octubre del 2020 el cual establece la política de tratamiento y protección de datos personales de la Universidad Popular del Cesar, así como también la conservación de documentos electrónicos, la

transparencia y accesibilidad de la información, la adecuación tecnológica y la responsabilidad e igualdad en relación al uso de medios electrónicos, sin embargo es imprescindible destacar que a pesar de lo anteriormente mencionado aún existe desconocimiento sobre si se cumple o no por parte de algunos de los sujetos de la población, adicionalmente se requiere orientación y capacitación sobre los temas mencionados.

Se puede constatar que actualmente se cuenta con una página web institucional como instrumento que permite que los distintos actores de la comunidad universitaria conozcan información de interés, además los funcionarios administrativos aseguran usar las Tecnologías de la Información y las Comunicaciones con el propósito de mejorar y optimizar los procesos manejados en su cargo y con ello reconocen la importancia del uso de las TICs para la toma de decisiones efectivas, sin embargo, afirman recibir con poca frecuencia capacitación y/o sensibilización al respecto, sumado a esto, se desconoce si se dispone de un Plan Estratégico de las Tecnologías de Información y las Comunicaciones que permita gestionar y establecer una estrategia de TI y que a su vez ayude en la toma de decisiones.

Por otro lado, la institución pone a disposición de los ciudadanos los datos generados por la académica, así como también, comunica y promueve su uso a la población estudiantil, administrativos y ciudadanos lo que resulta en mayor transparencia, generación de conocimiento, fomenta la investigación, la innovación y el desarrollo por parte de la comunidad ciudadana e interesados.

En cuanto a gestión de proyectos, se aplican buenas prácticas que satisfagan las necesidades y problemáticas que puedan presentarse en la universidad, además de ello, reconocen las ventajas de la prestación de servicios ciudadanos inteligentes, finalmente, la institución no cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial importante para garantizar la continuidad de los procesos de negocio y la gestión de riesgos.

4.1.7.4. Estado actual de la Universidad Popular del Cesar, Seccional Aguachica en cuanto a la aplicación de la estrategia Gobierno Digital.

La utilización de la entrevista, encuesta y lista de verificación como métodos para recopilar información, permitieron conocer la necesidad de ejecutar acciones que aseguren la continuidad de las operaciones, procesos y servicios esenciales del centro universitario, del mismo modo, diseñar y llevar a cabo un programa de capacitaciones en materia de seguridad de la información de la Universidad Popular del Cesar, Seccional Aguachica, con la finalidad de instaurar y fomentar una cultura de seguridad en la población administrativa.

Los resultados obtenidos evidenciaron aspectos positivos con respecto al uso de las Tecnologías de la Información y las Comunicaciones (TIC) para mejorar procesos, toma de decisiones y resolver o mitigar amenazas, uso y apropiación de proyectos de TI elaborados en la universidad, protección de datos personales, conservación de documentos electrónicos, transparencia y accesibilidad a la información, adecuación tecnológica, responsabilidad e igualdad con el uso de medios electrónicos.

Contrario a lo anterior, se observaron vulnerabilidades relacionadas a la ausencia de estrategias de seguridad de la información como son las copias de seguridad, formación del personal administrativo en temas de seguridad de la información y acciones de respuesta frente a eventos disruptivos; buenas prácticas para una gestión eficaz de la información, controles de seguridad contra software malicioso y riesgos digitales, sin embargo, la debilidad más relevante se centra en el factor humano, razón por la cual se hace indispensable realizar un programa de capacitaciones, de manera que se protejan los activos de información en cuanto a confidencialidad, integridad y disponibilidad de los datos, identificación y prevención de riesgos, buenas prácticas y cumplimiento de los objetivos institucionales y la normatividad colombiana.

4.2. ANALIZAR LOS COMPONENTES DEL MODELO GESTION DE CONTINUIDAD DEL NEGOCIO CON BASE EN LOS REQUERIMIENTOS NORMATIVOS.

El Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) ofrece a través del Modelo de Seguridad y Privacidad de la Información (MSPI) un conjunto de guías prácticas para ayudar y asistir a las entidades del estado a mitigar los riesgos asociados a la seguridad de la información, así como velar por la preservación de la confidencialidad, integridad y disponibilidad de los activos de información (Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, 2020). Dentro de este conjunto de guías se encuentra la "Guía para la preparación de las TIC para la continuidad de negocio" en su versión 1.0 la cual es el punto de referencia para el presente proyecto.

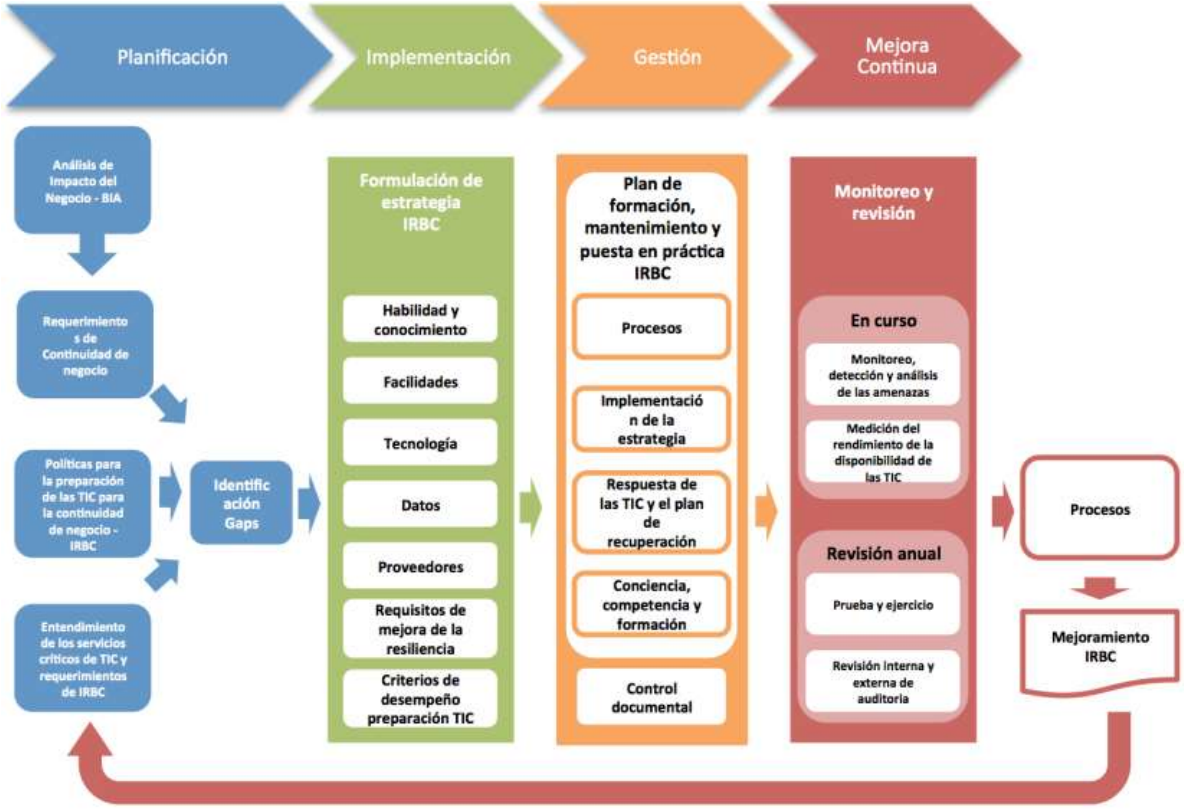
En este capítulo se integran los siguientes componentes. En la sección 4.2.1. presenta los componentes que comprenden la estrategia de gestión de continuidad del negocio por MinTIC. La sección 4.2.2. describe la política pública que define la estrategia de Gobierno Digital. La sección 4.2.3. presenta el marco normativo que rige en Colombia los Planes de Gestión de Continuidad del Negocio.

4.2.1. Componentes que comprenden la estrategia de gestión de continuidad del negocio por parte de MinTIC.

La guía para la preparación de las TIC para la continuidad del negocio está liderada por el Ministerio de las Tecnologías de la Información y las Comunicaciones, es un complemento del Modelo de Seguridad y Privacidad de la Información y se constituye como un referente de la continuidad del negocio para las entidades del estado, dentro de ese contexto, el modelo de operación de Continuidad del Negocio contempla su implementación en las cuatro (4) fases del ciclo del modelo para que las entidades puedan gestionar la seguridad y privacidad de la información, con el propósito de fortalecer la protección de los datos y dar cumplimiento a lo establecido en la estrategia de Gobierno en Línea, cubriendo de una manera integral cada uno de sus componentes (MinTIC, 2010b).

.

Figura 19. Marco Continuidad del Negocio para Seguridad y Privacidad de la Información.



Fuente: MinTIC

La guía para la preparación de las TIC para la continuidad del negocio descrito anteriormente es esencial para el desarrollo del presente proyecto de investigación, está dirigido a entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la Información (en adelante MSPI) en el marco de la Estrategia de Gobierno en Línea.

Cada una de las fases que abarca el modelo de operación contiene objetivos, metas y herramientas (guías) que permiten que la continuidad del negocio sea sostenible dentro de las entidades.

Componente de planificación. En este componente, se determina la estrategia metodológica, que permita establecer las políticas, objetivos, procesos y procedimientos, pertinentes que le permitan a la entidad, la preparación para la continuidad del negocio. Para efectuar el componente de planificación es primordial; (i) Definir los objetivos, alcance, límites y la

política para la continuidad del negocio; (ii) Asignar el recurso humano cualificado, comunicar sus respectivos roles y responsabilidades; (iii) Fijar un plan de requerimientos, categorizando las actividades para la continuidad, definiendo el nivel con el cual cada actividad critica necesita para su recuperación; (iv) Determinar la estrategia, la aproximación para implementar la resiliencia requerida de tal manera que los principios de prevención de incidentes, detección, respuesta, recuperación y restauración se pongan en marcha.

Componente de implementación. Este componente le permitirá a la Entidad llevar a cabo la implementación del componente de planificación, considerando los aspectos más relevantes en los procesos de implementación de la estrategia, las cuales deberán ser implementadas después de la aprobación de la alta dirección, quien es la encargada de gestionar y proporcionar los recursos necesarios, procedimientos y operación de la continuidad del negocio, al igual que los programas de entrenamiento y concientización. Para alcanzar la implementación de los elementos de la estrategia, es preciso llevar a cabo; (i) Concientización, habilidades y conocimiento general de la preparación de los elementos de servicios de TIC, personas, infraestructura, tecnología, datos, procesos y proveedores, así como sus componentes críticos; (ii) La infraestructura de los sistemas de recuperación de TIC y la información crítica deben, en lo posible, ser físicamente separada del sitio operacional para prevenir que sea afectada por el mismo incidente; (iii) Los acuerdos para la disponibilidad de los datos deben estar alineados con los requerimientos de la estrategia; (iv) La Entidad debe asegurar que los proveedores críticos están en capacidad de soportar los servicios de la estrategia, conforme a los requerimientos de la Entidad; (v) Implementar el plan de respuesta de incidentes que permita confirmar la naturaleza y grado del incidente, tomar control de la situación, contener el incidente y comunicar a las partes interesadas.

Componente de evaluación. Este componente le permitirá a la Entidad, evaluar el desempeño y la eficacia de la implementación, a través de instrumentos que permita determinar la efectividad de la implantación del MSPI. Para la medición de la efectividad de los procesos y controles del MSPI, se deben tomar los indicadores definidos en el componente de implementación para llevar a cabo el plan de seguimiento, evaluación y análisis del MSPI. Lo anterior se debe efectuar mediante; (i) Plan de seguimiento, evaluación y análisis para la continuidad del negocio; (ii) Auditoría Interna para la continuidad del negocio; (iii) Evaluación del desempeño de la estrategia.

Componente de mejora continua. Este componente le permitirá a la Entidad realizar acciones correctivas apropiadas a los potenciales impactos determinados por el análisis de impacto del negocio BIA de la Entidad. Para

lo anterior es necesario; (i) Definir las acciones correctivas, identificando las fallas; (ii) Realizar una auditoría interna; (iii) Comunicar los resultados y plan de mejoramiento; (iv) Debidamente revisado y aprobado por la alta Dirección (MinTIC, 2010b).

4.2.2. Política pública por la cual está definida la estrategia de gobierno digital.

La estrategia de Gobierno Digital es una de las diecinueve políticas de Gestión y Desempeño Institucional, se ubica en la dimensión operativa (3) de Gestión con Valores para Resultados que se desarrolla en el marco del Modelo Integrado de Planeación y Gestión (MIPG).

Agregado a lo anterior, Gobierno Digital es una política transversal que está estrechamente relacionada con las demás políticas de MIPG: Planeación Institucional, Gestión presupuestal y eficiencia del gasto público, Compras y contratación pública, Talento humano, Integridad, Transparencia, Acceso a la Información Pública y Lucha Contra la Corrupción, Fortalecimiento Organizacional y Simplificación de Procesos, Servicio al Ciudadano, Participación Ciudadana en la Gestión Pública, Racionalización de trámites, Seguridad Digital, Defensa jurídica, Mejora normativa, Gestión del Conocimiento y la Innovación, Gestión Documental, Gestión de la información estadística, Seguimiento y evaluación del desempeño institucional y Control interno.

4.2.2.1. MIPG.

"El Modelo Integrado de Planeación y Gestión (MIPG) se define como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

El principal propósito de MIPG es su contribución al fortalecimiento de las capacidades de las organizaciones, ya que se focaliza en las prácticas y procesos clave que ellas adelantan para convertir insumos en resultados, apuntando a transformar el Estado Colombiano, de un Estado legislativo a un Estado prestador de servicios.

MIPG funciona mediante tres componentes, la institucionalidad, la operación y la medición, descritos de la siguiente manera:

Institucionalidad. Este componente facilitará la implementación y evaluación del Modelo, así:

(i) **A nivel sectorial,** los Comités Sectoriales de Gestión y Desempeño Institucional presididos por el ministro o director del departamento administrativo del sector respectivo y de ellos harán parte los directores, gerentes o presidentes de los organismos y entidades adscritas o vinculadas, son los encargados de dirigir la implementación y la evaluación del Modelo en las entidades que integran el respectivo sector administrativo.

(ii) **A nivel territorial,** los Comités Departamentales, Distritales y Municipales de Desarrollo de Gestión y Desempeño Institucional, dirigidos por el gobernador o alcalde de la respectiva jurisdicción y estarán integrados por los consejos de gobierno y los gerentes, presidentes o directores de las entidades descentralizadas del orden departamental, distrital o municipal. Están a cargo de liderar la implementación de MIPG en el conjunto de entidades que hacen parte del ente territorial.

(iii) **A nivel institucional,** los Comités Institucionales de Gestión y Desempeño. En el nivel central estos son liderados por el viceministro o subdirector de departamento administrativo, y en el nivel descentralizado por los secretarios generales o administrativos. Estará a cargo de orientar la implementación y evaluación de MIPG en cada entidad u organismos público.

Operación. el Modelo parte de una visión múltiple de la gestión organizacional, que incluye dimensiones claves que a su vez agrupan un conjunto de políticas, prácticas, elementos o instrumentos con un propósito común, generales a todo proceso de gestión, pero adaptables a cualquier entidad pública, y que, puestas en práctica de manera articulada e intercomunicada, permitirán que MIPG opere.

Las dimensiones mencionadas con anterioridad se describen a continuación.

(i) **Gestión del Talento Humano,** es el conjunto de lineamientos, decisiones, prácticas y métodos adoptados y reconocidos por la entidad, para orientar y determinar el quehacer de las personas que la conforman, su aporte a la estrategia institucional, el logro de las metas estratégicas y los resultados propuestos.

(ii) **Direccionamiento estratégico y planeación,** esta dimensión busca orientar a las organizaciones, para que reflexionen sobre su propósito fundamental, identifiquen necesidades y problemas de los ciudadanos o grupos sociales a quienes debe dirigir sus servicios y garantizar sus derechos, entiendan cuáles son las prioridades de

los planes de desarrollo, y analicen sus capacidades internas y su entorno institucional.

(iii) **Gestión con valores para resultados**, en esta Dimensión se concretan las acciones que la entidad debe definir para una adecuada y mejor interlocución con los ciudadanos, los trámites que realizan los ciudadanos, el servicio y atención que estos merecen y la participación de los mismos en todo el ciclo de la gestión pública.

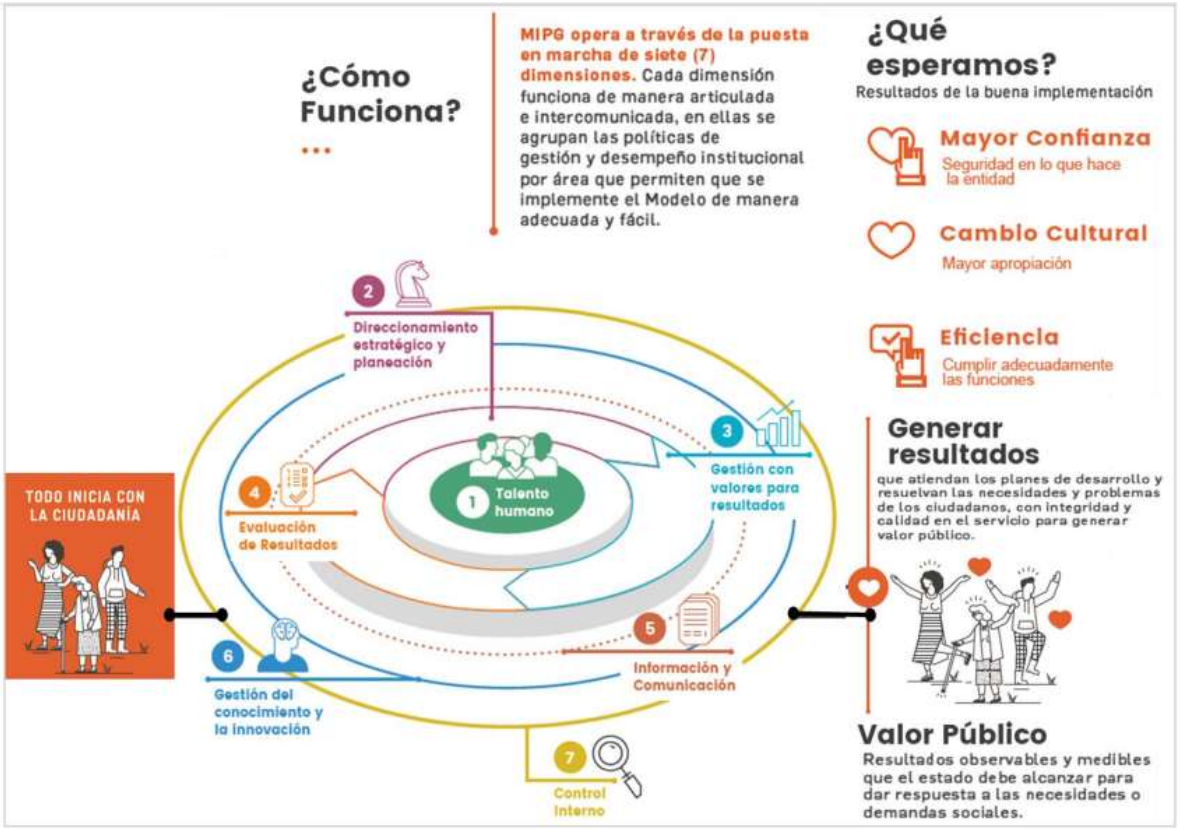
(iv) **Evaluación de resultados**, la evaluación se fundamenta en indicadores para monitorear y medir el desempeño de las organizaciones, por tanto, se deben enfocar en los criterios, directrices y normas que orientan la gestión y en los productos, resultados e impactos que esta genera. A partir de la información generada por la evaluación, se determinan las alternativas que permitan mejorar o fortalecer los cursos de acción emprendidos.

(v) **Información y la comunicación**, es la dimensión articuladora del Modelo que permiten a las organizaciones vincularse con su entorno y le facilitan la ejecución de sus operaciones internas ya que permite ampliar y profundizar en el uso y aprovechamiento de la información para los procesos internos de la entidad (toma de decisiones, elaboración de política pública, entre otros), así como la interacción con los ciudadanos.

(vi) **Gestión del conocimiento y la innovación**, dimensión transversal que impulsa la transformación de la información en capital intelectual para el Estado, permite el desarrollo de acciones para compartir el conocimiento entre los servidores públicos, de manera que se optimice su interpretación, uso, apropiación y, además, construye una cultura de análisis y retroalimentación para el mejoramiento gubernamental.

(vii) **Control Interno**, es el conjunto de prácticas, elementos e instrumentos que permiten a la entidad contar con una serie de pautas o directrices que le ayudan a controlar la planeación, gestión y evaluación de las organizaciones, a fin de establecer acciones de prevención, verificación y evaluación en procura del mejoramiento continuo de la entidad, involucrando a todos los servidores que laboran en ella.

Figura 20. Operación del Modelo Integrado de Planeación y Gestión (MIPG).



Fuente: Función publica

Medición. MIPG cuenta con una metodología de medición que se materializa en la operación estadística Medición del Desempeño Institucional (MDI), la cual se implementa en las entidades que están en el ámbito de aplicación de MIPG y del Modelo Estándar de Control Interno, La Medición del Desempeño Institucional se estructura como una operación estadística que se fundamenta en el análisis de los datos recolectados a través del Registro Administrativo Formulario Único de Reporte y Avance de Gestión (FURAG) (Funcion Publica, 2023)".

En síntesis, al análisis realizado se pudo constatar que el Plan de Gestión de Continuidad del Negocio para la Universidad Popular del Cesar, Seccional Aguachica se encuentra enmarcado dentro de la dimensión Gestión con Valores para Resultados del Modelo Integrado de Planeación y Gestión (MIPG).

Adicional a lo anterior, la realización del Plan de Gestión de Continuidad del Negocio se fundamenta en el marco jurídico y reglamentario colombiano que incluye diferentes leyes, decretos, normas, directrices, resoluciones y circulares que abordan, regulan y rigen temas de interés como lo son gobierno digital,

continuidad de negocio, control interno, seguridad de la información y ciberseguridad para las instituciones públicas como la Universidad Popular del Cesar, Seccional Aguachica.

4.2.2.2. Marco normativo en materia de Gobierno Digital y Continuidad del Negocio.

Ley 1978 de 2019. Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones. El artículo 35.5. Atribuye al Fondo de Tecnologías de la Información y las Comunicaciones la función de financiar planes, programas y proyectos para promover el desarrollo de contenidos, aplicaciones digitales y emprendimientos para la masificación de la provisión de trámites y servicios del Estado, que permitan implementar las políticas de Gobierno Digital y de Transformación Digital Pública (Congreso de la República de Colombia, 2019).

Decreto 620 de 2020. Por el cual se estable los lineamientos generales para el uso y operación de los servicios ciudadanos digitales.

El parágrafo del artículo 2.2.17.7.1. Señala que las entidades públicas del orden nacional y/o territorial, diseñarán y adaptarán los proyectos de tecnologías de la información para que se integren con los servicios ciudadanos digitales. Así mismo puntualiza que La política de Gobierno Digital es un mandato normativo, en consecuencia, corresponde su cumplimiento por virtud de las propias normas.

De acuerdo con el artículo 2.2.17.5.6. Los actores que traten información deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. Del mismo modo, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones (presidente de la República de Colombia, 2020).

Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga lo establecido en el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Como se determina en el artículo 2.2.9.1.2.1. Numeral 4 los sujetos obligados ejecutarán acciones orientadas a desarrollar servicios y

procesos inteligentes, tomar decisiones basadas en datos y consolidar un Estado abierto, con el fin de articular las Iniciativas Dinamizadoras de la Política de Gobierno Digital. Estas Líneas de Acción se materializarán en las sedes electrónicas de cada uno de los sujetos obligados, siguiendo los estándares señalados para tal fin (Presidente de la República de Colombia, 2022b).

Ley 1523 de 2012. Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones.

El artículo 2. Fija la responsabilidad de todas las autoridades y de los habitantes del territorio colombiano la gestión del riesgo, por tanto, las entidades públicas, privadas y comunitarias desarrollarán y ejecutarán los procesos de gestión del riesgo, conocimiento del riesgo, reducción del riesgo y manejo de desastres, en el marco de sus competencias, su ámbito de actuación y su jurisdicción, como componentes del Sistema Nacional de Gestión del Riesgo de Desastres.

El articulo 3 numeral 4 indica que toda persona natural o jurídica, bien sea de derecho público o privado, tiene el deber de adoptar las medidas necesarias para una adecuada gestión del riesgo en su ámbito personal y funcional, con miras a salvaguardarse.

Parágrafo del artículo 44 precisa que todas las entidades públicas, privadas o comunitarias velarán por la correcta implementación de la gestión del riesgo de desastres en el ámbito de sus competencias sectoriales y territoriales en cumplimiento de sus propios mandatos y normas que los rigen (Congreso de la República de Colombia, 2012a).

Decreto 1072 de 2015. (Decreto Único Reglamentario del Sector Trabajo). Reglamenta el Sistema de Gestión de Seguridad y Salud en el trabajo. De acuerdo con el artículo 2.2.4.6.8. Es obligación del empleador adoptar disposiciones efectivas para desarrollar las medidas de identificación de peligros, evaluación y valoración de los riesgos y establecimiento de controles que prevengan daños en la salud de los trabajadores y/o contratistas, en los equipos e instalaciones, de la misma manera debe implementar y desarrollar actividades de prevención de accidentes de trabajo y enfermedades laborales.

Aportando a lo anterior el empleador debe mantener disponibles y debidamente actualizados los documentos relacionados con el Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST expuestos en los numerales 3 y 12 respectivamente, enmarcados en el artículo 2.2.4.6.12. (i) La identificación anual de peligros y evaluación y valoración de los riesgos. (ii) La identificación de las amenazas junto con la evaluación de la vulnerabilidad y sus correspondientes planes de prevención, preparación y respuesta ante emergencias.

El artículo 2.2.4.6.25. Define el deber del empleador o contratante de implementar y mantener las disposiciones necesarias en materia de prevención, preparación y respuesta ante emergencias, con cobertura a todos los centros y turnos de trabajo y todos los trabajadores, independiente de su forma de contratación o vinculación, incluidos contratistas y subcontratistas, así como proveedores y visitantes. Para ello debe implementar un plan de prevención, preparación y respuesta ante emergencias el cual debe permitir su integración con otras iniciativas, como los planes de continuidad de negocio (Presidente de la República de Colombia, 2015).

Plan Nacional de Gestión del Riesgo de Desastres. "Una estrategia de desarrollo". Es el instrumento del Sistema Nacional de Gestión del Riesgo de Desastres creado por la Ley 1523 de 2012, que define los objetivos, programas, acciones, responsables y presupuestos, mediante las cuales se ejecutan los procesos de conocimiento del riesgo, reducción del riesgo y manejo de desastres en el marco de la planificación del desarrollo nacional.

El documento Plan Nacional de Gestión del Riesgo de Desastres está estructurado en dos componentes: un Componente General, el cual contiene el marco estratégico de la gestión del riesgo y un Componente Programático y de inversiones en el que se incorporan los programas, proyectos, objetivos de proyecto, metas, responsables de la implementación para el período 2015-2030 (Unidad Nacional para la Gestión del Riesgo de Desastres, 2022).

ISO 22301:2019. Es la norma internacional para sistemas de gestión de continuidad de negocio (SGCN) La cual proporciona un marco de mejores prácticas para apoyar a las organizaciones a gestionar eficazmente el impacto de una interrupción de su funcionamiento normal, el propósito de la norma es ayudar a las organizaciones a comprender la cantidad y el tipo de impacto que está dispuesta a aceptar tras una interrupción (Organización Internacional de Normalización, 2019a).

NTC-ISO 22301:2019. Seguridad y resiliencia. Sistema de gestión de continuidad de negocio, es un documento en el que se especifica los requisitos para implementar, mantener y mejorar un sistema de gestión con el propósito de protegerse, reducir la probabilidad de ocurrencia de, prepararse, responder y recuperarse de las interrupciones cuando estas surjan. Los requisitos que se especifican en el documento son genéricos y están destinados para ser aplicados en todas las organizaciones, o partes de estas, sin considerar el tipo, tamaño o naturaleza de la organización. El grado de aplicación de estos requisitos depende del ambiente operativo y la complejidad de la organización (ICONTEC, 2019a).

4.2.2.3. Marco normativo en materia de Control Interno.

Constitución Política de la República de Colombia 1991. En el artículo 209 establece que la administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley de igual manera en su artículo 269 enfatiza que, en las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno (Asamblea Nacional Constituyente, 1991c).

Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones. De acuerdo a la presente ley el control interno se define de la siguiente manera "sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos" (Congreso de la República de Colombia, 1993).

Decreto 1599 de 2005. Por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano. En el numeral 5.5. Fija la responsabilidad de La Oficina de Control Interno, Unidad de Auditoría o quien haga sus veces de realizar evaluación independiente al Sistema de Control Interno y la Gestión de la entidad pública, así como el seguimiento al Plan de Mejoramiento Institucional, generando las recomendaciones correspondientes y asesorando a la alta dirección para su puesta en marcha (Presidente de la República de Colombia, 2005).

Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. El artículo 76 ordena que, en toda entidad pública, deberá existir por lo menos una dependencia encargada de recibir, tramitar y resolver las quejas, sugerencias y reclamos que los ciudadanos formulen, y que se relacionen con el cumplimiento de la misión de la entidad. Por consiguiente, es deber de la oficina de control interno vigilar que la atención se preste de acuerdo con las normas legales vigentes y rendir a la administración de la entidad un informe semestral sobre el particular (Congreso de la República de Colombia, 2011).

Decreto 648 de 2017. Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública. El artículo 6 define los facilitadores como "instancias encargadas de orientar, asesorar, impulsar y poner en marcha estrategias para la debida implantación y el mejoramiento continuo del Sistema de Control Interno".

El artículo 17 determina de las Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control (Presidente de la República de Colombia, 2017).

4.2.2.4. Marco normativo en materia de Seguridad de la Información y Ciberseguridad.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política, así mismo contempla los principios para el tratamiento de datos personales y establece los deberes de los responsables del tratamiento y encargados del tratamiento (Congreso de la República de Colombia, 2012b).

Decreto 1377 de 2013. Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. El presente decreto reglamenta que no se podrá recolectar datos personales sin autorización del titular ni utilizar medios engañosos o fraudulentos para recolectar y realizar tratamiento de datos personales además los responsables del tratamiento deberán desarrollar políticas para el tratamiento de los datos personales y velar por el cabal cumplimiento a las mismas (Presidente de la República de Colombia, 2013).

Decreto 886 de 2014. Por el cual se reglamenta la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del Tratamiento. Conforme al artículo 2 las bases de datos que contengan datos personales cuyo tratamiento se realicen por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él serán objeto de inscripción en el Registro Nacional de Bases de Datos. El artículo 5 define la información mínima que debe contener el Registro Nacional de Bases de Datos de igual manera los artículos 6 y 7 exponen los deberes del responsable del Tratamiento de la base de datos y Encargado o los Encargados del Tratamiento de la Base de Datos respectivamente (Presidente de la República de Colombia, 2014).

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las

tecnologías de la información y las comunicaciones, entre otras disposiciones (Congreso de la República de Colombia, 2009) .

Constitución Política de la República de Colombia 1991. El artículo 15 señala que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (Asamblea Nacional Constituyente, 1991b) .

NTC-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. Es una norma que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de la organización, incluye además los requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización (ICONTEC, 2022b).

Circular Externa Conjunta No. 04 de 2019. Tratamiento de datos personales en sistemas de información interoperables. La presente circular expone los lineamientos que deben seguir las entidades públicas y particulares que ejercen funciones públicas para la protección del derecho de habeas data o el debido tratamiento de datos personales en sistemas de información interoperables (Superintendencia de Industria y Comercio & Agencia Nacional de Defensa Jurídica del Estado, 2019).

Decreto 338 de 2022. Por el cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital. El artículo 2.2.21.1.2.1. Expone el deber de las autoridades de adoptar el modelo de gobernanza, de aplicar los objetivos, principios, niveles e instancias, que permitan su materialización, con el fin de fortalecer la seguridad digital, la protección de las redes, las infraestructuras críticas, los servicios esenciales y los sistemas de información en el ciberespacio. El objetivo del modelo de gobernanza es facilitar la participación, articulación e interacción de las múltiples partes interesadas para fortalecer las capacidades en la gestión de riesgos de seguridad digital y de esta manera lograr un abordaje integral que promueva el adecuado aprovechamiento de las oportunidades que ofrece el entorno digital tal cual lo enuncia el articulo artículo 2.2.21.1.2.2 (Presidente de la República de Colombia, 2022a).

CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa. Este documento busca sentar las bases de política en temas de ciberseguridad y ciberdefensa en particular, por ello las entidades involucradas tendrán la responsabilidad de desarrollar estas bases y generar mecanismos que permitan

garantizar la seguridad de la información a nivel nacional teniendo en cuenta normas técnicas y estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad. Así mismo se define un plan de acción para la ejecución de la política en ciberseguridad y ciberdefensa, el cual estará a cargo de las entidades involucradas (Departamento Nacional de Planeación, 2011).

CONPES 3995. Política nacional de confianza y seguridad digital. El objetivo de este documento es establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital atreves del fortalecimiento de las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; así como también la actualización del marco de gobernanza en materia de seguridad digital y finalmente la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías (Departamento Nacional de Planeación, 2020).

Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. El propósito de la presente resolución es establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital. El artículo 17 señala el deber de los sujetos obligados a incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, entre los que se destaca la responsabilidad de contar con los recursos tecnológicos necesarios para realizar una adecuada gestión de seguridad de la información y la ciberseguridad de igual manera la obligación de colaborar y articular con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad a nivel nacional (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021).

Constitución Política de la República de Colombia 1991. El artículo 2 consagra que las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares, así también el artículo 78 reconoce que la ley regulará el control de calidad de bienes y servicios ofrecidos y prestados a la comunidad, así como la información que debe suministrarse al público en su comercialización (Asamblea Nacional Constituyente, 1991a).

4.2.3. Marco normativo que rigen en Colombia los Planes de Continuidad del Negocio.

De acuerdo a la revisión de la literatura en cuanto a la normativa nacional que rige a los Planes de Continuidad del Negocio se puede comprobar que dentro del marco normativo existen distintas normas, guías, directrices las cuales avalan y/o exigen a las instituciones públicas como la Universidad Popular del Cesar, Seccional Aguachica que tengan diseñado y/o construido un Plan de Gestión de Continuidad del Negocio como se muestra a continuación.

ISO 22301:2019. Es la norma internacional para sistemas de gestión de continuidad de negocio (SGCN) La cual proporciona un marco de mejores prácticas para apoyar a las organizaciones a gestionar eficazmente el impacto de una interrupción de su funcionamiento normal, el propósito de la norma es ayudar a las organizaciones a comprender la cantidad y el tipo de impacto que está dispuesta a aceptar tras una interrupción (Organización Internacional de Normalización, 2019b).

NTC-ISO 22301:2019. Seguridad y resiliencia. Sistema de gestión de continuidad de negocio, es un documento en el que se especifica los requisitos para implementar, mantener y mejorar un sistema de gestión con el propósito de protegerse, reducir la probabilidad de ocurrencia, de prepararse, responder y recuperarse de las interrupciones cuando estas surjan. Los requisitos que se especifican en el documento son genéricos y están destinados para ser aplicados en todas las organizaciones, o partes de estas, sin considerar el tipo, tamaño o naturaleza de la organización (ICONTEC, 2019b).

GTC-ISO 22313:2020. Seguridad y resiliencia. Sistemas de gestión de continuidad de negocio. Orientación sobre el uso de la NTC-ISO 22301. Es una norma que proporciona orientación y recomendaciones (basadas en las buenas prácticas internacionales) para aplicar los requisitos del sistema de gestión de continuidad de negocio (BCMS, por sus siglas en ingles) que figuran en la norma NTC-ISO 22301 (ICONTEC, 2020).

GTC-ISO-TS 22317:2022. Seguridad y resiliencia. Sistemas de gestión de continuidad de negocio. Directrices para el análisis de impacto del negocio. Esta norma proporciona directrices detalladas para que una organización implemente y mantenga un proceso formal y documentado de análisis de impacto en el negocio (BIA, por sus siglas en ingles) que se ajuste a sus necesidades (ICONTEC, 2022a).

CIRCULAR 025 DE 2020. Emitida por la Superintendencia Financiera de Colombia presenta instrucciones relacionadas con el riesgo operacional y establece el Sistema de Administración de Riesgo Operativo (SARO). El numeral 3.1.3.2. Administración de la continuidad del negocio, expresa que las entidades

deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya elementos como: prevención y atención de emergencias, administración de escenarios de crisis, planes de contingencia y capacidad de retorno a la operación normal, así mismo instaura los requisitos mínimos y necesarios con los que debe cumplir los planes de continuidad del negocio (Superintendencia Financiera de Colombia, 2020).

4.3. GUIA PARA LA GESTION DE CONTINUIDAD DEL NEGOCIO ORIENTADA A LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA.

La Gestión de Continuidad del Negocio permite identificar las potenciales amenazas a una organización, así como el impacto que la materialización de estas podría provocar en las operaciones del negocio (Cano Sotomayor et al., 2021). Es por ello la necesidad de identificar y evaluar los riesgos que pongan en peligro la continuidad del negocio.

En este capítulo se describen los componentes estratégicos que sustentan el presente proyecto. La sección 4.3.1. presenta el alcance del PGCN. En la sección 4.3.2. se presenta el análisis de la universidad. En la sección 4.3.3. se describe el Análisis de Impacto del Negocio (BIA). En la sección 4.3.4. se formulan las estrategias para la continuidad del negocio. En la sección 4.3.5. las estrategias para dar respuesta a la contingencia. En la sección 4.3.6. se proponen las estrategias para la recuperación.

4.3.1. Alcance del Plan de Gestión de Continuidad del Negocio.

4.3.1.1. Introducción.

Hoy día las organizaciones están expuestas cada vez más a eventos que podrían causar la interrupción o el cese de sus actividades por lo que es necesario estar preparados para afrontarlos, es en este contexto que cobra importancia la continuidad del negocio haciendo referencia a la capacidad que tiene una organización para mantener operando sus funciones críticas a pesar de la ocurrencia de un evento disruptivo. Para este fin se es necesario desarrollar un Plan de Gestión de Continuidad del Negocio, una guía que describe los procedimientos y estrategias establecidas para prevenir, afrontar y recuperarse de sucesos que pongan en riesgo la disponibilidad y continuidad de las operaciones e información de una empresa.

El principal objetivo del Plan de Gestión de Continuidad del Negocio es minimizar el impacto en las operaciones tras una interrupción garantizando la continuidad del negocio, evitando así las repercusiones significativas en los activos, la imagen y reputación de la institución, así como también alcanzar la resiliencia empresarial.

4.3.1.2. Alcance.

El Plan de Gestión de Continuidad del Negocio abarcara los Macroprocesos de Direccionamiento Estratégico, Macroproceso Misional y el Macroproceso de Apoyo de la Universidad Popular del Cesar descritos así:

El **Macroproceso Direccionamiento Estratégico** comprende los Microprocesos de:

(i) Gestión Estratégica. Pretende formular lineamientos, metodologías y estrategias que le permitan a la institución contar con instrumentos adecuados para la planeación, seguimiento y control de los procesos institucionales, en virtud de la misión y de las funciones encomendadas, a través del monitoreo del entorno (interno y externo), buscando mejorar su desempeño y dar respuesta a las necesidades de la Comunidad Universitaria y la sociedad en general.

(ii) Gestión de Mejoramiento Institucional. Busca proporcionar una estructura para el control de la estrategia, la gestión y la evaluación de la institución orientada hacia el cumplimiento de sus objetivos institucionales que contribuya a los fines esenciales el estado estableciendo una herramienta de gestión que permita dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de los servicios de la Universidad

(iii) Gestión de la Comunicación. Propender por una institución adecuadamente informada y comunicada a través de medios confiables, que sobre la base de la transparencia faciliten su direccionamiento estratégico, el logro de sus objetivos y la satisfacción de sus públicos internos y externos.

(iv) Gestión de Relaciones y Cooperación Interinstitucional. Promover la generación de alianzas para la comunidad universitaria con instituciones a nivel nacional e internacional.

El **Macroproceso Misional** comprende los Microprocesos de:

(i) Gestión de Docencia. Desarrollar competencias para el ejercicio profesional en una disciplina definida.

(ii) Gestión de Investigación. Consolidar la investigación como una función esencial de la institución contribuyendo al desarrollo local, regional, y nacional mediante la consolidación de grupos semilleros, proyectos de

investigación, la socialización de experiencias investigativas, la internacionalización de la investigación, y la protección de los derechos de autor.

(iii) Gestión de Extensión y Proyección Social. Realizar programas de extensión, asesoría y gestión en la medida de las necesidades demandadas por la comunidad y por los programas académicos.

El **Macroproceso de Apoyo** comprende los Microprocesos de:

(i) Gestión de Bienes y Servicios. Gestionar los requerimientos de las dependencias, en lo relacionado con la adquisición de bienes y servicios, control y aseguramiento de bienes y personas, procurando satisfacer a sus usuarios mediante la oportunidad y pertinencia de los bienes y servicios.

(ii) Gestión de Medios Educativos. Proveer a la comunidad universitaria de los medios educativos y tecnológicos disponibles para el desarrollo de sus actividades académicas en cuanto a la educación mediada por las TIC y el acceso a recursos bibliográficos.

(iii) Gestión Financiera. Gestionar y administrar eficientemente la utilización del recurso financiero de la Universidad Popular del Cesar, procurando dotar a todas las dependencias de este recurso de manera oportuna y racional para el desarrollo de sus actividades propias enmarcadas en el Plan Decenal Indicativo de Desarrollo de la Institución; asimismo, presentar los estados e informes financieros y tributarios de la Universidad, dando cumplimiento a la normatividad legal vigente y procurando el mejoramiento continuo en el desarrollo de sus procesos para suministrar información financiera, confiable y oportuna que revele razonablemente la situación financiera, económica y social de la Institución.

(iv) Gestión Talento Humano. Promover el desarrollo integral del Talento humano al servicio de la Universidad que garantice la excelencia en la prestación del servicio y que la Institución cuente con servidores íntegros, competentes y comprometidos, que contribuyan al logro de los objetivos y planes de la Universidad.

(v) Gestión Jurídica. Representar judicialmente a la Universidad Popular del Cesar en defensa de sus intereses, garantizando el control en la gestión de contratos, convenios, mediante la evaluación y verificación del cumplimiento de los requisitos de tipo legal e institucional, la asesoría, asistencia y apoyo en los conceptos de tipo

judicial que surjan de las actividades de la Universidad en las diferentes dependencias de manera oportuna.

(vi) Gestión Documental. Garantizar la conservación de la memoria documental de la Institución.

(vii) Gestión De Bienestar Institucional. Gestionar un conjunto de programas, proyectos, políticas y actividades que se orientan al desarrollo físico, psicoafectivo, espiritual, cultural y estético de los estudiantes, docentes y personal administrativo.

(viii) Gestión de Tecnologías de la Información y la Comunicación. Apoyar la gestión académica, Investigativa, de extensión y administrativa, brindando a la comunidad universitaria una infraestructura tecnológica y de sistemas de información moderna e innovadora, que favorezca el mejoramiento de la calidad en la educación impartida y el desarrollo institucional.

Los Macroprocesos y procesos mencionados anteriormente se encuentran representados y documentados en el mapa de procesos de la Universidad Popular del Cesar (2023).

4.3.2. Análisis de la organización.

La Universidad Popular del Cesar, Seccional Aguachica es una institución de educación superior oficial del orden nacional cuyos usuarios, jóvenes de la región del sur del departamento del Cesar y sur del departamento de Bolívar cuentan con la oportunidad de acceder a servicios educación superior a través de los programas Ingeniería de Sistemas, Ingeniería Agroindustrial, Ingeniería Ambiental y Sanitaria, Administración de empresas, Contaduría Pública, Economía, Tecnología Agropecuaria logrando así la formación integral de los mismos aportando al desarrollo de región.

Para lo anterior la Universidad Popular del Cesar, Seccional Aguachica dispone de una estructura orgánica fijado mediante los Acuerdos N° 011 de marzo 31 de (2016a) y N° 029 del 06 de agosto del (2002) determinando sus dependencias y sus respectivas funciones con el propósito de dar cumplimiento de sus objetivos, misión y visión. Sin embargo, para el presente proyecto se resaltará especialmente las dependencias de mayor criticidad (Dirección Académica, Dirección Administrativa y Financiera, Registro y Control) para la Seccional Aguachica debido a su importancia dentro de la organización.

Para este apartado se tomará en consideración las siguientes actividades: Identificación y clasificación de los activos de información, Identificación de las

amenazas y vulnerabilidades, Análisis de Impacto del Negocio (BIA) y análisis de riesgos.

4.3.2.1. Identificación y clasificación de los activos.

Los activos de información son aquellos recursos de alto valor producidos, gestionados y almacenados por la institución que permiten a la Universidad Popular del Cesar, Seccional Aguachica cumplir con su misión a través de los procesos de mayor interés los cuales se señalan a continuación.

Tabla 1. Procesos principales de cada dependencia critica de la universidad.

Dependencia	Procesos
Dirección Administrativa y Financiera	Proceso de contratación Liquidación de matriculas Tramite de nómina docente Talento humano
Dirección Académica	Proceso académico Gestión documental
Registro y Control	Proceso de inscripciones Administración del sistema académico

Fuente: los autores

Para la identificación de los activos se llevó a cabo una entrevista a los líderes de las áreas de Dirección Académica, Dirección Administrativa y Financiera, Registro y Control con el propósito de determinar aquellos activos de información que son de gran relevancia para cada una de las dependencias anteriormente mencionadas y que al no ser protegidos supondría consecuencias negativas para la universidad.

Tabla 2. Activos de información.

Tipo	Identificador	Activo
	INF-01	Planeación de horarios
	INF-02	Asignaciones académicas
	INF-03	Planes de mejoramiento

Información	INF-04	Planes de acción
	INF-05	Planes prospectivos
	INF-06	Evaluación docente y seguimiento del mismo
	INF-07	Evaluación de la hoja de vida de los docentes
	INF-08	Contratación de funcionarios y docentes
	INF-09	Planes de servicios
	INF-10	Proceso de inscripción y admisión
	INF-11	Matricula académica
	INF-12	Proceso de egreso o de grados
	INF-13	Registro de notas
	INF-14	Liquidaciones de los procesos de matricula
Software	SW-01	Sistema operativo
	SW-02	Suite de ofimática
Servicios	SERV-01	GESTASOFT
	SERV-02	ORFEO
	SERV-03	Google Drive
	SERV-04	Correo electrónico Institucional
Hardware	HW-01	Equipos de cómputo
	HW-02	Equipos de comunicaciones
	HW-03	Cableado estructurado
Recurso humano	RH-01	Líder de dirección académica y funcionarios
	RH-02	Líder de dirección administrativa y financiera y funcionarios
	RH-03	Líder de Registro y Control y funcionarios

Fuente: Los autores

Para la clasificación de los activos de información se toma como referencia lo recomendado por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC, 2016) a través de la Guía para la Gestión y Clasificación de Activos de Información la cual establece que la clasificación se basa en las propiedades de la seguridad de la información (confidencialidad, integridad, disponibilidad) para cada activo como se observa a continuación.

Clasificación de acuerdo con la confidencialidad.

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Figura 21. Clasificación por confidencialidad.

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PUBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Fuente: MinTIC

Clasificación de acuerdo con la integridad.

La integridad se refiere a la exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

Figura 22. Clasificación por integridad.

A **(ALTA)**	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M **(MEDIA)**	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B **(BAJA)**	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: MinTIC

Clasificación de acuerdo con la disponibilidad.

La disponibilidad se refiere a que la información debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiera.

Figura 23. Clasificación por disponibilidad.

1 **(ALTA)**	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 **(MEDIA)**	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 **(BAJA)**	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente: MinTIC

4.3.2.2. Criticidad de los activos.

Para determinar la criticidad de un activo de información se define los siguientes criterios.

Figura 24. Criterios de clasificación.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACION PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACION PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACION PUBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: MinTIC

Asimismo, se define tres (3) niveles que permiten determinar el valor general del activo en la entidad (es importante aclarar que los niveles pueden ser definidos a criterio de la entidad) con el fin identificar qué activos deben ser tratados de manera prioritaria.

Figura 25. Niveles de clasificación.

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: MinTIC

La guía para la Gestión y Clasificación de Activos de Información propone una serie de ítems para realizar el etiquetado de activos de información teniendo en cuenta las siguientes pautas generales.

Figura 26. Etiquetado de activos de información.

Propiedad	Criterio	Etiqueta
Confidencialidad	Información pública reservada	IPR
	Información pública clasificada	IPC
	Información pública	IPB
Integridad	Alta	A
	Media	M
	Baja	B
Disponibilidad	Alta	1
	Media	2
	Baja	3

Autor: Diego Tellez

Tabla 3. Criticidad de los activos de información.

Identificador	Confidencialidad	Integridad	Disponibilidad	Criticidad
INF-01	IPC	A	1	ALTA
INF-02	IPC	A	2	MEDIA
INF-03	IPC	A	1	ALTA
INF-04	IPC	A	1	ALTA
INF-05	IPC	A	1	ALTA
INF-06	IPR	A	1	ALTA
INF-07	IPR	A	1	ALTA
INF-08	IPR	A	1	ALTA
INF-09	IPC	A	1	ALTA
INF-10	IPC	A	1	ALTA
INF-11	IPB	A	1	ALTA
INF-12	IPC	A	1	ALTA
INF- 13	IPC	A	2	MEDIA
INF-14	IPC	A	1	ALTA
SW-01	IPR	A	1	ALTA
SW-02	IPC	A	2	MEDIA

SERV-01	IPC	A	1	ALTA
SERV-02	IPC	A	2	MEDIA
SERV-03	IPR	A	1	ALTA
SERV-04	IPR	A	1	ALTA
HW-01	IPR	A	1	ALTA
HW-02	IPR	A	1	ALTA
HW-03	IPR	A	1	ALTA
RH-01	IPR	A	1	ALTA
RH-02	IPR	A	1	ALTA
RH-03	IPR	A	1	ALTA

Fuente: Los autores

Una vez determinada la criticidad de cada uno de los activos de información se logra observar que 22 de esos activos tienen una criticidad alta y 4 con criticidad media, por tal razón se hace necesario gestionar los riesgos de los activos que fueron identificados y previamente clasificados.

4.3.2.3. Identificación de las amenazas y vulnerabilidades.

Una amenaza es considerada un evento o una acción que conlleva a que suceda un incidente en las organizaciones ya que generan un daño o una pérdida inmaterial de los activos de información (ISOTools, 2024). Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016b) y según la Norma Técnica Colombiana NTC-ISO/IEC 27005:2009 (ICONTEC, 2019c) se clasifica en amenazas comunes y amenazas humanas.

Para las amenazas comunes, estas pueden ser D (Deliberadas), todas aquellas acciones deliberadas que tiene como objetivo los activos de información; (A) Accidentales, para acciones humanas que pueden dañar accidentalmente los activos de información; y (E) Ambientales, para todos los incidentes que no se basa en las acciones humanas.

Tabla 4. Amenazas comunes.

Tipo	Amenaza	Origen
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E

Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Fallas del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Fuente: NTC-ISO/IEC 27005:2009 (Anexo C)

Las fuentes de amenazas humanas se desglosan específicamente en la siguiente tabla:

Tabla 5. Amenazas humanas.

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes,	Curiosidad Ego Inteligencia Ganancia monetaria Venganza	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador

deshonestos o despedidos)	Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

Fuente: NTC-ISO/IEC 27005:2009 (Anexo C)

Una vulnerabilidad es la debilidad de un activo o control que puede ser explotado por una o más amenazas (ISO, 2024). A continuación, se presenta ejemplos de vulnerabilidades en diversas áreas de seguridad:

Tabla 6. Vulnerabilidades.

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencias de pistas de auditoria
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido

	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlado de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Fallas en la producción de informes de gestión
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de fallas
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en área susceptible de inundación
	Red energética inestable

	Ausencia de protección física de la edificación (Puertas y ventanas)
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso formal para la revisión de los derechos de acceso
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
	Ausencia de auditorias
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento del servicio
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Ausencia de procedimientos de control de cambios
	Ausencia de procedimiento formal para la documentación del MSPI
	Ausencia de procedimiento formal para la supervisión del registro del MSPI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso de correo electrónico
	Ausencia de procedimientos para introducción del software en los sistemas operativos
	Ausencia de registros en bitácoras
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de política sobre limpieza de escritorio y pantalla
	Ausencia de autorización de los recursos de procesamiento de información

	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad
	Ausencia de revisiones regulares por parte de la gerencia
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.

Fuente: Guía de gestión de riesgos MinTIC

A continuación, se observa las amenazas y vulnerabilidades a las que están expuestas cada uno de los activos de información:

Tabla 7. Vulnerabilidades y amenazas de los activos de información de la UPCSA.

Activo	Vulnerabilidad	Amenaza
INF-02	Falta de conciencia acerca de la seguridad	Hurto de información
		Procesamiento ilegal de datos
	Ausencia de mecanismos de monitoreo	Negación de acciones
INF-01 INF-03 INF-04 INF-05 INF-09	Almacenamiento sin protección	Accidente importante
	Ausencia de documentación	Hurto de información
		Sabotaje del sistema
	Ausencia de copias de respaldo	Código malicioso
		Errores en el sistema
	Fallas en la producción de informes de gestión	Divulgación
		Ingreso de datos falso o corruptos
	Falta de conciencia acerca de la seguridad	Acto fraudulento
		Ingeniería social
	Ausencia de procedimientos para el manejo de información clasificada	Guerra de la información
		Observar información reservada
INF-06 INF-07	Asignación errada de los derechos de acceso	Abuso de los derechos
		Acceso no autorizado al sistema
	Ausencia de copias de respaldo	Manipulación con software
		Mal funcionamiento del equipo
		Errores en el sistema
	Ausencia de asignación	Negación de acciones

	adecuada de responsabilidades en seguridad de la información	Ingreso de datos falsos o corruptos
		Sabotaje del sistema
	Gestión deficiente de las contraseñas	Falsificación de derechos
		Acceso no autorizado al sistema
INF-08	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
		Divulgación
	Procedimientos inadecuados de contratación	Hurto de información
		Hurto de medios o documentos
		Procesamiento ilegal de datos
	Entrenamiento insuficiente en seguridad	Abuso de los derechos
		Error en el uso
	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
		Negación
INF-10	Asignación errada de los derechos de acceso	Divulgación
		Falsificación de derechos
	Falta de conciencia acerca de la seguridad	Hurto de información
		Corrupción de los datos
		Intrusión en el sistema
		Intrusión en privacidad personal
	Ausencia de procedimientos para el manejo de información clasificada	Observar información reservada
		Hurto de información
		Venta de información personal
INF-11	Almacenamiento sin protección	Hurto de medios o documentos
		Divulgación
	Ausencia de copias de respaldo	Manipulación con software
		Mal funcionamiento del software
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
		Intrusión al sistema
		Ingeniería social

INF-12	Entrenamiento insuficiente en seguridad	Abuso de los derechos
		Ingeniería social
INF- 13	Defectos bien conocidos en el software	Abuso de los derechos
		Mal funcionamiento del software
	Ausencia de copias de respaldo	
		Manipulación con software
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Asignación errada de los derechos de acceso	Abuso de los derechos
		Divulgación
		Manipulación en el sistema
		Ingreso de datos falsos o corruptos
INF-14	Entrenamiento insuficiente en seguridad	Ingeniería social
	Falta de conciencia acerca de la seguridad	Hurto de Información
		Intrusión en privacidad personal
	Asignación errada de los derechos de acceso	Divulgación
		Acceso no autorizado al sistema
	Procedimientos inadecuados de contratación	Chantaje
		Sabotaje del sistema
SW-01	Defectos bien conocidos en el software	Mal funcionamiento del software
		Abuso de los derechos
	Descarga y uso no controlado de software	Uso de software falso o copiado
	Falta de conciencia acerca de la seguridad	Error en el uso
		Código malicioso
	Ausencia de mecanismos de monitoreos establecidos para las brechas en seguridad	Intrusión al sistema
		Ingeniería social
	Defectos bien conocidos en el software	Mal funcionamiento del software

SW-02	Descarga y uso no controlado de software	Copia fraudulenta del software
	Falta de conciencia acerca de la seguridad	Error en el uso
		Acto fraudulento
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
SERV-01 SERV-02	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
SERV-03 SERV-04	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Entrenamiento insuficiente en seguridad	Ingeniería social
		Error en el uso
	Ausencia de políticas sobre el uso de correo electrónico	Código malicioso
		Suplantación de identidad
HW-01	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Mal funcionamiento del equipo
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
HW-02	Almacenamiento sin protección	Uso inadecuado del equipo
	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Falla del equipo
	Red energética inestable	Pérdida del suministro de energía
HW-03	Arquitectura de red insegura	Espionaje remoto
	Falta de conciencia acerca de la seguridad	Ingreso de datos falsos o corruptos
	Entrenamiento insuficiente en seguridad	Ingeniería social

RH-01 RH-02 RH-03	Procedimientos inadecuados de contratación	Sabotaje del sistema
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Acceso no autorizado al sistema

Fuente: Los autores

4.3.2.4. Análisis y evaluación de riesgos.

Para la realización del análisis de riesgos se toma como referencia la guía de gestión de riesgos del Ministerio de las Tecnologías de la Información y las Comunicaciones MinTIC (2016b) cuyo propósito es orientar a las entidades a gestionar los riesgos de seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la metodología de riesgos del Departamento Administrativo de la Función Pública (DAFP) y de esa manera ayudar a que las entidades logren vincular la identificación y análisis de riesgos de la entidad hacia los temas de la seguridad de la información.

La guía sugiere una serie de etapas basadas en la norma ISO 27005 para llevar a cabo el análisis de riesgos las cuales se muestran a continuación.

Figura 27. Metodología análisis de riesgos.

Fuente: MinTIC

(i) Identificación del riesgo: El propósito de esta fase es determinar que podría suceder que cause una pérdida potencial para comprender el cómo, donde, y por qué podría ocurrir está perdida.

(ii) Identificación de los activos: Esta fase se lleva a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

(iii) Identificación de las amenazas: Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad.

(iv) Identificación de controles existentes: La realización de esta fase tiene como objetivo evitar trabajo o costos innecesarios además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

(v) Identificación de las vulnerabilidades: Para elaborar de forma adecuada esta fase es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

(vi) Métodos para la valoración de las vulnerabilidades: Esta fase consiste en descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante.

(vii) Identificación de las consecuencias: En esta fase se identifican los daños o las consecuencias para entidad que podrían ser causadas por un escenario de incidente.

Para el desarrollo del presente proyecto la metodología del análisis de riesgos recomendada por MinTIC se adopta y adapta quedando de la siguiente manera:

Figura 28. Metodología para el análisis de riesgos UPC.

Fuente: MinTIC

(i) Identificación de los activos: Los activos de información se encuentran enlistados en el apartado 4.3.2.1. Identificación y clasificación de los activos (Tabla 2).

(ii) Identificación de las amenazas: Las amenazas se encuentran enlistadas en el apartado 4.3.2.3. Identificación de las amenazas y vulnerabilidades (Tabla 7).

(iii) Identificación de las vulnerabilidades: Las vulnerabilidades se encuentran enlistadas el apartado 4.3.2.3. Identificación de las amenazas y vulnerabilidades (Tabla 7).

(iv) Identificación del riesgo: Los riesgos se encuentran enlistados en la sección 4.3.2.4. Análisis y evaluación de riesgos (Tabla 8).

(v) Identificación de las consecuencias: Los daños a los que podría estar expuesta la universidad se enlistan en la sección 4.3.2.5. (Tabla 9).

Para evaluar los riesgos se tiene en cuenta la "Matriz de calificación, evaluación y respuesta a los riesgos" como resultado del análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, con la cual se califica los riesgos, las zonas de riesgos y por consiguiente se presenta las posibles formas de tratamiento de cada riesgo.

Figura 29. Matriz de calificación, evaluación y respuesta a los riesgos.

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada:* Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos del Departamento Administrativo de la Función Pública (DAFP)

A continuación, se presenta el análisis de riesgos de seguridad de la información teniendo en cuenta la identificación de las vulnerabilidades y amenazas para cada uno de los activos de información de las áreas de Dirección Académica, Dirección Administrativa y Financiera, Registro y Control, así como la matriz de calificación, evaluación y respuesta a los riesgos.

Tabla 8. Análisis de riesgos.

Análisis del riesgo						
Tipo de activo: Información						
Activo	**Riesgo**	**Calificación**		**Tipo Impacto**	**Evaluación**	**Medidas de Respuesta**
		Probabilidad	**Impacto**		**Zona de riesgo**	
INF-02	Daño a la reputación de la universidad por procesamiento ilegal de los datos debido a falta de conciencia acerca de la seguridad	1	4	Confidencialidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Exposición de datos por procesamiento ilegal de los datos y/o negación de acciones debido a la ausencia de mecanismo de monitoreo	3	4	Confidencialidad de la información	Extremo	

INF-01 INF-03 INF-04 INF-05 INF-09	Pérdida de datos e información crítica por accidente importante debido al almacenamiento sin protección de la información	2	4	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Interrupción de las operaciones o prestación de servicios por hurto de información y/o sabotaje del sistema debido a ausencia de documentación	2	4	Disponibilidad de la información	Alta	
	Pérdida de disponibilidad de la información y/o accesibilidad a los datos por código malicioso y/o errores en el sistema debido a ausencia de copias de respaldo	3	3	Disponibilidad de la información	Alta	
	Interrupción de las operaciones por divulgación y/o ingreso de datos falsos o corruptos debido a fallas en la producción de	2	4	Disponibilidad de la información	Alta	

	informes de gestión					
	Obtención de información confidencial por acto fraudulento y/o ingeniera social debido a falta de conciencia acerca de la seguridad de los datos	2	3	Confidencialidad de la información	Moderada	Asumir el riesgo, Reducir el riesgo
	Filtración y/o manipulación de datos por guerra de la información y/u observar información reservada debido a la ausencia de procedimientos para el manejo de información clasificada	3	3	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
INF-06 INF-07	Violación de datos por abuso de los derechos y/o acceso no autorizado al sistema debido a la asignación errada de los derechos de acceso	2	4	Confidencialidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir

	Pérdida de datos críticos por manipulación con software, mal funcionamiento del equipo y/o errores en el sistema debido a la ausencia de copias de respaldo	2	3	Integridad de la información	Moderada	Asumir el riesgo, Reducir el riesgo
	Incumplimiento de la normativa por negación de acciones, ingreso de datos falsos o corruptos y/o sabotaje del sistema debido a ausencia de asignación adecuada de responsabilidades en seguridad de la información	2	4	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Violación de datos por falsificación de derechos y/o acceso no autorizado al sistema debido a la gestión deficiente de las contraseñas	3	3	Confidencialidad de la información	Alta	
	Pérdida de datos críticos por	2	3	Integridad de la	Moderada	Asumir el riesgo,

INF-08	procesamiento ilegal de datos y/o divulgación debido a la habilitación innecesaria de servicios			información		Reducir el riesgo
	Pérdidas financieras por hurto de información, hurto de medios o documentos y/o procesamiento ilegal de datos debido a procedimientos inadecuados de contratación	2	4	Confidencialidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Interceptación y/o manipulación de datos por procesamiento ilegal de datos, abuso de derechos y/o errores en el uso debido a entrenamiento insuficiente en seguridad	2	3	Confidencialidad de la información	Alta	
	Exposición de datos por abuso de derechos y/o negación debido a ausencia de procedimiento formal para el	3	4	Confidencialidad de la información	Extrema	

	registro y retiro de usuarios					
INF-10	Pérdida y/o manipulación de datos sensibles por divulgación y/o falsificación de derechos debido a asignación errada de los derechos de acceso	3	4	Integridad de la información	Extrema	Reducir el riesgo, Evitar, Compartir o Transferir
	Pérdida de datos críticos por hurto de información, corrupción de los datos, intrusión en el sistema, intrusión en privacidad personal debido a falta de conciencia acerca de la seguridad de los datos e información	3	4	Integridad de la información	Extrema	
	Pérdida de datos críticos por observar información reservada, hurto de información y/o venta de información personal debido a ausencia de procedimientos para el manejo	3	4	Integridad de la información	Extrema	

	de información clasificada					
INF-11	Pérdida de datos críticos por hurto de medios o documentos y/o divulgación debido a almacenamiento sin protección	3	3	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Pérdida de datos críticos por manipulación con software y/o mal funcionamiento del software debido a ausencia de copias de respaldo de la información	3	3	Integridad de la información	Alta	
	Exposición de datos por hurto de medios o documentos, intrusión al sistema y/o ingeniería social debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	3	4	Confidencialidad de la información	Extrema	

INF-12	Interceptación y/o manipulación de datos por abuso de los derechos e ingeniería social debido a entrenamiento insuficiente en seguridad	3	3	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
INF-13	Interrupción del funcionamiento del sistema por abuso de derechos y/o mal funcionamiento del software debido a defectos bien conocidos en el software	2	3	Disponibilidad de la información	Moderada	Asumir el riesgo, Reducir el riesgo
	Pérdida de disponibilidad de la información y/o accesibilidad a los datos por mal funcionamiento del software y/o manipulación con software debido a la ausencia de copias de respaldo	2	3	Disponibilidad de la información	Moderada	
	Exposición de datos por procesamiento	2	3	Confidencialidad de la	Moderada	

	ilegal de datos debido a ausencia de mecanismos de monitoreo			información		
	Interceptación y/o manipulación de datos por abuso de derechos, divulgación, manipulación en el sistema y/o ingreso de datos falsos o corruptos debido a asignación errada de los derechos de acceso	3	3	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
INF-14	Interceptación y/o manipulación de datos por ingeniería social debido a entrenamiento insuficiente en seguridad	3	3	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Obtención de información confidencial por hurto de información y/o intrusión en privacidad personal debido a falta de seguridad acerca de la seguridad	2	3	Confidencialidad de la información	Moderada	Asumir el riesgo, Reducir el riesgo

	Pérdida y/o manipulación de datos por divulgación y/o acceso no autorizado al sistema debido a la asignación errada de los derechos de acceso	3	4	Integridad de la información	Extremo	Reducir el riesgo, Evitar, Compartir o Transferir
	Daño a la reputación de la universidad por chantaje y/o sabotaje del sistema debido a procedimientos inadecuados de contratación	2	4	Confidencialidad de la información	Alta	
Tipo de activo: Software						
Activo	**Riesgo**	**Calificación**		**Tipo Impacto**	**Evaluación**	**Medidas de Respuesta**
		Probabilidad	**Impacto**		**Zona de riesgo**	
SW-01	Interrupción del funcionamiento del sistema operativo por mal funcionamiento del software debido a defectos bien conocidos en los mismos	2	3	Disponibilidad de la información	Moderada	Asumir el riesgo, Reducir el riesgo

	Introducción de malware por uso de software falso o copiado debido a la descarga y uso no controlado del software	3	4	Integridad de la información	Extrema	Reducir el riesgo, Evitar, Compartir o Transferir
	Pérdidas financieras por código maliciosos y error en el uso de softwares debido a la falta de conciencia acerca de la seguridad	3	3	Confidencialidad de la información	Alta	
	Interrupción de servicios por intrusión al sistema e ingeniería social debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	3	4	Disponibilidad de la información	Extrema	
SW-02	Interrupción del funcionamiento del software por mal funcionamiento debido a defectos bien conocidos en los mismos	2	3	Disponibilidad de la información	Moderada	Asumir el riesgo, Reducir el riesgo

	Introducción de malware por copia fraudulenta del software debido a la descarga y uso no controlado del software	3	4	Integridad de la información	Extrema	Reducir el riesgo, Evitar, Compartir o Transferir
	Exposición de datos por errores en uso de software y actos fraudulentos debido a la falta de conciencia acerca de la seguridad	3	4	Confidencialidad de la información	Extrema	
	Pérdida de datos críticos por procesamiento ilegal de los datos debido a la ausencia de mecanismos de monitoreo	3	3	Integridad de la información	Alta	
Tipo de activo: Servicios						
Activo	**Riesgo**	**Calificación**		**Tipo Impacto**	**Evaluación**	**Medidas de Respuesta**
		Probabilidad	**Impacto**		**Zona de riesgo**	

SERV-01 SERV-02	Filtración y/o manipulación de datos por error en el uso del sistema debido a la ausencia de procedimientos para el manejo de información clasificada	3	4	Integridad de la información	Extrema	Reducir el riesgo, Evitar, Compartir o Transferir
SERV-03 SERV-04	Exposición de datos por abuso de derechos debido a la ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	2	4	Confidencialidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Manipulación de datos y/o de la información por falsificación de derechos debido a gestión deficiente de las contraseñas	3	3	Integridad de la información		
	Interceptación y/o manipulación de datos por ingeniería social debido a entrenamiento insuficiente en seguridad del personal	3	3	Integridad de la información	Alta	

	Filtración y/o pérdida de datos confidenciales por suplantación de identidad y código malicioso debido a la ausencia de políticas sobre el uso de correo electrónico	3	3	Integridad de la información	Alta	
Tipo de activo: Hardware						
Activo	**Riesgo**	**Calificación**		**Tipo Impacto**	**Evaluación**	**Medidas de Respuesta**
		Probabilidad	**Impacto**		**Zona de riesgo**	
HW-01	Pérdida de disponibilidad de servicios o información por mal funcionamiento del equipo debido a mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	3	3	Disponibilidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Pérdida de disponibilidad de la información por pérdida de suministro de energía debido a la susceptibilidad a las variaciones de voltaje	3	3	Disponibilidad de la información	Alta	

HW-02	Pérdida de información por uso inadecuado del equipo debido al almacenamiento sin protección	3	3	Disponibilidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Pérdida de datos críticos por falla del equipo debido a mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	2	4	Integridad de la información	Alta	
	Pérdida de disponibilidad de la información por pérdida de suministro de energía debido a una red energética inestable	3	3	Disponibilidad de la información	Alta	
HW-03	Interceptación y/o manipulación de datos por espionaje remoto debido a arquitectura de red insegura	2	4	Confidencialidad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
Tipo de activo: Recurso humano						
Activo	**Riesgo**	**Calificación**		**Tipo Impacto**	**Evaluación**	**Medidas de**

		Probabilidad	Impacto		Zona de riesgo	Respuesta
RH-01 RH-02 RH-03	Interrupción de las operaciones o prestación de servicios por ingreso de datos falsos o corruptos debido a la falta de conciencia acerca de la seguridad de la información	1	4	Integridad de la información	Alta	Reducir el riesgo, Evitar, Compartir o Transferir
	Daño a la reputación de la universidad por manipulación ejercida por ciberdelincuentes debido al entrenamiento insuficiente en seguridad al personal administrativo	1	4	Confidencialidad de la información	Alta	
	Pérdida de datos confidenciales por sabotaje a los sistemas debido a la inadecuada contratación de personal	2	4	Confidencialidad de la información	Alta	
	Pérdida y/o manipulación de datos sensibles por acceso no	3	4	Integridad de la información	Extrema	

	autorizado a los sistemas debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad					

Fuente: Los autores

4.3.2.5. Consecuencias para la entidad la materialización de riesgos.

Una eventualidad como la materialización de riesgos conlleva situaciones que afectan a la universidad y muy posiblemente a los distintos actores que la conforman, mismos que participan en los procesos y funciones de la institución. Por ello es importante conocer los daños o consecuencias resultantes de los riesgos para gestionarlos.

Agregando a lo anterior, a continuación, se enlistan las consecuencias a los que podría estar expuesta la entidad.

Tabla 9. Identificación de daños.

Identificación de daños		
Tipo de activo: Información		
Activo	**Riesgo**	**Consecuencias**
INF-02	Daño a la reputación de la universidad por procesamiento ilegal de los datos debido a falta de conciencia acerca de la seguridad	Incumplimiento regulatorio Impacto financiero Insatisfacción académica Dificultad para retener y atraer usuarios
	Exposición de datos por procesamiento ilegal de los datos y/o negación de acciones debido a la ausencia de mecanismo de monitoreo	Incumplimiento regulatorio Multas y/o sanciones

		Daños a la reputación Impacto financiero/operativo significativo Suspensión laboral
INF-01 INF-03 INF-04 INF-05 INF-09	Pérdida de datos e información crítica por accidente importante debido al almacenamiento sin protección de la información	Interrupción de las operaciones del negocio Daños a la reputación Pérdidas financieras Multas y/o sanciones
	Interrupción de las operaciones o prestación de servicios por hurto de información y/o sabotaje del sistema debido a ausencia de documentación	Daños a la reputación Costos adicionales Incumplimiento regulatorio Pérdidas económicas
	Pérdida de disponibilidad de la información y/o accesibilidad a los datos por código malicioso y/o errores en el sistema debido a ausencia de copias de respaldo	Interrupción de las operaciones del negocio Pérdida de confianza y/o credibilidad Incumplimiento regulatorio Pérdidas económicas
	Interrupción de las operaciones por divulgación y/o ingreso de datos falsos o corruptos debido a fallas en la producción de informes de gestión	Daños a la reputación Costos adicionales Incumplimiento regulatorio Pérdidas económicas

	Obtención de información confidencial por acto fraudulento y/o ingeniera social debido a falta de conciencia acerca de la seguridad de los datos	Pérdida de confianza Pérdidas económicas Multas y/o sanciones Interrupción de las operaciones del negocio
	Filtración y/o manipulación de datos por guerra de la información y/u observar información reservada debido a la ausencia de procedimientos para el manejo de información clasificada	Multas y/o sanciones Pérdidas económicas Daños a la reputación Pérdida de confianza y/o credibilidad Incumplimiento regulatorio
INF-06 INF-07	Violación de datos por abuso de los derechos y/o acceso no autorizado al sistema debido a la asignación errada de los derechos de acceso	Pérdidas económicas Pérdida de confianza y/o credibilidad Daños a la reputación Multas y/o sanciones Interrupción de las operaciones del negocio Pérdida de privacidad
	Pérdida de datos críticos por manipulación con software, mal funcionamiento del equipo y/o errores en el sistema debido a la ausencia de copias de respaldo	Pérdidas económicas Multas y/o sanciones Pérdida de confianza y/o credibilidad

		Dificultad para retener y atraer usuarios
	Incumplimiento de la normativa por negación de acciones, ingreso de datos falsos o corruptos y/o sabotaje del sistema debido a ausencia de asignación adecuada de responsabilidades en seguridad de la información	Multas y/o sanciones Pérdidas económicas Daños a la reputación Pérdida de confianza y/o credibilidad
	Violación de datos por falsificación de derechos y/o acceso no autorizado al sistema debido a la gestión deficiente de las contraseñas	Pérdidas económicas Interrupción de las operaciones del negocio Pérdida de privacidad Daños a la reputación
INF-08	Pérdida de datos críticos por procesamiento ilegal de datos y/o divulgación debido a la habilitación innecesaria de servicios	Pérdidas económicas Multas y/o sanciones Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Incumplimiento regulatorio
	Pérdidas financieras por hurto de información, hurto de medios o documentos y/o procesamiento ilegal de datos debido a procedimientos inadecuados de contratación	Multas y/o sanciones Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Daños a la reputación

	Interceptación y/o manipulación de datos por procesamiento ilegal de datos, abuso de derechos y/o errores en el uso debido a entrenamiento insuficiente en seguridad	Sanciones Incumplimiento regulatorio Pérdida de confianza Daños a la reputación Pérdidas económicas Interrupción de las operaciones del negocio
	Exposición de datos por abuso de derechos y/o negación debido a ausencia de procedimiento formal para el registro y retiro de usuarios	Daños a la reputación Multas y/o sanciones pérdida de privacidad Pérdidas económicas Interrupción de las operaciones del negocio
INF-10	Pérdida y/o manipulación de datos sensibles por divulgación y/o falsificación de derechos debido a asignación errada de los derechos de acceso	Pérdida de confianza y/o credibilidad Multas y/o sanciones Daños a la reputación Pérdida de privacidad Interrupción de las operaciones del negocio
	Pérdida de datos críticos por hurto de información, corrupción de los datos, intrusión en el sistema, intrusión en privacidad personal debido a falta de	Pérdidas económicas Multas y/o sanciones

	conciencia acerca de la seguridad de los datos e información	Pérdida de confianza y/o credibilidad Daños a la reputación Dificultad para retener y atraer usuarios Incumplimiento regulatorio
	Pérdida de datos críticos por observar información reservada, hurto de información y/o venta de información personal debido a ausencia de procedimientos para el manejo de información clasificada	Pérdidas económicas Multas y/o sanciones Pérdida de confianza y/o credibilidad Daños a la reputación Dificultad para retener y atraer usuarios Incumplimiento regulatorio
INF-11	Pérdida de datos críticos por hurto de medios o documentos y/o divulgación debido a almacenamiento sin protección	Pérdidas económicas Multas y/o sanciones Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Incumplimiento regulatorio
	Pérdida de datos críticos por manipulación con software y/o mal funcionamiento del software debido a ausencia de copias de respaldo de la información	Pérdidas económicas Multas y/o sanciones Pérdida de confianza y/o credibilidad

		Daños a la reputación Dificultad para retener y atraer usuarios Incumplimiento regulatorio
	Exposición de datos por hurto de medios o documentos, intrusión al sistema y/o ingeniería social debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	Daños a la reputación Pérdida de confianza y/o credibilidad Multas y/o sanciones Pérdidas económicas Interrupción de las operaciones del negocio Costos adicionales
INF-12	Interceptación y/o manipulación de datos por abuso de los derechos e ingeniería social debido a entrenamiento insuficiente en seguridad	Pérdida de confianza y/o credibilidad Multas y/o sanciones Daños a la reputación Pérdida de privacidad Interrupción de las operaciones del negocio
INF-13	Interrupción del funcionamiento del sistema por abuso de derechos y/o mal funcionamiento del software debido a defectos bien conocidos en el software	Daños a la reputación Pérdidas económicas Pérdida de datos Deficiencia en la gestión de servicios

	Pérdida de disponibilidad de la información y/o accesibilidad a los datos por mal funcionamiento del software y/o manipulación con software debido a la ausencia de copias de respaldo	Daños a la reputación Pérdida de confianza y/o credibilidad Pérdidas económicas Pérdida de productividad Incumplimiento regulatorio
	Exposición de datos por procesamiento ilegal de datos debido a ausencia de mecanismos de monitoreo	Multas y/o sanciones Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Pérdida de privacidad Interrupción de las operaciones del negocio
	Interceptación y/o manipulación de datos por abuso de derechos, divulgación, manipulación en el sistema y/o ingreso de datos falsos o corruptos debido a asignación errada de los derechos de acceso	Daños a la reputación Pérdida de privacidad Multas y/o sanciones Interrupción de las operaciones del negocio
	Interceptación y/o manipulación de datos por ingeniería social debido a entrenamiento insuficiente en seguridad	Daños a la reputación Pérdida de privacidad Multas y/o sanciones Interrupción de las operaciones del negocio

INF-14	Obtención de información confidencial por hurto de información y/o intrusión en privacidad personal debido a falta de seguridad acerca de la seguridad	Daños a la reputación Pérdida de privacidad e integridad Pérdida de confianza y/o credibilidad Interrupción de las operaciones del negocio
	Pérdida y/o manipulación de datos por divulgación y/o acceso no autorizado al sistema debido a la asignación errada de los derechos de acceso	Pérdida de confianza y/o credibilidad Multas y/o sanciones Daños a la reputación Pérdida de privacidad Interrupción de las operaciones del negocio
	Daño a la reputación de la universidad por chantaje y/o sabotaje del sistema debido a procedimientos inadecuados de contratación	Pérdida de valor Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Disminución de ingresos Posible pérdida de continuidad del negocio Multas y/o sanciones
Tipo de activo: Software		
Activo	**Riesgo**	**Consecuencias**

SW-01	Interrupción del funcionamiento del sistema operativo por mal funcionamiento del software debido a defectos bien conocidos en los mismos	Pérdida de datos Pérdidas económicas Daños a la reputación Pérdida de seguridad del sistema Interrupción de servicios
	Introducción de malware por uso de software falso o copiado debido a la descarga y uso no controlado del software	Multas y/o sanciones Pérdida de confianza y/o credibilidad Pérdida de datos Brechas de seguridad Interrupción de las operaciones del negocio Daños a la reputación
	Pérdidas financieras por código maliciosos y error en el uso de softwares debido a la falta de conciencia acerca de la seguridad	Pérdida de confianza y/o credibilidad Daños a la reputación Interrupción de las operaciones del negocio Reducción de personal administrativo y/o docente Recorte presupuestal
	Interrupción de servicios por intrusión al sistema e ingeniería social debido a la ausencia de mecanismos de	Pérdida de confianza y/o credibilidad Daños a la reputación

	monitoreo establecidos para las brechas de seguridad	Multas y/o sanciones Pérdidas económicas
SW-02	Interrupción del funcionamiento del software por mal funcionamiento debido a defectos bien conocidos en los mismos	Pérdida de datos Pérdidas económicas Daños a la reputación Pérdida de seguridad del sistema Interrupción de servicios
	Introducción de malware por copia fraudulenta del software debido a la descarga y uso no controlado del software	Multas y/o sanciones Pérdida de confianza y/o credibilidad Pérdida de datos Brechas de seguridad Interrupción de las operaciones del negocio Daños a la reputación
	Exposición de datos por errores en uso de software y actos fraudulentos debido a la falta de conciencia acerca de la seguridad	Multas y/o sanciones Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Pérdida de privacidad Interrupción de las operaciones del negocio

	Pérdida de datos críticos por procesamiento ilegal de los datos debido a la ausencia de mecanismos de monitoreo	Pérdidas económicas Multas y/o sanciones Pérdida de confianza y/o credibilidad Daños a la reputación Incumplimiento regulatorio
Tipo de activo: Servicios		
Activo	**Riesgo**	**Consecuencias**
SERV-01 SERV-02	Filtración y/o manipulación de datos por error en el uso del sistema debido a la ausencia de procedimientos para el manejo de información clasificada	Interrupción de las operaciones del negocio Pérdidas económicas Daños a la reputación Pérdida de confianza y/o credibilidad Pérdida de datos y/o privacidad
SERV-03 SERV-04	Exposición de datos por abuso de derechos debido a la ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Multas y/o sanciones Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Pérdida de privacidad Interrupción de las operaciones del negocio
	Manipulación de datos y/o de la información por falsificación de	Daños a la reputación

	derechos debido a gestión deficiente de las contraseñas	Pérdidas económicas Pérdida de confianza y/o credibilidad Incumplimiento regulatorio
	Interceptación y/o manipulación de datos por ingeniería social debido a entrenamiento insuficiente en seguridad del personal	Daños a la reputación Pérdida de privacidad Multas y/o sanciones Interrupción de las operaciones del negocio
	Filtración y/o pérdida de datos confidenciales por suplantación de identidad y código malicioso debido a la ausencia de políticas sobre el uso de correo electrónico	Daños a la reputación Pérdidas económicas Pérdida de confianza y/o credibilidad Multas y/o sanciones Incumplimiento regulatorio
Tipo de activo: Hardware		
Activo	**Riesgo**	**Consecuencias**
HW-01	Pérdida de disponibilidad de servicios o información por mal funcionamiento del equipo debido a mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Daños a la reputación Pérdida de confianza Pérdidas económicas Pérdida de productividad Incumplimiento regulatorio

	Pérdida de disponibilidad de la información por pérdida de suministro de energía debido a la susceptibilidad a las variaciones de voltaje	Daños a la reputación Pérdidas económicas Pérdida de productividad Multas y/o sanciones Dificultad para la toma de decisiones
HW-02	Pérdida de información por uso inadecuado del equipo debido al almacenamiento sin protección	Pérdida de integridad Daños a la reputación Incumplimiento regulatorio Interrupción de servicios y/o operaciones del negocio
	Pérdida de datos críticos por falla del equipo debido a mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Pérdida de integridad Daños a la reputación Incumplimiento regulatorio Interrupción de servicios y/o operaciones del negocio
	Pérdida de disponibilidad de la información por pérdida de suministro de energía debido a una red energética inestable	Daños a la reputación Pérdida de confianza y/o credibilidad Pérdidas económicas Pérdida de productividad Incumplimiento regulatorio

HW-03	Interceptación y/o manipulación de datos por espionaje remoto debido a arquitectura de red insegura	Daños a la reputación Pérdida de privacidad Multas y/o sanciones Interrupción de las operaciones del negocio
Tipo de activo: Recurso humano		
Activo	**Riesgo**	**Consecuencias**
RH-01 RH-02 RH-03	Interrupción de las operaciones o prestación de servicios por ingreso de datos falsos o corruptos debido a la falta de conciencia acerca de la seguridad de la información	Incumplimiento regulatorio Pérdidas económicas Multas y/o sanciones Daños a la reputación Pérdida de confianza
	Daño a la reputación de la universidad por manipulación ejercida por ciberdelincuentes debido al entrenamiento insuficiente en seguridad al personal administrativo	Pérdida de valor Pérdida de confianza y/o credibilidad Dificultad para retener y atraer usuarios Disminución de ingresos Posible pérdida de continuidad del negocio Multas y/o sanciones
	Pérdida de datos confidenciales por sabotaje a los sistemas debido a la inadecuada contratación de personal	Pérdidas económicas Daños a la reputación Pérdida de confianza

		Interrupción de las operaciones del negocio
	Pérdida y/o manipulación de datos sensibles por acceso no autorizado a los sistemas debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	Pérdida de confianza y/o credibilidad Multas y/o sanciones Daños a la reputación Pérdida de privacidad Interrupción de las operaciones del negocio

Fuente: Los autores

4.3.2.6. Tratamiento de riesgos.

Una vez se haya analizado y evaluado los riesgos a los que están expuestos cada uno de los activos de información de las dependencias se procede a identificar los controles para el tratamiento de los riesgos señalados en la Guía Controles de Seguridad y Privacidad de la Información del Ministerio de las Tecnologías de la Información y las Comunicaciones MinTIC (2016a), basados en el Anexo A de la norma NTC:ISO/IEC 27001:2013.

A continuación, se sugieren los controles para un buen manejo de los riesgos:

Tabla 10. Tratamiento de riesgos.

Tratamiento de riesgos		
Tipo de activo: Información		
Activo	**Riesgo**	**Controles**
INF-02	Daño a la reputación de la universidad por procesamiento ilegal de los datos debido a falta de conciencia acerca de la seguridad	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

		A.7.2.3. Proceso disciplinario A.18.2.2. Cumplimiento con las políticas y normas de seguridad
	Exposición de datos por procesamiento ilegal de los datos y/o negación de acciones debido a la ausencia de mecanismo de monitoreo	A.5.1.1. Políticas para la seguridad de la información A.7.2.3. Proceso disciplinario A.8.1.3. Uso aceptable de los activos A.9.1.1 Política de control de acceso A.9.4.1 Restricción de acceso Información A.18.2.2. Cumplimiento con las políticas y normas de seguridad
INF-01 INF-03 INF-04 INF-05	Pérdida de datos e información crítica por accidente importante debido al almacenamiento sin protección de la información	A.5.1.1. Políticas para la seguridad de la información A.11.1.4. Protección contra amenazas externas y ambientales A.12.3.1. Respaldo de información A.12.4.1. Registro de eventos A.16.1.2. Reporte de eventos de seguridad de la información

INF-09		
	Interrupción de las operaciones o prestación de servicios por hurto de información y/o sabotaje del sistema debido a ausencia de documentación	A.12.1.1. Procedimiento de operación documentados A.12.4.1. Registro de eventos A.12.6.1. Gestión de las vulnerabilidades técnicas A.16.1.2. Reporte de eventos de seguridad de la información A.17.1.2. Implementación de la continuidad de la seguridad de la información A.18.2.2. Cumplimiento con las políticas y normas de seguridad
	Pérdida de disponibilidad de la información y/o accesibilidad a los datos por código malicioso y/o errores en el sistema debido a ausencia de copias de respaldo	A.9.1.1. Política de control de acceso A.12.2.1. Controles contra códigos maliciosos A.12.3.1. Respaldo de información A.12.4.1. Registro de eventos A.17.1.2. Implementación de la continuidad de la seguridad de la información
	Interrupción de las operaciones por divulgación y/o ingreso de datos falsos	A.7.1.1. Selección

	o corruptos debido a fallas en la producción de informes de gestión	A.8.2.1. Clasificación de la información A.13.2.4. Acuerdos de confidencialidad o de no divulgación A.17.1.2. Implementación de la continuidad de la seguridad de la información A.18.1.3. Protección de registros
	Obtención de información confidencial por acto fraudulento y/o ingeniera social debido a falta de conciencia acerca de la seguridad de los datos	A.5.1.1. Políticas para la seguridad de la información A.7.1.1. Selección A.7.2.1. Responsabilidades de la dirección A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.7.2.3. Proceso disciplinario
	Filtración y/o manipulación de datos por guerra de la información y/u observar información reservada debido a la ausencia de procedimientos para el manejo de información clasificada	A.5.1.1. Políticas para la seguridad de la información A.8.2.3. Manejo de activos A.12.6.1. Gestión de las vulnerabilidades técnicas A.18.2.2. Cumplimiento con las políticas y normas de seguridad

		A.16.1.3. Reporte de debilidades de seguridad de la información
INF-06 INF-07	Violación de datos por abuso de los derechos y/o acceso no autorizado al sistema debido a la asignación errada de los derechos de acceso	A.5.1.1. Políticas para la seguridad de la información A.7.2.3. Proceso disciplinario A.9.1.1. Política de control de acceso A.9.2.2. Suministro de acceso de usuario A.9.4.1. Restricción de acceso a la información A.18.1.4. Privacidad y protección de datos personales
	Pérdida de datos críticos por manipulación con software, mal funcionamiento del equipo y/o errores en el sistema debido a la ausencia de copias de respaldo	A.5.1.1. Políticas para la seguridad de la información A.9.4.1. Restricción de acceso a la información A.12.3.1. Respaldo de información A.12.4.1. Registro de eventos A.12.4.2. Protección de la información de registro A.16.1.2. Reporte de eventos de seguridad de la información

	Incumplimiento de la normativa por negación de acciones, ingreso de datos falsos o corruptos y/o sabotaje del sistema debido a ausencia de asignación adecuada de responsabilidades en seguridad de la información	A.6.1.1. Roles y responsabilidades para la seguridad de la información A.7.2.3. Proceso disciplinario A.12.4.1. Registro de eventos A.16.1.1. Responsabilidad y procedimientos A.16.1.2. Reporte de eventos de seguridad de la información A.18.2.2. Cumplimiento con las políticas y normas de seguridad A18.2.3. Revisión del cumplimiento técnico
	Violación de datos por falsificación de derechos y/o acceso no autorizado al sistema debido a la gestión deficiente de las contraseñas	A.5.1.1. Políticas para la seguridad de la información A.9.3.1 Uso de la información de autenticación secreta A.9.4.2 Procedimiento de ingreso seguro A.9.4.3. Sistema de gestión de contraseñas A.12.4.1. Registro de eventos

		A.18.1.4. Privacidad y protección de datos personales
INF-08	Pérdida de datos críticos por procesamiento ilegal de datos y/o divulgación debido a la habilitación innecesaria de servicios	A.5.1.1. Políticas para la seguridad de la información A.7.2.3. Proceso disciplinario A.8.2.1. Clasificación de la información A.8.1.3. Uso aceptable de los activos A.9.1.1. Política de control de acceso A.9.2.2. Suministro de acceso de usuarios A.12.3.1. Respaldo de información A.13.2.4. Acuerdos de confidencialidad o de no divulgación
	Pérdidas financieras por hurto de información, hurto de medios o documentos y/o procesamiento ilegal de datos debido a procedimientos inadecuados de contratación	A.5.1.1. Políticas para la seguridad de la información A.6.1.1. Roles y responsabilidades para la seguridad de la información A.7.1.1. Selección A.7.2.3. Proceso disciplinario

		A.8.1.3. Uso aceptable de los activos
	Interceptación y/o manipulación de datos por procesamiento ilegal de datos, abuso de derechos y/o errores en el uso debido a entrenamiento insuficiente en seguridad	A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.8.1.3. Uso aceptable de los activos A.9.1.1. Política de control de acceso A.9.2.2. Suministro de acceso de usuarios A.9.4.1. Restricción de acceso a la información
	Exposición de datos por abuso de derechos y/o negación debido a ausencia de procedimiento formal para el registro y retiro de usuarios	A.5.1.1. Políticas para la seguridad de la información A.9.2.1. Registro y cancelación del registro de usuarios A.9.2.6. Retiro o ajuste de los derechos de acceso
INF-10	Pérdida y/o manipulación de datos sensibles por divulgación y/o falsificación de derechos debido a asignación errada de los derechos de acceso	A.5.1.1. Políticas para la seguridad de la información A.9.1.1. Política de control de acceso A.9.4.1. Restricción de acceso a la información A.12.3.1. Respaldo de información

	Pérdida de datos críticos por hurto de información, corrupción de los datos, intrusión en el sistema, intrusión en privacidad personal debido a falta de conciencia acerca de la seguridad de los datos e información	A.5.1.1. Políticas para la seguridad de la información A.12.3.1. Respaldo de información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.16.1.2. Reporte de eventos de seguridad de la información A.18.1.4. Privacidad y protección de datos personales
	Pérdida de datos críticos por observar información reservada, hurto de información y/o venta de información personal debido a ausencia de procedimientos para el manejo de información clasificada	A.5.1.1. Políticas para la seguridad de la información A.7.2.3. Proceso disciplinario A.12.3.1. Respaldo de información A.12.4.1. Registro de eventos A.18.1.4. Privacidad y protección de datos personales
INF-11	Pérdida de datos críticos por hurto de medios o documentos y/o divulgación debido a almacenamiento sin protección	A.5.1.1. Políticas para la seguridad de la información

		A.11.2.1. Ubicación y protección de equipos A.12.3.1. Respaldo de información A.12.4.1. Registro de eventos A.16.1.3. Reporte de debilidades de seguridad de la información
	Pérdida de datos críticos por manipulación con software y/o mal funcionamiento del software debido a ausencia de copias de respaldo de la información	A.5.1.1. Políticas para la seguridad de la información A.8.1.3. Uso aceptable de los activos A.12.3.1. Respaldo de información A.12.4.1. Registro de eventos A.12.6.1. Gestión de vulnerabilidades técnicas A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información
	Exposición de datos por hurto de medios o documentos, intrusión al sistema y/o ingeniería social debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	A.5.1.1. Políticas para la seguridad de la información A.11.2.1. Ubicación y protección de equipos

		A.12.4.1. Registro de eventos A.12.6.1. Gestión de vulnerabilidades técnicas A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información A.18.2.1. Revisión independiente de la seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información
INF-12	Interceptación y/o manipulación de datos por abuso de los derechos e ingeniería social debido a entrenamiento insuficiente en seguridad	A.5.1.1. Políticas para la seguridad de la información A.6.1.1. Roles y responsabilidades para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.9.4.1. Restricción de acceso a la información A.12.4.1. Registro de eventos

		A.16.1.2. Reporte de eventos de seguridad de la información
INF-13	Interrupción del funcionamiento del sistema por abuso de derechos y/o mal funcionamiento del software debido a defectos bien conocidos en el software	A.9.2.6. Retiro o ajuste de los derechos de acceso A.12.4.1. Registro de eventos A.12.6.1. Gestión de vulnerabilidades técnicas A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información A.17.1.2. Implementación de la continuidad de la seguridad de la información
	Pérdida de disponibilidad de la información y/o accesibilidad a los datos por mal funcionamiento del software y/o manipulación con software debido a la ausencia de copias de respaldo	A.12.4.1. Registro de eventos A.12.3.1. Respaldo de información A.12.1.2. Gestión de cambios A.12.4.1. Registro de eventos A.16.1.1. Responsabilidad y procedimientos A.16.1.2. Reporte de eventos de seguridad de la información

		A.18.2.3. Revisión del cumplimiento técnico
	Exposición de datos por procesamiento ilegal de datos debido a ausencia de mecanismos de monitoreo	A.5.1.1. Políticas para la seguridad de la información A.7.2.1. Responsabilidades de la dirección A.8.1.3. Uso aceptable de los activos A.8.2.3. Manejo de activos A.12.4.1. Registro de eventos A.18.2.1. Revisión independiente de seguridad de la información A.18.2.2. Cumplimiento con las políticas y normas de seguridad
	Interceptación y/o manipulación de datos por abuso de derechos, divulgación, manipulación en el sistema y/o ingreso de datos falsos o corruptos debido a asignación errada de los derechos de acceso	A.5.1.1. Políticas para la seguridad de la información A.7.1.1. Selección A.8.2.1. Clasificación de la información A.9.1.1. Política de control de acceso A.9.4.1. Restricción de acceso a la información

		A.12.4.2. Protección de la información de registro A.13.2.4. Acuerdos de confidencialidad o de no divulgación A.18.1.3. Protección de registros
INF-14	Interceptación y/o manipulación de datos por ingeniería social debido a entrenamiento insuficiente en seguridad	A.5.1.1. Políticas para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.12.4.1. Registro de eventos A.16.1.2. Reporte de eventos de seguridad de la información A.18.2.2. Cumplimiento con las políticas y normas de seguridad
	Obtención de información confidencial por hurto de información y/o intrusión en privacidad personal debido a falta de conciencia acerca de la seguridad	A.5.1.1. Políticas para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.8.1.3. Uso aceptable de los activos A.12.4.1. Registro de eventos

		A.16.1.2. Reporte de eventos de seguridad de la información A.18.1.4. Privacidad y protección de datos personales
	Pérdida y/o manipulación de datos por divulgación y/o acceso no autorizado al sistema debido a la asignación errada de los derechos de acceso	A.5.1.1. Políticas para la seguridad de la información A.8.2.1. Clasificación de la información A.9.1.1. Política de control de acceso A.9.4.1. Restricción de acceso a la información A.9.2.2. Suministro de acceso de usuarios A.12.3.1. Respaldo de información A.13.2.4. Acuerdo de confidencialidad o de no divulgación
	Daño a la reputación de la universidad por chantaje y/o sabotaje del sistema debido a procedimientos inadecuados de contratación	A.7.1.1. Selección A.7.2.3. Proceso disciplinario A.8.2.3. Manejo de activos A.9.4.1. Restricción de acceso a la información A.12.4.1. Registro de eventos

		A.16.1.2. Reporte de eventos de seguridad de la información A.18.2.2. Cumplimientos con las políticas y normas de seguridad
Tipo de activo: Software		
Activo	**Riesgo**	**Controles**
SW-01	Interrupción del funcionamiento del sistema operativo por mal funcionamiento del software debido a defectos bien conocidos en los mismos	A.12.4.1. Registro de eventos A.12.6.1. Gestión de vulnerabilidades técnicas A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información A.17.1.2. Implementación de la continuidad de la seguridad de la información
	Introducción de malware por uso de software falso o copiado debido a la descarga y uso no controlado del software	A.5.1.1. Políticas para la seguridad de la información A.7.2.3 Proceso disciplinario A.12.4.1. Registro de eventos A.12.6.1. Gestión de vulnerabilidades técnicas

		A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información A.18.2.2. Cumplimiento con las políticas y normas de seguridad
	Pérdidas financieras por código malicioso y error en el uso de softwares debido a la falta de conciencia acerca de la seguridad	A.5.1.1. Políticas para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.12.2.1. Controles contra códigos maliciosos A.12.6.1. Gestión de las vulnerabilidades técnicas
	Interrupción de servicios por intrusión al sistema e ingeniería social debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	A.9.1.1. Política de control de acceso A.12.6.1. Gestión de las vulnerabilidades técnicas A.17.1.2. Implementación de la continuidad de la seguridad de la información A.16.1.2. Reporte de eventos de seguridad de la información

		A.16.1.3. Reporte de debilidades de seguridad de la información A.18.2.1. Revisión independiente de la seguridad de la información
SW-02	Interrupción del funcionamiento del software por mal funcionamiento debido a defectos bien conocidos en los mismos	A.12.4.1. Registro de eventos A.12.6.1. Gestión de vulnerabilidades técnicas A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.3. Reporte de debilidades de seguridad de la información A.17.1.2. Implementación de la continuidad de la seguridad de la información
	Introducción de malware por copia fraudulenta del software debido a la descarga y uso no controlado del software	A.5.1.1. Políticas para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.7.2.3. Proceso disciplinario A.8.1.3. Uso aceptable de los activos

		A.12.2.1. Controles contra códigos maliciosos A.12.5.1. Instalación de software en sistemas operativos A.12.6.2. Restricciones sobre la instalación de software
	Exposición de datos por errores en uso de software y actos fraudulentos debido a la falta de conciencia acerca de la seguridad	A.5.1.1. Políticas para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.7.2.3 Proceso disciplinario A.8.1.3. Uso aceptable de los activos A.16.1.2. Reporte de eventos de seguridad de la información A.16.1.5. Respuesta a incidentes de seguridad de la información
	Pérdida de datos críticos por procesamiento ilegal de los datos debido a la ausencia de mecanismos de monitoreo	A.5.1.1. Políticas para la seguridad de la información A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información

		A.8.1.3. Uso aceptable de los activos A.12.3.1. Respaldo de información A.16.1.5. Respuesta a incidentes de seguridad de la información
Tipo de activo: Servicios		
Activo	**Riesgo**	**Controles**
SERV-01 SERV-02	Filtración y/o manipulación de datos por error en el uso del sistema debido a la ausencia de procedimientos para el manejo de información clasificada	A.5.1.1. Políticas para la seguridad de la información A.6.1.1. Roles y responsabilidades para la seguridad de la información A.6.1.2. Separación de deberes A.8.1.3. Uso aceptable de los activos A.12.4.1. Registro de eventos
SERV-03 SERV-04	Manipulación de datos y/o de la información por falsificación de derechos debido a gestión deficiente de las contraseñas	A.5.1.1. Políticas para la seguridad de la información A.9.4.1. Restricción de acceso a la información A.9.4.2. Procedimiento de ingreso seguro A.9.4.3. Sistema de gestión de contraseñas

	Interceptación y/o manipulación de datos por ingeniería social debido a entrenamiento insuficiente en seguridad del personal	A.5.1.1. Políticas para la seguridad de la información A.7.2.1. Responsabilidades de la dirección A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información
	Filtración y/o pérdida de datos confidenciales por suplantación de identidad y código malicioso debido a la ausencia de políticas sobre el uso de correo electrónico	A.5.1.1. Políticas para la seguridad de la información A.7.2.1. Responsabilidades de la dirección A.7.2.2. Toma de conciencia, educación y formación en la seguridad de la información A.12.2.1. Controles contra códigos maliciosos A.12.3.1. Respaldo de información A.13.2.3. Mensajería electrónica
Tipo de activo: Hardware		
Activo	**Riesgo**	**Controles**
	Pérdida de disponibilidad de servicios o información por mal funcionamiento del equipo debido a mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	A.11.2.4. Mantenimiento de equipos A.17.1.2. Implementación de la continuidad de la seguridad de la información

HW-01	Pérdida de disponibilidad de la información por pérdida de suministro de energía debido a la susceptibilidad a las variaciones de voltaje	A.11.1.3. Seguridad de oficinas, recintos e instalaciones A.11.2.2. Servicios de suministro A.17.2.1. Disponibilidad de instalaciones de procesamiento de información
HW-02	Pérdida de información por uso inadecuado del equipo debido al almacenamiento sin protección	A.5.1.1. Políticas para la seguridad de la información A.8.1.3. Uso aceptable de los activos A.12.3.1. Respaldo de información
	Pérdida de datos críticos por falla del equipo debido a mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	A.5.1.1. Políticas para la seguridad de la información A.11.2.4. Mantenimiento de equipos A.12.3.1. Respaldo de información A.17.1.2. Implementación de la continuidad de la seguridad de la información
	Pérdida de disponibilidad de la información por pérdida de suministro	A.11.1.3. Seguridad de oficinas, recintos e instalaciones

	de energía debido a una red energética inestable	A.11.2.2. Servicios de suministro A.17.2.1. Disponibilidad de instalaciones de procesamiento de información
HW-03	Interceptación y/o manipulación de datos por espionaje remoto debido a arquitectura de red insegura	A.5.1.1. Políticas para la seguridad de la información A.11.1.4. Protección contra amenazas externas y ambientales A.11.2.3. Seguridad del cableado
Tipo de activo: Recurso humano		
Activo	**Riesgo**	**Controles**
RH-01 RH-02 RH-03	Interrupción de las operaciones o prestación de servicios por ingreso de datos falsos o corruptos debido a la falta de conciencia acerca de la seguridad de la información	A.5.1.1. Políticas para la seguridad de la información A.7.1.1. Selección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.17.1.2. Implementación de la continuidad de la seguridad de la información
	Daño a la reputación de la universidad por manipulación ejercida por ciberdelincuentes debido al	A.5.1. Directrices establecidas por la dirección para la seguridad de la información

	entrenamiento insuficiente en seguridad al personal administrativo	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
	Pérdida de datos confidenciales por sabotaje a los sistemas debido a la inadecuada contratación de personal	A.5.1.1. Políticas para la seguridad de la información A.7.1.1. Selección A.12.3.1. Respaldo de información
	Pérdida y/o manipulación de datos sensibles por acceso no autorizado a los sistemas debido a la ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	A.5.1.1. Políticas para la seguridad de la información A.9.1.1. Política de control de acceso A.9.2.3. Gestión de derechos de acceso privilegiado A.12.3.1. Respaldo de información A.18.2.2. Cumplimiento con las políticas y normas de seguridad

Fuente: los autores

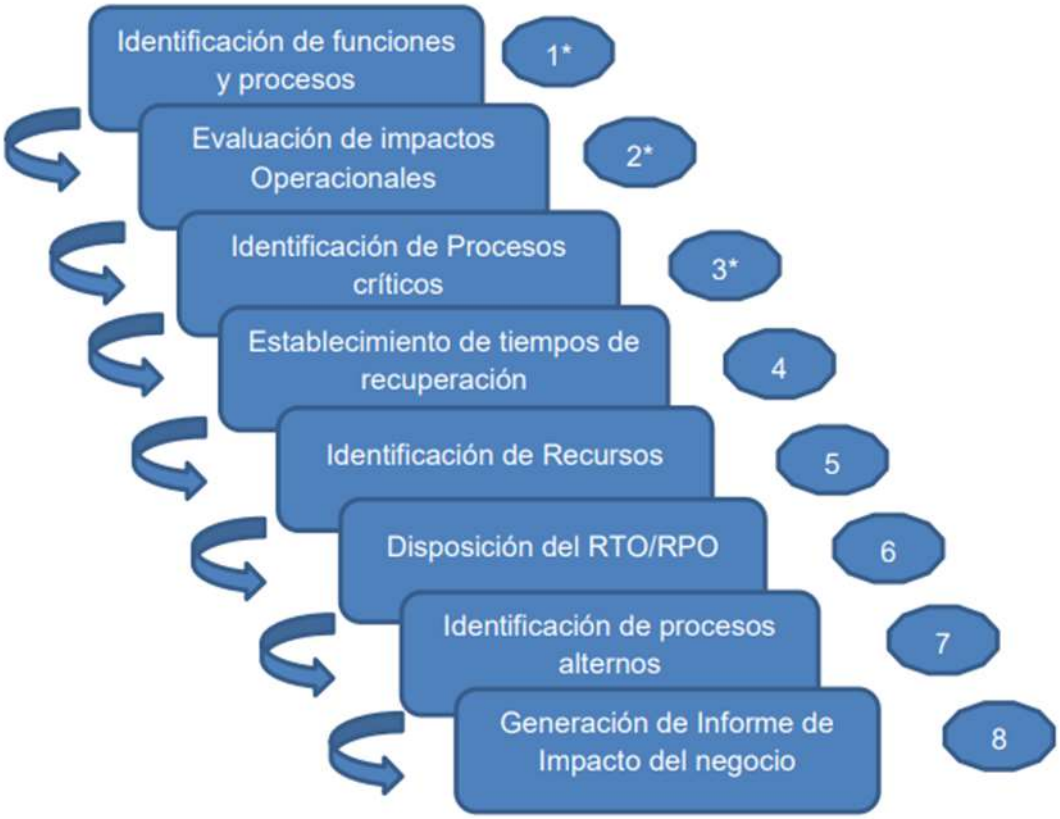
4.3.3. Análisis de Impacto del Negocio (BIA).

El Análisis de Impacto del Negocio – BIA por sus siglas en inglés (Bussiness Impact Analysis), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

El BIA está determinado por la construcción de un Plan de Continuidad del Negocio para cada organización, que le permita a cada entidad continuar funcionando a pesar de un desastre ocurrido.

Para esta fase se seguirá la metodología para realizar el Análisis de Impacto de Negocios BIA recomendada por el Ministerio de las Tecnologías de la Información y las Comunicaciones MinTIC (2015) la cual consiste en definir una serie de pasos interactivos con el objeto de identificar los impactos de las interrupciones y de esa manera tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre, estos pasos se muestran en la siguiente ilustración:

Figura 30. Metodología del Análisis de Impacto del Negocio.



Fuente: MinTIC

(i) Identificación de funciones y procesos: En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad.

(ii) Evaluación de impactos operacionales: El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

Tabla 11. Niveles de criticidad de una entidad.

Nivel	Descripción
Nivel A	La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
Nivel B	La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
Nivel C	La operación no es una parte integral del negocio.

Fuente: MinTIC

(iii) Identificación de procesos críticos: Esta fase se da con base en la clasificación de los impactos operacionales de las organizaciones.

(iv) Establecimiento de tiempos de recuperación: Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación, se trata de una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios. Los tiempos de recuperación de describen a continuación:

Tabla 12. Descripción de tiempos de recuperación.

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Fuente: MinTIC

Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio).

(v) Identificación de recursos: Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades.

(vi) Disposición de los RTO/RPO (Recovery Time Objective / Recovery Point Objective):

- Tiempo de Recuperación Objetivo (RTO): Comprende el tiempo disponible para recuperar recursos alterados.

  Adicionalmente, se aplica el WRT, es decir el tiempo que es requerido para completar el trabajo que ha estado interrumpido con el propósito de volverlo a la normalidad.

- Punto de Recuperación Objetivo (RPO): El rango de tolerancia que una Entidad puede tener sobre la pérdida de información y el evento de desastre.

(vii) Identificación de procesos alternos: La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para cada proceso crítico que se establezca (en los servicios), se debe poseer un procedimiento manual de continuidad del servicio.

(viii) Generación de informe de impacto del negocio: En este punto es necesario presentar un informe de impacto de negocio que corresponde a la guía para el BIA con los resúmenes del listado de procesos críticos, listado de prioridades de sistemas y aplicaciones, listado de tiempos MTD, RTO y RPO y listado de procedimientos alternos.

4.3.3.1. Informe BIA.

Con la finalidad de reunir información que permita conocer los procesos y/o servicios de la Universidad Popular del Cesar, Seccional Aguachica y sus tiempos de respuesta ante el impacto de una interrupción de negocio, se llevó a cabo una entrevista (ver anexo MM) a los lideres de las dependencias de Dirección Académica, Dirección Administrativa y Financiera, y al Centro de Admisiones, Registro y Control Académico, de manera que contribuya a la toma de decisiones

así como también sirva de base para el desarrollo del Plan de Gestión de Continuidad del Negocio.

4.3.3.1.1. Objetivo.

Determinar los procesos de vital importancia para el funcionamiento de la Universidad Popular del Cesar, Seccional Aguachica, así como los tiempos de recuperación de los mismos de tal forma que se pueda comprender el impacto producido por la interrupción de los procesos.

4.3.3.1.2. Alcance.

El Análisis de Impacto del Negocio (BIA) abarcara los procesos a cargo de las áreas de Dirección Académica, Dirección Administrativa y Financiera, y la oficina de Registro y Control Académico de la Universidad Popular del Cesar, Seccional Aguachica.

4.3.3.1.3. Metodología.

La información recolectada a través de la entrevista aplicada a los lideres de las áreas anteriormente mencionadas, se evidencia y se documenta en el desarrollo de la metodología del Análisis de Impacto del Negocio (BIA) recomendada por MinTIC que se adopta y adapta para el presente quedando de la siguiente manera:

Figura 31. Metodología BIA.

Fuente: MinTIC

(i) Identificación de funciones y procesos: A continuación, se observa un listado de funciones esenciales descritos en la Resolución 1709 de 29 de junio de 2023 (Romero Ramírez, 2023) así como los procesos de las áreas de Dirección Académica, Dirección Administrativa y Financiera, Registro y Control.

Tabla 13. Funciones y procesos.

Área	Funciones esenciales	Procesos
Dirección académica	• Asistir a la Dirección de la Seccional en el cumplimiento de la directrices y políticas trazadas por la Universidad, en asuntos académicos. • Dirigir, controlar, asesorar, coordinar y evaluar los procesos académicos administrativos que conforman el área académica de la Seccional. • Fomentar el desarrollo de procesos orientados al mejoramiento permanente de la calidad y eficiencia de los programas y servicios que ofrece la seccional.	Programar el calendario académico. Analizar y programar asignaturas, horarios y espacios físicos. Programar actividades

	• Velar por el cumplimiento de los acuerdos y disposiciones que emanen del Consejo Superior, del Consejo Académico, sobre los asuntos de docencia, de investigación y de extensión. • Proponer criterios y procedimientos para la selección, capacitación, promoción y evaluación de personal docente. • Coordinar y orientar la evaluación permanente de los sistemas y estrategias empleadas en el proceso de enseñanza-aprendizaje. • Enviar a la oficina de Dirección las necesidades presupuestales tanto de funcionamiento, como de inversión de las dependencias adscritas. • Orientar y coordinar los procesos de admisión. Registro y control académico. • Presentar informes a la Dirección sobre el desarrollo de sus actividades y su autoevaluación. • Las demás que le sean asignadas y corresponder a la naturaleza de la dependencia.	académicas docentes. Elaboración del plan de acción. Elaboración del plan de capacitación docente.
Dirección administrativa y financiera	• Coordinar y controlar las actividades del personal administrativo de la Seccional y la de los servicios generales de acuerdo con las normas legales y reglamentarias vigentes. • Diseñar formatos preformas codificados y coordinar con la oficina de Informática y Sistemas la sistematización de las operaciones referentes a las actividades que se requieran. • Controlar el cumplimiento de los contratos de prestación de servicio que suscriba la Seccional para tal efecto.	Contratación.

	• Propender por el cumplimiento de las normas sobre la administración del personal. • Elaborar el plan anual de compras de la Seccional. • Coordinar y controlar las actividades financieras, presupuestales y contables de la Seccional de acuerdo con las normas legales y reglamentarias vigentes. • Dirigir, coordinar y controlar el recaudo de los ingresos y la cancelación de las obligaciones a cargo de la Seccional. • Prepara con la Oficina de Planeación y Desarrollo Universitario el proyecto anual de presupuesto de la Seccional. • Elaborar los estatutos financieros de la Seccional y presentar los informes de resultados a la Dirección. • Presentar propuestas tendientes a fortalecer y mejorar la estructura financiera y económica indicando fuentes, formas de consecución y desembolsos de pagos. • Elaborar y proyectar flujos de caja que muestren el comportamiento de ingresos y egresos de la Seccional que ayuden a la toma de decisiones. • Orientar las certificaciones de disponibilidad presupuestal y reservas, que demanden las diversas obligaciones que la Seccional requiera. • Proponer actividades de inversión para los excedentes de caja a corto plazo, indicando tiempo pactado y monto de benéficos. • Ejecutar los procesos de la organización contable de la Seccional en lo referente al presupuesto.	Presupuesto. Matricula financiera.

	• Llevar y controlar la ejecución de gasto, atendiendo al Programa Anual de Caja PAC. • Enviar a la Vicerrectoría o Dirección de la Seccional mensualmente copia de la ejecución presupuestal de la Seccional. • Ejecutar registros contables de operaciones financieras que registre y efectué la Seccional. • Preparar de acuerdo a las normas contables los estados financieros que registre y producir los informes correspondientes. • Conciliar periódicamente, en coordinación con la Sección de Contabilidad de la Universidad y la Sección de Almacén e Inventarios de la Universidad las cuentas de inventarios y almacén, bien sea elementos devolutivos u otros. • Recaudar los ingresos y efectuar el pago de las obligaciones de la Universidad. • Presentar informes periódicos a la Vicerrectoría o Dirección de la Seccional sobre el desarrollo de sus actividades y su autoevaluación. • Las demás que le sean asignadas y corresponden a la dependencia.	
Registro y control	• Realizar la inscripción de los aspirantes y legalizar la vinculación de estudiantes a la Seccional. • Procesar y llevar registros actualizados de rendimiento académico de los estudiantes y velar por la aplicación de las correspondientes medidas de seguridad en los registros y archivos. • Tramitar las solicitudes presentadas por los estudiantes para su traslado, de acuerdo a la	

	reglamentación vigente, y aprobadas por las instancias o dependencias respectivas. • Elaborar, analizar y presentar a la Dirección Académica y demás dependencias competentes los informes estadísticos y recomendaciones. • Elaborar pautas sobre requisitos de admisión de alumnos e instruir a los aspirantes sobre lo mismo. • Efectuar las matrículas y llevar los registros correspondientes, de acuerdo a los procedimientos establecidos. • Llevar la ficha académica a cada estudiante según modelo que se adopte. • Elaborar las certificaciones que se soliciten y expedirlas de acuerdo al sistema vigente. • Publicar y comunicar los resultados de las pruebas de admisión al igual que de las notas. • Divulgar e informar sobre los diferentes procesos académicos de la institución. • Las demás que le sean asignadas y corresponden a la naturaleza de la dependencia.	Inscripción – Admisión. Matricula. Egreso.

Fuente: Los autores

(ii) Evaluación de impactos operacionales: En el siguiente recuadro se muestra la valoración de impacto de acuerdo a los procesos que soportan al negocio.

Tabla 14. Valoración operacional.

Dirección académica			
Proceso (Servicios)	**Nivel**	**Tolerancia a fallas (Horas)**	**Descripción**

Programar el calendario académico.	A	24 horas	Proyectar el calendario académico, sustentación del proyecto de acuerdo, revisión, análisis, aprobar el calendario académico, comunicar el acuerdo de calendario académico.
Analizar y programar asignaturas, horarios y espacios físicos.	A	72 horas	Revisar el histórico real de las asignaturas desarrolladas en el semestre inmediatamente anterior, determinar la demanda potencial por asignaturas, proyectar las asignaturas y horarios a ofrecer en el semestre de acuerdo a la demanda, revisar del programa las asignaturas con horarios y espacios físicos, programación definitiva con horarios y espacios físicos.
Programar actividades académicas docentes.	A	24 horas	Analizar las necesidades de docencia, investigación y extensión, para asignar a cada profesor las actividades académicas a desarrollar, revisar y aprobar las necesidades docentes propuestas por los directores de departamento y/o coordinadores de programas, asignar labores académicas docentes, el consejo de programas avala la asignación académica presentada por cada director de departamento y/o

			coordinadores de programas, análisis de la viabilidad financiera, aprobar la asignación académica presentada por la Seccional, comunicar las asignaciones de actividades académicas docentes.
Elaboración del plan de acción.	A	24 horas	Determinar las acciones de gestión bajo las cuales los departamentos y demás unidades administrativas cumplen con la misión institucional, consolidar los planes de acción recibidos de las unidades académicas y administrativas, enviar el Plan de Acción consolidado de la vicerrectoría general de la Seccional.
Elaboración del plan de capacitación docente.	A	24 horas	Informar a los departamentos el presupuesto disponible para capacitación docente, consolidar las necesidades de capacitación docente de la Seccional, presentar Plan de Capacitación consolidado al consejo de programas para aval, presentar el Plan de Capacitación consolidado al consejo académico, seguimiento trimestral a la ejecución del Plan de Capacitación docente.
Dirección administrativa y financiera			

Proceso (Servicios)	Nivel	Tolerancia a fallas (Horas)	Descripción
Contratación	A	72 horas	Desarrollar el proceso de contratación con el fin de cubrir las necesidades de recursos de las diferentes dependencias de la Seccional.
Presupuesto	A	72 horas	Controlar la ejecución presupuestal y hacer seguimiento al plan de compras.
Matricula financiera	B	48 horas	Realizar aprobación de los diferentes descuentos solicitados por los estudiantes y su respectiva reliquidación de matrícula.
Registro y control académico			
Proceso (Servicios)	**Nivel**	**Tolerancia a fallas (Horas)**	**Descripción**
Inscripción - admisión	A	1 hora	Aperturar el sistema académico según calendario vigente establecido por el Consejo Académico de la Institución.
Matricula	A	1 hora	Aperturar el sistema académico según calendario vigente establecido por el Consejo Académico de la Institución.
Egreso	A	1 hora	Se apertura según fechas establecidas en la Circular Conjunta de Grados.

Fuente: Los autores

(iii) Identificación de procesos críticos: En el siguiente recuadro se enlistan aquellos procesos que se consideran críticos para el negocio de acuerdo al impacto operacional.

Tabla 15. Identificación de procesos críticos.

	Dirección Académica
Valor	**Identificación de procesos críticos**
A	Programar el calendario académico.
A	Analizar y programar asignaturas, horarios y espacios físicos.
A	Programar actividades académicas docente.
A	Elaboración del Plan de Acción.
A	Elaboración del Plan de Capacitación Docente.
Dirección administrativa y financiera	
Valor	**Identificación de procesos críticos**
A	Contratación
A	Presupuesto
Registro y control académico	
Valor	**Identificación de procesos críticos**
A	Inscripción - admisión
A	Matricula
A	Egreso

Fuente: Los autores

(iv) Establecimiento de tiempos de recuperación: En el siguiente recuadro se establecen los tiempos máximos de inactividad que puede soportar un proceso crítico paralizado antes de que sucedan consecuencias negativas para el negocio.

Tabla 16. Identificación de procesos críticos.

Dirección académica		
Procesos críticos (Servicios)	**MTD (en días)**	**Prioridad de recuperación**
Programar el calendario académico.	1 día	2
Analizar y programar asignaturas, horarios y espacios físicos.	3 días	4

Programar actividades académicas docente.	1 día	2
Elaboración del Plan de Acción.	1 día	2
Elaboración del Plan de Capacitación Docente.	1 día	2
Dirección administrativa y financiera		
Procesos críticos (Servicios)	**MTD (en días)**	**Prioridad de recuperación**
Contratación	3 días	4
Presupuesto	3 días	4
Registro y control académico		
Procesos críticos (Servicios)	**MTD (en días)**	**Prioridad de recuperación**
Inscripción - admisión	0,08 día	1
Matricula	0,08 día	1
Egreso	0,08 día	1

Fuente: Los autores

(v) Identificación de recursos: A continuación, se observan aquellos recursos críticos que apoyan las diferentes funciones y procesos críticos del negocio.

Tabla 17. Identificación de recursos críticos.

Dirección académica	
Procesos críticos (Servicios)	**Identificación de recursos críticos**
Programar el calendario académico.	Gmail – recurso humano
Analizar y programar asignaturas, horarios y espacios físicos.	Gestasoft – Gmail – recurso humano
Programar actividades académicas docente.	Gestasoft – Gmail – recurso humano
Elaboración del Plan de Acción.	Gmail – recurso humano
Elaboración del Plan de Capacitación Docente.	Gmail – recurso humano
Dirección administrativa y financiera	
Procesos críticos (Servicios)	**Identificación de recursos críticos**

Contratación	Orfeo - software Gestasoft - Correo electrónico - recurso humano
Presupuesto	Software Gestasoft - recurso humano
Registro y control académico	
Procesos críticos (Servicios)	**Identificación de recursos críticos**
Inscripción - admisión	Sistema académico – conectividad – recurso humano
Matricula	Sistema académico – conectividad – recurso humano
Egreso	Sistema académico – conectividad – recurso humano

Fuente: Los autores

(vi) Disposición de los RTO/RPO: Con base en la fase anterior se estipulan el Tiempo de Recuperación Objetivo (RTO) y el Punto de Recuperación Objetivo (RPO).

Tabla 18. Valoración RTO/RPO de los procesos críticos.

Dirección académica				
Procesos críticos (Servicios)	**Identificación de recursos críticos**	**Tiempo de Recuperación Objetivo (RTO)**	**Punto de Recuperación Objetivo (RPO)**	**Tiempo de Recuperación de Trabajo (WRT)**
Programar el calendario académico.	Gmail, recurso humano	24 horas	2 horas	48 horas
Analizar y programar asignaturas, horarios y espacios físicos.	Gestasoft, Gmail, recurso humano	72 horas	2 horas	96 horas
Programar actividades académicas docente.	Gestasoft, Gmail, recurso humano	24 horas	3 horas	48 horas
Elaboración del Plan de Acción.	Gmail, recurso humano	24 horas	4 horas	48 horas

Elaboración del Plan de Capacitación Docente.	Gmail, recurso humano	24 horas	2 horas	72 horas
Dirección administrativa y financiera				
Procesos críticos (Servicios)	**Identificación de recursos críticos**	**Tiempo de Recuperación Objetivo (RTO)**	**Punto de Recuperación Objetivo (RPO)**	**Tiempo de Recuperación de Trabajo (WRT)**
Contratación	Orfeo, software Gestasoft, correo electrónico, recurso humano	48 horas	24 horas	24 horas
Presupuesto	Software Gestasoft, recurso humano	72 horas	24 horas	24 horas
Registro y control académico				
Procesos críticos (Servicios)	**Identificación de recursos críticos**	**Tiempo de Recuperación Objetivo (RTO)**	**Punto de Recuperación Objetivo (RPO)**	**Tiempo de Recuperación de Trabajo (WRT)**
Inscripción - admisión	Sistema académico, conectividad, recurso humano	2 horas	2 horas	2 horas
Matricula	Sistema académico, conectividad, recurso humano	2 horas	2 horas	2 horas
Egreso	Sistema académico, conectividad, recurso humano	2 horas	2 horas	2 horas

Fuente: Los autores

A continuación, se observa el listado de los procesos críticos, los recursos críticos, así como la prioridad de recuperación y los requerimientos de tiempo de

recuperación los cuales corresponden al Tiempo Máximo de Inactividad Tolerable (MTD), el Tiempo de Recuperación Objetivo (RTO) y el Punto de Recuperación Objetivo (RPO) de cada uno de los procesos, lo anterior resulta primordial para reanudar aquellos servicios que han sido interrumpidos y en consecuencia asegurar la continuidad del negocio.

Tabla 19. Resumen.

Resumen						
Áreas	**Procesos críticos**	**Recursos críticos**	**Prioridad de recuperación**	**MTD**	**RTO**	**RPO**
Dirección Académica	Programar el calendario académico.	Gmail, recurso humano	2	1 día	24 horas	2 horas
	Analizar y programar asignaturas, horarios y espacios físicos.	Gestasoft, Gmail, recurso humano	4	3 días	72 horas	2 horas
	Programar actividades académicas docente.	Gestasoft, Gmail, recurso humano	2	1 día	24 horas	3 horas
	Elaboración del Plan de Acción.	Gmail, recurso humano	2	1 día	24 horas	4 horas
	Elaboración del Plan de Capacitación Docente.	Gmail, recurso humano	2	1 día	24 horas	2 horas
Dirección administrativa y financiera	Contratación	Orfeo, software Gestasoft, Correo electrónico, recurso humano	4	3 días	48 horas	24 horas
	Presupuesto	Software Gestasoft, recurso humano	4	3 días	72 horas	24 horas
		Sistema académico				

Registro y control académico	Inscripción - admisión	, conectividad, recurso humano	1	0,08 día	2 horas	2 horas
	Matricula	Sistema académico , conectividad, recurso humano	1	0,08 día	2 horas	2 horas
	Egreso	Sistema académico , conectividad, recurso humano	1	0,08 día	2 horas	2 horas

Fuente: Los autores

4.3.4. Estrategias para la gestión de continuidad.

De acuerdo con los resultados del Análisis de Impacto del Negocio (BIA) se establecen a continuación, las estrategias para la continuidad del negocio en la Universidad Popular del Cesar, Seccional Aguachica.

Los recursos que se deben tener en cuenta en las estrategias para la gestión de continuidad del negocio son de talento humano, datos e información, infraestructura física, equipos y consumibles, financieros, logísticos y de proveedores.

Para los procesos de inscripción-admisión, matricula y egreso del área del Centro de Admisiones, Registro y Control Académico identificados como críticos se plantean las siguientes estrategias de Gestión de la Continuidad del Negocio considerando el Tiempo de Recuperación Objetivo (RTO) de dos (2) horas y su prioridad de recuperación frente a otros procesos.

Tabla 20. Estrategias para la continuidad de los procesos de registro y control.

Procesos críticos	Estrategias	Responsable	Periodicidad	Observación

Inscripción-admisión. Matricula.	Copias de seguridad y restauración de datos (Backups).	Todos los actores del proceso.	Diario	Implementar un servidor de nube o plataformas de datos en la nube.
	Seguridad de la información.	Área de TI. Todos los actores del proceso.	A definir según las acciones de seguridad.	Implementar acciones de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información vital del proceso.
	Sitio alterno.	Alta dirección. Área de TI. Coordinador del Plan de Gestión de Continuidad.	Semestral	Establecer un sitio alterno que cuente con los recursos necesarios para la continuidad de las operaciones (recursos tecnológicos, humanos, de seguridad).
	Colaborador de respaldo o "backup".	Líder del proceso. Alta dirección. Líder del área administrativa y financiera.	A definir según el motivo y criticidad del proceso.	Se recomienda realizar contratos de emergencia. Se recomienda contratar personas que hayan ocupado previamente el cargo y que cumplan con el perfil que requiere el cargo.
	Plataforma o sistema académico	Líder del proceso. Área de TI.	Durante el evento de interrupción.	Activar cuando el sistema académico principal falle.

Egreso.	de respaldo redundante.			
	Canales de atención secundarios.	Líder del proceso.	Durante el evento de interrupción.	Establecer los medios de atención idóneos para continuar con la operación atendida por personal capacitado.
	Seguro, pólizas.	Alta dirección.	Anual.	Se recomienda adquirir un seguro que cubra costos de recuperación, pérdidas financieras. (responsabilidad civil, todo riesgo empresarial, interrupción de negocio, cibernéticos).
	Actualización de datos	Líder del proceso	Semestral	Definir medios, formatos o sistemas alternativos que permitan la actualización continua de los datos.

Fuente: Los autores

Para los procesos críticos del área de Dirección Académica; programar el calendario académico, programar actividades académicas docente, elaboración del Plan de Acción, elaboración del Plan de Capacitación Docente, los cuales tienen un RTO de veinticuatro (24) horas y el proceso, analizar y programar asignaturas, horarios y espacios físicos con un RTO de setenta y dos (72) horas, se formula las siguientes estrategias.

Tabla 21. Estrategias para la continuidad de los procesos de Dirección Académica.

Procesos críticos	Estrategias	Responsable	Periodicidad	Observación

Programar el calendario académico. Analizar y programar asignaturas, horarios y espacios físicos. Programar actividades académicas docente. Elaboración del Plan de Acción. Elaboración del Plan de Capacitación Docente.	Plan de Recuperación ante Desastres de Tecnología (DRP)	Líder de TI. Coordinador del Plan de Gestión de Continuidad.	Semestral	Se recomienda elaborar e implementar un DRP para proteger los sistemas de TI que apoyan los procesos de la UPC-SA.
	Inventario de respaldo de activos.	Líder del proceso. Líder del área administrativa y financiera. Líder del área de TI. Coordinador del Plan de Gestión de Continuidad.	Semestral	Planear y gestionar un inventario de respaldo de activos o recursos que permita asegurar la disponibilidad y operatividad de los procesos.
	Seguridad de la información.	Área de TI. Todos los actores del proceso.	A definir según las acciones de seguridad.	Implementar acciones de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información vital del proceso.
	Copias de seguridad y restauración de datos (Backups).	Todos los actores del proceso.	Diario	Implementar un servidor de nube o plataformas de datos en la nube.
	Sitio alterno.	Alta dirección. Área de TI. Coordinador del Plan de Gestión de Continuidad.	Semestral	Establecer un sitio alterno que cuente con los recursos necesarios para la continuidad de las operaciones

				(recursos tecnológicos, humanos, de seguridad).
	Capacitación y concienciación sobre seguridad.	Alta dirección. Líder del proceso. Líder de TI.	Semestral	Desarrollar un programa de capacitación y concienciación sobre seguridad para todos los funcionarios de la UPC-SA.
	Trabajo remoto	Todos los actores del proceso.	Durante el evento de interrupción.	Establecer medidas de ciberseguridad.

Fuente: Los autores

Para los procesos críticos de la Dirección Administrativa y Financiera; contratación y presupuesto con un RTO de cuarenta y ocho (48) horas y setenta y dos (72) horas respectivamente, se presentan las siguientes estrategias.

Tabla 22. Estrategias para la continuidad de los procesos de Dirección Administrativa y Financiera.

Procesos críticos	**Estrategias**	**Responsable**	**Periodicidad**	**Observación**
Contratación	Copias de seguridad y restauración de datos (Backups).	Todos los actores del proceso.	Diario	Implementar un servidor de nube o plataformas de datos en la nube.
Presupuesto	Seguridad de la información.	Área de TI. Todos los actores del proceso.	A definir según las acciones de seguridad.	Implementar acciones de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información vital del proceso.

	Sitio alterno.	Alta dirección. Área de TI. Coordinador del Plan de Gestión de Continuidad.	Semestral	Establecer un sitio alterno que cuente con los recursos necesarios para la continuidad de las operaciones (recursos tecnológicos, humanos, de seguridad).
	Trabajo remoto	Todos los actores del proceso.	Durante el evento de interrupción.	Establecer medidas de ciberseguridad.
	Proveedores alternos	Líder del proceso.	Semestral y/o anual.	Diversificar y gestionar proveedores.
	Capacitación y concienciación sobre seguridad.	Alta dirección. Líder del proceso. Líder de TI.	Semestral	Desarrollar un programa de capacitación y concienciación sobre seguridad para todos los funcionarios de la UPC-SA.
	Plan financiero	Líder del proceso. Alta dirección.	Anual	Establecer un plan financiero para asumir costos que puedan generarse tras un evento de desastre.
	Colaborador de respaldo o "backup".	Líder del proceso. Alta dirección.	A definir según el motivo y criticidad del proceso.	Se recomienda realizar contratos de emergencia. Se recomienda contratar personas que hayan ocupado previamente el cargo y que cumplan con el perfil que

				requiere el cargo.

Fuente: Los autores

En adición a lo anterior, se considera los procesos de gestión investigativa para el planteamiento de las estrategias de continuidad como se muestra a continuación.

Tabla 23. Estrategias para la continuidad de Gestión Investigativa.

Procesos críticos	Estrategias	Responsable	Periodicidad	Observación
Plan de investigación. Aval y consolidación de grupos y semilleros de investigación. Convocatoria interna para financiación de proyectos a grupos y semilleros de investigación. Gestión de recursos a través de convocatorias externas. Socialización de experiencias de investigación. Seguimiento a la investigación.	Copias de seguridad y restauración de datos (Backups).	Todos los actores del proceso.	Diario	Implementar un servidor de nube o plataformas de datos en la nube.
	Seguridad de la información.	Área de TI. Todos los actores del proceso.	A definir según las acciones de seguridad.	Implementar acciones de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información vital del proceso.
	Trabajo remoto	Todos los actores del proceso.	Durante el evento de interrupción.	Establecer medidas de ciberseguridad.
	Acuerdos con investigadores e instituciones.	Alta dirección.	Anual.	Establecer convenios para dar continuidad y garantizar la disponibilidad de recursos, así como la gestión de la investigación en tiempos de crisis.

Plan de mejoramiento.	Sistema o Plataforma redundante.	Área de TI Líder del proceso.	Durante el evento de interrupción.	Activar cuando la plataforma principal falle.
	Capacitación y concienciación sobre seguridad.	Alta dirección. Líder del proceso. Líder de TI.	Semestral	Desarrollar un programa de capacitación y concienciación sobre seguridad para todos los actores del proceso.
	Plan de recuperación.	Líder de TI. Equipo de recuperación.	Anual	Realizar e implementar un plan de recuperación especialmente enfocado a este proceso.

Fuente: Los autores

Así mismo, se contemplan las siguientes estrategias para el proceso, gestión de extensión y proyección social.

Tabla 24. Estrategias para la continuidad de gestión de extensión y proyección social.

Procesos críticos	Estrategias	Responsable	Periodicidad	Observación
Planeación y gestión de servicios y programas.	Copias de seguridad y restauración de datos (Backups).	Todos los actores del proceso.	Diario	Implementar un servidor de nube o plataformas de datos en la nube.
Desarrollo de programas y servicios. Proyección social proyectos y programas.	Seguridad de la información.	Área de TI. Todos los actores del proceso.	A definir según las acciones de seguridad.	Implementar acciones de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información

Programas de proyección social por convenios. Seguimiento y evaluación de servicios y programas. Ejecución de los programas de egresado. Mejora continua.				vital del proceso.
	Trabajo remoto.	Todos los actores del proceso.	Durante el evento de interrupción.	Establecer medidas de ciberseguridad.
	Capacitaciones.	Alta dirección. Líder del proceso. Líder de TI.	Semestral	Realizar un programa de capacitaciones dirigido a todos los actores del proceso acerca de las buenas prácticas de seguridad de la información, de modo similar, a cómo responder frente a un evento perturbador.
	Plan estratégico de comunicaciones.	Líder del proceso. Alta dirección.	Anual	Realizar un plan estratégico de comunicaciones que permita responder y enfrentarse de manera adecuada y oportuna a un evento imprevisto minimizando así el impacto del mismo.
	Plan financiero.	Líder del proceso. Alta dirección.	Anual	Establecer un plan financiero para asumir costos e interrupciones que puedan generarse tras un evento de desastre, de igual manera que garantice la

				disponibilidad de recursos tecnológicos esenciales.

Fuente: Los autores

4.3.4.3. Roles y responsabilidades.

Con el propósito de dar continuidad a los procesos y/o servicios que han sufrido una interrupción se establecen roles con sus respectivas responsabilidades, quienes serán los encargados de poner en marcha el Plan de Gestión de Continuidad del Negocio, como se muestra a continuación.

Comité de Continuidad del Negocio: Esta conformado por un grupo de personas que pertenecen a la Universidad Popular del Cesar, Seccional Aguachica que tienen como principal objetivo mantener el buen funcionamiento de las operaciones para de esa manera garantizar la continuidad de los procesos esenciales de la misma.

Es responsable de; (i) dirigir las acciones pertinentes antes, durante y después del evento de desastre o de interrupción; (ii) apoyar al coordinador del Plan de Gestión de Continuidad; (iii) aprobar los resultados y/o documentación del Análisis de Impacto del Negocio, Análisis de riesgos, estrategias de continuidad, capacitación y sensibilización a las partes interesadas, actualización (anual) y pruebas del Plan de Gestión de Continuidad del Negocio; (iv) Decidir si se activa y ejecuta el Plan de Continuidad o no; (v) Analizar y suministrar los recursos e información necesaria para efectos del Plan de Gestión de Continuidad del Negocio; (vi) Mantener actualizada la información de contacto de cada uno de los integrantes del Comité de Continuidad del Negocio; (vii) Estar en continua actualización sobre las estrategias/procedimientos de continuidad y del Plan de Gestión de Continuidad en general de tal manera que se asegure la resiliencia operativa.

Tabla 25. Roles y responsabilidades.

Rol	Responsabilidad
Coordinador del Plan de Gestión de Continuidad	Es el responsable de dirigir el Plan de Gestión de Continuidad del Negocio, así como de analizar la situación de emergencia. Coordinar las acciones de respuesta y recuperación ante un evento disruptivo. Comunicar a la alta dirección, lideres de dependencias y demás funcionarios las acciones a seguir.

	Hacer seguimiento y documentar el proceso de recuperación. Citar a los demás integrantes del comité de continuidad del negocio a las sesiones y actas de las mismas. Promover el conocimiento del Plan de Gestión de Continuidad del Negocio además de los programas de capacitación y concientización.
Lideres de dependencias	Serán los responsables de identificar los riesgos y vulnerabilidades, determinar el impacto de una interrupción en los servicios, brindar los recursos necesarios para efectuar el plan y afrontar el evento disruptivo.
Equipo de recuperación	Serán los encargados de implementar las estrategias de continuidad, restablecer los sistemas para la continua operación de los servicios informáticos y de los servicios críticos.
Equipo de pruebas	Responsables de efectuar pruebas que aseguren la efectividad de las actividades de recuperación, así como también de garantizar la funcionalidad del Plan de Gestión de Continuidad del Negocio.
Equipo de comunicación	Responsables de establecer comunicación con las partes interesadas (internas y/o externas) durante un evento de riesgo o de desastre.
Equipo de logística	Es responsable de la logística necesaria para recuperación.
Personal suplente	Serán los encargados de cubrir las ausencias y apoyar en las actividades de continuidad del negocio.

Fuente: los autores

4.3.4.4. Árbol de llamadas.

Una vez identificados los roles de las personas responsables de gestionar la continuidad de las operaciones y/o servicios de la Universidad Popular del Cesar, Seccional Aguachica, se enlista a continuación la información de contacto en caso de incidente e interrupción.

Tabla 26. Contacto comité de continuidad.

Comité de continuidad			
Nombre	**Cargo**	**Teléfono**	**Correo**

Wilfred Torres	Vicerrector General	3133490166	vicerrectoriaguachica@unicesar.edu.co
Emiliano Piedrahita	Director Académico	3012667384	direccionacademicaaguachica@unicesar.edu.co
Deimer Martínez	Jefe de Registro y Control Académico	(605) 588 5592 Ext. 1306	registroaguachica@unicesar.edu.co
Juvenal Flórez	Jefe de Dirección Administrativa y Financiera	3185480293	financieraaguachica@unicesar.edu.co
Miguel Piñerez	Jefe de Dirección de Departamento de Ciencias Contables	3135804117	miguelpinerez@unicesar.edu.co
Wilson Sánchez	Jefe de Coordinación de Tecnología Agropecuaria	3165366386	wilsonsanchez@unicesar.edu.co
Yiceth González	Jefe de Dirección de Departamento de Ciencias Administrativas	3114301428	yicethgonzalez@unicesar.edu.co
Luis Restrepo	Jefe de Dirección de Departamento de Ciencias económicas	3104716817	luisrestrepo@unicesar.edu.co
Héctor Alvernia	Jefe de Dirección de Departamento de Ciencias		agroindustriaaguachica@unicesar.edu.co

	Agro-industriales		
Lizeth Badillo	Jefe de Dirección de departamento de Sistemas e informática	3186909946	ingsistemasaguachica@unicesar.edu.co
Rocio Ropero	Jefe de Dirección de departamento de ciencias Ambientales y sanitaria	3163356536	rocioropero@unicesar.edu.co
Flor Moncada	Jefe de Bienestar Institucional	3172737823	flormoncada@unicesar.edu.co
Wilfer Escalante	Líder de área de TI	3154696946	wescalante@unicesar.edu.co

Fuente: los autores

Tabla 27. Servicios de emergencia.

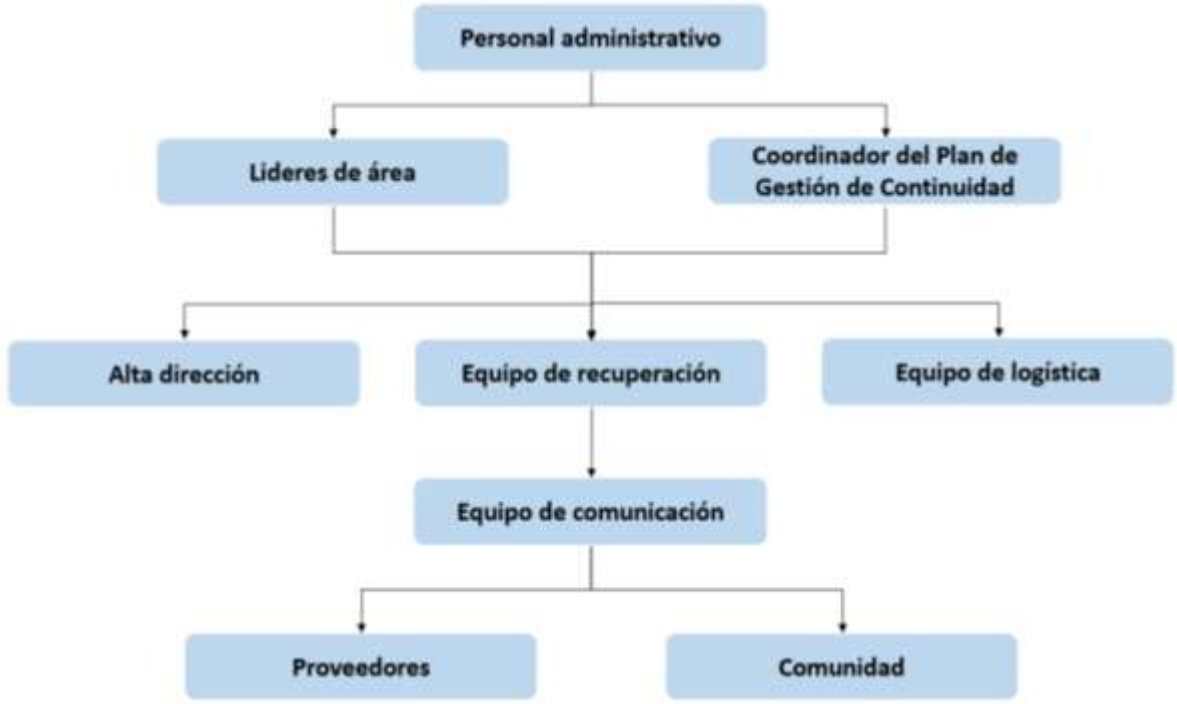
Líneas de emergencia		
Servicios	**Teléfono**	**Correo**
Bomberos	5655577–3126839329	c_b_v_aguachica@hotmail.com
Policía Nacional	3107391237	deces.eaguachica@policia.gov.co
Defensa Civil	3204337700	sec.cesar@defensacivil.gov.co
Cruz roja	3182065346	aguachica@cruzrojacolombiana.org
Gestión del Riesgo	3166175521	rovasa08@gmail.com
Departamento Administrativo de Salud de Aguachica	-	saludpublica@aguachica-cesar.gov.co secretariadesalud@aguachica-cesar.gov.co
CENS	115 018000414115	cens@cens.com.co
Ambulancias	#828 3218819338 3227777001 3135866340	-

Fuente: los autores

*Es necesario registrar o apuntar aquellas personas con las que no se entablo comunicación para su posterior seguimiento.

A continuación, se muestra el flujo de llamadas para comunicar la ocurrencia de un evento disruptivo.

Figura 32. Flujo de llamadas.



Fuente: los autores

Para convocar reuniones o encuentros, así como de comunicar las acciones propias del Plan de Gestión de Continuidad del Negocio es responsabilidad del Coordinador del plan y a su vez los jefes de las distintas dependencias, es imperativo la existencia y participación de una persona suplente en el supuesto de que el principal responsable no pueda asumir sus obligaciones.

Los medios para establecer comunicación con los miembros internos de la universidad durante un evento disruptivo o interrupción son: comunicación directa, correos, chats de emergencia, reuniones, llamadas, página web, videoconferencia; para establecer comunicación externa: comunicados de prensa, llamadas, redes sociales, correos, página web, entrevistas.

4.3.5. Iniciativas para dar respuesta a la contingencia.

Las iniciativas que se plantean en el presente apartado tienen como principal propósito, brindar alternativas que permitan responder de manera adecuada a los posibles eventos no deseados y en consecuencia garantizar la continuidad de los servicios, operaciones y/o procesos de la Universidad Popular del Cesar, Seccional Aguachica.

4.3.5.1. Activación del Plan de Gestión de Continuidad del Negocio.

El Comité de Continuidad del Negocio será el órgano responsable de activar el Plan de Gestión de Continuidad del Negocio cuando se presente un evento disruptivo que ponga en riesgo la continuidad de las operaciones, de igual modo cuando lo considere oportuno y necesario y será este mismo órgano quien desactive el plan una vez se hayan restablecido las operaciones.

Para activar el plan se debe cumplir previamente con tres (3) etapas; (i) Alerta del evento, una vez se haya identificado la ocurrencia de un evento disruptivo o un riesgo inminente que pueda afectar los procesos vitales, se debe dar aviso de carácter inmediato al coordinador del Plan de Gestión de Continuidad o en su defecto a la alta dirección de la universidad, brindando detalles acerca del mismo para una posterior evaluación por parte del comité de continuidad, es importante que los funcionarios reciban la debida capacitación y concientización sobre cómo actuar de forma efectiva ante un evento no deseado; (ii) Evaluación, el comité de continuidad se encargara de recopilar la información necesaria, analizar la situación y decidir si se ejecuta el Plan de Gestión de Continuidad del Negocio, de lo contrario tomara las medidas necesarias para contener el evento y evitar que afecte considerablemente los activos, servicios o procesos claves de la universidad; (iii) Activación del plan, tan pronto como se da la orden de ejecutar el Plan de Gestión de Continuidad del Negocio cada uno de los equipos debe actuar con base a sus responsabilidades, así también, se procede a notificar al resto del personal clave activando el árbol de llamadas.

4.3.5.2. Respuesta a la contingencia.

Es primordial efectuar acciones de respuesta que permitan estar preparados para afrontar una posible eventualidad u ocurrencia de un evento disruptivo que ponga en riesgo la disponibilidad y continuidad de las operaciones críticas de la Universidad Popular del Cesar, Seccional Aguachica, por tal razón se establecen a continuación las acciones en cuestión.

Tabla 28. Acciones de respuesta a contingencias.

Tipo de eventos	Actividad	Descripción	Responsable
Indisponibilidad e interrupción de los servicios.	Identificar y analizar el incidente.	Identificar e informar el evento al líder del proceso o al coordinador de gestión de continuidad una vez haya ocurrido el evento a través de correo electrónico, personalmente o llamada telefónica brindando una descripción detallada sobre el mismo.	Equipo de recuperación.
	Evaluar daños al proceso y componentes del mismo.	Realizar una investigación y evaluar el incidente y sus causas para posteriormente hacer una valoración de los daños causados por el evento de desastre.	Equipo de recuperación.
	Alertar sobre el incidente.	Comunicar la situación presentada a las partes involucradas y a los servicios de emergencia de ser necesario a través de los canales de comunicación establecidos.	Equipo de comunicación.
	Ejecutar acciones.	Poner en marcha acciones para	Equipo de recuperación.

		mitigar o disminuir el impacto del incidente una vez se haya identificado y valorado el estado actual del proceso y/o evento disruptivo.	

Fuente: los autores

4.3.6. Estrategias de recuperación.

A fin de hacer frente a la ocurrencia de un evento disruptivo, se muestra a continuación una serie de estrategias que le permitirán a la Universidad Popular del Cesar, Seccional Aguachica, recuperar cada uno de sus procesos críticos.

Tabla 29. Acciones de recuperación.

Plan de capacitaciones y simulacros.	
Responsables: Alta dirección, Área de talento humano.	**Periodicidad:** Semestral y/o anual
Tipo de estrategia: Prevenir	
Adoptar un Plan de capacitaciones y simulacros pre-evento y post-evento dirigido a todos los actores de cada proceso critico de la universidad a fin de gestionar y responder de manera adecuada frente a distintas situaciones de emergencia e interrupción, este debe desarrollarse bajo una estrategia basada en las necesidades de capacitación y simulacro, además de contener protocolos de acción, roles y responsabilidades, los recursos necesarios para el cumplimiento del mismo, así como un cronograma de actividades.	
Acuerdos con proveedores estratégicos.	
Responsable: Líder del área administrativa y financiera.	**Periodicidad:** Anual
Tipo de estrategia: Transferir	
Establecer acuerdos con proveedores estratégicos es clave para gestionar riesgos, reducir el impacto de un evento de desastre, así como las consecuencias del mismo sobre los procesos, asegura además la disponibilidad de servicios, sistemas y recursos durante una interrupción.	

Mantenimiento y actualización del Plan de Gestión de Continuidad del Negocio.	
Responsable: Área de TI, Coordinador del Plan de Gestión de Continuidad.	**Periodicidad:** Anual
Tipo de estrategia: Mitigar	
Efectuar el mantenimiento y actualización del Plan de Gestión de Continuidad del Negocio con el propósito de adaptarlo según las necesidades que se presenten, una vez terminada esa fase es importante socializarlo con las partes involucradas. Es imperativo que en el marco del mantenimiento y actualización del plan se elabore un itinerario para efectuar pruebas en escenarios de contingencias los más real y acertados posible, el objetivo es verificar la eficacia y efectividad del plan.	
Plan de Gestión de Riesgos.	
Responsable: Área de TI	**Periodicidad:** Anual
Tipo de estrategia: Mitigar	
Crear y efectuar un Plan de Gestión de Riesgos a cada uno de los procesos misionales permitiendo identificar vulnerabilidades, amenazas y riesgos que puedan afectar a la Universidad Popular del Cesar, Seccional Aguachica y a su vez proteger los activos que permite el desarrollo de dichos procesos y el cumplimiento de los objetivos institucionales. El plan debe considerar protocolos de acción coherentes de acuerdo al perfil de los actores internos de la universidad.	
Plan de Recuperación ante Desastres de Tecnología (DRP).	
Responsable: Área de TI	**Periodicidad:** Anual
Tipo de estrategia: Mitigar	
Diseñar e implementar un Plan de Recuperación de Desastres de Tecnología y telecomunicaciones para garantizar la seguridad física y lógica de la universidad tras la ocurrencia de interrupciones o eventos disruptivos que afecten los procesos misionales y la entrega de servicios. Es preciso identificar y analizar escenarios de desastre, recursos y acciones para gestionarlos, designar roles y responsabilidades, realizar un programa de acciones para el mantenimiento, actualización y pruebas del plan.	

Fuente: los autores

4.4. CRONOGRAMA DE IMPLEMENTACIÓN, EVALUACIÓN, SEGUIMIENTO Y MEJORA CONTINUA DEL PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO PARA LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA.

Para la Universidad Popular del Cesar, Seccional Aguachica es importante mejorar continuamente con respecto a sus procesos y servicios, es por esa razón que cobra importancia el presente capítulo, el cual se compone de la definición del propósito del cronograma y la construcción del mismo.

4.4.1. Definir el propósito y el alcance del cronograma de implementación, evaluación y mejora continua del Plan de Gestión de Continuidad del Negocio.

Este cronograma está diseñado para implementar, evaluar, hacer seguimiento y mejorar continuamente el Plan de Gestión de Continuidad del Negocio en la Universidad Popular del Cesar, Seccional Aguachica, alineado con los estándares de la ISO 22301:2019, el Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital del Ministerio de Tecnología de la Información y las Comunicaciones (MinTIC).

4.4.2. Diseñar el cronograma de implementación, evaluación, seguimiento y mejora continua del Plan de Gestión de Continuidad del Negocio.

Tabla 30. Cronograma fase planear.

FASE 1: PLANEAR					
Eje estratégico	**Actividades**	**Responsables**	**Duración**	**Producto esperado**	**Indicadores**
Socialización del PGCN	Presentación del plan a la Alta Dirección; Sensibilización a líderes; Estrategia de divulgación	Dirección TIC, Comité de Continuidad, vicerrectoría	2 semanas	Acta de aprobación, Plan de sensibilización y socialización	N° líderes sensibilizados, % dependencias notificadas
Conformación del Comité de Continuidad	Concretar miembros; Asignar roles;	Vicerrectoría, Oficina Jurídica	1 semana	Resolución de conformación del comité	Comité con miembros por macroproceso

	Oficializar funciones				
Asignación de recursos	Destinar presupuesto; Asignar responsables financieros y técnicos	Dir. Administrativa y Financiera,	2 semanas	Presupuesto aprobado, POA actualizado	% del presupuesto asignado
Actualización documental	Integrar al sistema de gestión; Ajuste del PETI; Registro documental	Oficina de Calidad, Planeación	1 semana	Plan publicado y registrado	% integración documental

Fuente: los autores.

Tabla 31. Cronograma fase hacer.

FASE 2: HACER					
Eje estratégico	**Actividades**	**Responsables**	**Duración**	**Producto esperado**	**Indicadores**
Capacitación al personal clave	Cronograma de formación; Capacitar jefes y administrativos.	Dir Administrativa y financiera, Oficina de Sistemas	1 mes	Registros de asistencia, Pruebas de evaluación	% asistencia, % aprobación
Ejecución de simulacros	Definir escenarios; Simular recuperación; Documentar hallazgos	Comité Continuidad, Oficina de Riesgos, Seguridad Info	1 mes	Informe de simulacros, Plan de mejora	Tiempo respuesta, % procesos validados
Implementación de controles técnicos	Configurar backups; Redundancia de red; Activar UPS/DRP	Oficina de TIC, Proveedor TI	2 meses	Servicios críticos con respaldo	% servicios con respaldo activo
Pruebas de recuperación de datos	Restaurar backups; Verificar integridad; Medir RTO y RPO	Soporte técnico, Oficina de TIC	2 semanas	Informe de validación, Logs recuperación	% recuperación exitosa, RTO/RPO

Fuente: los autores.

Tabla 32. Cronograma fase verificar.

FASE 3: VERIFICAR					
Eje estratégico	**Actividades**	**Responsables**	**Duración**	**Producto esperado**	**Indicadores**
Auditoría interna del PGCN	Listas de chequeo; Evaluar cumplimiento e indicadores	Control Interno, Calidad, Auditoría	2 semanas cada 6 meses	Informe auditoría, Hallazgos	% cumplimiento, hallazgos cerrados
Revisión de incidentes	Análisis post mortem; Revisión causas y consecuencias	Comité Continuidad, Jurídica, TIC	Permanente	Informe de lecciones aprendidas	% eventos sin impacto crítico
Evaluación de competencias	Evaluaciones periódicas; Retroalimentación	Dir Administrativa y financiera Comité Capacitación	1 semana cada 4 meses	Resultados de evaluación	% competencia certificada

Fuente: los autores.

Tabla 33. Cronograma fase actuar.

FASE 4: ACTUAR					
Eje estratégico	**Actividades**	**Responsables**	**Duración**	**Producto esperado**	**Indicadores**
Revisión del plan	Actualizar BIA; Ajustar roles y estrategias	Comité Continuidad, Planeación, Seguridad Info	1 mes anual	Versión actualizada del plan	Versión firmada/publicada
Divulgación de actualizaciones	Circular interna; Talleres breves; Publicación en intranet	Comunicaciones, Comité Continuidad	2 semanas	Registros asistencia, Circulares	% personal informado
Integración con procesos estratégicos	Incluir en POA y MIPG; Cruzar con mapa de riesgos	Planeación, Comité Estratégico	3 semanas	Inclusión del PGCN en POA y MIPG	% procesos integrados

Fuente: los autores

5. CONCLUSIONES.

A partir de la aplicación de los instrumentos de recolección de información se logró constatar la necesidad latente de proteger los procesos vitales de la Universidad Popular del Cesar, Seccional Aguachica, así como su activo más importante, la información que se maneja en ella, por medio de herramientas para gestionar la continuidad operativa dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en el Modelo de Seguridad y Privacidad de la Información (MSPI).

El Plan de Gestión de Continuidad del Negocio para la Universidad Popular del Cesar, Seccional Aguachica se diseñó siguiendo los procedimientos impartidos por las guías del Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital del MinTIC que, a su vez se basan en estándares internacionales, siendo las guías en cuestión; guía para la Continuidad del Negocio, guía para la Gestión y Clasificación de Activos de Información, guía para realizar el Análisis de Impacto de Negocios (BIA), guía de gestión de riesgos y guía Controles de Seguridad y Privacidad de la Información.

Durante el desarrollo del Plan de Gestión de Continuidad del Negocio para la Universidad Popular del Cesar, Seccional Aguachica se pudo identificar las vulnerabilidades existentes en cuanto a seguridad y protección de la información, así como la carencia de aplicabilidad de buenas prácticas para respaldar activos, procesos críticos y misionales, razón por la que cobró sentido la elaboración del presente documento a razón de la disponibilidad de los procesos durante y después de un evento disruptivo.

Del mismo modo se analizaron los componentes (planificación, implementación, evaluación y mejora continua) para que tanto entidades del estado como privados puedan gestionar la seguridad y privacidad de la información en el marco de la continuidad del negocio, así como también los componentes (institucionalidad, operación y medición) del Modelo Integrado de Planeación y Gestión, además de la base legal que sustenta la realización del Plan de Gestión de Continuidad del Negocio corroborando así su alineación con las políticas públicas que se detallan en el cuerpo del presente documento.

Se realizo un análisis de la Universidad Popular del Cesar, Seccional Aguachica para posteriormente identificar y clasificar los activos críticos con los que cuenta el claustro educativo para su correcto funcionamiento y entrega de servicios, se analizaron los riesgos que podrían afectar los activos críticos con base en la guía de gestión de riesgos del MinTIC, seguido de ello se logró identificar los procesos

y recursos críticos manejados por las principales áreas de la universidad y sus objetivos de recuperación a través del Análisis de Impacto del Negocio (BIA), lo que permitió establecer las estrategias para la gestión de la continuidad que se detallan en este documento y por último se construyó un cronograma que permitirá gestionar la continuidad de los procesos críticos y mejora del Plan de Gestión de Continuidad del Negocio.

6. RECOMENDACIONES.

Se sugiere que se implemente el Plan de Gestión de Continuidad del Negocio se dé a conocer y se socialice con el personal administrativo, así como también, realizar eventos de capacitación y concienciación que involucren actividades de simulacro respecto a las buenas prácticas de la gestión y seguridad de la información además de las acciones de respuesta frente a situaciones de contingencia o ante la ocurrencia de eventos disruptivos que afecten directamente a los procesos críticos de la Universidad Popular del Cesar, Seccional Aguachica.

Realizar de manera periódica, el seguimiento y pruebas para verificar la eficacia y efectividad de las estrategias del Plan de Gestión de Continuidad del Negocio, seguido de ello, llevar a cabo la revisión y actualización del mismo para obtener los mejores resultados que busquen propender por la mejora continua.

Establecer acuerdos con proveedores estratégicos como parte fundamental de la gestión de la continuidad de los procesos de la Universidad Popular del Cesar, Seccional Aguachica, estos deben estar en la capacidad de suministrar servicios y productos que permitan mitigar y/o minimizar riesgos en tiempos de crisis lo que en consecuencia le garantiza resistir y recuperarse ante eventos disruptivos.

7. PARTICIPANTES DEL PROYECTO

Para este proyecto se proponen los siguientes participantes; quienes son las personas que están directa o indirectamente relacionados con la ejecución de un proyecto, como se observa en la tabla.

Tabla 34. Participantes del proyecto

Director	Erney Alberto Ramírez Camargo
Co-director	Didier Fernando Guerrero Sumalave
Docente de la asignatura	Katherine Beleño Caselles
Evaluador	Luis Palmera Quintero
Evaluador	Miguel Alberto Rincón Pinzón
Población objetivo	Personal administrativo de la Universidad Popular del Cesar, Seccional Aguachica

Fuente: los autores

8. RECURSOS DISPONIBLES

A continuación, se señalan los recursos disponibles para la realización del presente proyecto.

Tabla 35. Recursos disponibles del proyecto

Elementos	**Cantidad**	**Valor Unitario**	**Valor total**
Computador Portátil	2	1.650.900	3.201.800
Cuaderno	2	2.000	4.000
Lapicero	2	1.500	3.000
TOTAL	----	-----	1.938.400

Fuente: Los autores

9. CRONOGRAMA DE ACTIVIDADES

Objetivo	Actividades	Mes	1				2				3				4				5				6			
		Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Realizar un diagnóstico sobre la situación actual de la Universidad en cuanto a la aplicación de la estrategia de Gobierno Digital.	Diseñar y elaborar una encuesta, entrevista y lista de verificación, que será aplicada a los lideres de las distintas dependencias de la Universidad Popular del Cesar Seccional Aguachica																									
	Aplicar los instrumentos de recoleccion de información a los lideres de las distintas dependencias de la Universidad Popular del Cesar Seccional Aguachica																									
	Interpretar y documentar la información que se recolectará en las encuestas y las entrevistas, para determinar el estado actual de la seguridad de la información																									
Analizar los componentes del modelo gestión de continuidad del negocio con base en los requerimientos normativos.	Indagar los componentes que comprenden la estrategia de gestión de continuidad del negocio por parte del Ministerio de Tecnologías de la Información y las Comunicaciones.																									
	Investigar la politica publica por la cual esta definida la estrategia de gobierno digital.																									
	Estudiar el marco normativo que rigen en Colombia los planes de continuidad del negocio.																									
Elaborar una guía para la gestión de continuidad del negocio orientada a la Universidad Popular del Cesar, Seccional Aguachica	Establecer el alcance del plan de gestion de continuidad del negocio																									
	Realizar un analisis de la organización																									
	Determinar la estrategia para la gestion de continuidad																									
	Seleccionar iniciativas para dar respuesta a la contingencia																									
	Efectuar prueba y revisión del plan de gestión de continuidad																									
Construir el cronograma de implementación, evaluación, seguimiento y mejora continua del plan de gestión de continuidad del negocio para la Universidad Popular del Cesar.	Definir el proposito y el alcance del cronograma de implementación, evaluación, seguimiento y mejora continua del plan de gestion de continuidad																									
	Diseñar el cronograma de implementación, evaluación, seguimiento y mejora continua del plan de gestion de continuidad																									

BIBLIOGRAFIA

Amazon. (2022). *Objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO)*. https://docs.aws.amazon.com/es_es/wellarchitected/latest/reliability-pillar/recovery-time-objective-rto-and-recovery-point-objective-rpo.html

Andrade Serrano, H., Otero Dajud, E. R., Varón Cotrino, G., & Rodriguez Camargo, J. A. (2009). *Ley 1273 de 2009 Nivel Nacional*. 2009. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Asamblea Nacional Constituyente. (1991a). *Constitución Política de la República de Colombia 1991, Art. 2-78*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Asamblea Nacional Constituyente. (1991b). *Constitución Política de la República de Colombia 1991, Art. 15*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Asamblea Nacional Constituyente. (1991c). *Constitución Política de la República de Colombia 1991, Art. 209-269*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125

Ati Guillen, T. M. (2018). *Diseño del plan de recuperación de desastres y continuidad del negocio basado en Cobit, Itil y de acuerdo a la norma ISO 22301, para el centro de procesamiento de datos (CPD) de la carrera de ingeniería en ciencias de la computación de la Universidad*.

Cano Sotomayor, E., Plaza Aranda, I., & Ramírez Chávez, E. (2021). Gestión de la Continuidad de Negocio: Caso Ravmar Freight del Sector Logístico. *360: Revista de Ciencias de La Gestión*, *6*, 1–15. https://doi.org/10.18800/360gestion.202106.014

Congreso de la República de Colombia. (1993). *Ley 87, Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones*. 29 de Noviembre de 1993. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=300

Congreso de la República de Colombia. (2009). *Ley 1273, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. 05 de Enero de 2009. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2011). *Ley 1474, Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión*

pública. 12 de Julio de 2011. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43292

Congreso de la República de Colombia. (2012a). *Ley 1523, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones*. 24 de abril de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=47141

Congreso de la República de Colombia. (2012b). *Ley 1581, Por la cual se dictan disposiciones generales para la protección de datos personales*. 17 de Octubre de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2019). *Ley 1978, Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones*. 25 de julio de 2019. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210

Consejo Superior Universitario de la Universidad Popular del Cesar. (2002). *Acuerdo N° 029, Por medio de la cual se modifica la Estructura Orgánica de la Universidad Popular del Cesar en la Seccional Aguachica*. 6de agosto de 2002. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=84614

Consejo Superior Universitario de la Universidad Popular del Cesar. (2016a). *Acuerdo N° 011, Por el cual se actualiza y se adopta el Proyecto Educativo Institucional (PEI)*. 31 de marzo de 2016.

Consejo Superior Universitario de la Universidad Popular del Cesar. (2016b). *Acuerdo No. 024 del 22 de abril de 2016 - Actualización de Misión y Visión*. https://drive.google.com/file/d/1ZgRIArIWUuB3j0E7ENvI3yxzTOutTJo3/view?pli=1

Del corral, C., & Pinargote, C. (2019). *PROPUESTA DE DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA LAS OPERACIONES ALINEADO A COBIT 5 PARA CORPQSF S.A*.

Delgado, K. (2015). *Diseño Y Propuesta De Una Metodología Para La Implementación De Un Sistema De Gestión De Continuidad Del Negocio, Basado En La Norma Iso/Iec 22301:2012*. 193.

Departamento Nacional de Planeación. (2011). *CONPES 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa*. 14 de Julio de 2011. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (2020). *CONPES 3995, Política Nacional de Confianza y Seguridad Digital* . 01 de Julio de 2020.

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Funcion Publica. (2023). *Marco General del Modelo Integrado de Planeación y Gestión*.

García Ferrando, M. (1993). La encuesta. In *El análisis de la realidad social. Métodos y técnicas de investigación*.

Gaviria Trujillo, C., & Villegas Ramirez, F. (1993). *Ley 44 de 1993*. 1993. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3429

Gobernación de Guaviare. (2020). *Información en Línea*. https://www.guaviare.gov.co/glosario/informacion-en-linea

Gordillo Almeida, A. C. (2017). *Sistema de Gestión de Seguridad de la Información para Emelnorte prototipo: proceso de levantamiento de un nuevo cliente*.

Guevara Gomez, D. F. (2020). *Resolución N° 0090, Por la cual se ajusta el Manual Especifico de Funciones y Competencias Laborales del Personal Administrativo de la Universidad Popular del Cesar*. 24 de enero de 2020. https://www.unicesar.edu.co/transparencia/manuales-de-funciones/

Hernández Sampieri, R., Fernández Collado Carlos, & Baptista Lucio, P. (2014). *Metodología de la investigación* (Sexta edición). McGraw Hill.

IBM. (2022). *Plan de Recuperación de Desastres (DRP)*. https://www.ibm.com/mx-es/services/business-continuity/disaster-recovery-plan

ICONTEC. (2019a). *NTC-ISO 22301:2019, Seguridad y resiliencia. Sistema de gestión de continuidad de negocio. Requisitos.* https://tienda.icontec.org/gp-seguridad-y-resiliencia-sistema-de-gestion-de-continuidad-de-negocio-requisitos-ntc-iso22301-2019.html

ICONTEC. (2019b). *NTC-ISO 22301:2019, Seguridad y resiliencia. Sistema de gestión de continuidad de negocio. Requisitos.* https://tienda.icontec.org/gp-seguridad-y-resiliencia-sistema-de-gestion-de-continuidad-de-negocio-requisitos-ntc-iso22301-2019.html

ICONTEC. (2019c). *NTC-ISO/IEC 27005:2009, Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información*. https://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

ICONTEC. (2020). *GTC-ISO 22313:2020, Seguridad y resiliencia. Sistemas de gestión de continuidad de negocio. Orientación sobre el uso de la NTC-ISO 22301*. https://tienda.icontec.org/seguridad-y-resiliencia-sistemas-de-gestion-de-continuidad-de-negocio-orientacion-sobre-el-uso-de-la-ntc-iso-22301.html

ICONTEC. (2022a). *GTC-ISO-TS 22317:2022, Seguridad y resiliencia. Sistemas de gestión de continuidad de negocio. Directrices para el análisis de impacto en el negocio*. https://tienda.icontec.org/gp-gtc-iso-ts-seguridad-y-resiliencia-sistemas-de-gestion-de-continuidad-de-negocio-directrices-para-el-analisis-de-impacto-en-el-negocio-gtc-iso-ts22317-2022.html

ICONTEC. (2022b). *NTC-ISO-IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos*.

ISO. (2018). *ISO 31000:2018 - Risk management - Guidelines*. 2018. https://www.iso.org/standard/65694.html

ISO. (2019). *NTC/ISO 22301*. 2019. https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=76603

ISO. (2024). *ISO 27000, Referencias Normativas* . https://www.normaiso27001.es/referencias-normativas-iso-27000/#def377

ISOTools. (2022a). *ISO 22301: Sistema de Gestión de Continuidad de Negocio*. ISOTools. https://www.isotools.cl/iso-22301-sistema-gestion-continuidad-negocio/#:~:text=Continuidad de negocio es el,cibernéticos%2C accidentes o errores humanos.

ISOTools. (2022b). *Punto de Recuperación Objetivo*. https://www.isotools.org/2019/07/16/punto-recuperacion-objetivo-rto-analisis-partida-ante-una-contingencia-de-continuidad-negocio/

ISOTools. (2024). *ISO 27001 ¿Cuáles son las amenazas y la vulnerabilidades?* https://pe.isotools.us/iso-27001-cuales-son-las-amenazas-y-vulnerabilidades/

León, K., & Rios, D. (2017). *Plan de Continuidad del Negocio para el área de Tecnologías de la Información del proyecto Ruta del Sol - Sector 2 .*

Malaver, J. (2020). *Diseño e implementación del plan de continuidad del negocio en BANCOMPARTIR*. *1*.

Matos, A. (2021). *Propuesta de un plan de continuidad de negocio en el área de producción de una empresa cosmética peruana.*

Mendez Alvarez, C. E. (2001). *METODOLOGIA: Diseño y Desarrollo del proceso de investigación. Tercera Edición*. 2001. https://pure.urosario.edu.co/es/publications/metodologia-diseño-y-desarrollo-del-proceso-de-investigación-terc

Meza Daza, E. A. (2018). *Resolución N° 022, Por la cual se ajusta el Manual Especifico de Funciones y Competencias Laborales del Personal Administrativo de la Universidad Popular del Cesar, Seccional Aguachica*. 16 de enero de 2018. https://drive.google.com/file/d/1tm7qmXKW5x3kT3Np7w1YEYC8DNILyGMK/view

Mineducación. (2022). *Guía de implementación de la política de gobierno digital*. 9–11.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016a). *Controles de Seguridad y Privacidad de la Información* . https://gobiernodigital.mintic.gov.co/692/articles-5482_G8_Controles_Seguridad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016b). *Guía de gestión de riesgos*. https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Resolución N° 00500, Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*. 10 de Marzo de 2021. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

MinTIC. (2010a). *Guía para la preparación de las TIC para la continuidad del negocio*. *10*, 35.

MinTIC. (2010b). *Guía para la preparación de las TIC para la continuidad del negocio*. *10*, 35.

MinTIC. (2015). *Guía para realizar el Análisis de Impacto de Negocios BIA*. https://gobiernodigital.mintic.gov.co/692/articles-5482_G11_Analisis_Impacto.pdf

MinTIC. (2016). Guía para la gestión y clasificación de activos de información. *Ministerio de Tecnologías de La Información y Comunicaciones*, *5*, 18.

Mintic. (2018). *MANUAL DE GOBIERNO DIGITAL Implementación*. *2018*, 1–38.

MinTIC. (2022a). *Gobierno en Línea (GEL)*. https://www.mintic.gov.co/portal/inicio/Glosario/G/5306:Gobierno-en-Linea-GEL

MinTIC. (2022b). *Manual de Gobierno Digital.* Gobierno Digital. https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/

Montserrath Range, C. (2017). *ISM | La importancia de Gestionar la Continuidad del Negocio*.

Ojeda Ramirez, B., & Suárez Mogollón, J. (2021). *Entrevista*.

Organización Internacional de Normalización. (2019a). *ISO 22301:2019, Guia de Implementación de Sistemas de Gestión de Continuidad de Negocio*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

Organización Internacional de Normalización. (2019b). *ISO 22301:2019, Guia de Implementación de Sistemas de Gestión de Continuidad de Negocio*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

Perez, E. J. (1991). *Constitución Política de la República de Colombia*. https://normograma.mintic.gov.co/mintic/docs/constitucion_politica_1991.htm

Presidente de la República de Colombia. (2005). *Decreto 1599, Por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano*. 20 de Mayo de 2005. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=16547#:~:text=Adopta%20el%20Modelo%20Est%C3%A1ndar%20de,la%20Ley%2087%20de%201993.

Presidente de la República de Colombia. (2013). *Decreto 1377, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015*. 27 de Junio de 2013.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Presidente de la República de Colombia. (2014). *Decreto 886, Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos*. 13 de Mayo de 2014. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Presidente de la República de Colombia. (2015). *Decreto 1072, Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo*. 26 de mayo de 2015. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=72173

Presidente de la República de Colombia. (2017). *Decreto 648, Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública*. 19 de Abril de 2017. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=80915#

Presidente de la República de Colombia. (2020). *Decreto 620, Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales*. 2 de mayo de 2020. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337

Presidente de la República de Colombia. (2022a). *Decreto 338, Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones*. 08 de Marzo de 2022. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Presidente de la República de Colombia. (2022b). *Decreto 767, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*. 16 de mayo 2022.

Ramos Montiel, R. R., Cabrera Cabrera, G. E., Urgiles Urgiles, C. D., & Jara Centeno, F. E. (2018). *Aspectos metodológicos de la investigación | RECIAMUC*. 2018. https://reciamuc.com/index.php/RECIAMUC/article/view/111/226

Rincón Páez, R. (2020). *Historia – UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA*. http://aguachica.unicesar.edu.co/historia/

Rivera Florez, G. A., Gil Botero, E., Gutierrez Botero, M. L., Rozo Rengifo, J. S., & Garcés Cordoba, M. (2018). *Ley 1915 de 2018*. 2018. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87419

Rodríguez, C. (2020). *La Importancia de un Plan de Continuidad de Negocio*.

Romero Ramírez, R. (2023). *Resolución 1709, Por medio de la cual de actualiza la estructura orgánica de la Universidad Popular del Cesar*. 29 de junio de 2023. https://drive.google.com/file/d/1T3HcTRS_plDDO0-bgLobgU01TKbcKno5/view

Sánchez, K. (2015). Diseño del Plan de Continuidad del Negocio para la E.S.E Hospital Emiro Quintero Cañizares de Ocaña mediante el estándar ISO 27001. *Universidad Francisco de Paula Santander*.

Santos Calderon, J. M., Cristo Bustos, J. F., Molano Vega, D., Gaviria Muñoz, S., & Caballero Durán, L. (2014). *Decreto 2573 de 2014*. 2014. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596

Santos Calderón, J. M., & Vargas Lleras, G. (2010). *Decreto 3942 de 2010*. 2010. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=40624

Schettini, P., Cortazzo, I., Burone, E., Elverdín, F., Farías, M. L., Nogueira, M. C., Torillo, D. L., Trindade, V. A., & Veiga, M. S. (2016). *Técnicas y estrategias en la investigación cualitativa*.

Segura, G. (2019). *Diseño del Plan de Continuidad de Negocio ante Desastres Tecnológicos para la empresa IREX de Costa Rica S.A.*

Superintendencia de Industria y Comercio, & Agencia Nacional de Defensa Jurídica del Estado. (2019). *Circular Externa Conjunta N° 4*. 05 de Septiembre de 2019. https://www.sic.gov.co/sites/default/files/files/Normativa/Circulares/DOC090619_09062019183011.pdf

Superintendencia Financiera de Colombia. (2020). *Circular 25, Boletín Ministerio de Hacienda, Capítulo Superintendencia Financiera de Colombia, No. 546 de 10 de julio de 2020*. https://normativa.colpensiones.gov.co/compilacion/docs/circular_superfinanciera_0025_2020.htm#documento_top

Tellez, C. (2015). *Diseñar un Plan de Continuidad del Negocio en el proceso de administracion de recursos TI de la oficina de informatica y telematica de la alcaldia de Santiago de Cali*.

Torchio, A. (2020). *La importancia del Plan de Continuidad de Negocio – CUATROi*.

Unidad Administrativa Especial de Reahbilitacion y Mantenimiento Vial. (2020). *PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 57*, 1–22.

Unidad Nacional para la Gestión del Riesgo de Desastres. (2022). *Plan Nacional de Gestión del Riesgo de Desastres*. https://portal.gestiondelriesgo.gov.co/Documents/PNGRD/PNGRD-2022-

Actualizacion-VF.pdfhttps://portal.gestiondelriesgo.gov.co/Documents/PNGRD/PNGRD-2022-Actualizacion-VF.pdf

Universidad Popular del Cesar. (2016). *Acuerdo 011 del 31 de marzo del 2016, Proyecto Educativo Institucional, PEI*. *011*, 1–75.

Universidad Popular del Cesar. (2023). *Mapa de Procesos de la Universidad Popular del Cesar*. https://sites.google.com/unicesar.edu.co/sac/sistema-de-gesti%C3%B3n-de-calidad/mapa-de-procesos

Valderrama Rojas, C. L., Botero Barco, A., & Barranco Alvis, N. J. (2022). *Decreto 767 de 2022 - Gestor Normativo - Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766

Vega Velasco Walter. (2008). *POLITICAS Y SEGURIDAD DE LA INFORMACION*. *2*, 63–69.

Velasco Chaves, L. F., Barguil Assis, D. A., Garcia Turbay, L. A., Castaño Perez, M. A., & Lozada Vargas, J. C. (2019). *Proyecto de Ley 062 de 2019*. 2019. http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2019-2020/1525-proyecto-de-ley-062-de-2019

Web, C. turismo. (2020). *Aguachica Cesar*.

ANEXOS

Anexo A. Aceptación para desarrollo de proyecto de grado.

Universidad Popular del Cesar

Vicerrectoría General
Seccional Aguachica

La UPC es de todos!

Aguachica, noviembre 30 de 2021.

Jóvenes
BRESLY SELENY OJEDA RAMIREZ
JULIETH PAOLA SUÁREZ MOGOLLÓN
Estudiantes VIII semestre programa Ingenieria de Sistemas.

Ref.: Aceptación desarrollo trabajo de grado.

Cordial saludo:

De acuerdo a su solicitud nos permitimos informarles que se acepta su propuesta para desarrollar la asignatura proyecto de grado I, con el trabajo de investigación titulado: "***DISEÑO DEL PLAN DE GESTION DE CONTINUIDAD DEL NEGOCIO PARA LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA, ALINEADO CON LA POLITICA DE GOBIERNO DIGITAL DEL MINISTERIO DE LAS TIC***", y puedan aplicar un instrumento de datos (encuesta) en la Institución, bajo la responsabilidad del Ing. Erney Alberto Ramírez Camargo, docente del programa de Ingenierías de Sistemas.

Atentamente,

YERLY CRISTANCHO PORTILLO
Vicerrector General Seccional Aguachica

ISO 9001 icontec CO-SC-CER551826

I.Net

Anexo B. Entrevista realizada a Andrea Navarro Claro encargada de Gestión de Calidad en la UPC-SA.[1]

La siguiente entrevista tiene como finalidad identificar la problemática a desarrollar en nuestro proyecto de investigación el cual consiste en el DISEÑO DEL PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA desarrollado por las estudiantes Julieth Paola Suárez Mogollón y Bresly Seleny Ojeda Ramírez estudiantes del programa de ingeniería de sistemas

1. ¿Existe un Plan de Gestión de Continuidad de Negocio en la Universidad Popular del Cesar, Seccional Aguachica?

   Respuesta: No sé, si lo hay lo desconozco.

2. ¿Conoce usted que función cumple un Plan de Gestión de Continuidad del Negocio?

   Respuesta: Que está relacionado con la planeación para sobrevivir ante un desastre o riesgo materializado.

3. ¿Considera importante implantar un Plan de Gestión de Continuidad de Negocio (ISO 22301) en la UPC-SA? ¿por qué?

   Respuesta: Si, para tener el control de los riesgos que se pueden materializar, por lo que la empresa puede verse afectada de forma sustancial.

4. ¿Durante las actividades administrativas y académicas de la Universidad Popular del Cesar, seccional Aguachica se ha presentado una situación que le impida el normal desarrollo de las mismas? ¿cuál?

   Respuesta: En el momento desconozco si se ha presentado algún tipo de situación que impida el funcionamiento; y si he realizado el protocolo lo hace desde la sede central.

[1] Tomado y adaptado de "Plan de Continuidad de Negocios para la Pontificia Universidad Católica del Ecuador" por C. Granizo, 2019 (https://repositorio.puce.edu.ec/server/api/core/bitstreams/2f2fa8dc-e486-47f2-a3cb-e24280013e8f/content) y "Desarrollo de un Plan de Continuidad del Negocio aplicado al departamento de sistemas y procesos en los puntos críticos de la empresa Factorytech S.A." por J. Castro y E. Morales, 2016 (https://repositorio.ug.edu.ec/server/api/core/bitstreams/8a31b1ac-3ab2-4f8e-8cfc-a56f4b1a04dd/content)

5. ¿Cuáles son las estrategias con las que cuenta la UPCSA, para responder ante incidentes o interrupciones de sus operaciones?

   Respuesta: Todo se maneja desde la sede central, en la Seccional se viene trabajando en la implementación de la oficina de gestión TICS.

6. ¿Se han evaluado los riesgos para determinar el impacto de dichas interrupciones tanto en términos de magnitud de daños como de periodo de recuperación?

   Respuesta: Como tal no, todo lo hace la sede central.

7. ¿Cómo cree que ayudara el diseño de un Plan de Gestión de Continuidad del Negocio en la recuperación y mantenimiento de las actividades del negocio en niveles aceptables frente a un incidente o interrupción?

   Respuesta: En la eficiencia del proceso.

8. ¿Considera usted que un Plan de Gestión de Continuidad del Negocio ayudara a una rápida recuperación de los servicios en caso de algún desastre o vulnerabilidad de la información?

   Respuesta: Realizando un análisis del impacto en la empresa.

9. ¿Qué aspectos considera importante que deben estar inmersos en el Plan de Gestión de Continuidad del Negocio para poder recuperar de manera rápida y eficiente los servicios provenientes de las diferentes dependencias de la UPC-SA?

   Respuesta: Falta de formación y concienciación entre los funcionarios. Procesos de gestión ante incidentes de seguridad ineficaces o mal planteados.

10. ¿Cree usted que exista pérdidas financieras al momento de ocurrir una catástrofe ya sea natural o causada por el hombre dentro de la universidad la cual causaría la interrupción de los procesos o servicios de la universidad?

    Respuesta: Los daños y destrucción de la infraestructura en la Seccional.

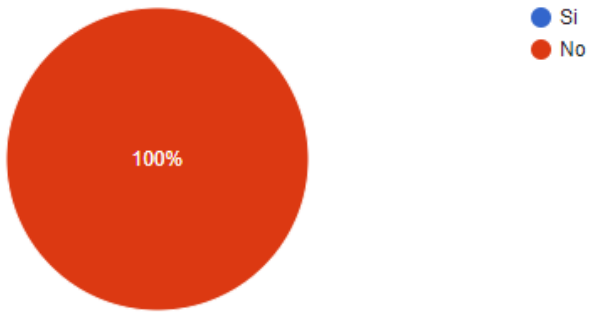
Anexo C. Encuesta realizada a Andrea Navarro Claro encargada de Gestión de Calidad en la UPC-SA.[2]

La siguiente encuesta tiene como finalidad identificar la problemática a desarrollar en nuestro proyecto de investigación el cual consiste en el DISEÑO DEL PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA desarrollado por las estudiantes Julieth Paola Suárez Mogollón y Bresly Seleny Ojeda Ramírez estudiantes del programa de ingeniería de sistemas.

[2] Tomado y adaptado de:
Tomado y adaptado de "Plan de Continuidad de Negocios para la Pontificia Universidad Católica del Ecuador" por C. Granizo, 2019 (https://repositorio.puce.edu.ec/server/api/core/bitstreams/2f2fa8dc-e486-47f2-a3cb-e24280013e8f/content) y "Desarrollo de un Plan de Continuidad del Negocio aplicado al departamento de sistemas y procesos en los puntos críticos de la empresa Factorytech S.A." por J. Castro y E. Morales, 2016 (https://repositorio.ug.edu.ec/server/api/core/bitstreams/8a31b1ac-3ab2-4f8e-8cfc-a56f4b1a04dd/content)

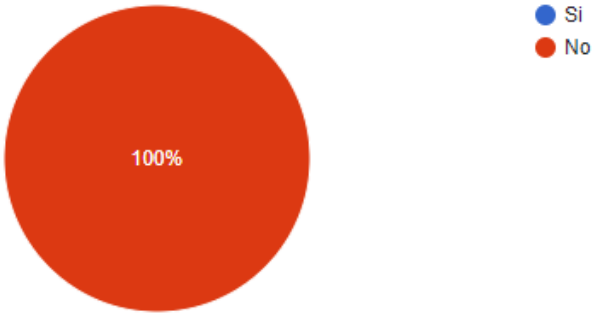
1. Dentro de la Universidad como institución publica se ha implementado alguna de las fases de la política de gobierno digital?

1 respuesta



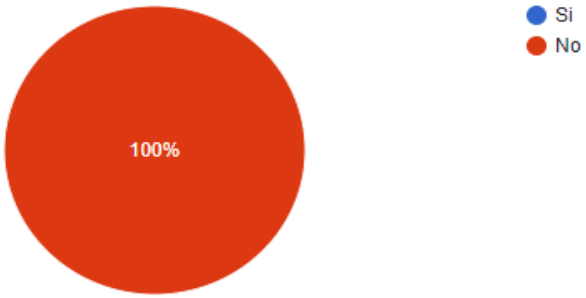
2. ¿Conoce ud en que consiste un Plan de Gestión de Continuidad del Negocio?

1 respuesta



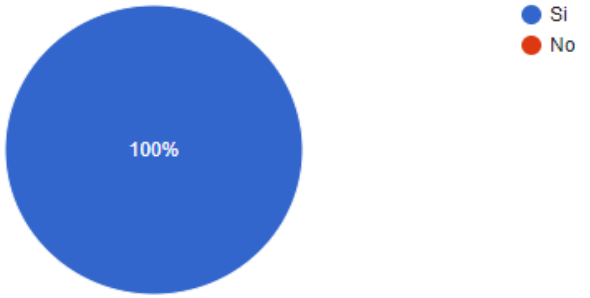
3. ¿En el departamento de las TI hay implementado un Plan de Gestión de Continuidad del Negocio?

1 respuesta



4. Existen un plan de contingencia en el caso de que sus procedimientos (procesos) fallen?

1 respuesta



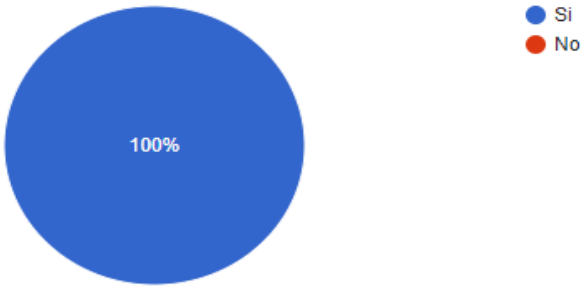
5. La interrupción en el funcionamiento normal de su departamento generaría alguna implicación legal y fiscal en caso de que se interrumpa dicha actividad?

1 respuesta

No estoy segura

6. Existe un responsable de seguridad de la información designado por la máxima autoridad de la UPC-SA?

1 respuesta



7. Estaría ud de acuerdo en implementar una norma o estándar que brinde seguridad de la información a la UPC-SA?

1 respuesta

Si, pero es decisión de la ala gerencia

8. Conoce ud los riesgos a los que está expuesta la información en su entorno laboral?

1 respuesta

No

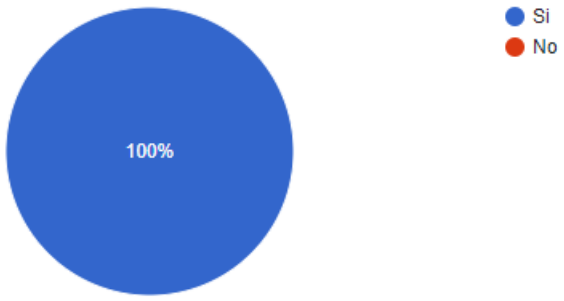
9. Identifique el periodo de mayor trabajo del año. ¿Hay alguna precaución en el caso de que se presente una emergencia en ese lapso?

1 respuesta

En el inicio de cada semestre academico

10. Considera que el Plan de Gestión de Continuidad del Negocio mejoraría los procesos con los que cuenta la UPC-SA actualmente?

1 respuesta



Anexo D. Diseño de encuesta para ser aplicado al personal administrativo de la Universidad Popular del Cesar, Seccional Aguachica.

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: _____

Nombre del encuestado(a): _____

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - ○ Si
   - ○ No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - ○ Con mucha frecuencia
   - ○ Frecuentemente
   - ○ Con poca frecuencia
   - ○ Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - ○ Nunca
   - ○ Casi nunca
   - ○ A menudo
   - ○ Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - ○ Si
   - ○ No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - ○ Si
   - ○ No
   - ○ NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - Si
   - No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - Si
   - No

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - Si
   - No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - Si
   - No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - Si
    - No
    - NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - Si
    - No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ○ No
    - ○ NS/NR

Anexo E. Diseño de entrevista para ser aplicado al personal administrativo de la Universidad Popular del Cesar, Seccional Aguachica.

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: _____

Nombre del entrevistado(a): _____

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?
2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?
3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?
4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?
5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?
6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?
7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?
8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?
9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?
10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

Anexo F. Diseño de lista de chequeo para ser aplicado al personal administrativo de la Universidad Popular del Cesar, Seccional Aguachica.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:			
OFICINA:			
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?			
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?			
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?			
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?			
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?			
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?			
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?			
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?			

¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?			
¿Los funcionarios aplican buenas prácticas de gestión de proyectos que satisfagan las necesidades y problemáticas que se presentan en la Universidad?			
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?			
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?			

Anexo G. Encuesta a Dirección Académica.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección académica.

Nombre del encuestado(a): Yiceth Alejandra González Duarte

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [ ] Frecuentemente
   - [x] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [ ] Nunca
   - [x] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [ ] Si
   - [x] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [ ] Si
   - [x] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   ☒ Si
   ○ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   ○ Si
   ☒ No
   ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   ○ Si
   ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   ○ Si
   ☒ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    ☒ Si
    ○ No
    ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    ☒ Si
    ○ No
    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - [x] Si
    - [ ] No
    - [ ] NS/NR

Anexo H. Encuesta a Dirección Administrativa y Financiera.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección administrativa y financiera

Nombre del encuestado(a): Juvenal Florez Vergara

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [x] Frecuentemente
   - [ ] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [ ] Nunca
   - [x] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [x] Si
   - [ ] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [x] Si
   - [ ] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ☒ Si
   - ○ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ○ Si
   - ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ○ Si
   - ☒ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - [x] Si
    - [ ] No
    - [ ] NS/NR

Anexo I. Encuesta a Oficina de Admisiones, Registro y Control Académico.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Centro de Admisiones, Registro y Control Académico

Nombre del encuestado(a): Deime Fernando Martínez Ruiz

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [x] Frecuentemente
   - [ ] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [ ] Nunca
   - [x] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [x] Si
   - [ ] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [ ] Si
   - [ ] No
   - [x] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ☒ Si
   - ○ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ○ Si
   - ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ○ No
    - ☒ NS/NR

Anexo J. Encuesta a Bienestar Institucional.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Bienestar Institucional

Nombre del encuestado(a): Flor Angela Moncada Ariza

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [ ] Frecuentemente
   - [x] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [ ] Nunca
   - [x] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [ ] Si
   - [x] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [x] Si
   - [ ] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ○ Si
   - ☒ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ○ Si
   - ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ☒ No
    - ○ NS/NR

Anexo K. Encuesta a Dirección de Departamento de Sistemas e Informática.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Departamento de Sistemas e Informática

Nombre del encuestado(a): Lizeth Badillo Durán

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [x] Frecuentemente
   - [ ] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [x] Nunca
   - [ ] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [x] Si
   - [ ] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [x] Si
   - [ ] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   ☒ Si
   ○ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   ☒ Si
   ○ No
   ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   ○ Si
   ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   ○ Si
   ☒ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    ☒ Si
    ○ No
    ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    ☒ Si
    ○ No
    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No
    - ○ NS/NR

Anexo L. Encuesta a Dirección de Departamento de Ciencias Ambientales y Sanitarias.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Dpto. Ciencias Ambientales y Sanitarias.

Nombre del encuestado(a): Rocio Ropero Pallares

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [ ] Frecuentemente
   - [x] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [x] Nunca
   - [ ] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [ ] Si
   - [x] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [ ] Si
   - [x] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ○ Si
   - ☒ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ☒ Si
   - ○ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ○ Si
    - ☒ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ○ No
    - ⊗ NS/NR

Anexo M. Encuesta a Dirección de Departamento de Ciencias Agroindustriales.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección Departamento de Ciencias Agroindustriales

Nombre del encuestado(a): Héctor Camilo Alvernia Verjel

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   ☒ Si
   ○ No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   ○ Con mucha frecuencia
   ☒ Frecuentemente
   ○ Con poca frecuencia
   ○ Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   ○ Nunca
   ○ Casi nunca
   ☒ A menudo
   ○ Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   ☒ Si
   ○ No
   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   ☒ Si
   ○ No
   ○ NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   ☒ Si
   ○ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   ○ Si
   ☒ No
   ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   ○ Si
   ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   ☒ Si
   ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    ☒ Si
    ○ No
    ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    ☒ Si
    ○ No
    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?

- [x] Si
- [ ] No
- [ ] NS/NR

Anexo N. Encuesta a Dirección de Departamento de Ciencias Administrativas.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Departamento de ciencias administrativas

Nombre del encuestado(a): Yazmin Hernández Álvarez

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - ○ Si
   - ☒ No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - ○ Con mucha frecuencia
   - ○ Frecuentemente
   - ○ Con poca frecuencia
   - ☒ Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - ○ Nunca
   - ☒ Casi nunca
   - ○ A menudo
   - ○ Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - ○ Si
   - ☒ No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - ○ Si
   - ☒ No
   - ○ NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ☒ Si
   - ○ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ○ Si
   - ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - [x] Si
    - [ ] No
    - [ ] NS/NR

Anexo O. Encuesta a Dirección de Departamento de Ciencias Económicas.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Economía

Nombre del encuestado(a): Luis Hernando Restrepo Sierra

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [ ] Frecuentemente
   - [x] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [ ] Nunca
   - [x] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [x] Si
   - [ ] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [x] Si
   - [ ] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ○ Si
   - ○ No
   - ☒ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ☒ Si
   - ○ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ☒ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ☒ No
    - ○ NS/NR

Anexo P. Encuesta a Dirección de Departamento de Ciencias Contables.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Contaduría pública

Nombre del encuestado(a): Miguel Antonio Piñerez Flórez

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - ○ Si
   - ☒ No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - ○ Con mucha frecuencia
   - ○ Frecuentemente
   - ○ Con poca frecuencia
   - ☒ Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - ○ Nunca
   - ○ Casi nunca
   - ☒ A menudo
   - ○ Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - ☒ Si
   - ○ No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - ○ Si
   - ☒ No
   - ○ NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ☒ Si
   - ○ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ○ Si
   - ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - [x] Si
    - [ ] No
    - [ ] NS/NR

Anexo Q. Encuesta a Coordinación de Tecnología Agropecuaria.

ENCUESTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Tecnología agropecuaria

Nombre del encuestado(a): Wilson Antonio Sánchez Hernández

Cantidad de preguntas 12

1. ¿Realiza backups (copias de seguridad) de información física y digital más relevante que se maneja en su oficina?
   - [x] Si
   - [ ] No

2. ¿Con que frecuencia realiza backups de la información más relevante que se maneja en su oficina?
   - [ ] Con mucha frecuencia
   - [ ] Frecuentemente
   - [x] Con poca frecuencia
   - [ ] Con ninguna frecuencia

3. ¿El personal administrativo recibe capacitaciones relacionados a las buenas prácticas para una gestión eficiente de la información?
   - [ ] Nunca
   - [x] Casi nunca
   - [ ] A menudo
   - [ ] Muy a menudo

4. ¿Sabe cómo proceder en caso de presentarse un incidente natural o un desastre causado por el hombre, a fin de proteger su integridad personal así como de la información crítica que se maneja en la dependencia en la cual labora?
   - [ ] Si
   - [x] No

   Rta _____

5. ¿Se llevan a cabo controles para proteger los equipos de cómputo e información contra software malicioso?
   - [ ] Si
   - [x] No
   - [ ] NS/NR

6. ¿En la dependencia en la que usted labora se implementan estrategias para mitigar los riesgos digitales que podrían presentarse?
   - ○ Si
   - ☒ No

7. ¿La universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos en su oficina?
   - ☒ Si
   - ○ No
   - ○ NS/NR

8. ¿En algún momento las actividades a su cargo se han visto afectadas por sanciones a la Universidad Popular del Cesar Seccional Aguachica debido a incumplimientos legales/contractuales?
   - ○ Si
   - ☒ No

9. ¿En la Universidad Popular del Cesar Seccional Aguachica se han presentado eventos (huelga, manifestaciones, motines, imposibilidad de acceder a las instalaciones) que interrumpan el normal cumplimiento de su labor?
   - ☒ Si
   - ○ No

10. ¿Existen estrategias para la prestación de servicios y la continuidad de las operaciones en caso de que exista la imposibilidad de acceder a las instalaciones de la Universidad ante la ocurrencia de un evento disruptivo?
    - ☒ Si
    - ○ No
    - ○ NS/NR

11. De acuerdo a su percepción ¿el uso de las TI mejora los procesos y ayuda a resolver amenazas que pueden presentarse en la Universidad Popular del Cesar Seccional Aguachica?
    - ☒ Si
    - ○ No

    Rta _____

12. ¿En la dependencia en la cual usted labora se efectúan iniciativas de uso y apropiación de proyectos de TI que se elaboren en la Universidad Popular del Cesar Seccional Aguachica?
    - ○ Si
    - ☒ No
    - ○ NS/NR

Anexo R. Entrevista a Dirección Académica.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección Académica

Nombre del encuestado(a): Yiceth Alejandra González Duarte

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Gestión Docencia.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Drive, disco duro.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Auditoria a la sede central.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Vicerrectoria General.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Dirección de programas, Biblioteca, Registro y Control, salas de informática, Investigación.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Muy poco.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: 1 año.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: No tengo conocimiento.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Interrumpe el proceso académico, daño de los equipos.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Sede Central.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: No.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Si.

Anexo S. Entrevista a Dirección Administrativa y Financiera.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección Administrativa y Financiera

Nombre del encuestado(a): Juvenal Flórez Vergara.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Contratación.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Disco duros, medios físicos, Google Driver, software de ORFEO tipo documental.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Utilización de mecanismos de descarga en el driver u ORFEO para descargas y recuperación.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Si.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Vicerrectoría, Dirección Académica, investigación.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Anualmente, se incluye en plan de capacitación.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: Nunca.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Trabajar desde equipos periféricos.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Ninguno.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: No.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: No.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Si.

Anexo T. Entrevista a Oficina Registro y Control Académico.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Centro de Admisiones, Registro y Control Académico.

Nombre del encuestado(a): Deimer Fernando Martínez Ruiz

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Admisión y Grados, por el nuevo aplicativo.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Equipo portátil autorizado por la institucional, para continuar con mis labores.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Reportar a oficina de sistemas y a Control Interno Disciplinario.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Dirección Académica.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Dirección Administrativa y Financiera y Consejo de Programas De Seccional.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Anualmente cuando hay alguna actualización.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: Nunca.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Reportar a la oficina de sistema de la sede central y si hay daños materiales o de equipos a la oficina de almacén e inventarios.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Atención al público y comunidad estudiantil.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Externos no, internos si entre otras dependencias.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: No.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Hay una póliza vigente.

Anexo U. Entrevista a Bienestar Institucional.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Bienestar Institucional.

Nombre del encuestado(a): Flor Angela Moncada Ariza.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Todos los procesos son importantes.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Memoria y drive son los mecanismos utilizados para la protección de la información. En cuanto a la continuidad de los procesos se hace gestión y se busca apoyo.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Informar a los superiores.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Bienestar Institucional es transversal y dependemos de la Oficina de Dirección Administrativa y Financiera.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: No.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Casi nunca.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: No ha habido.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Desconectar el equipo y se tiene la precaución de estar guardando permanentemente.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Estadísticas e información general de Bienestar Institucional.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Si.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: No solo pérdidas. No se cumplirían metas, indicadores y otros.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: No lo se.

Anexo V. Entrevista a Dirección de Departamento de Sistemas e Informática.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Sistemas e Informática.

Nombre del encuestado(a): Lizeth Badillo Durán.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: En el Departamento de Sistemas e Informática, la información más crucial y delicada incluye datos sobre el vortal, asignaciones académicas, horarios y documentos que respaldan el documento maestro, así como el plan de mejoramiento del programa. Estos elementos constituyen la columna vertebral de nuestras operaciones, asegurando la efectividad y el progreso continuo de nuestros programas educativos. La gestión adecuada de esta información es esencial para garantizar el funcionamiento eficiente y la mejora constante de nuestro departamento.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: El Drive representa nuestro sistema principal para almacenar la información mencionada anteriormente. Este robusto sistema nos proporciona una plataforma segura y accesible, permitiéndonos gestionar de manera eficiente los datos críticos del Departamento de Sistemas e Informática. Gracias a Drive, podemos garantizar la integridad y disponibilidad de nuestra información, lo que es esencial para nuestro éxito y progreso continuo.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: En caso de robo de archivos o filtración de información crucial, es imperativo que notifiquemos el incidente a la oficina correspondiente. En el caso de los archivos del vortal, nos dirigimos al departamento de Registro y Control, quienes llevan a cabo una auditoría exhaustiva del sistema. En cuanto a los archivos almacenados en Drive, procedemos enviando un correo a la dirección del programa para informar el incidente. Posteriormente, se realiza una auditoría detallada para evaluar la magnitud del problema y tomar las medidas adecuadas.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Si.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Todos.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Nunca.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: Nunca.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: No lo conozco.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: 1. La falta de energía puede afectar la comunicación interna a través de correos electrónicos y sistemas de mensajería, lo que dificulta la coordinación y la colaboración entre los miembros del departamento.

   2. La falta de energía eléctrica puede dejar sistemas y redes vulnerables, lo que aumenta el riesgo de intrusiones y ciberataques.

   3. La interrupción en el suministro eléctrico puede causar la pérdida de datos y progreso en proyectos de desarrollo de software u otros proyectos tecnológicos en curso.

   4. Los servidores y sistemas de prueba pueden apagarse, lo que lleva a la suspensión temporal del desarrollo y las pruebas de software.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Si.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: El impacto varía según el día; si se trata de un día de pagos, ciertamente se vería afectado. Sin embargo, en un día normal, las consecuencias no serían graves.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: No conozco.

Anexo W. Entrevista a Dirección de Departamento de Ciencias Ambientales y Sanitarias.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Ciencias Ambientales y Sanitarias.

Nombre del encuestado(a): Rocio Ropero Pallares.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Planeación académica y asignación de carga académica, diseño de horarios, seguimiento de gestión docencia, proyección de presupuesto.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Guardar copia de los archivos en disco duro y algunos en drive.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Reportar el incidente a Gestión TIC.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: A Dirección Académica.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Planeación Académica (Asignación docente, horarios, proyección de presupuesto), renovación de registros calificados, autoevaluación, reforma curricular, gestión docencia, elaboración y seguimiento al plan de acción anual.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

Respuesta: Semestralmente.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: Nunca.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Esperar a que se reestablezca.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Todos los mencionados en el numeral 5.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Si, Practicas de estudiantes, procesos de grado.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: Así es, se deja de captar recursos y producir indicadores de calidad en los programas.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: No tengo conocimiento.

Anexo X. Entrevista a Dirección de Departamento de Ciencias Agroindustriales.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Ciencias Agroindustriales.

Nombre del encuestado(a): Héctor Camilo Alvernia Verjel.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Información relevante del programa como la carga académica de cada periodo, base de datos de los docentes, plan de acción de cada año, proyección social.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Drive, disco duro, contraseñas.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Asistencia técnica del equipo TIC.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Si.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Necesidades de asignaturas, actividades de proyección social

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Trimestral.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: Esporádicamente.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Suspender actividades.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Administrativos y académicos.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: No.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: Si.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Si.

Anexo Y. Entrevista a Dirección de Departamento de Ciencias Administrativas.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Ciencias Administrativas.

Nombre del encuestado(a): Yazmin Hernández Álvarez.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Inscripción de estudiantes - manejo y sistematización de proyectos

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: De manera física en la oficina y algunas en el correo correspondiente.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: No hay definido un acción a seguir.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Si.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Registro y control, planeación, dirección académica.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: No se cuenta con ese plan.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: No se cuenta con simulacros.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Planta eléctrica.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Todos los procesos.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Afectaría la sede principal.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: Si.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: No conozco.

Anexo Z. Entrevista a Dirección de Departamento de Ciencias Económicas.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Ciencias Económicas.

Nombre del encuestado(a): Luis Hernando Restrepo Sierra.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: Procesos de renovación de registros, manejo de autoevaluación, control estadístico de procesos y control de sistemas de información.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Manejo de información en línea.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Realizar la notificación de la novedad a la dependencias asociadas.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Se está bajo la dirección de Dirección Académica.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Comités del programas, equipos de trabajo, docentes y estudiantes.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Mínimo una vez al año.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

   Respuesta: No se han realizado.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Inspección de que no hayan sufrido afectaciones el hardware y los archivos en inventarios.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: No habría pérdidas de los archivos porque están en línea, pero desde luego se afectarían la infraestructura física.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Si.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: Si.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Si.

Anexo AA. Entrevista a Dirección de Departamento de Ciencias Contables.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Dirección de Departamento de Ciencias Contables.

Nombre del encuestado(a): Miguel Antonio Piñerez Flórez.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: SST.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Drive.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Plan de mejoramiento.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: Si.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Todos.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: Semestral y/o anual.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

Respuesta: En mis 2 años de labor, ninguno.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Esperar a que se restablezca el servicio.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: Todos.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Pregunta confusa, no puedo dar fe de lo que se pueda presentar o suceder en otras instituciones.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: Lógicamente.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Si.

Anexo BB. Entrevista a Coordinación de Tecnología Agropecuaria.

ENTREVISTA

Objetivo: Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar, Seccional Aguachica.

Oficina: Coordinación de Tecnología Agropecuaria.

Nombre del encuestado(a): Wilson Antonio Sánchez Hernández.

Cantidad de preguntas 12

1. ¿Cuáles son los procesos más críticos que manejan en su oficina?

   Respuesta: informacion de estudiantes y docentes.

2. ¿Qué mecanismo utiliza para la protección de la información y la continuidad de los procesos más relevantes que maneja en su oficina?

   Respuesta: Ninguna.

3. ¿Cuál es la acción a seguir del personal administrativo en caso de que ocurra robo de archivos o se filtre información importante?

   Respuesta: Informar a la directiva.

4. ¿El departamento en el cual labora obedece a las funciones de otros departamentos?

   Respuesta: No.

5. ¿Cuáles procesos y/o departamentos dependen de la función que se realiza en el departamento en la cual usted labora?

   Respuesta: Gestión docencia – estudiantes.

6. ¿Cada cuánto se capacita y se forma al personal administrativo para atender y afrontar eventos no deseados que interrumpan el normal desarrollo de sus actividades?

   Respuesta: No hay capacitaciones en el tema.

7. ¿Cada cuánto se realizan simulacros para determinar los tiempos de respuesta y recuperación ante la posible interrupción de sus operaciones que puedan representar una amenaza significativa?

Respuesta: No hay.

8. ¿En caso de que ocurra un fallo eléctrico cual es el procedimiento a seguir?

   Respuesta: Desconectar los equipos.

9. ¿Cuáles procesos o actividades se verían afectados si se llegase a materializar un evento como el anteriormente mencionado?

   Respuesta: La seguridad de la oficina y de los medios informáticos y físicos.

10. Si se llegase a presentar un evento catastrófico (inundación, terremotos, huracanes, terrorismo) que ponga en riesgo las instalaciones de la Universidad Popular del Cesar seccional Aguachica y su operatividad ¿afectaría a otras instituciones y sus procesos?

    Respuesta: Si.

11. ¿Considera usted que si se llegase a presentar la interrupción de un proceso crítico, este generaría pérdidas financieras de gran magnitud?

    Respuesta: Si.

12. ¿Es de su conocimiento si la universidad Popular del Cesar Seccional Aguachica tiene una póliza o cuenta con los recursos financieros para afrontar una posible interrupción de los procesos críticos llevados a cabo en su oficina?

    Respuesta: Si existe.

Anexo CC. Lista de chequeo a Dirección Académica.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	YICETH ALEJANDRA GONZALEZ DUARTE		
OFICINA:	DIERCCION ACADÉMICA		
PREGUNTAS	CUMPLE		OBSERVACIONES
	SI	NO	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?	X		
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?	X		
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?	X		

Anexo DD. Lista de chequeo a Dirección Administrativa y Financiera.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	JUVENAL FLOREZ VERGARA		
OFICINA:	DIRECCION ADMINISTRATIVA Y FINANCIERA		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?	X		**Acuerdo no. 019 fecha: 5 de octubre de 2020**
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		**Página web institucional**
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		**Acuerdo no. 019 fecha: 5 de octubre de 2020**
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?	X		
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		**Plan de capacitación docentes y administrativos**
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?		X	

Anexo EE. Lista de chequeo a Oficina de Admisiones, Registro y Control Académico.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO: DEIME FERNANDO MARTINEZ RUIZ			
OFICINA: CENTRO DE ADMISIONES REGISTRO Y CONTOL ACADEMICO			
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?	X		
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?			**Lo desconozco**
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		**Muy pocas veces**
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?		X	
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?	X		

Anexo FF. Lista de chequeo a Bienestar Institucional.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	Flor Ángela Moncada Ariza		
OFICINA:	Bienestar Institucional		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?		X	**Se requiere orientación, capacitación sobre el tema**
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?			**Desconozco**
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?			**Desconozco**
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?		X	
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?			**Personalmente, este aspecto se considera de trascendencia**
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?			**Desconozco**

Anexo GG. Lista de chequeo a Dirección de Departamento de Sistemas e Informática.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	Lizeth Badillo Duran		
OFICINA:	Coord. Ing. De Sistemas		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?	X		
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?	X		
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		**Solo a los involucrados**
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		**Solo a los involucrados**
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?			**Desconozco**

Anexo HH. Lista de chequeo a Dirección de Departamento de Ciencias Ambientales y Sanitarias.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	ROCIO ROPERO PALLARES		
OFICINA:	DEPARTAMENTO DE CIENCIAS AMBIENTALES Y SANITARIAS		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?		X	
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?		X	**DESCONOZCO SI EXISTE**
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?		X	
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?		X	
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?			**DESCONOZCO SI EXISTE**
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?		X	

Anexo II. Lista de chequeo a Dirección de Departamento de Ciencias Agroindustriales.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	HÉCTOR CAMILO ALVERNIA VERJEL		
OFICINA:	DEPARTAMENTO DE CIENCIAS AGROINDUSTRIALES		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?	X		
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes pùblicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?		X	
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?	X		
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?		X	

Anexo JJ. Lista de chequeo a Dirección de Departamento de Ciencias Administrativas.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	YAZMIN HERNANDEZ ALVAREZ		
OFICINA:	DEPARTAMENTO DE CIENCIAS ADMINSITRATIVAS		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?		X	
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?		X	
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?	X		

Anexo KK. Lista de chequeo a Dirección de Departamento de Ciencias Económicas.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	LUIS HERNANDO RESTREPO SIERRA		
OFICINA:	DTO DE ECONOMIA		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?	X		
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?		X	**No estoy seguro de que se tenga**
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?	X		
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?		X	**Se está en proceso de implementación**
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?		X	
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?		X	

Anexo LL. Lista de chequeo a Dirección de Departamento de Ciencias Contables.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	MIGUEL PIÑEREZ		
OFICINA:	CONTADURÍA PÚBLICA		
PREGUNTAS	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?			**NO SÉ**
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?			**NO SÉ**
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?	X		
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?		X	
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?	X		
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?		X	

Anexo MM. Lista de chequeo a Coordinación de Tecnología Agropecuaria.

LISTA DE CHEQUEO			
OBJETIVO	Diagnosticar el estado actual en cuanto a la aplicación de Gobierno Digital en la Universidad Popular del Cesar Seccional Aguachica.		
NOMBRE COMPLETO:	WILSON ANTONIO SANCHEZ HERNANDEZ		
OFICINA:	TECNOLOGIA AGROPECUARIA		
PREGUNTAS	CUMPLE		OBSERVACIONES
	SI	NO	
¿Se garantiza la protección de los datos personales, la conservación de documentos electrónicos, la transparencia y accesibilidad de la información, la adecuación tecnológica, así como la responsabilidad e igualdad en relación al uso los medios electrónicos?		X	
¿La universidad cuenta con un instrumento por medio del cual proporciona información a los diferentes públicos objetivos?	X		
¿La universidad cuenta con una política de seguridad de la información que permita proteger la integridad, confidencialidad y disponibilidad de los datos?	X		
¿La Universidad cuenta con un Plan Estratégico de las Tecnologías de la Información y Comunicaciones?		X	
¿Los funcionarios hacen uso de las TICs con la finalidad de mejorar/optimizar los procesos a su cargo?	X		
¿Los funcionarios reciben capacitación y/o sensibilización en Tecnologías de la Información y la Comunicación?		X	
¿Los funcionarios reconocen la importancia del uso de las TI para la toma de decisiones?	X		
¿La universidad pone a disposición de los ciudadanos los datos generados por la academia?	X		
¿La universidad comunica y promueve el uso de datos abiertos a la población estudiantil, administrativos y ciudadanos?		X	
¿Los funcionarios aplican buenas prácticas de gestión de proyectos, que satisfagan las necesidades y problemáticas que se presentan en la Universidad?	X		
¿Se reconocen las ventajas que brinda la prestación de servicios ciudadanos digitales?	X		
¿La universidad cuenta con las competencias necesarias para efectuar funciones de arquitectura empresarial?		X	

Anexo NN. Diseño de la entrevista aplicada a los lideres de las áreas de Dirección Académica, Dirección Administrativa y Financiera y Centro de Admisiones, Registro y Control Académico de la Universidad Popular del Cesar, Seccional Aguachica.

ENTREVISTA

Objetivo: Recolectar información sobre los procesos de las principales dependencias de la Universidad Popular del Cesar Seccional Aguachica, la información que se provea será usada para la valoración del Análisis de Impacto del Negocio (BIA).

1. ¿Cuáles son las funciones y procesos que apoyan la misión y los objetivos a alcanzar en su dependencia?

2. Por favor indique el nivel de impacto (valor negativo) de una interrupción de los procesos de su dependencia de acuerdo al esquema de valoración A, B o C.

3. ¿Cuál es el nivel de tolerancia a fallas (horas, días) que puede soportar cada uno de los procesos una vez efectuada una interrupción/falla?

4. ¿Qué funciones críticas de la dependencia apoyan a cada uno de los procesos o servicios que se manejan en su oficina y por favor enliste aquellos procesos considerados críticos?

5. De acuerdo a su percepción ¿cuál considera que es el tiempo máximo de inactividad (MTD) que cada uno de los procesos de su dependencia puede tolerar antes de que se produzcan consecuencias desastrosas para la dependencia y para la universidad?

6. Señale la prioridad de recuperación de cada uno de los procesos críticos de su dependencia.

   Por ejemplo, un proceso que tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia (Ejemplo tomado de MinTIC).

7. ¿Cuáles son los recursos críticos (activos, servicios, aplicaciones, módulos o sistemas) que apoyan a los procesos críticos de su dependencia?

8. Por favor indique el Tiempo de Recuperación Objetivo (RTO), Tiempo de Recuperación de Trabajo (WRT) y el Punto de Recuperación Objetivo (RPO) de cada uno de los procesos críticos de su dependencia.