CORPORACIÓN UNIVERSITARIA UNITEC	**RESUMEN ANALÍTICO DE INVESTIGACIÓN (RAI)**		
	Código:	**Fecha:**	**Versión No.**

Fecha de elaboración: 29.04.2023 [del RAI]			
Tipo de documento	TID:	Obra Creación:	Proyecto Investigación:
Título	ESTRATEGIAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN Y DEMÁS RECURSOS INTERNOS DE UNA RED INFORMÁTICA, MEDIANTE LAS BUENAS PRÁCTICAS DE LA NORMA ISO 27000 DE CONTINUIDAD DEL NEGOCIO EN UNA ENTIDAD FINANCIERA DE OPERACIÓN NACIONAL		
Autor(es)	**Robert Castro Lisca**		
Tutor(es)	**Fabio Antonio González**		
Fecha de finalización	13.04.2023 [del proyecto de investigación]		
Temática			
Tipo de investigación	**Cualitativa**		

Resumen

La norma ISO 27000 permite el desarrolló de buenas prácticas para las organizaciones. Las buenas prácticas de continuidad del negocio hacen parte de la política de seguridad de la información, como el uso restringido de la información.

La continuidad del negocio el siguiente trabajo se realiza con la finalidad de evaluar los posibles riesgos que se pueden presentar en una entidad financiera de operación nacional ante las eventuales debilidades que pueda presentar los procesos, planes y estrategias de continuidad del negocio en el interior de la organización.

El objetivo de este trabajo es evaluar las buenas prácticas de la ISO 27000 en la dirección de continuidad del negocio en la organización financiera de operación Nacional.

Dentro de los resultados obtenidos en este trabajo están: El conocimiento de la estructura de la dirección de continuidad del negocio apoyado por el centro de cómputo de contingencia y el Centro de operación de contingencia como línea de apoyo vital a los procesos críticos de la entidad financiera.

Palabras clave

Activo de Información, amenazas, Aplicaciones, Autenticidad, BIA, confidencialidad, Disponibilidad, incidente, integridad, Metro Mirror, planificación, riesgo, RTO, seguridad, Servidor, Telecomunicaciones, vulnerabilidad

Planteamiento del problema

Esta investigación pretende evaluar las posibles falencias en el sistema de continuidad del negocio bajo las buenas prácticas de la norma ISO 27000.La presentación actual de la problemática se centra en los siguientes aspectos, el antes, el durante y el después de ejecutar las diferentes pruebas de recuperación tecnológicas y de recuperación de procesos.

Antes: hace referencia a los preparativos previos a la materialización de un riesgo, el enfoque esta dado al alistamiento de la infraestructura, la logística y copias de respaldo de los Activo de Información. De acuerdo al SIC.gov.co son Datos o información propiedad de una empresa u organización. Son almacenados en medio físico o lógico y que es considerada como sensitiva o critica para el cumplimiento de objetivos misionales.

A nivel tecnológico se preparan dos frentes los planes de recuperación tecnológica en infraestructura que hace referencia a todos los dispositivos de almacenamiento, Storage, granja de servidores dispositivos de comunicación como switch, encriptadores, nexus, Access point, entré otros.

De acuerdo con la información tomada de la intranet corporativa de la entidad (2023)

: Creada en el año 1990 como una entidad de ahorro y vivienda.

En el año 2000 se funciona con dos cooperativas y otra entidad de ahorro y vivienda convirtiéndose en un banco con presencia a nivel nacional

Desde su inicio y como uno de sus pilares la organización se ha destacado por estar siempre a la vanguardia tecnológica lo cual le ha permitido el reconocimiento en el sector financiero.

Igualmente, en ir de la mano de la tecnología por la naturaleza de su operación se ha destacado porque sus procesos sean organizados eficientes y seguros.

Como es parte de sus principios la entidad financiera siempre ha buscado las estrategias normas y procedimientos que le permitan respaldar y proteger no solo sus procesos sino también uno de sus principales activos la información y data tanto de sus usuarios internos como externos.

La entidad hace presencia alrededor del país en las 10 principales ciudades y 23 poblaciones estratégicas con un total de 277 oficinas.

Su sede principal está ubicada en la ciudad de Bogotá donde se cuenta con más de 800 empleados operando desde dirección general.

Pregunta

¿Cómo evaluar las Estrategias de seguridad para la protección de la información y demás recursos internos de una red informática, mediante las buenas prácticas de la norma ISO 27000 de continuidad del negocio en una entidad financiera de operación nacional?

Objetivos

Objetivo General

Como evaluar las estrategias de seguridad de la información y demás recursos internos e un a red informática, mediante las buenas prácticas de la norma ISO 27000 de continuidad del negocio dentro de una entidad financiera de operación nacional.

Objetivos Específicos

- Conocer las generalidades de la infraestructura en producción de la entidad financiera.
- Conocer las generalidades de la infraestructura en contingencia de la entidad financiera.
- Evaluar las políticas de seguridad de la información que actualmente maneja la Entidad Financiera.
- Definir la seguridad física y del entorno de la información.
- Conocer los procesos críticos que tiene definida la entidad y como son respaldados
- Evaluar como la entidad Protege, preserva y administra la información, junto con los equipos y recursos tecnológicos adecuados.
- Caracterizar los procedimientos y protocolos ante una situación de ciberataque.
- Describir los escenarios más críticos o propicios en los cuales se puede ver expuesta ante un ciberataque la Entidad Financiera.
- Analizar qué controles de acceso cuenta la entidad en sus centros de cómputo tanto de producción como el centro de cómputo de contingencia y que fortalezas y debilidades existen a raíz de su ubicación geográfica.

Marco teórico

Resuma únicamente los principales referentes teóricos o artísticos que siguió su trabajo. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Dentro de la entidad bancaria se cuenta con una granja de servidores de 820 servidores de los ellos cuales 600 están configurados como servidores virtuales 10 servidores físicos y 210 con sistema operativo AIX propio del proveedor de tecnología IBM los cuales prestan un servicio una población promedio de 450 usuarios distribuidos en las principales ciudades de Colombia y algunas ciudades y municipios intermedios donde se ofrecen los servicios financieros y bancarios al público en general.

Como principal mecanismo de respaldo esta organización, se cuenta con la dirección de continuidad del negocio que a su vez es compensable del centro de cómputo

alterno ubicado aproximadamente 5 kilómetros a la salida de la ciudad de Bogotá sede principal de la organización y donde además se encuentra la dirección general y administrativa de la entidad.

Adicionalmente también se cuenta con un centro de operación de contingencia donde se dispone de 100 puestos de trabajo y desde donde se puede operar en caso de presentarse una situación de no disponibilidad de los sitios propios de producción, allí están configurados principalmente los proceso llamados críticos del banco.

De acuerdo al autor Smith.W en su libro Planes de contingencia centro de cómputo (2019)

Los Planes de Contingencias le permitirán mantener la continuidad de sus sistemas de información frente a eventos críticos, de su entidad y minimizar el impacto negativo sobre la misma, sus empleados y usuarios. Deben ser parte integral de su organización y servir para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

Método

Resuma únicamente los principales elementos metodológicos que empleó en su investigación. Señale los números de las páginas de su documento en los que se encuentra la información completa.

De acuerdo al análisis de la investigación y acciones correctivas que van a ser presentadas para la evaluación y mejor toma de decisión en el ámbito de la seguridad informática, hemos encontrado que lo realizaremos basándonos en el siguiente método de investigación:

Método Cualitativo: De nuestras hipótesis e ideas debemos llegar a una conclusión, para que así tanto nosotros como la empresa podamos tomar las acciones correctivas a seguir para asegurar el cumplimiento de lo propuesto.

De acuerdo a Baez.J en su libro Investigación Cualitativa, es el conjunto de todas las cosas que se hacen para seguir la pista de los mercados y encontrar los

rasgos de las personas y a las cosas sus propiedades y atributos sean estas o estos naturales o adquiridos.

Resultados, hallazgos u obra realizada

Presente el resumen de los principales resultados o hallazgos de su investigación o una sinopsis de la obra creada. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Se conoció la generalidad de la infraestructura tanto en el ambiente de producción como en ambiente de contingencia y se compararon los dos centros de cómputo los cuales trabajan de manera sincrónica y sus capacidades son muy similares.

Dentro de la evaluación de las politicas de seguridad de la entidad financiera están sustentadas principalmente en dos áreas administradoras, Seguridad de la información y Riesgo, dos áreas de apoyo que ejecutan las politicas que son seguridad informática y continuidad del negocio y otras áreas de apoyo como telemática y el área de telecomunicaciones.

Los dueños de proceso que son generalmente los jefes o directores del área desde donde opera el proceso los responsables de reportar la materialización de un riesgo como primera instancia al director de continuidad o la dirección de seguridad de la información igualmente está establecido dentro de la organización un comité de riesgo que también está en la capacidad de toma de decisiones frente a estas situaciones.

Dentro de la seguridad física de la información se encuentran en la organización los dos principales dispositivos de almacenamiento llamados Storage uno Z vs y vm y el XIV

El Z que es administrado por un tercero IBM pero supervisado por el área de System que hace parte de la gerencia de infraestructura de la organización es el encargado de almacenar la data transaccional de entidad a nivel nacional por ahí pasan todos los movimientos financieros de la organización y es llamada la alcancía porque ahí

está hospedado el dinero, tiene la par en el centro de cómputo de contingencia y siempre se encuentran conectados de manera sincrónica, para su respaldo también cuenta con copia primarias, secundarias y terciarias, y almacenamiento histórico en cintas.

El segundo Storage que es el XIV es administrado por el área de infraestructura de La organización y es principalmente donde se hospedan los aplicativos y data de procesos de la organización también ahí se encuentran los archivos vitales de cada área, están las bases de datos de la aplicaciones y desarrollos de la organización.

El acceso físico a los centros de cómputos esta dado por medio de puertas biométricas, registro por planillas, autorizaciones dadas y exclusivamente por el director o el gerente de infraestructura a personal restringido, bitácora de actividades, cuenta con sistema cerrado de cámaras las cuales graban 7 días por 24 horas y están monitoreadas por el centro de cómputo.

Esta área esta respalda por ups contratadas a terceros y cuenta con conexión directa a la planta eléctrica del edifico con una promesa de interrupción en caso de falla de fluido eléctrico de máximo 5 minutos tiempo que operarían las Ups en caso de ser requerido.

Sistema de detección de humo con extintores de gas no agua ya que este sistema es especial para operaciones donde hay servidores equipos electrónicos y centros de cómputo.

Conclusiones

Presente el resumen de las conclusiones a las que llegó. Señale los números de las páginas de su documento en los que se encuentra la información completa.

Luego de presentar los resultados, se evalúa que los procesos, pruebas, estrategias y metodología presentada por el área de continuidad del negocio, dentro de la organización presenta y refleja un alto grado de madurez ya que ante los riesgos materializados que conllevaron a las activaciones reales de contingencias, se ha tenido respuesta en un tiempo más que aceptable a la promesa de RTO (tiempo de recuperación Objetivo) de 6.5 horas, las activando sus protocolos y estrategias y cumpliendo en todas

las contingencias históricas. Frente hipótesis propuestas Es posible evaluar los riesgos de los procesos de continuidad del negocio en una entidad financiera de cubrimiento nacional, gracias a la herramienta DOFA producto de la observación en los procesos, la metodología las buenas y las malas prácticas en el desarrollo de las actividades propias del área evaluada y del desarrollo de la actividad de entrevista al director del área de continuidad del negocio de la entidad financiera estudiada se pudo evaluar aspectos relevantes que se describen a continuación:

Durante las pruebas de recuperación tecnológicas y al finalizar las mismas, por la dinámica de estos ejercicios, los analistas e ingenieros resuelven los inconvenientes que se generen en ese momento, pero muchas veces ese conocimiento en resolución de inconvenientes no queda debidamente registrado en un manual o documentación oficial de la prueba. Se sugiere y surge la necesidad de realizar una reunión de cierre de prueba para ajustar inconvenientes, oficializar documentación, validar formatos y registros y así evitar reprocesos que se presentan en las pruebas posteriores.

Se evidencio que existe alto grado de rotación en el personal crítico de los procesos y al ser ellos que desarrollarían las contingencias, suele suceder que ese personal se retira de la organización y en bajo índice hay una persona igualmente capacitada para sumir este rol.

Productos derivados

Referencie los artículos, libros, capítulos de libro, ponencias, etc., que fueron resultado de su proceso investigativo.

PROYECTO DE INVESTIGACIÓN.
ESTRATEGIAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN Y DEMÁS RECURSOS INTERNOS DE UNA RED INFORMÁTICA, MEDIANTE LAS BUENAS PRÁCTICAS DE LA NORMA ISO 27000 DE CONTINUIDAD DEL NEGOCIO EN UNA ENTIDAD FINANCIERA DE OPERACIÓN NACIONAL

Robert Castro Lisca
Cód. 12226022

Corporación universitaria UNITEC

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SEMINARIO DE INVESTIGACIÓN II / SEMANAS - CP - 122A3

Bogotá
Lunes, 10 de abril de 2023

PROYECTO DE INVESTIGACIÓN.
ESTRATEGIAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN Y DEMÁS RECURSOS INTERNOS DE UNA RED INFORMÁTICA, MEDIANTE LAS BUENAS PRÁCTICAS DE LA NORMA ISO 27000 DE CONTINUIDAD DEL NEGOCIO EN UNA ENTIDAD FINANCIERA DE OPERACIÓN NACIONAL

Robert Castro Lisca
Cód. 12226022

Presentado para obtener el título de: Especialista en Seguridad de la Información

Ingeniero FABIO ANTONIO GONZALEZ MENDIETA

Corporación universitaria UNITEC
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
Bogotá
Lunes, 10 de abril de 2023

DEDICATORIA

Dedicado este trabajo a la memoria de la mujer que me dio la vida y que me acaba de dejar en este mundo, pero desde el cielo me acompaña y da la fuerza y apoyo y que es un Ángel que me estará cuidando por siempre.

A mi esposa, quien es mi compañera de vida, apoyo y ayuda en todos los momentos buenos y malos de mi vida.

A mí a amado hijo que es la inspiración y fuente de todo lo que hago.

AGRADECIMIENTOS

El presente proyecto fue realizado en la ciudad de Bogotá para la corporación universitaria UNITEC como parte de mi formación como especialista en seguridad de la información y fue construido gracias a las siguientes personas.

Al Ingeniero Fabio Antonio González, quiero agradecerle por la dedicación en cada una de las sesiones que nos reunimos y gracias por compartir su conocimiento y valioso tiempo por lo cual pude realizar la investigación y trabajo que en este momento presento.

A mi familia deseo agradecerles el tiempo qué deje de compartir en especial los fines de semana que era el tiempo de ellos y que ese esfuerzo se vea recompensado y dedicado también para ellos.

Contenido

Objetivo General 5
Objetivos Específicos 5
DEDICATORIA 3
AGRADECIMIENTOS 4
TABLA DE ILUSTRACIONES 7
Resumen. 8
ABSTRACT 10
Palabras claves. 12
1. PLANTEAMIENTO DEL PROBLEMA 13
1.1 JUSTIFICACIÓN. 17
1.2 PREGUNTA PROBLEMA 21
1.3 OBJETIVOS 22
1.3.1 Objetivo General 22
1.3.2 Objetivos Específicos 22
2. MARCO TEÓRICO Y ESTADO DEL ARTE 23
2.1 Antecedentes 23
2.1.1 Marco conceptual 26
2.2 Marco Referencial. 30
2.3 Plan de recuperación de procesos (PRP) 33
2.4 Plan de recuperación tecnológico (DRP). 34
2.5 Plan de emergencias. 37
2.6 Marco legal. 38
Estado del arte. 41
3. MARCO METODOLÓGICO 43
3.1 Hipótesis planteada 45

Hipótesis Nula 45
3.2 Método de investigación 45
3.3 Instrumentos para la investigación 46
Oportunidades. 47
Fortalezas. 47
Amenazas 48
3.4 Instrumento de investigación la Entrevista 49
4. RESULTADOS Y HALLAZGOS. 53
5. CONCLUSIONES 55
6. REFERENCIAS BIBLIOGRÁFICAS 56

TABLA DE ILUSTRACIONES

Ilustración 1 Escenarios de afectación y estrategia establecida 15
Ilustración 2 Escenarios de afectación y estrategia establecida 15
Ilustración 3 Escenarios de afectación y estrategia establecida 16
Ilustración 4 Roles y responsabilidades de los lideres procesos de negocio 17
Ilustración 5 Fases BCP 19
Ilustración 6 Mapa de calor Impacto y Probabilidad 28
Ilustración 7 Mapa de calor Impacto y Probabilidad fuente Mintic 29
Ilustración 8 Mapa conceptual del sistema de gestión de Continuidad del Negocio 32
Ilustración 9 Ciclo de los planes de recuperación de los Procesos 34
Ilustración 10 Estructura Organizacional DRP 35

Resumen.

La norma ISO 27000 permite el desarrolló de buenas prácticas para las organizaciones. Las buenas prácticas de continuidad del negocio hacen parte de la política de seguridad de la información, como el uso restringido de la información.

La continuidad del negocio el siguiente trabajo se realiza con la finalidad de evaluar los posibles riesgos que se pueden presentar en una entidad financiera de operación nacional ante las eventuales debilidades que pueda presentar los procesos, planes y estrategias de continuidad del negocio en el interior de la organización.

El objetivo de este trabajo es evaluar las buenas prácticas de la ISO 27000 en la dirección de continuidad del negocio en la organización financiera de operación Nacional.

Dentro de los resultados obtenidos en este trabajo están: El conocimiento de la estructura de la dirección de continuidad del negocio apoyado por el centro de cómputo de contingencia y el Centro de operación de contingencia como línea de apoyo vital a los procesos críticos de la entidad financiera.

De acuerdo a Ladino.a (2019) La norma ISO 27000 es certificable. Esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación. Antes de solicitar la auditoría las empresas necesitan contar con un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI debe estar implementado en la empresa como mínimo con tres meses de antelación.
Cada uno de los puntos exigidos en la norma pertenece a una etapa de un proceso: Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar), que se aplica para estructurar todos los procesos del SGSI. El SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes.

De acuerdo con la anterior y dada la experiencia y la madurez del proceso dentro dela organización financiera, liderada por los dueños de proceso que son generalmente los jefes o directores del área desde donde opera el proceso los responsables de reportar la materialización de un riesgo como primera instancia al director de continuidad o la dirección de seguridad de la información igualmente está establecido dentro de la organización un comité de riesgo que también está en la capacidad de toma de decisiones frente a estas situaciones.

Dentro de la evaluación de las politicas de seguridad de la entidad financiera están sustentadas principalmente en dos áreas administradoras, Seguridad de la información y Riesgo, dos áreas de apoyo que ejecutan las politicas que son seguridad informática y continuidad del negocio y otras áreas de apoyo como telemática y el área de telecomunicaciones.

Según Intranet corporativa de la entidad (2023) Dentro de la seguridad física de la información se encuentran en la organización los dos principales dispositivos de almacenamiento llamados Storage uno Z vs y vm y el XIV

El Z que es administrado por un tercero IBM pero supervisado por el área de System que hace parte de la gerencia de infraestructura de la organización es el encargado de almacenar la data transaccional de entidad a nivel nacional por ahí pasan todos los movimientos financieros de la organización y es llamada la alcancía porque ahí está hospedado el dinero, tiene la par en el centro de cómputo de contingencia y siempre se encuentran conectados de manera sincrónica, para su respaldo también cuenta con copia primarias, secundarias y terciarias, y almacenamiento histórico en cintas.

Se realizará un diagnóstico con la metodología cualitativa, utilizando como herramientas de estudio una entrevista al director del área de continuidad del negocio y la técnica de análisis que diagnostica de riesgos DOFA (Debilidades, Oportunidades, Fortaleza y Amenazas.

Siendo una de las principales conclusiones al finalizar el estudio es que se evidencio que al existir un alto grado de rotación en el personal crítico de los procesos y al ser ellos que desarrollarían las contingencias, suele suceder que ese personal se retira de la organización y en bajo índice hay una persona igualmente capacitada para sumir este rol.

ABSTRACT

The ISO 27000 standard allows the development of good practices for organizations. Good business continuity practices are part of the information security policy, such as the restricted use of information.

Business continuity The following work is carried out in order to assess the possible risks that may arise in a financial entity with a national operation in the face of eventual weaknesses that business continuity processes, plans and strategies may present within the company. organization.

The objective of this work is to evaluate the good practices of ISO 27000 in the direction of business continuity in the financial organization of National operation.

Among the results obtained in this work are: Knowledge of the structure of the business continuity management supported by the contingency computer center and the contingency operation center as a vital support line for the critical processes of the financial institution .

According to Ladino.a (2019) The ISO 27000 standard is certifiable. This means that a company can request an audit from an accredited certifying entity and if it passes, obtain the certification. Before requesting the audit, companies need to have an Information Security Management System (ISMS). The ISMS must be

implemented in the company at least three months in advance.

Each of the points required in the standard belongs to a stage of a process: Plan – Do – Check – Act (Plan-Do-Verify-Act), which is applied to structure all ISMS processes. The ISMS takes the information security requirements and the expectations of the parties as input elements.

In accordance with the above and given the experience and maturity of the process within the financial organization, led by the process owners who are generally the heads or directors of the area from where the process operates, who are responsible for reporting the materialization of a risk as the first At the request of the director of continuity or the information security department, a risk committee is also established within the organization that is also capable of making decisions in the face of these situations.

Within the evaluation of the security policies of the financial institution, they are mainly supported by two administrative areas, Information Security and Risk, two support areas that execute the policies that are computer security and business continuity and other support areas such as telematics and telecommunications area.

According to the entity's corporate intranet (2023) Within the physical security of the information, the two main storage devices called Storage one Z vs and vm and the XIV are found in the organization.

The Z, which is managed by a third party IBM but supervised by the System area that is part of the organization's infrastructure management, is in charge of storing the transactional data of the entity at the national level, through which all the financial movements of the organization pass. and it is called the piggy bank because the money is stored there, it has the same number in the contingency computing center and they are always connected synchronously, for its backup it also has primary, secondary and tertiary copies, and historical storage on tapes.

A diagnosis will be made with the qualitative methodology, using as study tools an interview with the director of the business continuity area and the analysis technique that diagnoses SWOT risks (Weaknesses, Opportunities, Strengths and Threats).

Being one of the main conclusions at the end of the study is that it was evidenced that when there is a high degree of rotation in the critical personnel of the processes and since they are the ones who would develop the contingencies, it usually happens that these personnel withdraw from the organization and in low index there is a person equally qualified to assume this role.

Palabras claves.

Activo de Información, Amenazas, Aplicaciones, Autenticidad, BIA, Confidencialidad, Disponibilidad, Incidente, Integridad, Metro Mirror, Planificación, Riesgo, RTO, Seguridad, Servidor, Telecomunicaciones, Vulnerabilidad

1. PLANTEAMIENTO DEL PROBLEMA

Esta investigación pretende evaluar las posibles falencias en el sistema de continuidad del negocio bajo las buenas prácticas de la norma ISO 27000.

La presentación actual de la problemática se centra en los siguientes aspectos, el antes, el durante y el después de ejecutar las diferentes pruebas de recuperación tecnológicas y de recuperación de procesos.

Antes: hace referencia a los preparativos previos a la materialización de un riesgo, el enfoque esta dado al alistamiento de la infraestructura, la logística y copias de respaldo de los Activo de Información. De acuerdo al SIC.gov.co son Datos o información propiedad de una empresa u organización. Son almacenados en medio físico o lógico y que es considerada como sensitiva o critica para el cumplimiento de objetivos misionales.

A nivel tecnológico se preparan dos frentes los planes de recuperación tecnológica en infraestructura que hace referencia a todos los dispositivos de almacenamiento, Storage, granja de servidores dispositivos de comunicación como switch, encriptadores, nexus, Access point, entré otros.

De acuerdo con la información tomada de la intranet corporativa de la entidad (2023)

: Creada en el año 1990 como una entidad de ahorro y vivienda.

En el año 2000 se funciona con dos cooperativas y otra entidad de ahorro y vivienda convirtiéndose en un banco con presencia a nivel nacional

Desde su inicio y como uno de sus pilares la organización se ha destacado por estar siempre a la vanguardia tecnológica lo cual le ha permitido el reconocimiento en el sector financiero.

De acuerdo con Diaz. (2020). Ir de la mano de la tecnología por la naturaleza de su operación se ha destacado porque sus procesos sean organizados eficientes y seguros.

Como es parte de sus principios la entidad financiera siempre ha buscado las estrategias normas y procedimientos que le permitan respaldar y proteger no solo sus procesos sino también uno de sus principales activos la información y data tanto de sus usuarios internos como externos.

La entidad hace presencia alrededor del país en las 10 principales ciudades y 23 poblaciones estratégicas con un total de 277 oficinas.

Su sede principal está ubicada en la ciudad de Bogotá donde se cuenta con más de 800 empleados operando desde dirección general.

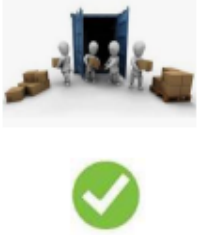
En total la entidad cuenta con 4500 empleados en todo Colombia.

En el año 2005 las directivas de la entidad financiera determinaron la necesidad de desarrollar e implementar un plan de recuperación de tecnológica para ser aplicado en caso de que se presenten eventos de falla mayor que afecten los servicios de las áreas de negocio

A través de análisis y metodologías, el área de continuidad del negocio ha identificado y determinado los posibles escenarios que puedan afectar la operación y normal funcionamiento de las áreas y proceso críticos de la organización por lo tanto ha establecido e implementado una estrategia de contingencia.

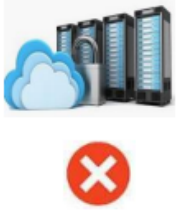
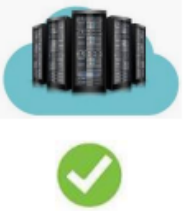
De acuerdo al norma NTC/ISO 22301" La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales y riesgos de tipo operacional a la organización y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses de los accionistas, la reputación, la marca y las actividades de creación de valor, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCP al día.

Ilustración 1Escenarios de afectación y estrategia establecida

Escenarios de Afectación y Estrategia Establecida				
Escenario de No disponibilidad			**Estrategia Implementada**	
• No disponibilidad o acceso a las sedes físicas en Dirección General,	• No disponibilidad o acceso por destrucción, orden público o afectación mayor o parcial de la infraestructura física o sedes del Banco donde operan procesos críticos ubicadas en Dirección General..		• Activación del Centro de Operaciones en Contingencia COC para procesos críticos según los tiempos de recuperación. • Activación de los Planes de Recuperación de Procesos Críticos. • Ubicación en otras sedes Staff del Banco para procesos no críticos según los tiempos de recuperación y el plan de contingencia por proceso. (Previo análisis y aprobación del Comité de Manejo de Crisis). • Acceso Remoto. (Previo análisis y aprobación del Comité de Manejo Crisis).	
• No disponibilidad de Proveedores críticos.	• No disponibilidad, afectación, falla total o parcial de los servicios contractuales con proveedores críticos.		• Activación de los planes de contingencia del Proveedor.	

Fuente: Pagina corporativa de la entidad

Ilustración 2 Escenarios de afectación y estrategia establecida

Escenarios de Afectación y Estrategia Establecida				
Escenario de No disponibilidad			**Estrategia Implementada**	
• No disponibilidad del Centro de Computo de Principal	• No disponibilidad de acceso ni de elementos físicos y tecnológicos, destrucción, afectación, falla total o parcial de la infraestructura tecnológica del Banco ubicada en el Centro de Cómputo Principal piso 25 • Incluye eventos relacionados a **Ciberseguridad.**		• Activación del Centro de Computo de Contingencia CCC.	

Fuente: Pagina corporativa de la entidad

Ilustración 3Escenarios de afectación y estrategia establecida

• Eventos con afectación reputacional.	• Afectación de la marca e imagen del Banco.		• Activación de los Comités Estratégicos del Manejo de Crisis y Comunicación en Crisis. Para la toma de decisiones y el manejo de la comunicación corporativa.	
• No disponibilidad de personal crítico para la ejecución de procesos.	• No disponibilidad del personal critico que ejecuta o interviene en actividades y procedimientos de procesos críticos.		• Activación del Backup o personal de remplazo, asignación de actividades a otros colaboradores, según la definición del dueño de proceso. • Acceso Remoto. (Previo análisis y aprobación CMC).	

Fuente: Pagina corporativa de la entidad

De acuerdo a Aguiñaga. (2019) en el manejo de crisis en las corporaciones para que la activación de las estrategias anteriormente mencionadas, sea efectiva, se requiere de la participación de los lideres y dueños de cada proceso y las áreas de la organización involucradas, en la ejecución de actividades, roles y responsabilidades preventivas que tiene definidos dentro del plan de continuidad del negocio, antes de un evento de contingencia.

Ilustración 4 Roles y responsabilidades de los lideres procesos de negocio

ROLES Y RESPONSABILIDADES GENERALES – LIDERES Y ÁREAS / PROCESOS DE NEGOCIO			
FASE	RESPONSABILIDAD – EQUIPO DE RECUPERACIÓN DE PROCESOS	ROL RESPONSABLE	
		LIDER DEL ÁREA/DUEÑO DE PROCESO	/EQUIPO TRABAJO/ COLABORADORES
ANTES (Prevención)	Participar activa y oportunamente en las actividades realizadas por la Dirección de Continuidad del Negocio, como lo son: la ejecución de pruebas de Contingencia, los programas de sensibilización y capacitación, la activación de contingencias reales y en la elaboración, actualización y mantenimiento de los Planes de Recuperación del Proceso y Análisis de Impacto al Negocio BIA para cada uno de los procesos.	SI	SI
ANTES (Prevención)	Informar a la Dirección de Continuidad del Negocio, sobre cualquier evento o situación específica que pueda afectar el normal funcionamiento del Proceso y que no se encuentre establecida y documentada en el Plan de Contingencia del Proceso.	SI	SI
ANTES (Prevención)	Mantener un esquema de comunicación permanente y asertiva con la Dirección de Continuidad del Negocio.	Si	SI
ANTES (Prevención)	Mantener actualizados los datos de contacto (Árbol de Llamadas), de los colaboradores del equipo de trabajo en caso de presentarse un evento que requiera de su ubicación y contacto, adicionalmente se debe informar al área de Continuidad del Negocio cada vez que se presenten cambios para realizar la respectiva actualización del Plan de Contingencia del respectivo proceso.	SI	SI
ANTES (Prevención)	Garantizar que al interior del equipo de trabajo todos los colaboradores estén capacitados y entrenados para desarrollar cualquier actividad del proceso. Esto con el fin de evitar que la ausencia del personal sea causante de la no ejecución de actividades ante eventos de contingencia ocasionados por fallas e interrupciones totales o parciales del proceso y/o durante la ejecución de Pruebas de Contingencia del Proceso.	SI	
ANTES (Prevención)	Verificar que los colaboradores del equipo de trabajo cuenten con los roles, claves y accesos vigentes y actualizados permanentemente, con el propósito evitar que las actividades del proceso no se puedan ejecutar debido a la imposibilidad de acceder a los aplicativos, servidores, carpetas, herramientas informáticas entre otros, ante eventos de contingencia ocasionados por fallas e interrupciones totales o parciales del proceso y/o durante la ejecución de Pruebas de Contingencia del Proceso.	SI	SI
ANTES (Prevención)	Asegurar que la información o documentos críticos para el desarrollo del proceso este custodiada y guardas en carperas en el servidor Neusa1 y no en los equipos locales de cada colaborador, lo anterior con el fin de lograr su fácil acceso ante eventos de contingencia ocasionados por fallas e interrupciones totales o parciales del proceso y/o durante la ejecución de Pruebas de Contingencia del Proceso.	SI	SI

Fuente: Pagina corporativa de la entidad

Es importante resaltar que todas las estrategias de contingencia implementadas son sometidas periódicamente a un riguroso plan de pruebas con el fin de asegurar su efectividad.

1.1 JUSTIFICACIÓN.

Continuidad del negocio es donde se desarrollan las principales estrategias y actividades que permite mitigar los principales riesgos tecnológicos presentados en la organización, esta dirección se trabaja y desarrolla su esfuerzo en tres frentes, un antes un durante y un después de la materialización del riesgo.

Dentro de las estrategias de seguridad para la protección de la información y demás recursos internos una organización dentro de las buenas prácticas de la norma ISO 27000 de Continuidad del Negocia dentro de la organización

Esto permitirá identificar los beneficios que provee para la organización la elaboración y documentación de los procedimientos utilizados en las pruebas tecnológicas cerradas programadas sobre la infraestructura. La mitigación de errores operativos, la valoración de las estrategias plantadas por la dirección de continuidad del negocio.

De acuerdo con Garavito. (2016).los beneficios de la implementación de un plan de continuidad de negocio son: apoyo en los objetivos estratégicos, creación de una ventaja competitiva, protección y mejora de la reputación y credibilidad, contribución a la resiliencia organizacional, reducción de la exposición legal y financiera, reducción de costos directos e indirectos de las interrupciones, protección de la vida, propiedad y medio ambiente, consideración de las expectativas de las partes interesadas, proveer confianza en la capacidad de la organización para alcanzar el éxito, mejorar la capacidad para permanecer efectivo durante las interrupciones, demostrar un control proactivo de los riesgos de manera efectiva y eficiente, abordar vulnerabilidades operativas.

Según Montoya. (2016) y acogido por la norma ISO 22301:2019, es importante plantear el plan de continuidad de negocio como un sistema vivo y efectivo para estos tiempos de crisis. Como todo sistema de gestión, se basa en el Ciclo PHVA «Planear, Hacer, Verificar y Actuar», que incluye un plan efectivo para el control de la continuidad de negocios con sus responsabilidades, simulacros, controles operacionales y procesos de mejora continua.

De acuerdo a la norma Ocampo (2017) el Plan de Continuidad del negocio (BCP) busca sostener en niveles previamente definidos y aceptados, los procesos críticos del negocio a través de la estructuración de procedimientos e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre. Por otra parte, el DRP y los planes de contingencia, forman parte del BCP y están enfocados frecuentemente a recuperar los activos asociados a las Tecnologías de la información. Por otro lado, el Plan de Continuidad del Negocio busca respaldar integralmente los intereses de las diferentes partes que intervienen en la organización, así como preservar los indicadores de generación de valor (reputación, marca, confianza, entre otros). Asimismo, se busca optimizar la capacidad de recuperación ante pérdidas significativas en recursos productivos u operativos (personal).

Ilustración 5Fases BCP

Fuente: Norma ISO 22301

A nivel social la continuidad del negocio tiene en cuenta los beneficios que presenta para los colaboradores de la organización desde varios puntos en los cuales encontramos:

La posibilidad de poder operar las estaciones de contingencia desde un punto diferente al de producción ya que el área donde está ubicado el Staff del banco es de alto impacto por temas de manifestaciones y paros, como lo es el centro internacional de la ciudad de Bogotá

El trabajó en casa nació precisamente de una contingencia, surgida por el momento crítico que se presentó por la declaración de emergencia sanitaria decretada por el gobierno el 6 de marzo de 2020 de acuerdo al decreto 417 de ese mismo año y como lo anunciaron en su momento, los jefes y directores de la organización “el Home Office llego para quedarse dentro de la compañía”.

Dentro del sistema de continuidad del negocio la continuidad del negocio se encuentra también el plan de emergencia que es el instrumento principal que define todos los sistemas, procedimientos, funciones, responsabilidades generales aplicables para enfrentar las situaciones de desastre, calamidad o emergencia, en sus distintas fases. Este plan tiene tres características principales debe ser: Eficiente, Oportuno y Eficaz, Con el fin de que mitigue o reduzca los efectos negativos o lesivos de las situaciones que se presenten en cualquier nivel o lugar del banco. cuyo objetivo principal es eestablecer los procedimientos y acciones, que deben realizar los colaboradores para prevenir o afrontar una situación de emergencia, con el fin de organizar el

control de la misma y evitar pérdidas humanas, materiales y económicas, haciendo uso de los recursos existentes en las instalaciones.

Proteger la vida, el bienestar y la integridad de las personas. Preservar los bienes, la imagen y la seguridad legal del Banco. Divulgar el plan de emergencias a todos los miembros de la empresa. Preparar, programar y realizar simulacros para verificar la eficiencia del plan de emergencias. Definir y mitigar el grado de vulnerabilidad presente en la compañía. Dar un alto valor a la gestión del Riesgo ante desastres. Facilitar la continuidad del negocio. Minimizar los daños de los recursos materiales y el medio ambiente

1.2 PREGUNTA PROBLEMA

¿Cómo evaluar las Estrategias de seguridad para la protección de la información y demás recursos internos de una red informática, mediante las buenas prácticas de la norma ISO 27000 de continuidad del negocio en una entidad financiera de operación nacional?

1.3 OBJETIVOS

1.3.1 Objetivo General

Como evaluar las estrategias de seguridad de la información y demás recursos internos e un a red informática, mediante las buenas prácticas de la norma ISO 27000 de continuidad del negocio dentro de una entidad financiera de operación nacional.

1.3.2 Objetivos Específicos

- Conocer las generalidades de la infraestructura en producción de la entidad financiera.
- Conocer las generalidades de la infraestructura en contingencia de la entidad financiera.
- Evaluar las políticas de seguridad de la información que actualmente maneja la Entidad Financiera.
- Definir la seguridad física y del entorno de la información.
- Conocer los procesos críticos que tiene definida la entidad y como son respaldados
- Evaluar como la entidad Protege, preserva y administra la información, junto con los equipos y recursos tecnológicos adecuados.
- Caracterizar los procedimientos y protocolos ante una situación de ciberataque.
- Describir los escenarios más críticos o propicios en los cuales se puede ver expuesta ante un ciberataque la Entidad Financiera.
- Analizar qué controles de acceso cuenta la entidad en sus centros de cómputo tanto de producción como el centro de cómputo de contingencia y que fortalezas y debilidades existen a raíz de su ubicación geográfica.
- Realizar las pruebas de seguridad, simulación de ciberataque para validar los sistemas de seguridad actuales de la entidad financiera

2. MARCO TEÓRICO Y ESTADO DEL ARTE

Dentro de la entidad bancaria se cuenta con una granja de servidores de 820 servidores de los ellos cuales 600 están configurados como servidores virtuales 10 servidores físicos y 210 con sistema operativo AIX propio del proveedor de tecnología IBM los cuales prestan un servicio una población promedio de 450 usuarios distribuidos en las principales ciudades de Colombia y algunas ciudades y municipios intermedios donde se ofrecen los servicios financieros y bancarios al público en general.

Como principal mecanismo de respaldo esta organización, se cuenta con la dirección de continuidad del negocio que a su vez es compensable del centro de cómputo alterno ubicado aproximadamente 5 kilómetros a la salida de la ciudad de Bogotá sede principal de la organización y donde además se encuentra la dirección general y administrativa de la entidad.

Adicionalmente también se cuenta con un centro de operación de contingencia donde se dispone de 100 puestos de trabajo y desde donde se puede operar en caso de presentarse una situación de no disponibilidad de los sitios propios de producción, allí están configurados principalmente los proceso llamados críticos del banco.

De acuerdo al autor Smith. (2019) en su libro Planes de contingencia centro de cómputo

Los Planes de Contingencias le permitirán mantener la continuidad de sus sistemas de información frente a eventos críticos, de su entidad y minimizar el impacto negativo sobre la misma, sus empleados y usuarios. Deben ser parte integral de su organización y servir para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

2.1 Antecedentes

De acuerdo a la investigación de García (2021) La continuidad en el negocio es de suma importancia en todas las organizaciones para mantener sus procesos y servicios, operando de mantera continua. Al no contar con planes de continuidad del negocio la organización puede asumir el riesgo de contar con incidentes imprevistos, que en el peor de los casos pueda detener los procesos, viéndose afectados y por consiguiente no se cumpla con los objetivos organizacionales, provocando pérdidas económicas o generar una mala imagen o reputación; también existe una exigencia por parte de gobierno en línea hacia las entidades públicas en el

cumplimiento de seguridad de la información, por lo que se sumerge en parte en la continuidad del negocio.

De acuerdo a las exigencias de gobierno en línea, la Alcaldía de Santiago de Cali, garantizando a la alcaldía un marco que asegure que pueden continuar operando durante las circunstancias más difíciles e inesperada, proporcionando la capacidad de la prestación de sus productos, manteniendo su reputación y protegiendo a sus empleados. Además, esta es particularmente importante en aquellas organizaciones que trabajan en entornos de altos riesgos donde la habilidad de continuar trabajando es de suma importancia para los negocios, clientes y partes interesadas, por lo que parte de esta norma nos ayuda en la evaluación de los riesgos disminuyendo el impacto en la organización en el evento de una falla – esto incluye las empresas de servicios públicos, financieras, de telecomunicaciones, de transportes y el sector público.

Alcaldía de Santiago de Cali, lograra mantener la continuidad en los procesos al momento que ocurran fallas que puedan colocar en peligro sus operaciones. Al Cliente, debido a la implementación de la organización de este sistema le permitirá continuar sus tareas o servicios brindados al momento que ocurra una discontinuidad de las operaciones.

De acuerdo a Montoya 2016," Garantizar la continuidad de los procesos críticos del negocio soportados por los servicios tecnológicos prestados a la organización ante un evento de falla mayor o desastre total, que permita a los clientes internos y externos continuar con su operación normal en el tiempo objetivo de recuperación establecido por las áreas de negocio y de acuerdo al manejo de incidentes. El RTO de los servicios críticos del negocio se deben recuperar en un término no mayor a 6.5 horas a partir de la ocurrencia de la interrupción", definir los procedimientos necesarios que permitan recuperar la operación ante una interrupción de uno o más servicios críticos del Centro del Cómputo Principal, haciendo uso de los recursos tecnológicos contratados que incluye la automatización de procesos que serán ejecutados automáticamente permitiendo el encendido de infraestructura, los equipos de especialistas de recuperación y los diferentes procedimientos anexos a este documento los cuales se aplican en el Centro de Cómputo de Contingencia, ante el evento que conduzca a la declaración de contingencia.

Las aplicaciones críticas del negocio de cara al cliente externo y aquellas internas que soportan la producción de la organización. No se consideran dentro del alcance las aplicaciones de desarrollo y pruebas, y la recuperación ante eventos de deterioro o pérdida de data de los diferentes sistemas o componentes tecnológicos. Las aplicaciones críticas están soportadas con infraestructura tecnológica dedicada en el centro de cómputo de contingencia. El plan define la información, las actividades y los procedimientos sobre la solución de recuperación, describe las responsabilidades de los Equipos de Recuperación a nivel tecnológico a ejecutar para restablecer la disponibilidad de las aplicaciones críticas respaldadas en el Centro de Cómputo de Contingencia ante un evento que afecte los servicios críticos del negocio.

De acuerdo al documento de la Escuela Superior de Administración pública (2018) con respecto a la continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre.

La planeación de la continuidad del negocio es el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

De acuerdo a la Norma NTC/ISO 22301 La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica, amenazas potenciales y riesgos de tipo operacional a la organización y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses de los accionistas, la reputación, la marca y las actividades de creación de valor, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCP (plan de Continuidad del negocio) al día.

Una estrategia de continuidad es un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre o una interrupción mayor. Son consideradas como estrategias no sólo los recursos y actividades requeridas frente a la interrupción, sino los requeridos para mitigar la probabilidad de ocurrencia y el impacto de la interrupción

2.1.1 Marco conceptual

Activo de Información. Datos o información propiedad de una empresa u organización. Son almacenados en medio físico o lógico y que es considerada como sensitiva o critica para el cumplimiento de objetivos misionales (www.sic.gov.co).

Amenazas. Son representadas como el riesgo para los activos en la seguridad de la información en general, las cuales pueden ser persistidas al interior o exterior de la organización (Hodeghatta & Nayak, 2014, p. 31).

Aplicaciones: Son programas de computador que están diseñados con capacidades lógicas y matemáticas para procesar información. El término Aplicación se utiliza para agrupar un conjunto de programas que responden a requerimientos particulares de áreas de negocio. (Hodeghatta & Nayak, 2014, p. 31).

Autenticidad: Características fundamentales para una empresa, donde la seguridad de la información permite la protección de la identidad de los usuarios o información que caracteriza a la organización (Hodeghatta & Nayak, 2014, p. 31).

BIA (Business Impact Analysis): Es el análisis de impacto al negocio que nos permite identificar las funciones críticas de las áreas del negocio del banco, los tiempos objetivos de recuperación, aplicaciones utilizadas, recursos y los impactos cualitativos y cuantitativos ante una contingencia. (Hodeghatta & Nayak, 2014, p. 31).

Confidencialidad. Es el proceso inclinado hacia la generación de métodos para la restricción en el acceso a la información, para que no sea divulgada de la manera equivocada (Hodeghatta & Nayak, 2014, p. 31).

Disponibilidad. Garantizar el ejercicio del uso adecuado del servicio cuando es solicitado por personas que requieren información (ISO 27001:2015).

Incidente de seguridad. Subraya el impacto que generan las operaciones comerciales con respecto a la seguridad de la información, poniendo en riesgo la confidencialidad, integridad y disponibilidad

ISO 27001 (2015).

Integridad. Salvaguardar el acceso, que conlleve a la restricción o manipulación indebida, modificación o destrucción de la información manteniendo la autenticidad

Hodeghatta H (2014), seguridad informática.

Metro Mirror: Es una tecnología de replicación de datos de sistemas de almacenamiento que cubre grandes distancias entre dos puntos en áreas metropolitanas

Planificación: es un proceso sistemático en el que primero se establece una necesidad, y acto seguido, se desarrolla la mejor manera de enfrentarse a ella, dentro de un marco estratégico que permite identificar las prioridades y determina los principios funcionales.

Riesgo: Según el Instituto de Gestión de Riesgos (Institute of Risk Management), organismo líder a nivel mundial en todo lo que compete a la gestión de los riesgos que enfrentan las empresas, el riesgo cibernético se define como cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización

Fuente página banco de la república. Instituto de Gestión de Riesgos (Institute of Risk Management)

RTO (Recovery Time Objective): Es el tiempo objetivo de recuperación, que puede soportar las áreas de negocio ante una interrupción de los servicios soportados en el Centro de Cómputo Principal. Este tiempo esta medido en horas.

Telecomunicaciones: Son servicios de transmisión de datos de un punto a otro, que son procesados por computadores. Estos servicios son prestados por proveedores a través de canales y equipos de comunicación. El conjunto de enlaces, equipos y computadores conforman las redes, como, por ejemplo, la conocida Internet.

Seguridad: La seguridad debe ser descifrada como el estado subjetivo que permite percibir el desplazamiento dentro de un espacio exento de riesgos reales o potenciales

ISO 27001:(2015).

Vulnerabilidad. Es la debilidad del sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema

(ISO 27001:2015).

De acuerdo al documento técnico del plan de continuidad del negocio cuyo autor Marchionni. (2020), entendimiento en función pública: El Plan de Continuidad reúne un conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la misionalidad de la entidad y la prestación de sus servicios se establece en tres momentos:

Preventivo: Dentro de este aspecto se involucran los recursos humanos, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan articular a la gestión institucional en los diferentes procesos.

Reactivo: Este aspecto va dirigido a fortalecer las políticas internas y comunicarlas oportunamente para ponerlas en marcha una vez detectada la contingencia.

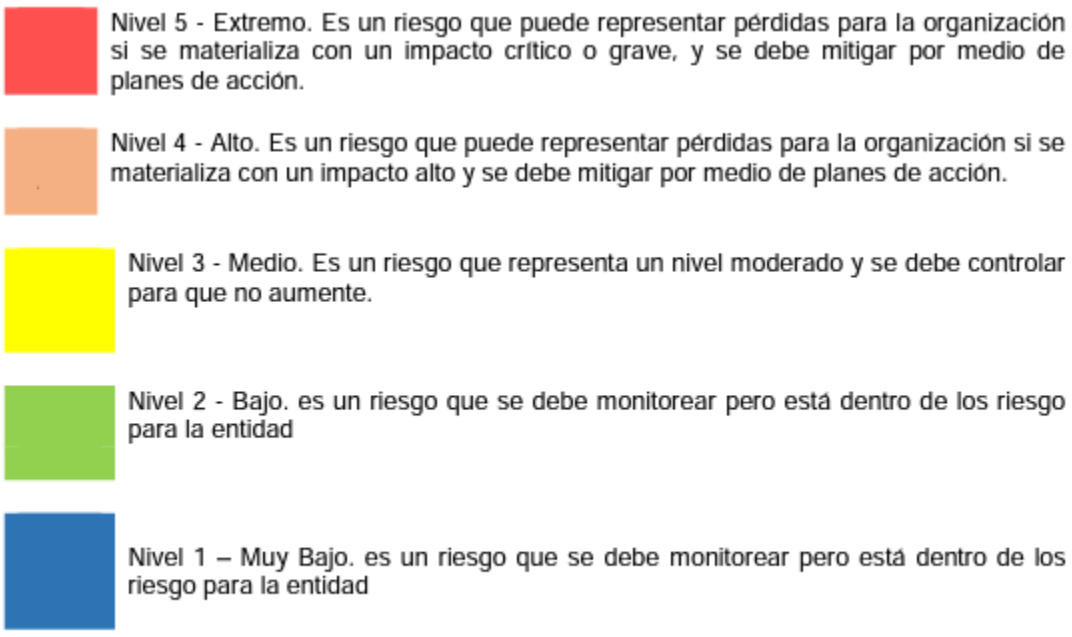
Recuperación: Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia. La descripción consecutiva de las actividades en los diferentes momentos estará definida en el documento denominado "plan de continuidad" anexo a este documento técnico.

Ilustración 6 Mapa de calor Impacto y Probabilidad

		IMPACTO				
		NIVEL1	NIVEL2	NIVEL3	NIVEL4	NIVEL5
PROBABILIDAD	NIVEL5	5	10	15	20	25
	NIVEL4	4	8	12	16	20
	NIVEL3	3	6	9	12	15
	NIVEL2	2	4	6	8	10
	NIVEL1	1	2	3	4	5

Fuente: Propia realizada por el autor

Ilustración 7Mapa de calor Impacto y Probabilidad fuente Mintic



Fuente: mitic.co

La presente investigación permitirá establecer definiciones a cerca de términos desarrollados en el documento, determinando su importancia. A continuación, se describen conceptos considerados como significativos para el estudio.

la organización financiera, llevar un manejo adecuado de la información, evidenciando métodos dirigidos a la seguridad física y de cada uno de sus procesos, con el fin de salvaguardar la información confidencial de la empresa.

De acuerdo con el autor Garcia. (2021), aaquellas empresas que brindan este tipo de información lo que hacen es mostrar datos o aspectos que le parecen más importantes por sus motivaciones particulares y que consideren fundamentales.”

De acuerdo al documento de la MINTIC llamado Guía para para la preparación de las TIC, la continuidad del negocio Es el instrumento principal que define todos los sistemas, procedimientos, funciones, responsabilidades generales aplicables para enfrentar las situaciones de desastre, calamidad o emergencia, en sus distintas fases. Este plan tiene tres características principales debe ser: Eficiente, Oportuno y Eficaz, Con el fin de que mitigue o reduzca los

efectos negativos o lesivos de las situaciones que se presenten en cualquier nivel o lugar del banco

2.2 Marco Referencial.

La seguridad de la información es un requisito cada día más importante en el entorno profesional, por ello se utiliza la norma ISO 27000 como base en la organización en la gestión del sistema de seguridad de la información ya que existen entidades organización, empresas y corporaciones entre otras que desprotegen la información sensible, debido a las malas prácticas.

De acuerdo a la publicación de Marco "Los proyectos de informatización de los entornos empresariales, junto con la infraestructura TI, también tiene que incluir un sistema que permita conservar y mantener los datos y los documentos que los contienen durante, al menos, su período de vigencia legal. En la práctica se aplicará con las mismas medidas de seguridad de forma independiente a la índole de los datos de los documentos, pudiéndose considerar la protección de datos un subconjunto dentro de la estructura de seguridad de la información."

El cumplimiento de todas las disposiciones legales por parte de los sistemas de información, procesos empresariales y proyectos de consultoría, lo que suele ser suficiente para un país determinado. En última instancia, son los intereses de las personas físicas cuyos datos aparecen en los documentos, y no los intereses empresariales, además de su principal propósito.

Las organizaciones necesitan contar con una solución sistemática con la que puedan asegurar su información con un enfoque basado en la gestión, que al mismo tiempo cumpla con las exigencias jurídicas. El cumplimiento con las leyes relativas a la seguridad es un paso importante, pero no garantiza la cobertura internacional de los proyectos y la importación o exportación de las soluciones de consultoría.

La norma ISO 27001 estandariza de forma universal todos los criterios jurídicos y permite evitar las amenazas mediante un enfoque basado en la gestión de riesgos. En la mayoría de los casos se evita tener que realizar adaptaciones a las exigencias legales en cada mercado. En los casos en los que los sistemas de información y los procesos cumplan con todas

las exigencias legales de la normativa de protección de datos, partirán de una posición mucho más ventajosa con respecto a los casos del que se parte de cero.

La norma se encuentra centrada en garantizar la confidencialidad, la integridad, la disponibilidad y la autenticidad de la información para intentar evitar las incidencias de tipo físico o lógico que pueda comprometer los niveles de competitividad, de rentabilidad, de conformidad legal y de imagen empresarial, siendo necesarios para conseguir los objetivos de la empresa y asegurar la continuidad del negocio.

Es necesario otorgar una capa de seguridad de los entornos de gestión documental con las siguientes medidas de control, identificación de los cambios y revisiones de los documentos, acceso legible a las últimas versiones de los documentos, identificación correcta de los documentos internos y externos, disponibilidad de los documentos para aquellos que los precisen en su ejercicio laboral, control de la distribución de los documentos, prevenir el uso indebido de documentos obsoletos en procesos de negocio actuales y asegurar la disponibilidad de su consulta en cualquier caso.

Es necesario que se constituya un modelo flexible que se adapte a cualquier tipo de tamaño de empresa y permita obtener el reconocimiento necesario por parte de una entidad de certificación independiente, la cual demuestra de forma pública el compromiso de la empresa con la protección de la seguridad y es una garantía que otorga confianza en el cliente, con respecto a otras organizaciones que no la tengan en cuenta.

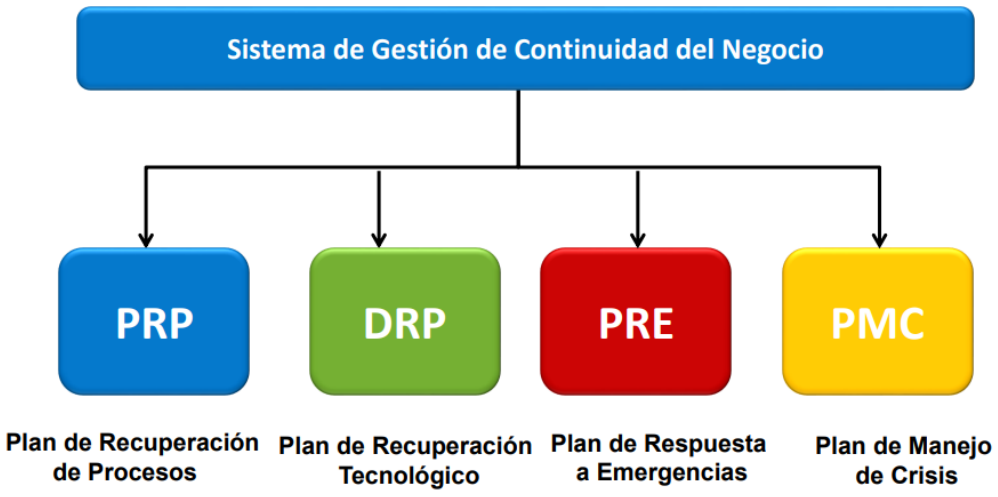
De acuerdo con Ladino. (2019).La norma ISO 27001 cumple el papel de formalizar por escrito las pautas adecuadas para que la organización pueda utilizar de manera segura los elementos de hardware y software que integran su sistema de información. Como es un sistema de gestión, en la línea de la ISO 9001 permite la elaboración de política, procedimientos y manuales técnicos que describan en relación con todos los aspectos de la gestión por procesos, los recursos humanos, la protección jurídica, la protección física y la gestión de la continuidad del negocio, que se relacionan con la seguridad de la información.

Es necesario que la implementación se lleve a cabo mediante especialistas, que utilizan metodologías de gestión de proyectos y llevan a cabo un complejo trabajo documental

para realizar las auditorías, definir las políticas de actuación, realización de evaluaciones e implementación de procedimientos. La contratación suele ser externa al no contar con grupo especializado entre su personal interno. Los casos en los que las organizaciones no se dedican al ámbito tecnológico, y que generan un gran volumen de información, difícilmente de abarcar sin la tecnología y los conocimientos adecuados. La externalización del servicio puede ser una alternativa mucho más apropiada:

- Por la experiencia del personal contratado.
- Por las instalaciones especialmente ideadas para la seguridad que posee la empresa.
- Para que un tercero se encargue de garantizar la tediosa tarea del cumplimiento legal a lo largo del tiempo.
- Por disponer de hardware y software específico, necesario para este tipo de gestión de información.
- Por aportar valor al cliente, abaratando sus costes y ahorrando su tiempo de gestión.

Ilustración 8 Mapa conceptual del sistema de gestión de Continuidad del Negocio



Fuente: Pagina corporativa de la entidad

2.3 Plan de recuperación de procesos (PRP)

El Plan de recuperación de procesos es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos críticos del negocio generando un impacto mínimo o nulo ante un evento o incidente de interrupción. El PRP se activará cuando el evento supere el máximo tiempo que una unidad de negocio puede esperar por la disponibilidad de un proceso.

Sus principales objetivos son:

Definir los planes a ejecutar en caso de presentarse un evento de falla mayor o desastre total que interrumpa la operación normal de los procesos críticos del negocio.

Planear y ejecutar pruebas de continuidad del negocio con las diferentes áreas para garantizar la funcionalidad y eficacia de los planes.

Activar los planes de recuperación a los procesos críticos del negocio en el Centro de Operaciones de Contingencia (COC).

Garantizar la continuidad de las funciones críticas del negocio, de manera que el impacto sea menor por el incidente presentado y de acuerdo a los tiempos objetivos de recuperación (RTO)

De acuerdo por lo descrito por Rosales (2019) Los Planes se desarrollan con el objetivo de mantener o restablecer las operaciones de los negocios en plazos determinados una vez que ocurra alguna interrupción o falla en los procesos críticos de los negocios. Para esto cada área con procesos críticos para el Banco, designó a los expertos de dichos procesos para realizar sus planes. Descripción de: • Tareas preventivas - Antes • Tareas de recuperación- Durante • Tareas respuesta – Después Información de: • Proveedores • Datos personales del equipo de trabajo • Software y Hardware requerido para operar los procesos.

Para garantizar el mantenimiento de los planes de recuperación de procesos, se delegaron las siguientes responsabilidades a los líderes de cada área:

Ilustración 9 Ciclo de los planes de recuperación de los Procesos

Preventivas- Antes	Revisar y mantener actualizado el Plan de recuperación de procesos de cada área y cumplir con el plan de pruebas diseñado por continuidad del Negocio en el COC para garantizar el respaldo de los procesos.
Respuesta- Durante (Manejo de Incidentes y Movilización)	Informar sobre la situación del área Coordinar la movilización de los funcionarios al centro de operación en contingencia, si es necesario.
Recuperación- Después (Operación en contingencia y Retorno a la Normalidad)	Coordinar el desarrollo de las actividades definidas en el plan de cada área.

Fuente: Página corporativa de la entidad

2.4 Plan de recuperación tecnológico (DRP).

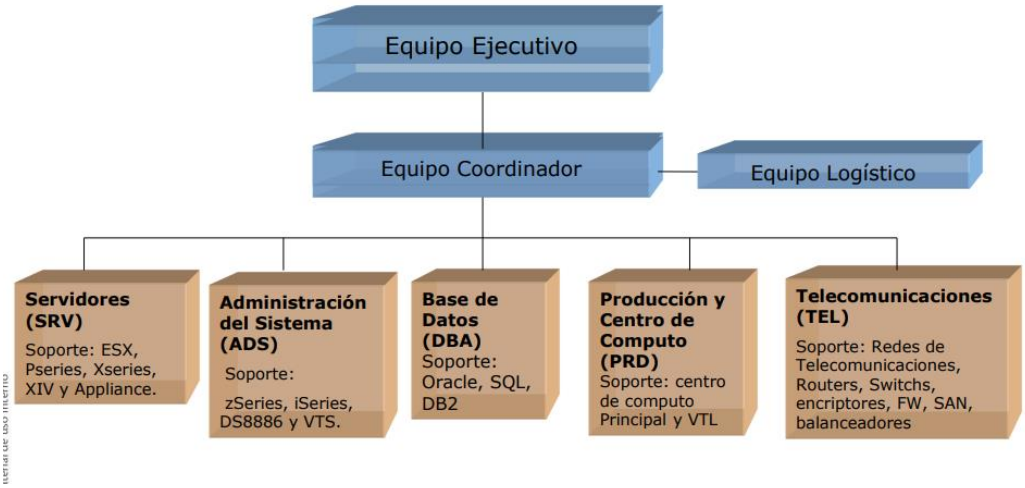
El Plan de Recuperación Tecnológica permite dar continuidad a los procesos críticos del negocio ante una situación de contingencia que pueda afectar uno o más servicios tecnológicos que soporta la operación del Banco, ubicados en el Centro de Cómputo Principal.

De acuerdo a lo ilustrado por Giménez.(2019). La infraestructura tecnológica de contingencia, los planes, las aplicaciones, y los equipos de recuperación conforman el Plan de Recuperación tecnológica, el cual se encuentra conformado en las siguientes fases: Operación Normal, Manejo de Incidentes, Movilización, Operación en Contingencia • Retorno a la Normalidad.

En el desarrollo del Plan se definió el siguiente contenido para la ejecución del plan de recuperación tecnológica.

Información general del plan de recuperación de la organización, equipos de trabajo y responsabilidades, Contar con infraestructura tecnológica de contingencia para respaldar los servicios críticos del negocio, las directrices de respaldo, la Metodología de pruebas del plan de recuperación. • Mantenimiento del plan de recuperación.

Ilustración 10 Estructura Organizacional DRP



Fuente: Pagina corporativa de la entidad

Las responsabilidades se clasifican en tres fases, antes, durante y después de una contingencia:

Las responsabilidades antes de la contingencia identifican elementos que cada equipo debe asegurar durante la operación normal para que el plan pueda ejecutarse tal y como está diseñado.

Las responsabilidades durante la contingencia se traducen en actividades a ser realizadas por cada equipo en respuesta a un evento que origine la declaración de la contingencia.

Las responsabilidades después de la contingencia se traducen en actividades a ser realizadas por cada equipo para retornar la operación al Centro de Cómputo Principal, sea este el mismo Centro afectado por el evento que originó la contingencia u otro seleccionado para tal fin, implicando que este retorno devolverá la operación del Banco a su normalidad y posterior evaluación y ajuste del Plan de Recuperación.

Hace referencia al descripción de estudios relacionados que se encuentran relacionados con la variable de investigación los cuales fueron soportes en el cumplimiento de los objetivos y son descritos a continuación Inicialmente, se tiene en cuenta el estudio realizado por Cadavid (2018), con el trabajo de investigación titulado Hallazgos de vulnerabilidades en los sistemas

operativos y base de datos de la empresa ALDIM Acciones logísticas en distribución de mercancías, para optar el título de Especialista en seguridad Informática. El propósito de esta investigación está orientado a la búsqueda de vulnerabilidades, amenazas y riesgos presentes tanto en los sistemas operativos como en bases de datos, por medio del proceso de pentesting aplicados a la seguridad informática, estableciendo recomendaciones que permitan un enfoque de un sistema de control eficiente.

Así mismo, se tiene el trabajo investigativo de Suarez (2015), llamado análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez padilla & cia. Ltda., que brinda una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización, exigencia para obtener el título de Magister en Seguridad Informática, a través de la Universidad Nacional Abierta y a Distancia.

Sustentado con aportes de los autores Diaz (2020), El estudio está enfocado en la realización de análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora. Las dimensiones de estudio están concernidas en la categorización y análisis de riesgos de los activos de información.

Metodológicamente hablando, fue una exploración de tipo descriptiva con enfoque cualitativo, basadas en referencias literarias junto a la elaboración de matrices de riesgos para verificar el estado real de la empresa dentro del factor de seguridad de la información, realizando entrevista de tipo abierta a los trabajadores de la empresa. Así mismo, las pruebas estuvieron basadas en el cumplimiento de lo establecido por la norma ISO/IEC 27001: 2013.

Los hallazgos se fundamentaron en los datos aportados por los entrevistados, dando a conocer que la empresa, no dispone de un SGSI, debido a la carencia de personal calificado e idóneo para la asignación de responsabilidades dentro del sistema, donde se demuestra la ausencia de actividades para la protección de los activos y otros aspectos que deben ser cubiertos por la organización.

De acuerdo a Camelo. (2019).La investigación permitió evidenciar que los datos conservados por una empresa son de suma importancia, resaltando así mismo, la designación de políticas, roles y responsabilidades, importantes en el aseguramiento del éxito dentro de una estructura organizacional bajo los lineamientos que deben ser dirigidos por la alta gerencia,

donde todos los integrantes que hacen parte de esta, ya sea a nivel interno como externo deben conocer.

Objetivos por cada equipo del DRP

Ejecutivo: Fijar directrices y tomar las decisiones de relevancia en la ejecución del plan de recuperación del Centro de Cómputo del Banco. Citar al Equipo de Activación del Comité de Manejo de Crisis en caso de una declaración de contingencia.

Coordinador: Administrar los elementos de contingencia (Contratos y planes), tomar decisiones tácticas y operativas necesarias para que los miembros de los equipos de recuperación ejecuten las tareas asignadas en los planes. Supervisar a los equipos de recuperación en su tarea operativa y participar en las reparaciones y/o reconstrucción de los servicios afectados por la contingencia.

Logístico: Gestionar la existencia, disponibilidad, entrega de los recursos y suministros que apoyen la operación en el Centro de Cómputo de Contingencia. Participar activamente en las pruebas cerradas del DRP, dar continuidad al servicio de soporte a usuarios durante una contingencia y apoyar las labores de divulgación.

Telecomunicaciones: Garantizar que el servicio de comunicaciones entre los diferentes nodos del Banco, incluyendo el CCC y el COC, permanezcan activos y con un nivel de desempeño adecuado a las necesidades de comunicación y réplica del Banco. En contingencia, ejecutar los planes y pruebas que permitan garantizar la continuidad de la operación y la restauración del servicio original en aspectos propios de su especialidad

2.5 Plan de emergencias.

Es el instrumento principal que define todos los sistemas, procedimientos, funciones, responsabilidades generales aplicables para enfrentar las situaciones de desastre, calamidad o emergencia, en sus distintas fases. Este plan tiene tres características principales debe ser: Eficiente, Oportuno y Eficaz, Con el fin de que mitigue o reduzca los efectos negativos o lesivos de las situaciones que se presenten en cualquier nivel o lugar de la organización

Plan de manejo de crisis.

Estar preparado adecuadamente para el manejo de una crisis potencial o real, con el fin de: Proteger la reputación del Banco.

Proteger la integridad de los colaboradores, clientes y demás personas que puedan verse afectadas.

Reconocer las crisis potenciales, analizarlas y tomar las acciones necesarias cuando se presenten y evaluar si está controlada y superada.

Proveer información oportuna, veraz, precisa y consistente sobre la situación a todas las audiencias.

Contar con un plan actualizado y mejorado continuamente

2.6 Marco legal.

Siempre que se desea implementar un sistema de gestión toda organización debe cumplir obligatoriamente con todas las leyes, normas y decretos entre otros De manera general puedo mencionar el tema de seguridad social, cumplir con la Cámara de Comercio, permisos, licencias de construcción, entre otros; pero en lo que se refiere específicamente a Seguridad de la Información, estas son las Leyes vigentes al día de hoy:

Derechos de Autor

Decisión 351 de la C.A.N.

Ley 23 de 1982

Decreto 1360 de 1989

Ley 44 de 1993

Decreto 460 de 1995

Decreto 162 de 1996

Ley 545 de 1999

Ley 565 de 2000

Ley 603 de 2000

Ley 719 de 2001

Propiedad Industrial

Decisión 486 de la C.A.N.

Decreto 2591 de 2000

Ley 463 de 1998

Ley 170 de 1994

Ley 178 de 1994

Propiedad Intelectual

Decisión 345 de la C.A.N.

Decisión 391 de la C.A.N.

Decisión 523 de la C.A.N.

Comercio Electrónico y Firmas Digitales

Ley 527 de 1999

Decreto 1747 de 2000

Resolución 26930 de 2000

Para finalizar, el 5 de enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano: Capítulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;

Capitulo Segundo: De los atentados informáticos y otras infracciones.

Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

Actualización agosto 2013, LEY 603 DE 2000, esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. Ver esta ley.

Ley estatutaria 1266 del 31 de diciembre de 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Ver

esta ley.

Ley 1273 del 5 de enero 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. Ver esta ley .

Ley 1341 del 30 de julio de 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

ley estatutaria 1581 de 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

Aspectos claves de la normatividad:

Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.

Establece los principios que deben ser obligatoriamente observados por quienes hagan uso, de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.

Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.

Crea una especial protección a los datos de menores de edad.

Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.

Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.

Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.

Crea el Registro Nacional de Bases de Datos.

Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

Decreto 1078 de 2015 Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea y continuidad del negocio

NTC/ISO 22301:2012 Norma internacional para la gestión de la continuidad de negocio.

Es así como se da paso dentro del proceso de investigación a la definición de Continuidad del negocio es la Capacidad de una organización para continuar suministrando productos o servicios a niveles aceptables previamente determinados tras un evento o incidente de interrupción que sea causado por el hombre o la naturalezacondiciones de seguridad óptimas para el tratamiento de datos en un sistema informático.

Estado del arte.

Tipo y diseño de estudio es de orden Cualitativo

Participantes y fuentes de datos en la presente investigación están basados por la herramienta de análisis DOFA

> Según Humphrey. (1969) "*Durante el proceso de la investigación y a la pregunta de que es bueno y malo para cumplir los objetivos organizacionales llegaron a la conclusión de lo que es bueno en el presente es Satisfactorio, lo que en el futuro es una Oportunidad, lo que es malo en el presente es una Falto o un Fallo y lo que es malo en el futuro es una Amenaza*"

La recolección de Datos esta dad en la investigación de campo dentro de la organización, la observación de los proceso y estrategias, la lectura de la documentación autorizad por el director del área de continuidad del negocio y una entrevista dada por el mismo director de continuidad.

3. MARCO METODOLÓGICO

Teniendo en cuenta el planteamiento del problema propuesto en el presente proyecto, el enfoque que se quiere buscar en esta investigación es cualitativo, ya que se busca validar las debilidades, oportunidades, amenazas y fortalezas en los procesos y estrategias desarrolladas por la continuidad del negocio en una entidad financiera que presta sus servicios a nivel mediante la aplicación de una entrevista con el director de continuidad del negocio de la entidad.

> Teniendo en cuenta lo argumentado por Durkheim (1917), "*La investigación cuantitativa considera que el conocimiento debe ser objetivo, y que este se genera a partir de un proceso deductivo en el que, a través de la medicación numérica y el análisis estadístico inferencial, se prueban hipótesis previamente formuladas*".

Cuando hablamos de métodos cualitativos, investigaciones cualitativas o metodología cualitativa, nos referimos al tipo de procedimientos de recopilación de información más empleados en las ciencias sociales.

Se trata de métodos de base lingüístico-semiótica. Emplean técnicas distintas a la encuesta y al experimento, tales como entrevistas abiertas, grupos de discusión, o técnicas de observación participante.

Todo método cualitativo aspira a recoger los discursos completos sobre un tema específico, para luego proceder a su interpretación, enfocándose así en los aspectos culturales e ideológicos del resultado, en lugar de los numéricos o proporcionales.

Esto implica comprender el contexto natural y cotidiano del fenómeno estudiado. También considera los significados que se le atribuyen y las valoraciones que las personas hacen. Dicho de otro modo, y parafraseando a Bonilla. (2011), el método cualitativo plantea comprender lo que la gente piensa y dice.

Con referencia y de acuerdo a la editorial Ruiz. (2019) las Características del método cualitativo son:

Las investigaciones cualitativas suelen ser multi-metódicas en su aproximación al objeto de estudio, es decir, que suelen aplicar distintos métodos de obtención de información al mismo tiempo. Arroja datos de tipo descriptivo: el contenido cultural de las personas, los datos observables de lo que dicen, etc.

De acuerdo a Benavides. (2017), este tipo de investigaciones no suelen plantear una hipótesis a priori, sino que aspira a utilizar la lógica de la inducción para dar respuesta a las preguntas que motivan el estudio.

Las dos herramientas de estudio utilizadas son: una encuesta con el director del área de Continuidad del Negocio de una entidad financiera con operación a nivel nacional y la otra herramienta es el análisis de riesgos DOFA (Debilidades Oportunidades, Fortalezas y amenazas)

El proyecto tendrá como tipo de investigación exploratoria; por cuanto se pretende identificar vulnerabilidades, amenazas y riesgos de la seguridad de los activos de información y demás recursos internos

Se investigará como está conformado tanto el centro de cómputo principal como su centro de cómputo alterno o de contingencia, como se comunican entre ellos, que procesos se consideran críticos y que parámetro lo permite establecer establece la criticidad en los procesos.

Se exploran las estrategias establecidas en continuidad del negocio para respaldar los procesos las aplicaciones como la data del banco.

Se analizarán los casos del porque se tuvo que declaran una contingencia real, la causa y su secuencia de solución.

3.1 Hipótesis planteada

Es posible evaluar los riesgos de los procesos de continuidad del negocio en una entidad financiera de cubrimiento nacional, gracias a la herramienta DOFA producto de la observación en los procesos, la metodología las buenas y las malas prácticas en el desarrollo de las actividades propias del área evaluada y del desarrollo de la actividad de entrevista al director del área de continuidad del negocio de la entidad financiera estudiada.

Hipótesis Nula

No es posible evaluar los riesgos de los procesos de continuidad del negocio en una entidad financiera de cubrimiento nacional,

De acuerdo con Álvarez. (2004). Seguridad informática para las empresas de acuerdo al grado de confidencialidad no es posible acceder a la información y los datos que se puedan analizar y dar un diagnóstico real de la situación actual de la organización o porque ya alcanzo el grado de madurez donde la organización no cuenta aparentemente con debilidades o deficiencias que permiten realizar sugerencias de mejora a sus procesos organizacionales.

3.2 Método de investigación

De acuerdo al análisis de la investigación y acciones correctivas que van a ser presentadas para la evaluación y mejor toma de decisión en el ámbito de la seguridad informática, hemos encontrado que lo realizaremos basándonos en el siguiente método de investigación.

Método Cualitativo: De nuestras hipótesis e ideas debemos llegar a una conclusión, para que así tanto nosotros como la empresa podamos tomar las acciones correctivas a seguir para asegurar el cumplimiento de lo propuesto.

De acuerdo a Baez. (2009) en su libro Investigación Cualitativa, es el conjunto de todas las cosas que se hacen para seguir la pista de los mercados y encontrar los rasgos al

as personas y a las cosas sus propiedades y atributos sean estas o estos naturales o adquiridos.

3.3 Instrumentos para la investigación

Análisis DOFA

Debilidades:

Falencia en el canal de comunicación entre producción y contingencia ya que cuando una aplicación cambia de versión o se actualiza en producción, hay ocasiones que la dirección de Continuidad del negocio no se detecta esta novedad, solo cuando se presenta una prueba controlada o peor aun cuando se activa una contingencia y dicha aplicación no funciona correctamente,

- La cantidad de equipos configurados como contingencia en el centro de cómputo de continuidad es insuficiente ante la demanda contemplada en una contingencia real total que, aunque solo se han presentado contingencias parciales y se ha cumplido la debilidad se presentaría ante una contingencia real ya que no se cubriría el cien por ciento de los procesos críticos.

  El soporte técnico es tercerizado y ante la rotación continua del personal en la investigación se detectó la poca documentación de la manera como se instalan y se configuran las aplicaciones.
- La falta de interés por algunos dueños de procesos en producción en la realización de ejercicios de pruebas en el centro de cómputo y de contingencia, argumentando el desplazamiento a sitio ya que este se encuentra entre 50 minutos a una hora del lugar de origen que para este estudio es dirección general o la falta de recurso en producción ya que se envía uno de los funcionarios no habría quien cubrirá sus funciones en producción.

- De acuerdo a Bernal. (2010) La costumbre de los usuarios a solo estar en ambiente de producción y como su nombre solo produciendo.

Los jefes tienen esa preocupación y no todos prestan preocupación por probar su continuidad en los procesos y lo que puede ocurrir si en caso de falla o interrupción en producción y no se está preparado para activar la contingencia de su proceso.

Oportunidades.

- Mejoramiento en los tiempos de respuesta en caso de presentarse una contingencia de cualquier proceso critico dentro de la organización.
- Mejoramiento continuo de la infraestructura de contingencia ya que por politicas se debe ir de la mano de los cambios en producción.
- programas de capacitaciones constantes al equipo de continuidad del negocio que vallan de manera transversal a los cambios, actualizaciones y mejoras que se presente en producción.

De acuerdo al siguiente enunciado de Leyva. (2021) de Es importante indicar que las buenas prácticas y la incorporación de nuevas tecnologías de la información y comunicación, darán un valor agregado para que los recursos de red de una entidad permanezcan seguros y así evitar ataques donde haya sustracción o robo de información, como también el hackeo de cuentas de usuarios internos que puedan poner en riesgo la estabilidad económica de una entidad.

Fortalezas.

- Madurez en sus procesos, estrategias y buenas prácticas gracias a sus constantes pruebas controladas en los programas y aplicaciones por una trayectoria de más de 13 años ya que la dirección de continuidad del negocio fue implementada para la organización en el año 2010.
- La dirección de continuidad del negocio está respaldada por la alta gerencia de la organización siendo un proceso de soporte a los procesos llamados críticos y además por regulación a todas las entidades del sector financiero que deben contar con esta área, siendo auditada por la superintendencia financiera de acuerdo a la norma ISO 22301.

- De acuerdo con Berrio. (2016) el manejo adecuado y oportuno de los inventarios tecnológicos tanto en producción como en Contingencia garantizan la sincronia.
- el correcto manejo de la documentación dentro del equipo de continuidad del negocio la cual se encuentra referencia, versionada y codificada además de estar respaldada en servidores de Backus de La organización.
- Manejo de cronograma anual de pruebas tanto de recuperación de los procesos críticos a nivel terminales como cerradas tecnológicas donde se prueba la infraestructura del centro de cómputo de contingencia.

Amenazas

- La salida de personal crítico para los procesos sin compartir la curva de aprendizaje par sus reemplazos ya que son por lo general salidas esporádicas sin previo aviso a sus jefes.
- Desactualización de los aplicativos de los planes de recuperación de procesos.

Ataque cibernético que afecte los principales servidores y aplicaciones de la organización y que a su vez se repliquen en los servidores de contingencia ya que estas copias son sincrónicas.

- Fallas o incumplimiento contractuales por parte de terceros.
- Se analizo que los directores y jefes llevan mucho tiempo en la organización,

Su poder de decisión está limitada al posible miedo al cambio.

- la posibilidad de ser atacados por terceros o personas que dentro de la organización puedan aprovechar su condición conocimiento para intentar sacar provecho de los recursos y la información de la organización.

De acuerdo a la apreciación de Cortés. H (2019) "*A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla*".

3.4 Instrumento de investigación la Entrevista

Entrevista con el director de continuidad del negocio de la entidad financiera.

1. ¿cuánto tiempo lleva laborando en la entidad?

R/ 28 años

2. ¿Cuánto tiempo lleva trabajando en la dirección de Continuidad del Negocio?

R/10 años

3. ¿Por favor nos puede indicar cuál cree usted que es la principal fortaleza de continuidad del negocio en esta organización?

R/ la experiencia y la seguridad de estar listos para afrontar las contingencias que se puedan presentar

4. ¿Cuándo fue la última contingencia y porque ocurrió?

R/ en diciembre de 2021 contingencia grave ya que por un error humano se apagó abruptamente el sistema central del banco, dejando fuera de servicio toda la operación a nivel País.

5. ¿se pudo haber evitado?

R/ si fue uno por falta de capacitación de la ingeniera que materializo el hecho y porque no hubo en su momento un sistema de seguridad física del equipo que es vital para la operación del banco.

6. ¿Cómo se recuperó la operación del banco?

R/ se activaron los protocolos de contingencia y primordialmente de acuerdo al escenario la movilización al sistema central alterno del banco.

Telecomunicaciones, seguridad informática, riesgo, seguridad de la información apoyaron la directriz dada y documentada por la dirección de continuidad del negocio

7. ¿En cuánto tiempo se restableció el servicio?

R/ tenemos un tiempo de recuperación tecnológica por protocolo de máximo 6 horas, pero para esa situación en particular se retornó a operación en 2 horas. Fue un éxito para nosotros

8. ¿Cuál cree usted que es la principal debilidad de continuidad del negocio?

R/ el factor humano, la falta de capacitación y experiencia los equipos rara vez fallan el ser humano si lo hace y también considero que la tercerización de proceso ya que la entidad puede perder el control de los procesos.

9. ¿Cree usted que el presupuesto que maneja el área de continuidad del negocio es el apropiado para la operación?

R/al final de cada año nos reunimos con financiera y con el comité de riesgo y del presupuesto base se analizan que proyectos se manejaran durante el siguiente año, y por lo general el comité lo aprueba, igualmente se deja un rublo para eventualidades, pero el valor exacto no se dice por confidencialidad.

10. ¿Cree usted que los controles establecidos evitan que se materialicen los riesgos?

R/ aunque en esta organización existe un área en particular que trabaja todo lo relacionado con riesgo, nosotros Continuidad, por ser un área de apoyo y por ser miembro del comité de crisis estamos en el derecho de realizar recomendaciones, pero creo particularmente que no hay Organización por ciento blindada a sufrir ataques cibernéticos que tanto están de moda o errores humanos como lo indique al inicio de esta entrevista.

11. ¿Usted cuál que es el futuro de continuidad del negocio?

R/La nube definitivamente, todo apunta que vamos para allá.

12. ¿La entidad ya tiene servicios en estas plataformas?

R/si, aunque son pocas ya se están viendo los beneficios de estos servicios y se está trabajando para llevar muchos procesos más este año, considero que al finalizar estaremos por lo menos con la mitad de las aplicaciones en la nube.

13. Particularmente Continuidad del Negocio ¿Qué proyecto maneja a corto plazo?

En este momento estamos liderando el tema de Home Office, que ya no sea conexión remota a las terminales físicas de la organización, sino que le demos un portátil a cada funcionario con esa modalidad de trabajo y desde la casa pueda acceder por LAN extendida directamente a las aplicaciones data y servicios del banco sin está conectado a la terminal del banco.

14. ¿se corre algún riesgo al permitir que los funcionarios accedan a la información desde la casa?

R. siempre existirán los riesgos, pero también el banco cuenta con herramientas que permiten minimizarlos como para este caso son: la doble autenticación, el manejo del

firewall, la VPN y el antivirus corporativo, además de la restricción de puertos de salida de información y otras restricciones internas de las politicas de dominio de la organización.

4. RESULTADOS Y HALLAZGOS.

Se conoció la generalidad de la infraestructura tanto en el ambiente de producción como en ambiente de contingencia y se compararon los dos centros de cómputo los cuales trabajan de manera sincrónica y sus capacidades son muy similares.

Dentro de la evaluación de las politicas de seguridad de la entidad financiera están sustentadas principalmente en dos áreas administradoras, Seguridad de la información y Riesgo, dos áreas de apoyo que ejecutan las politicas que son seguridad informática y continuidad del negocio y otras áreas de apoyo como telemática y el área de telecomunicaciones.

Los dueños de proceso que son generalmente los jefes o directores del área desde donde opera el proceso los responsables de reportar la materialización de un riesgo como primera instancia al director de continuidad o la dirección de seguridad de la información igualmente está establecido dentro de la organización un comité de riesgo que también está en la capacidad de toma de decisiones frente a estas situaciones.

Dentro de la seguridad física de la información se encuentran en la organización los dos principales dispositivos de almacenamiento llamados Storage uno Z vs y vm y el XIV

El Z que es administrado por un tercero IBM pero supervisado por el área de System que hace parte de la gerencia de infraestructura de la organización es el encargado de almacenar la data transaccional de entidad a nivel nacional por ahí pasan todos los movimientos financieros de la organización y es llamada la alcancía porque ahí está hospedado el dinero, tiene la par en el centro de cómputo de contingencia y siempre se encuentran conectados de manera sincrónica, para su respaldo también cuenta con copia primarias, secundarias y terciarias, y almacenamiento histórico en cintas.

El segundo Storage que es el XIV es administrado por el área de infraestructura de La organización y es principalmente donde se hospedan los aplicativos y data de procesos de la

organización también ahí se encuentran los archivos vitales de cada área, están las bases de datos de la aplicaciones y desarrollos de la organización.

El acceso físico a los centros de cómputos esta dado por medio de puertas biométricas, registro por planillas, autorizaciones dadas y exclusivamente por el director o el gerente de infraestructura a personal restringido, bitácora de actividades, cuenta con sistema cerrado de cámaras las cuales graban 7 días por 24 horas y están monitoreadas por el centro de cómputo.

Esta área esta respalda por ups contratadas a terceros y cuenta con conexión directa a la planta eléctrica del edifico con una promesa de interrupción en caso de falla de fluido eléctrico de máximo 5 minutos tiempo que operarían las Ups en caso de ser requerido.

Sistema de detección de humo con extintores de gas no agua ya que este sistema es especial para operaciones donde hay servidores equipos electrónicos y centros de cómputo.

Un hallazgo durante una de las pruebas DRP en las cuales se estuvo presente, se presentó cuando el servidor que hace las veces de controlador de dominio principal y que a su vez hace parte de los 5 servidores de dominio que trabajan en anillo, en el momento de replicarse a contingencia, presento fallas en la hora de configuración, y se describe de la siguiente manera:

Como la prueba era en ambienté cerrado y copia de la infraestructura de producción, no se pudo recrear de manera correcta en el ambiente de contingencia debido a que este servidor replico el error de horario en los demás servidores y a su vez las terminales que se requerían matricular no les permite ingresar al dominio, se debió cancelar las pruebas de recuperación tecnológica y teniendo en cuenta que por normativa interna de la organización se deben ejecutar como mínimo dos pruebas al ambiente de contingencia, recalco en un inconformidad ante los entes de control y un incumplimiento en los cronogramas del área y el alto riesgo que se pueda materializar la situación descrita en una contingencia real.

5. CONCLUSIONES

Luego de presentar los resultados, se evalúa que los procesos, pruebas, estrategias y metodología presentada por el área de continuidad del negocio, dentro de la organización presenta y refleja un alto grado de madurez ya que ante los riesgos materializados que conllevaron a las activaciones reales de contingencias, se ha tenido respuesta en un tiempo más que aceptable a la promesa de RTO (tiempo de recuperación Objetivo) de 6.5 horas, las activando sus protocolos y estrategias y cumpliendo en todas las contingencias históricas. Frente hipótesis propuestas Es posible evaluar los riesgos de los procesos de continuidad del negocio en una entidad financiera de cubrimiento nacional, gracias a la herramienta DOFA producto de la observación en los procesos, la metodología las buenas y las malas prácticas en el desarrollo de las actividades propias del área evaluada y del desarrollo de la actividad de entrevista al director del área de continuidad del negocio de la entidad financiera estudiada se pudo evaluar aspectos relevantes que se describen a continuación:

Durante las pruebas de recuperación tecnológicas y al finalizar las mismas, por la dinámica de estos ejercicios, los analistas e ingenieros resuelven los inconvenientes que se generen en ese momento, pero muchas veces ese conocimiento en resolución de inconvenientes no queda debidamente registrado en un manual o documentación oficial de la prueba.

Se sugiere y surge la necesidad de realizar una reunión de cierre de prueba para ajustar inconvenientes, oficializar documentación, validar formatos y registros y así evitar reprocesos que se presentan en las pruebas posteriores.

Se evidencio que existe alto grado de rotación en el personal crítico de los procesos y al ser ellos que desarrollarían las contingencias, suele suceder que ese personal se retira de la organización y en bajo índice hay una persona igualmente capacitada para sumir este rol.

Se personalizan los procesos y por parte de los jefes del área no ven la real necesidad de que su equipo de trabajo este en la capacidad de respaldar o remplazar las funciones de sus mismos compañeros

6. REFERENCIAS BIBLIOGRÁFICAS

Aguiñaga, D. (2019) Manejo de crisis gobierno corporativo de México

Álvarez. G. (2004). Seguridad informática para las empresas y particulares. Madrid, España: McGRAW-HILL.

Bacon, A. (2020). Metodología y crisis

Báez, J. (2009). Investigación Cualitativa.

Benavides. A (2017). Modelo de sistemas de gestión de la información bajo la norma ISO 27001:2015 para las instituciones públicas de educación básica.

Bernal, C. (2010). Metodología de la Investigación. Administración, economía, humanidades y ciencias sociales. Bogotá, Colombia: Pearson. 3ª edición.

Berrio, M. (2016). Metodología para la evolución del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO 27001. Tesis de Maestría: Universidad Nacional de Colombia. Medellín.

Bonilla, E. (2011). Metodología de la investigación. Un enfoque práctico. Bogotá: Gente Nueva Editorial.

Camelo, L. (2010). Seguridad de la información en Colombia. Experiencia personal: dificultades en la implementación de un SGSI. Disponible en internet: (seguridaddelainformacionencolombia.blogsplot.com.co/2010/02/experiencia-personal-dificultades-en-la-htm)

Castellanos, J. (2019). Publicación importancia de las TIC para la competitividad de las Pymes en Colombia, Universidad Pontificia Bolivariana PUENTE Revista científica.

Cortes, H. (2019). Principios de Ciberseguridad. Ingeniería Social: Phishing y Baiting

Diaz, M. (2020). Guía práctica de la norma UNE ISO 27000.

Durkheim (1917). Conocimiento objetivo y lo cualitativo

Garavito, C. (2016). Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Según norma ICONTEC

García, M. (2021). Activos Intangibles

Giménez, J. (2019). Seguridad de equipos informáticos.

Humphrey, R. (1969) lo bueno y lo malo de la investigación

Ladino, A. (2019). Fundamentos Del Sistema De Gestión De La Seguridad 27001.

Leyva. N. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje. Sociedad & Tecnología, 4(2), 205-222.

Marchionni, E. (2020). Administración de servidores

Montoya, A. (2016). Guía de Continuidad del negocio.NTC/ISO 22301.

Ocampo, C. (2017). Sistema de detección de intrusos en redes corporativas; 2017

Rosales, I. (2019). Gestión Ethical

Ruiz, H. (2019). Redes hacia la integración académica.

Smith, W. (2019). Planes de contingencia centro de cómputo

Suarez, D. (2015). Análisis y diseño de un sistema de gestión de seguridad informática en la empresa Suarez padilla $ cia Tesis de Maestría: Universidad Nacional Abierta y a Distancia. Bogotá, Colombia.

CORPORACIÓN UNIVERSITARIA
UNITEC

Por intermedio del presente documento en mi calidad de autor o titular de los derechos de propiedad intelectual de la obra que adjunto, titulada **ESTRATEGIAS DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN Y DEMÁS RECURSOS INTERNOS DE UNA RED INFORMÁTICA, MEDIANTE LAS BUENAS PRÁCTICAS DE LA NORMA ISO 27000 DE CONTINUIDAD DEL NEGOCIO EN UNA ENTIDAD FINANCIERA DE OPERACIÓN NACIONA**L, autorizo a la Corporación universitaria Unitec para que utilice en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador o titular de la obra objeto del presente documento.

La presente autorización se da sin restricción de tiempo, ni territorio y de manera gratuita.

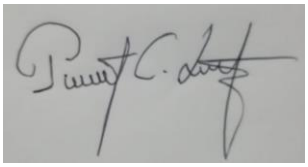
Entiendo que puedo solicitar a la Corporación universitaria Unitec retirar mi obra en cualquier momento tanto de los repositorios como del catálogo si así lo decido.

La presente autorización se otorga de manera no exclusiva, y la misma no implica transferencia de mis derechos patrimoniales en favor de la Corporación universitaria Unitec, por lo que podré utilizar y explotar la obra de la manera que mejor considere. La presente autorización no implica la cesión de los derechos morales y la Corporación universitaria Unitec los reconocerá y velará por el respeto a los mismos.

La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato electrónico, y en general para cualquier formato conocido o por conocer. Manifiesto que la obra objeto de la presente autorización es original y la realicé sin violar o usurpar derechos de autor de terceros, por lo

tanto, la obra es de mi exclusiva autoría o tengo la titularidad sobre la misma. En caso de presentarse cualquier reclamación o por acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión asumiré toda la responsabilidad, y saldré en defensa de los derechos aquí autorizados para todos los efectos la Corporación universitaria Unitec actúa como un tercero de buena fe. La sesión otorgada se ajusta a lo que establece la ley 23 de 1982.
Para constancia de lo expresado anteriormente firmo, como aparece a continuación.

Firma



Robert Castro Lisca
Nombre
CC. 79.187.886