UNIVERSIDAD CENTRAL

VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ANÁLISIS DE LA EFICACIA OPERATIVA DE LOS CONTROLES GENERALES EN UNA ENTIDAD BANCARIA PARA EL AÑO FISCAL 2023

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO DE LICENCIATURA EN INGENIERÍA INFORMÁTICA CON ÉNFASIS EN GERENCIA INFORMÁTICA

ELABORADO POR:

ING. MARICRUZ QUESADA SÁNCHEZ

TUTOR:

ING. MARCO VARGAS DURÁN

SEDE CENTRAL

ABRIL, 2025

Índice General

Capítulo I: Introducción 5
Planteamiento del Problema 5
Objetivo General 6
Objetivos Específicos 7
Justificación 7
Antecedentes 8
Antecedentes internacionales 8
Antecedentes nacionales 9
Proyecciones 11
Limitaciones 13
Capitulo II: Marco teórico 15
Componentes del control interno. 22
Controles Generales de TI 24
Importancia de los controles generales de TI en el sector bancario 25
Clasificación de los Controles Generales de TI 26
Control de Acceso 27
Control de Cambios 27
Controles de Operación 28
Normas Internacionales de Control Interno y TI 29
Marco COSO (committee of sponsoring organizations of the treadway commission) 29
COBIT (control objectives for information and related technologies) 30
ISO/IEC 27001 (Gestión de Seguridad de la Información) 31
ITIL (Biblioteca de Infraestructura de TI) 31
Regulaciones financieras aplicables al sector bancario 32
Leyes y regulaciones nacionales sobre seguridad informática y auditoría 33
Eficacia operativa de controles de TI 33
Métodos y enfoques para la evaluación de controles de TI 34
Auditorías internas y externas 35
Evaluaciones de riesgos 35
Pruebas de cumplimiento 36
Cumplimiento normativo y disponibilidad de sistemas 36

Impacto de los controles generales de TI en la operación del banco 37
Seguridad de la Información y protección de datos 37
Prevención del fraude y riesgos financieros 38
Impacto en la experiencia del cliente y la confianza institucional 38
Diseño y funcionamiento de controles. 39
Diseño de controles efectivos. 40
Tipos de controles internos: preventivos, detectivos y correctivos. 41
Procedimientos y políticas internas 42
Normativas y estándares 42
Normas internacionales y locales sobre control interno. 43
Relevancia de estas normativas en el sector bancario. 43
Controles generales de tecnología de información (CGTI) 43
Importancia de los CGTI en el control interno 44
Componentes de los CGTI 44
Evaluación y pruebas de los controles generales de tecnología de información (CGTI) 45
Impacto de las deficiencias de control. 47
Informe y corrección de deficiencias. 47
Capitulo III: Marco metodológico 49
Enfoque de la investigación 49
Métodos de Investigación 49
Tipos de investigación 50
Fuentes de información. 50
Primarias 51
Secundarias 51
Terciarias 51
Sujetos de información 52
Población 52
Muestra 52
Tipo de muestra. 52
Consideraciones éticas 53
Técnicas 53
Instrumentos 54
Información documental 54
Entrevistas no estructuradas 55

Proceso para la Recolección y Análisis de Datos 55
Capitulo IV: Análisis de resultados 56
Historia de la entidad 57
Alcance de la investigación 58
Alcance del sistema a evaluar en la investigación 58
Entendimiento de controles de la organización 61
Desarrollo de la investigación 73
Controles de seguridad de accesos: 80
Análisis del impacto de las deficiencias 92
Capitulo V: Conclusiones y recomendaciones 95
Hallazgo 1 95
Recomendación 1 95
Causa raíz 1 96
Plan de acción de la administración 1 96
Hallazgo 2 96
Recomendación 2 97
Causa raíz 2 97
Plan de acción de la administración 2 98
Referencias 98
Apéndices 103
Entrevistas 103

Capítulo I: Introducción

En este apartado se define el problema de investigación, para lo cual se desarrolla un objetivo general y los objetivos específicos, así como una justificación con la cual se expone la importancia de este. Con respecto a los antecedentes, se detalla el fundamento histórico que le precede; por último, se proyectan los resultados esperados.

Planteamiento del Problema

Los Controles Generales de Tecnología de la Información (CGTI) son esenciales para garantizar la seguridad, confiabilidad y eficiencia en la gestión de los sistemas informáticos de las instituciones bancarias. Estos controles se han convertido en un aspecto cada vez más relevante debido a los riesgos a los que se enfrenta el sector bancario en la era digital. Las amenazas cibernéticas, los ataques de malware, el acceso no autorizado a datos sensibles y las brechas de seguridad son solo algunas de las vulnerabilidades que enfrentan los bancos, lo que los hace propensos a violaciones de la Seguridad de la Información. Para mitigar estos riesgos, las entidades bancarias deben contar con mecanismos de control robustos que les permitan asegurar la protección de los datos y la operación de sus aplicaciones.

Los CGTI tienen como objetivo principal establecer las políticas y prácticas necesarias para la gestión adecuada de los sistemas informáticos dentro de las instituciones financieras. Estos controles incluyen, entre otras cosas, la protección de la infraestructura tecnológica, la gestión de accesos y permisos de los usuarios, la segregación de funciones y la revisión periódica de los perfiles de los empleados que

tienen acceso a sistemas clave. En el caso específico de los bancos, los CGTI también deben asegurar que los procesos críticos que soportan la información financiera cumplan con las normativas y estándares de seguridad establecidos por las autoridades regulatorias del sector.

Una auditoría de los controles generales de TI permite a la entidad obtener un grado de confianza sobre el estado de sus sistemas y procesos tecnológicos. A través de esta auditoría, se puede verificar si las prácticas de gestión de TI son adecuadas y si los controles establecidos son efectivos para proteger la información financiera y garantizar su integridad, disponibilidad y confidencialidad. Los resultados de una auditoría de CGTI proporcionan a los responsables de la entidad una visión clara sobre las áreas en las que los controles podrían ser insuficientes o ineficaces, lo que les permite tomar medidas correctivas y mejorar la Seguridad de la Información.

A través de una gestión adecuada de los controles generales de TI, las instituciones bancarias pueden reducir significativamente el riesgo de sufrir violaciones de seguridad, proteger la confidencialidad de los datos de los clientes y garantizar que la información financiera se mantenga disponible e íntegra en todo momento. La implementación de controles efectivos no solo beneficia a la entidad en términos de seguridad, sino que también fortalece su reputación y confiabilidad ante los clientes, inversores y autoridades regulatorias. Por lo tanto, los CGTI desempeñan un papel crucial en la capacidad de un banco para operar de manera segura y cumplir con los requisitos legales y operativos que aseguran la estabilidad del sistema financiero.

Objetivo General

- Evaluar la eficacia de los controles generales de TI en el banco, a través de la ejecución de una auditoría, para áreas de mejora y así se evalúa la seguridad, confiabilidad y disponibilidad de los sistemas principales para el año 2023.

Objetivos Específicos

- Identificar el marco de control interno, realizando entrevistas con los dueños de los controles identificados, para el funcionamiento y diseño de los controles, políticas y procedimientos.
- Evaluar los Controles Generales de Tecnología de Información (CGTI) identificados y diseñados, generando muestreo acorde a la población identificada, concluyendo cada control.
- Analizar las deficiencias o desviaciones identificadas, clasificando por el nivel de impacto, para que la entidad ejecute un plan de remediación a cada punto.

Justificación

La creciente necesidad de abordar los riesgos de Tecnologías de la Información (TI) a los que están expuestas las entidades bancarias justifica plenamente la realización de este proyecto. Los riesgos derivados de la evolución y complejidad del entorno digital representan una amenaza constante para la seguridad, confidencialidad, disponibilidad e integridad de los datos, especialmente en el ámbito financiero. La exposición de los bancos a estos riesgos, si no se mitiga adecuadamente, puede generar consecuencias tanto para la entidad como para los clientes y otras partes interesadas.

Resolver el problema de la ineficiencia y vulnerabilidad en los controles generales de TI es crucial para la seguridad y estabilidad de la entidad bancaria. La evaluación permitirá identificar áreas de mejora y brechas que podrían estar dejando al banco vulnerable, garantizando que las medidas implementadas estén alineadas con las mejores prácticas de seguridad y las regulaciones del sector financiero.

El proyecto debe realizarse para asegurar que el core bancario utilizado por el banco es seguro, confiable y capaz de responder de la mejor manera ante una amenaza o

vulnerabilidad que pueda surgir. La evaluación de los Controles Generales de TI (CGTI) es una práctica fundamental para garantizar que los controles implementados sean adecuados para prevenir, detectar y corregir los riesgos que afectan a los sistemas de TI del banco.

Este análisis permitirá determinar si los controles implementados son efectivos para mitigar los riesgos de TI y financieros que la entidad enfrenta. Uno de los principales objetivos es garantizar que los controles generales de TI sean lo suficientemente robustos para proteger la información financiera que maneja el banco, asegurando su confidencialidad, integridad y disponibilidad. Esto es fundamental, ya que los datos financieros son activos altamente sensibles y cualquier brecha en su seguridad puede tener consecuencias devastadoras tanto para el banco como para sus clientes. Los controles deben ser diseñados y evaluados para prevenir el acceso no autorizado, proteger los datos frente a posibles manipulaciones y asegurar que la información esté siempre disponible para su uso legítimo.

Antecedentes

En este apartado se muestran diferentes trabajos de investigación, tanto a nivel nacional como internacional. Adicionalmente, la importancia de estos se relaciona con el tema de interés en estudio, el cual trata sobre el análisis de la eficacia operativa de los controles generales de TI para el banco. Se pudo identificar diversos marcos de regulación, estándares de buenas prácticas y artículos sobre el fondo de esta tesis.

Antecedentes internacionales

Lopez (2015), en su tesis “Propuesta de implementación de una metodología de auditoría de seguridad informática.

El estudio basó su investigación en evaluar las metodologías de auditoría de seguridad más utilizadas en aquel momento para desarrollar la implementación de la que se considere más oportuna. De la investigación realizada se pude observar que se desarrolló una guía de implementación de la metodología OSSTMM que le va a permitir a los estudiantes recién graduados y con poca experiencia en seguridad informática poder ejecutar sus primeras auditoria siguiendo una metodología de reconocido prestigio.

Marrugo y Salgados (2015), en su tesis "Evaluación a la guía de auditoria elaborada para el desarrollo de aplicaciones y control de cambios de los sistemas de información en producción de la empresa BANCSMÏA S.A.

El estudio basó su investigación en evaluar la guía de auditoría elaborada para el desarrollo de aplicaciones y control de cambios de los sistemas de información en producción en la empresa Bancamía S.A. De la investigación realizada se pude observar que se identificaron, analizaron y evaluaron las principales variables contempladas en la guía de auditoría para el desarrollo de aplicaciones y control de cambios. Como parte de la investigación se desarrollo un informe con el detalle de los principales hallazgos identificados y se les hicieron recomendaciones acordes a los estándares definidos, esto debido a que se analizó el riesgo tan alto al que se exponen las entidades del sector financiero ya que son entidades muy expuestas a la perdida, fuga y plagio de la información de sus clientes.

Antecedentes nacionales

Con relación de los antecedentes nacionales Guzmán (2007) defendió su tesis de postgrado denominada: "Auditoría de la seguridad de las Tecnologías de Información del Instituto Costarricense de Acueductos y Alcantarillados, (AyA). El objetivo general de esta investigación fue evaluar la Seguridad de las Tecnologías de Información en el Centro de Informática del Instituto Costarricense de Acueductos y Alcantarillados, para

comprobar la existencia y cumplimiento de procedimientos y políticas organizacionales que sirvan de apoyo a las prácticas de seguridad física y lógica relacionadas con los sistemas de información en conformidad con la normativa vigente.

El estudio basó la investigación en determinar la situación actual de la Administración de la Seguridad de las tecnologías de Información en el Centro de Informática del Instituto Costarricense de Acueductos y Alcantarillados con el propósito de valorar aspectos claves que permitan determinar la criticidad del área. De la investigación realizada se llega a conclusión que gran parte de la población laboral del Instituto carece de concientización y conocimientos de los aspectos de Seguridad de las Tecnologías de información, aspecto de alta criticidad que debe ser atendido en el menor tiempo posible, al igual se identificó que cuentan con un plan de continuidad del negocio, pero el mismo debe ser mejorado. Se realizaron varias recomendaciones con el fin de robustecer los controles evaluado donde se identificaron oportunidades de mejoras.

Chavarría (2018), en su tesis “Auditoría de la seguridad de información en una empresa privada costarricense” donde su objetivo fue realizar una auditoría de la Seguridad de la Información en una empresa de sector privado costarricense, la metodología se basó en evaluar de las actividades de control del proceso interno para administrar la Seguridad de la Información de la empresa y los datos del Sistema de Administración de nómina. De dicha investigación se determinó la suficiencia de la seguridad de la compañía y se emitieron las recomendaciones correspondientes a los aspectos identificados como puntos de mejora, con el objetivo de robustecer los puntos identificados y que esto permita al negocio operar correctamente.

Adicionalmente Brenes (2022), en su tesis “Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras”, pretende elaborar una propuesta de mejora de los Controles Generales

de TI para los procesos “Acceso a Programas y Datos” y “Operación de Computadoras” por medio de una comparativa de la metodología actual con COBIT 2019 con el fin de identificar posibles brechas en los procesos; en un período de 15 semanas para una empresa de Auditoría.

El estudio basó su metodología de investigación en comparar la metodología implementada por la firma para la evaluación de los Controles Generales de TI con un marco de referencia reconocido a nivel global para la identificación de las posibles brechas en los procesos de Operación de Computadoras y Accesos a Programas y Datos. De la investigación realizada se pude observar que se identificaron oportunidades de mejora para los controles y procesos que se evaluaron dando recomendaciones viables a implementar.

Proyecciones

La presente investigación tiene como objetivo principal la evaluación de los Controles Generales de TI en los procesos de Administración de Cambios, Administración de Accesos y Administración de la Red del banco para el año 2023. Esta evaluación busca identificar las deficiencias existentes en los controles actuales y proporcionar recomendaciones adecuadas para mejorar cada aspecto detectado. A corto plazo, se espera realizar una revisión exhaustiva de los controles actuales, lo que permitirá detectar rápidamente las áreas de oportunidad y formular soluciones viables que no solo contribuyan a la mejora de los sistemas, sino que también aseguren el funcionamiento continuo del negocio. La clave de este enfoque es garantizar que las medidas correctivas sean factibles y apropiadas para la estructura operativa del banco, de modo que se puedan implementar sin causar interrupciones en las operaciones diarias.

A mediano plazo, la investigación tiene como objetivo abordar las deficiencias que presenten un mayor riesgo para la Seguridad de la Información y los sistemas del

banco. En particular, se pretende que los hallazgos con un nivel de riesgo alto sean remediados lo más pronto posible, dado que su resolución es crucial para mitigar posibles incidentes de seguridad que puedan afectar la integridad y disponibilidad de los datos financieros. Una vez que estos controles de alto riesgo hayan sido corregidos, el banco podrá realizar una nueva validación para asegurarse de que las soluciones implementadas están funcionando de manera eficaz. Este proceso de validación será fundamental para confirmar que los controles ahora son lo suficientemente robustos y que cumplen con los estándares de seguridad requeridos por la entidad.

A largo plazo, se espera que todos los hallazgos identificados durante la evaluación sean corregidos, independientemente del nivel de riesgo que representen. El objetivo final es garantizar que todos los controles generales de TI sean lo suficientemente sólidos como para proteger los sistemas de información del banco y, de esta manera, asegurar la confidencialidad, integridad y disponibilidad de los datos financieros. La completa remediación de los hallazgos permitirá que el banco valide el funcionamiento adecuado de todos los controles de TI, lo que contribuirá a confirmar que los sistemas son confiables y seguros frente a cualquier tipo de amenaza o vulnerabilidad. Además, esto generará un entorno operativo en el que se podrá confiar plenamente en los sistemas de TI del banco para la gestión de datos críticos y la ejecución de servicios financieros.

Sin embargo, es importante reconocer que la implementación de los controles generales de TI no será un proceso completamente sencillo. Algunos de los hallazgos pueden requerir esfuerzos significativos por parte de la administración de TI, lo que incluye la capacitación continua del personal, el desarrollo de nuevas políticas y procedimientos, así como la inversión en tecnologías que faciliten la ejecución de controles. Estos esfuerzos no solo son necesarios para corregir las deficiencias actuales, sino que también permitirán que el banco se adapte a las nuevas amenazas y desafíos del

entorno tecnológico. En muchos casos, también será necesario un esfuerzo de concientización a nivel organizacional, para asegurar que todos los empleados comprendan la importancia de los controles de TI y su responsabilidad en la protección de la información.

A medida que avanza la remediación de los hallazgos, se espera que la administración de TI pueda establecer planes de acción claros, asignando responsables y plazos específicos para cada tarea de mejora. De esta manera, la corrección de las deficiencias podrá ser gestionada de forma eficiente, asegurando que se logre una mejora continua en los controles generales de TI. En este sentido, la administración de TI debe comprometerse a realizar un seguimiento constante de los avances y, si es necesario, ajustar los enfoques para garantizar que los controles se implementen de manera efectiva. A largo plazo, este proceso de mejora continua contribuirá significativamente a la robustez de los sistemas de información del banco, lo que permitirá reducir los riesgos asociados con la falta de controles adecuados y mejorar la seguridad general de los datos.

Una vez que se hayan implementado y validado los controles corregidos, el objetivo será alcanzar un nivel de madurez óptimo en los Controles Generales de TI. Esto implicará la implementación de prácticas que permitan no solo la protección frente a amenazas actuales, sino también la preparación para gestionar riesgos futuros, contribuyendo a la estabilidad y seguridad de la infraestructura tecnológica del banco a largo plazo. Los sistemas deberán ser capaces de operar de manera eficiente, protegiendo tanto la información confidencial como los procesos clave del banco, sin que los usuarios o las amenazas externas puedan comprometer su funcionamiento.

Limitaciones

Esto es una tesis de carácter confidencial, no puede ser publicada ni utilizada la información que es descrita acá ya que es información privada y confidencial.

Capitulo II: Marco teórico

En este capítulo se desarrollan los conceptos para una mejor comprensión de la evaluación de los Controles Generales de TI para el Banco. A lo largo del tiempo, los riesgos a los que estan expuesto los bancos, lo sensibles que son las operaciones financieras, así como la dependencia que existe hoy día de los procesos automatizados que corren en los sistemas donde se llevan los estados financieros y la contabilidad son mayor.

Debido a lo anterior, es importantes un control interno robusto que permita garantizar la integridad, eficiencia y seguridad de sus operaciones. En un entorno financiero que cada vez es más complejo y regulado, los controles internos se convierten en una herramienta indispensable para la gestión y el crecimiento de los bancos.

En este capítulo vamos a poder profundizar en elementos importantes para poder desarrollar nuestra investigación, como lo es el entendimiento de TI de la entidad, el control interno, los controles generales de TI, área de controles a evaluar, control de accesos, control de cambios, controles de operaciones, las diferente normativas y marcos regulatorios en los que se basan los controles generales.

Durante el entendimiento realizado a la entidad se identificaron aspectos muy importantes como la implementado la herramienta CyberArk, cuyo objetivo es proteger, gestionar y monitorear las cuentas privilegiadas para prevenir accesos no autorizados y ciberataques.

CyberArk proporciona funcionalidades clave como:

Gestión de contraseñas: Almacena credenciales privilegiadas en un "cofre" digital seguro, permitiendo la gestión centralizada de accesos y auditorías.

Rotación automática de contraseñas: Reduce el riesgo de compromisos al cambiar las credenciales en intervalos regulares.

Control de accesos: Administra permisos basados en políticas de seguridad, integrando autenticación multifactor para mayor protección.

Monitorización y registro: Supervisa y registra las actividades de las cuentas privilegiadas para detectar posibles amenazas.

Supervisión de sesiones privilegiadas: Registra y analiza sesiones de acceso para disuadir el mal uso de credenciales.

Auditoría y cumplimiento: Genera informes detallados para garantizar el cumplimiento normativo y la trazabilidad de accesos.

Integración con otros sistemas de seguridad: Permite construir un marco de seguridad más robusto y coherente.

Además de la gestión de accesos privilegiados, otro control fundamental para el banco es la Recertificación de Usuarios. Este proceso asegura que los usuarios cuenten con permisos adecuados y que no tengan accesos innecesarios o inapropiados. Para ello, se establecen políticas claras, procedimientos detallados y revisiones periódicas de los accesos de los usuarios. La recertificación permite prevenir accesos no autorizados, reducir riesgos de seguridad y garantizar el cumplimiento de las mejores prácticas en gestión de identidades.

Otro aspecto crítico en la seguridad del sistema es la configuración de parámetros de contraseñas, que permite definir políticas de seguridad como:

Longitud mínima y complejidad de las contraseñas.

Caducidad y rotación periódica de credenciales.

Historial de contraseñas para evitar reutilización.

Límites en intentos fallidos de inicio de sesión para prevenir bloqueos indebidos.

Aspectos Claves sobre la Segregación de Funciones

La segregación de funciones es un principio fundamental en la gestión de riesgos y el control interno de las organizaciones. Su implementación efectiva permite minimizar errores, evitar fraudes y garantizar la transparencia en los procesos. A continuación, se detallan los aspectos clave de la segregación de funciones:

1. Limitación del acceso completo a las transacciones: Ninguna persona debe tener acceso total para autorizar, procesar y revisar una transacción. La separación de estos roles reduce el riesgo de errores o actividades fraudulentas, promoviendo la seguridad y la confiabilidad en la gestión de recursos.

2. Definición y separación de responsabilidades: Es crucial establecer responsabilidades claras y diferenciadas dentro de los procesos operativos. Por ejemplo, en un proceso de compras, una persona puede solicitar el pedido, otra aprobarlo y una tercera procesar el pago. Esto ayuda a evitar conflictos de interés y garantiza una adecuada rendición de cuentas.

3. Implementación de controles de acceso: Es fundamental restringir el acceso a funciones y datos críticos solo a personas autorizadas. Esto se puede lograr mediante el uso de credenciales de usuario, permisos específicos y autenticación multifactor, lo que refuerza la seguridad en el manejo de la información.

4. Supervisión y revisión constante: Se deben establecer mecanismos de supervisión y auditoría para asegurar el cumplimiento de las políticas de segregación de funciones. Las auditorías internas y revisiones periódicas permiten detectar irregularidades y mejorar continuamente los procesos.

5. Capacitación del personal: Es esencial que los empleados comprendan la importancia de la segregación de funciones y sigan los procedimientos adecuados. Programas de formación continua pueden ayudar a sensibilizar al personal sobre los riesgos asociados y la manera de mitigarlos.

6. Documentación clara y actualizada: Mantener políticas y procedimientos bien documentados garantiza una correcta aplicación de la segregación de funciones y facilita la identificación de oportunidades de mejora. Además, permite una referencia clara para auditorías y revisiones regulatorias.

La segregación de funciones es una práctica indispensable en cualquier organización, independientemente de su sector. Su implementación requiere una planificación cuidadosa y un entendimiento profundo de los procesos y riesgos asociados. En sectores altamente regulados, como el financiero, su aplicación es aún más crítica debido al elevado riesgo de fraude y pérdida de datos.

Control interno

El control interno representa la base sobre la cual las organizaciones aseguran el cumplimiento de sus objetivos estratégicos y operativos. En mi opinión, el control interno no solo se centra en la prevención y detección de errores, sino también en la creación de un entorno de confianza y responsabilidad. La implementación de controles sólidos permite a las instituciones mitigar riesgos, cumplir con regulaciones, y promover la sostenibilidad organizacional en el largo plazo. Estos controles operan como un marco estructurado que guía las actividades de la organización hacia el cumplimiento de sus metas, protegiendo los activos e información valiosa, y asegurando la correcta ejecución de las tareas asignadas.

De acuerdo con Hernández y Mendoza (2018), "el control interno es un conjunto de procesos diseñados para garantizar la eficiencia de las operaciones, la seguridad de los activos, y la integridad de la información financiera, asegurando el cumplimiento de leyes y regulaciones aplicables". Esto destaca su carácter integral como herramienta esencial en la gestión organizativa. El control interno no solo se limita a la parte operativa, sino que también abarca la gestión de riesgos y la mejora continua de los procesos. Cada

componente del control interno tiene un papel clave en la organización, desde la planificación hasta la ejecución, lo que refuerza su importancia para el buen funcionamiento institucional. La correcta implementación de estos controles promueve una cultura organizacional sólida basada en la transparencia y en la rendición de cuentas, aspectos cruciales para la sostenibilidad a largo plazo.

El control interno también está estrechamente vinculado con la capacidad de adaptación de las organizaciones a entornos cambiantes. En un mundo globalizado y con constantes avances tecnológicos, las instituciones deben ser ágiles para gestionar no solo los riesgos financieros, sino también los cibernéticos, operacionales y de cumplimiento.

Un control interno robusto no solo detecta y mitiga riesgos, sino que también ofrece la flexibilidad necesaria para adaptar los procesos a nuevas regulaciones o cambios en el mercado, asegurando la continuidad del negocio y la protección de los recursos. Esto incluye el monitoreo continuo de las actividades y la retroalimentación constante, lo que permite ajustar los controles de manera eficiente frente a nuevas amenazas o ineficiencias detectadas.

Además, los controles internos tienen un impacto directo en la mejora de la competitividad de la organización. Al establecer un sistema confiable de controles, las organizaciones no solo cumplen con los estándares regulatorios, sino que también optimizan sus procesos, reducen costos operacionales, mejoran la toma de decisiones y fortalecen la confianza de los inversores y otras partes interesadas. La implementación adecuada de estos controles facilita la transparencia en la gestión financiera y operativa, promoviendo la integridad organizacional. Por lo tanto, un control interno bien diseñado y ejecutado es un motor de eficiencia que impulsa la competitividad de la institución en su sector.

En este sentido, las organizaciones deben invertir de manera constante en la evaluación y actualización de sus sistemas de control interno, asegurando que sigan siendo efectivos ante los nuevos desafíos del entorno y que puedan prevenir fraudes, errores y el incumplimiento de regulaciones. La adaptabilidad y la evaluación continua son cruciales para mantener la efectividad de los controles internos en un panorama organizacional que evoluciona rápidamente. A través de este enfoque proactivo, las organizaciones pueden gestionar sus riesgos de manera eficiente y garantizar el cumplimiento de sus objetivos estratégicos a largo plazo.

El control interno debe ser considerado un proceso continuo y dinámico, ya que las organizaciones están en constante evolución. En mi perspectiva, este no puede ser estático ni reactivo, sino que debe anticiparse a los riesgos, adaptándose a las necesidades y desafíos actuales. Su éxito radica en su correcta implementación y en la participación activa de todos los niveles jerárquicos. En este sentido, el control interno debe ser flexible y estar alineado con los objetivos estratégicos de la organización, permitiendo que se ajuste a medida que las condiciones del entorno cambian. Esta capacidad de adaptación garantiza que el control interno no solo sea una herramienta de corrección, sino también un mecanismo proactivo para gestionar riesgos y mejorar los procesos organizacionales.

Según Harmui y Varela (2013), "el control interno debe entenderse como un sistema integral que involucra no solo políticas y procedimientos, sino también la cultura organizacional, el liderazgo y la ética corporativa". Este enfoque subraya la importancia de la dimensión humana en el control interno. Las políticas y procedimientos, aunque fundamentales, no son suficientes por sí solos. Es crucial que todos los miembros de la organización comprendan y apoyen los controles establecidos, ya que su compromiso y conducta ética son elementos clave para la efectividad de estos controles. La cultura organizacional juega un papel fundamental, ya que influye en cómo se perciben y se

cumplen las normas dentro de la entidad. Un ambiente que promueve la ética, la transparencia y la responsabilidad contribuye a un control interno más eficaz y a una mayor cohesión entre las diferentes áreas de la organización.

En este contexto, el liderazgo desempeña un papel central en la implementación y mantenimiento de un control interno exitoso. Los líderes deben ser los principales impulsores de una cultura de control interno sólido, estableciendo el ejemplo a seguir y fomentando la importancia de los controles en todos los niveles. La capacidad de los líderes para comunicar claramente la importancia del control interno y la responsabilidad compartida en su implementación es crucial para lograr la participación activa de todo el personal. Además, el liderazgo debe asegurarse de que los controles sean accesibles, comprendidos y que se ajusten continuamente a las necesidades y retos emergentes de la organización.

Además de los factores humanos y culturales, el control interno debe incorporar tecnologías avanzadas para mejorar su eficacia. Las herramientas tecnológicas pueden facilitar la automatización de ciertos procesos, la supervisión en tiempo real y la detección de anomalías, lo que permite a las organizaciones identificar y mitigar riesgos de manera más eficiente. Estas tecnologías complementan las políticas y procedimientos tradicionales, proporcionando una capa adicional de protección ante los riesgos emergentes, como los cibernéticos. Sin embargo, es fundamental que las tecnologías empleadas estén alineadas con los valores y principios éticos de la organización, garantizando que se utilicen de manera adecuada y que no infrinjan la privacidad ni los derechos de los individuos.

El control interno también debe estar alineado con un enfoque preventivo, en lugar de solo ser reactivo a los problemas una vez que estos ocurren. Esto implica una evaluación constante de los riesgos potenciales y el diseño de estrategias para prevenirlos

antes de que se materialicen. En la práctica, esto significa que las organizaciones deben estar siempre alertas a las tendencias y cambios del mercado, así como a las amenazas emergentes, para poder adaptar sus controles en consecuencia. Un sistema de control interno preventivo no solo mejora la eficiencia operativa, sino que también ayuda a la organización a cumplir con sus objetivos a largo plazo, asegurando su sostenibilidad y éxito en un entorno competitivo y en constante cambio.

El control interno debe ser un proceso integral y flexible, que abarque tanto los aspectos operacionales como humanos de la organización. Su éxito depende de una correcta implementación que involucre a todos los niveles jerárquicos, un liderazgo efectivo y una cultura organizacional ética. La combinación de políticas y procedimientos sólidos, junto con el compromiso de las personas y el uso de tecnologías adecuadas, asegura que el control interno sea un motor clave para la mitigación de riesgos y el cumplimiento de los objetivos estratégicos de la organización.

Componentes del control interno.

Los componentes del control interno, como el entorno de control, la evaluación de riesgos y el monitoreo, son pilares esenciales para garantizar su eficacia. En mi opinión, estos deben integrarse armónicamente, ya que cualquier deficiencia en uno de ellos puede comprometer el sistema completo. La interacción fluida entre estos componentes permite que los controles sean más que una serie de procedimientos aislados; se convierten en un sistema cohesivo que permite a la organización no solo prevenir y detectar riesgos, sino también adaptarse de manera proactiva a las circunstancias cambiantes. Una estructura balanceada y bien supervisada fortalece la resiliencia organizacional ante cambios y riesgos, asegurando que la entidad esté siempre preparada para gestionar amenazas y aprovechar oportunidades. La eficacia del control interno depende de que cada componente no solo se implemente correctamente, sino que

también se mantenga actualizado y alineado con los objetivos estratégicos de la organización.

El marco COSO (2013) identifica cinco componentes clave del control interno: "entorno de control, evaluación de riesgos, actividades de control, información y comunicación, y monitoreo". Estos elementos proporcionan un esquema estructurado para implementar y evaluar la efectividad de los controles internos en cualquier tipo de organización. El entorno de control establece las bases para todos los demás componentes, ya que define la cultura organizacional, la ética y la integridad, y la responsabilidad de la alta dirección. Un entorno de control fuerte promueve la transparencia, la coherencia y la rendición de cuentas, elementos esenciales para que los controles internos sean efectivos. Esto no solo afecta la forma en que los empleados cumplen con sus tareas, sino que también influye en la toma de decisiones y en la percepción general de la organización.

La evaluación de riesgos es otro componente esencial que asegura que la organización identifique y analice los riesgos que podrían obstaculizar el logro de sus objetivos. Esta evaluación no se limita a los riesgos financieros, sino que abarca una amplia gama de factores, incluidos los riesgos operacionales, tecnológicos, legales y de cumplimiento. El riesgo siempre está presente, y la clave está en identificarlo a tiempo para poder tomar medidas preventivas. La evaluación de riesgos debe ser un proceso continuo, ya que los entornos empresariales y las amenazas evolucionan constantemente. Solo con una evaluación continua de los riesgos, la organización podrá ajustar sus controles internos para minimizar las probabilidades de que estos se materialicen y afecten la operación.

Por su parte, las actividades de control son los procedimientos y políticas establecidos para mitigar los riesgos identificados y asegurar que los objetivos se

cumplan. Estas actividades deben estar alineadas con la evaluación de riesgos y deben ser suficientemente flexibles para adaptarse a las condiciones cambiantes del entorno. Desde controles físicos hasta procedimientos de auditoría, todas las actividades deben estar documentadas, comunicadas y supervisadas. Los controles deben ser efectivos pero también eficientes, lo que significa que no deben generar cargas operativas innecesarias ni interferir con la capacidad de la organización para lograr sus objetivos.

El componente de información y comunicación garantiza que la información relevante fluya de manera oportuna y adecuada a todas las partes interesadas, desde la alta dirección hasta el personal operativo. La comunicación clara y precisa es vital para que todos los miembros de la organización comprendan sus roles y responsabilidades dentro del sistema de control interno. La información relevante debe ser accesible y estar disponible en el momento adecuado para facilitar la toma de decisiones. Sin una comunicación efectiva, los controles internos no pueden ser implementados de manera coherente ni monitoreados adecuadamente.

Finalmente, el monitoreo es el componente que permite evaluar la efectividad continua de los controles internos. El monitoreo permite detectar fallos o debilidades en los controles, lo que facilita la toma de decisiones correctivas. Este proceso no es algo que se realiza de manera puntual, sino que debe ser un proceso constante a través de auditorías internas, revisiones periódicas y otros mecanismos de retroalimentación. A través del monitoreo, las organizaciones pueden identificar rápidamente las áreas que requieren ajustes o mejoras, lo que garantiza que el sistema de control interno permanezca eficaz y relevante.

Controles Generales de TI

Para la presente investigación que está enfocada en la evaluación de los Controles Generales de Tecnologías de Información (CGTI) juegan un papel fundamental en

garantizar la estabilidad y seguridad de los sistemas informáticos. Estos controles no solo permiten mitigar riesgos relacionados con accesos no autorizados, fallos operativos y vulnerabilidades de seguridad, sino que también optimizan el rendimiento y confiabilidad de la infraestructura tecnológica. Sin una adecuada implementación y monitoreo de estos controles, las organizaciones financieras se exponen a incidentes que pueden afectar la integridad de sus operaciones y la confianza de sus clientes.

Según la Information Systems Audit and Control Association (ISACA, 2022), los controles generales de TI son "los principios, prácticas y procedimientos diseñados para garantizar la integridad, confiabilidad y seguridad de los sistemas de información dentro de una organización". Estos controles abarcan aspectos clave como la gestión y administración de accesos, la administración de cambios, operaciones, red y la Seguridad de la Información. Su correcta implementación permite establecer una base sólida para la gestión de riesgos tecnológicos y el cumplimiento normativo en el sector financiero.

Comprender la definición de los controles generales de TI es el primer paso para evaluar su importancia dentro del entorno bancario. A medida que los sistemas financieros dependen más de la tecnología, resulta esencial analizar cómo estos controles contribuyen a la estabilidad operativa y a la protección contra amenazas digitales. En el siguiente apartado, se explorará la relevancia de estos controles en el sector bancario y su impacto en la seguridad, eficiencia y cumplimiento regulatorio.

Importancia de los controles generales de TI en el sector bancario

En el sector bancario, los controles generales de TI son una pieza clave para garantizar la seguridad y eficiencia de las operaciones. La banca moderna depende casi en su totalidad de sistemas digitales para procesar transacciones, gestionar información confidencial y brindar servicios en línea a los clientes. Sin estos controles, las instituciones financieras estarían expuestas a riesgos como fraudes, ciberataques y fallos

operativos que podrían afectar su estabilidad y reputación. Además, una gestión adecuada de estos controles permite a los bancos mejorar su competitividad y cumplir con las crecientes exigencias regulatorias.

De acuerdo con el Comité de Supervisión Bancaria de Basilea (2021), “la implementación de controles generales de TI efectivos es fundamental para preservar la integridad del sistema financiero, reducir la vulnerabilidad ante ataques cibernéticos y garantizar el cumplimiento de normativas internacionales”. En este sentido, estos controles ayudan a mitigar riesgos operativos, asegurando la continuidad de los servicios bancarios y la protección de la información sensible de los clientes. Asimismo, su correcta aplicación facilita auditorías y supervisiones por parte de organismos reguladores.

De acuerdo con el Comité de Supervisión Bancaria de Basilea (2021), “la implementación de controles generales de TI efectivos es fundamental para preservar la integridad del sistema financiero, reducir la vulnerabilidad ante ataques cibernéticos y garantizar el cumplimiento de normativas internacionales”. En este sentido, estos controles ayudan a mitigar riesgos operativos, asegurando la continuidad de los servicios bancarios y la protección de la información sensible de los clientes. Asimismo, su correcta aplicación facilita auditorías y supervisiones por parte de organismos reguladores.

Clasificación de los Controles Generales de TI

Los controles generales de TI se dividen en diversas categorías, cada una con un propósito específico para garantizar la seguridad, confiabilidad y eficiencia de los sistemas de información en el sector bancario. Entre los más relevantes se encuentran los controles de acceso, que regulan quién puede ingresar a los sistemas; los controles de cambios, que supervisan las modificaciones en la infraestructura tecnológica; los controles de operación, que garantizan la estabilidad y continuidad de los servicios; y los

controles de seguridad, que protegen la información contra amenazas y ataques. A continuación, se desarrolla cada uno de estos controles en detalle.

Control de Acceso

Los controles de acceso son fundamentales en cualquier entidad financiera, ya que permiten restringir el uso de sistemas y datos sensibles únicamente a personas autorizadas. Sin una correcta gestión de accesos, los bancos corren el riesgo de sufrir fraudes, robos de información y ataques internos o externos. Además, estos controles no solo protegen la información, sino que también garantizan que cada usuario tenga permisos adecuados según su rol, evitando accesos innecesarios o peligrosos.

Según la norma ISO/IEC 27001 (2022), "la gestión de accesos es un principio clave en la Seguridad de la Información, ya que asegura que solo personas autorizadas puedan interactuar con los recursos de TI, reduciendo la exposición a riesgos". Esto significa que, a través de mecanismos como autenticación multifactorial, control de privilegios y monitoreo de accesos, las instituciones pueden fortalecer la protección de sus sistemas críticos.

Si bien los controles de acceso garantizan que solo los usuarios adecuados puedan interactuar con los sistemas, es igualmente importante supervisar los cambios realizados dentro de la infraestructura tecnológica. La administración de cambios es crucial para evitar modificaciones no autorizadas que puedan comprometer la seguridad y estabilidad de los sistemas bancarios, lo cual se explorará en el siguiente apartado.

Control de Cambios

La gestión de cambios en los sistemas de TI es esencial para evitar errores, fallos o brechas de seguridad en las plataformas bancarias. Cuando una organización implementa cambios sin un proceso adecuado de validación y autorización, puede generar interrupciones en los servicios o, peor aún, exponer vulnerabilidades que los

ciberdelincuentes podrían aprovechar. Por ello, un control riguroso sobre las modificaciones garantiza que cada actualización o mejora se realice de manera segura y sin afectar la operatividad del banco.

El marco COBIT 2019 establece que “una adecuada gestión de cambios permite minimizar interrupciones en los servicios tecnológicos y reducir el impacto de modificaciones inesperadas, garantizando la continuidad y seguridad de las operaciones”. Esto significa que las entidades bancarias deben establecer procedimientos claros para la evaluación, autorización, implementación y monitoreo de cambios en sus sistemas.

Una vez que los cambios son aprobados e implementados, es crucial monitorear el correcto funcionamiento de los sistemas para asegurar la continuidad de las operaciones. Aquí es donde entran en juego los controles de operación, los cuales supervisan el desempeño y estabilidad de los sistemas bancarios, garantizando que se mantengan en funcionamiento sin interrupciones.

Controles de Operación

La continuidad operativa es un pilar clave en el sector bancario, ya que cualquier interrupción en los sistemas puede traducirse en pérdidas económicas y afectación a los clientes. Los controles de operación permiten supervisar el rendimiento de la infraestructura tecnológica, detectar fallos en tiempo real y ejecutar medidas correctivas cuando sea necesario. Contar con estos controles reduce la posibilidad de interrupciones inesperadas y ayuda a mantener un servicio eficiente y confiable.

De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST, 2021), “los controles de operación permiten a las organizaciones gestionar los procesos tecnológicos de manera efectiva, asegurando la disponibilidad y estabilidad de los servicios críticos”. Esto implica que los bancos deben implementar estrategias de

monitoreo proactivo, automatización de procesos y respuesta rápida ante incidentes para garantizar una operatividad óptima.

Si bien los controles de operación aseguran que los sistemas tecnológicos funcionen correctamente, no serían efectivos sin un sólido esquema de seguridad que proteja los datos y los activos digitales del banco. La siguiente sección abordará los controles de seguridad, fundamentales para prevenir amenazas cibernéticas y garantizar la confidencialidad e integridad de la información bancaria.

Normas Internacionales de Control Interno y TI

En la presente investigación es de suma importancia los diversos marcos normativos ya que ayudan a las organizaciones a garantizar la seguridad, eficiencia y cumplimiento regulatorio de sus operaciones. Entre los más relevantes en el sector bancario se encuentran COSO, COBIT, ISO/IEC 27001 e ITIL. Estos estándares proporcionan metodologías y buenas prácticas para la administración de riesgos, Seguridad de la Información y gestión de procesos de TI. A continuación, se detallan sus características y su impacto en el sector financiero.

Marco COSO (committee of sponsoring organizations of the treadway commission)

El marco COSO es una herramienta fundamental para la gestión de riesgos y el control interno dentro de las organizaciones. En el sector bancario, su aplicación permite identificar, evaluar y mitigar riesgos financieros y operativos, incluidos aquellos relacionados con la tecnología. Adoptar un enfoque basado en COSO no solo mejora la gobernanza y transparencia dentro de las instituciones financieras, sino que también fortalece la confianza de los reguladores y clientes.

De acuerdo con COSO (2017), “un sistema efectivo de control interno proporciona una seguridad razonable en el logro de los objetivos de una organización en

materia de operaciones, informes y cumplimiento". Esto significa que su implementación en el sector bancario contribuye a una mejor supervisión de los procesos tecnológicos y financieros, asegurando la alineación con los objetivos estratégicos del banco.

Si bien COSO establece un marco general para el control interno, existen modelos más específicos para la gestión de TI, como COBIT. Este marco es ampliamente utilizado en instituciones financieras para asegurar la alineación entre los objetivos del negocio y la administración de la tecnología.

COBIT (control objectives for information and related technologies)

COBIT es una herramienta esencial para la gobernanza de TI en el sector bancario, ya que proporciona un enfoque estructurado para la gestión de riesgos tecnológicos, el cumplimiento regulatorio y la optimización de recursos tecnológicos. Su implementación permite a los bancos garantizar que la tecnología se utilice de manera eficiente, minimizando riesgos operativos y mejorando la toma de decisiones estratégicas.

Según ISACA (2019), "COBIT proporciona un marco integral para el gobierno y la gestión de la información y la tecnología empresarial, asegurando el cumplimiento normativo y la optimización de los procesos de TI". Esto es clave en el sector bancario, donde la estabilidad y seguridad de los sistemas tecnológicos impactan directamente en la confianza de los clientes y en el cumplimiento de regulaciones.

A pesar de que COBIT se centra en la gobernanza y el control de TI, la Seguridad de la Información es otro aspecto crítico en el sector financiero. Aquí es donde ISO/IEC 27001 desempeña un papel crucial al proporcionar lineamientos específicos para la protección de datos y la mitigación de riesgos cibernéticos.

ISO/IEC 27001 (Gestión de Seguridad de la Información)

Para la presente investigación, la Seguridad de la Información es un pilar esencial para los bancos. La norma ISO/IEC 27001 ayuda a las instituciones financieras a establecer un sistema de gestión de Seguridad de la Información (SGSI) sólido, reduciendo vulnerabilidades y mejorando la respuesta ante incidentes cibernéticos. Su implementación es clave para garantizar la confidencialidad, integridad y disponibilidad de los datos bancarios.

Según la ISO/IEC 27001 (2022), "un sistema de gestión de Seguridad de la Información permite a las organizaciones proteger sus activos de información mediante un enfoque sistemático basado en la evaluación de riesgos". En el sector bancario, esto se traduce en la aplicación de controles específicos para prevenir fraudes, ciberataques y accesos no autorizados a información confidencial.

Además de la Seguridad de la Información, la gestión eficiente de los servicios de TI es crucial para el éxito operativo de un banco. ITIL, un marco de referencia para la administración de servicios tecnológicos, permite a las instituciones financieras optimizar sus procesos de TI y mejorar la calidad del servicio.

ITIL (Biblioteca de Infraestructura de TI)

En un entorno bancario altamente dependiente de la tecnología, la gestión eficiente de los servicios de TI es crucial para garantizar la continuidad operativa y la satisfacción del cliente. ITIL proporciona un conjunto de mejores prácticas que ayudan a las instituciones financieras a mejorar la entrega y administración de servicios tecnológicos, asegurando una infraestructura de TI estable y eficiente.

ITIL 4 (2019) establece que "la gestión de servicios de TI debe centrarse en la entrega de valor al negocio y en la mejora continua, asegurando que los servicios

tecnológicos satisfagan las necesidades estratégicas de la organización". En el contexto bancario, esto implica optimizar procesos como la gestión de incidentes, cambios y disponibilidad, garantizando una operación ininterrumpida.

Si bien las normas y marcos mencionados establecen lineamientos para el control interno y la gestión de TI, es fundamental considerar las regulaciones específicas que rigen el sector bancario. En el siguiente apartado, se analizarán los estándares financieros y normativas nacionales que garantizan la estabilidad y seguridad de las instituciones bancarias.

Regulaciones financieras aplicables al sector bancario

El sector bancario opera bajo estrictas regulaciones diseñadas para garantizar la estabilidad del sistema financiero, prevenir fraudes y proteger a los clientes. Entre las normativas más importantes se encuentran **Basilea II y III**, que establecen lineamientos sobre capital y gestión de riesgos, así como las **leyes y regulaciones nacionales sobre seguridad informática y auditoría**, que varían según el país.

Basilea II y III

Los acuerdos de Basilea son esenciales para la regulación del sector bancario, ya que establecen requisitos de capital y normas de gestión de riesgos que buscan fortalecer la estabilidad financiera. En un mundo donde las crisis económicas y los riesgos cibernéticos son cada vez más frecuentes, estas regulaciones permiten a los bancos prepararse mejor ante escenarios adversos.

El Comité de Basilea (2017) señala que "los acuerdos de Basilea II y III fortalecen los requisitos de capital y establecen mejores prácticas para la gestión de riesgos financieros, promoviendo la estabilidad y solidez del sistema bancario global". Estas normativas ayudan a los bancos a enfrentar riesgos operacionales, incluyendo los asociados a la seguridad de TI.

Además de las regulaciones internacionales como Basilea, cada país cuenta con normativas específicas en materia de seguridad informática y auditoría. Estas leyes refuerzan el cumplimiento de estándares globales y establecen obligaciones adicionales para la protección de los sistemas financieros.

Leyes y regulaciones nacionales sobre seguridad informática y auditoría

Cada país establece normativas específicas para regular la seguridad informática y la auditoría en el sector financiero. Estas regulaciones son fundamentales para garantizar la protección de los datos de los clientes, evitar fraudes y fortalecer la supervisión gubernamental sobre los bancos. El cumplimiento de estas leyes no solo evita sanciones, sino que también refuerza la confianza en la institución financiera.

Según el Banco Mundial (2021), “las regulaciones nacionales sobre ciberseguridad y auditoría financiera son esenciales para reducir la vulnerabilidad de los sistemas bancarios y proteger la estabilidad económica de los países”. Estas normativas exigen controles estrictos en cuanto a protección de datos, monitoreo de transacciones y auditorías periódicas.

El cumplimiento de las normativas y regulaciones mencionadas es clave para la evaluación de la eficacia operativa de los controles de TI en los bancos. En el próximo capítulo, se analizarán los métodos y enfoques utilizados para medir la efectividad de estos controles y su impacto en la seguridad y eficiencia de las instituciones financieras.

Eficacia operativa de controles de TI

La eficacia operativa en el ámbito de la tecnología de la información (TI) tiene la capacidad de los procesos, sistemas y controles tecnológicos para cumplir sus objetivos con el menor consumo de recursos posible, garantizando simultáneamente seguridad, confiabilidad y cumplimiento normativo. En el sector bancario, la eficacia operativa de

los controles de TI es fundamental para asegurar la estabilidad de las operaciones, prevenir fraudes y mitigar riesgos cibernéticos.

Desde una perspectiva práctica, la eficacia operativa en TI no solo implica que los sistemas funcionen correctamente, sino que lo hagan de manera eficiente y alineada con los objetivos estratégicos de la organización. En un entorno bancario altamente regulado, la eficacia operativa se convierte en un elemento clave para minimizar riesgos, optimizar costos y mejorar la experiencia del cliente. Sin controles efectivos, los bancos pueden enfrentar problemas como accesos no autorizados, interrupciones en los servicios y sanciones por incumplimiento normativo.

Según IT Governance Institute (2020), "la eficacia operativa en TI se alcanza cuando los procesos tecnológicos logran sus objetivos estratégicos con el menor impacto en los recursos, maximizando la seguridad y minimizando los riesgos". Esto implica que la implementación de controles debe evaluarse constantemente para asegurar que sean adecuados, actualizados y alineados con las mejores prácticas de la industria.

Para determinar si los controles de TI en una institución bancaria son realmente eficaces, es necesario contar con métodos y enfoques de evaluación que permitan medir su desempeño. En el siguiente apartado se analizarán las principales estrategias utilizadas para evaluar la efectividad de los controles generales de TI.

Métodos y enfoques para la evaluación de controles de TI

Existen diversos enfoques para evaluar la eficacia de los controles generales de TI en el sector bancario. Las auditorías internas y externas, las evaluaciones de riesgos y las pruebas de cumplimiento son algunas de las herramientas más utilizadas para verificar el adecuado funcionamiento de los controles y su alineación con los estándares regulatorios y de seguridad.

Auditorías internas y externas

Las auditorías son una de las herramientas más eficaces para evaluar el desempeño de los controles de TI en la banca. Mientras que las auditorías internas permiten a la organización detectar fallos y mejorar sus procesos antes de una inspección regulatoria, las auditorías externas brindan una visión imparcial sobre la seguridad y cumplimiento de los sistemas. La combinación de ambas garantiza una supervisión completa y efectiva.

Según la ISACA (2021), "las auditorías de TI permiten evaluar la conformidad de los controles con los estándares establecidos, identificar brechas de seguridad y proponer mejoras para garantizar una gestión efectiva de la tecnología". En el sector bancario, estas auditorías son esenciales para cumplir con normativas como ISO 27001, COBIT y Basilea III.

Si bien las auditorías permiten verificar el cumplimiento de los controles, otro enfoque clave es la evaluación de riesgos, que ayuda a identificar y mitigar amenazas antes de que se conviertan en incidentes críticos.

Evaluaciones de riesgos

Las evaluaciones de riesgos son una herramienta proactiva que permite a los bancos anticiparse a posibles fallos o vulnerabilidades en sus sistemas de TI. Identificar riesgos con antelación no solo ayuda a minimizar impactos negativos, sino que también optimiza la asignación de recursos y mejora la resiliencia organizacional.

Según el NIST (2022), "la evaluación de riesgos en TI debe considerar amenazas internas y externas, vulnerabilidades en los sistemas y el impacto potencial en la organización". En el sector bancario, este enfoque permite priorizar acciones para mitigar riesgos como accesos no autorizados, ciberataques y fallos en la continuidad del negocio.

Además de las auditorías y la gestión de riesgos, otro método esencial para evaluar la eficacia de los controles de TI en la banca es la realización de pruebas de cumplimiento,

que garantizan que los sistemas y procesos cumplan con regulaciones y estándares establecidos.

Pruebas de cumplimiento

Las pruebas de cumplimiento permiten a las entidades financieras verificar que sus sistemas de TI operan conforme a regulaciones y estándares internacionales. Este tipo de evaluación es crucial para evitar sanciones y garantizar que los controles implementados realmente protejan la información y la infraestructura tecnológica.

Según el Comité de Basilea (2023), “las pruebas de cumplimiento ayudan a asegurar que las instituciones financieras se adhieren a los marcos regulatorios y operan dentro de los límites de riesgo aceptables”. Estas pruebas incluyen la revisión de políticas de seguridad, auditorías de accesos y simulaciones de ciberataques para evaluar la solidez de los controles de TI.

Para evaluar la eficacia de los controles de TI en un banco, es esencial definir indicadores de desempeño y métricas que permitan medir su impacto en la operatividad y seguridad de la institución. En el siguiente apartado se analizarán los principales indicadores utilizados en la industria financiera.

Cumplimiento normativo y disponibilidad de sistemas

El cumplimiento normativo y la disponibilidad de los sistemas críticos son factores determinantes en la eficacia operativa de los controles de TI. Un banco que no cumpla con los estándares regulatorios puede enfrentar sanciones y pérdida de confianza por parte de sus clientes.

Según la OCDE (2023), “las instituciones financieras deben garantizar la disponibilidad de sus sistemas y el cumplimiento de las normativas para evitar interrupciones operativas y sanciones regulatorias”.

Impacto de los controles generales de TI en la operación del banco

Los controles generales de TI tienen un impacto significativo en la operatividad de las instituciones bancarias, ya que garantizan la Seguridad de la Información, la continuidad del negocio y la prevención de fraudes. Su correcta implementación no solo protege los activos tecnológicos, sino que también fortalece la confianza de clientes y reguladores en el sistema financiero.

Seguridad de la Información y protección de datos

La Seguridad de la Información es un pilar fundamental en la banca, ya que maneja grandes volúmenes de datos sensibles de clientes y transacciones financieras. Si los controles de TI no son eficaces, la institución queda expuesta a ataques cibernéticos, filtraciones de datos y sanciones regulatorias. Implementar estrategias robustas de protección es clave para minimizar estos riesgos y garantizar la integridad de la información.

Según la ISO/IEC 27001 (2022), “la gestión de la Seguridad de la Información debe garantizar la confidencialidad, integridad y disponibilidad de los datos, mediante controles que reduzcan la exposición a riesgos cibernéticos y operacionales”. En el sector bancario, cumplir con estos principios es esencial para evitar incidentes de seguridad con impacto financiero y reputacional.

Sin embargo, la Seguridad de la Información por sí sola no es suficiente para garantizar la estabilidad operativa de un banco. Es igualmente importante contar con planes de continuidad del negocio y estrategias de gestión de incidentes para responder eficazmente ante cualquier contingencia tecnológica.

Prevención del fraude y riesgos financieros

El fraude bancario ha evolucionado con el uso de tecnologías avanzadas, lo que hace que los bancos deban implementar controles de TI cada vez más sofisticados para detectar y prevenir actividades sospechosas. La supervisión constante de transacciones y el uso de inteligencia artificial pueden mejorar significativamente la detección de patrones fraudulentos.

De acuerdo con el Comité de Basilea (2022), “los bancos deben aplicar controles automatizados que permitan identificar transacciones inusuales, restringir accesos no autorizados y minimizar la posibilidad de fraudes internos y externos”. La implementación de herramientas como la autenticación multifactor y el monitoreo en tiempo real ayuda a reducir estos riesgos.

Además del impacto financiero, la eficacia de los controles de TI también influye directamente en la percepción del cliente sobre la seguridad y confiabilidad del banco, lo que afecta su experiencia y su nivel de confianza en la institución.

Impacto en la experiencia del cliente y la confianza institucional

Un banco que invierte en controles de TI eficientes no solo protege su infraestructura, sino que también mejora la experiencia del cliente. La rapidez en las transacciones, la protección de datos personales y la disponibilidad de servicios digitales seguros aumentan la confianza de los usuarios y fortalecen la relación con la institución.

Según un estudio de Deloitte (2023), “el 85% de los clientes bancarios consideran la seguridad de sus datos como un factor decisivo al elegir una entidad financiera”. Esto demuestra que la implementación de controles de TI no solo tiene un impacto técnico y financiero, sino que también influye en la lealtad y satisfacción del cliente.

Los controles generales de TI son esenciales para la seguridad, continuidad y estabilidad operativa del sector bancario. Además de reducir riesgos financieros y

tecnológicos, su correcta implementación fortalece la confianza del cliente y mejora la competitividad del banco en un entorno digital en constante evolución.

Diseño y funcionamiento de controles.

Diseñar y operar controles efectivos es un reto que exige conocimiento técnico, análisis de riesgos y una comprensión profunda de las operaciones. Considero que el diseño debe estar alineado con los objetivos estratégicos, mientras que su funcionamiento debe ser dinámico, adaptándose continuamente a los cambios en el entorno interno y externo. Los controles no deben ser vistos como elementos aislados o estáticos, sino como una parte integral y flexible que acompaña el crecimiento y evolución de la organización. Esto requiere que las áreas encargadas de implementarlos y supervisarlos se mantengan constantemente actualizadas y sean capaces de ajustar las estrategias de control a medida que se presentan nuevos desafíos, amenazas y oportunidades. El control interno no solo debe mitigar los riesgos, sino también optimizar los procesos y fomentar un entorno organizacional que favorezca la transparencia, la eficiencia y la sostenibilidad.

De acuerdo con COSO (2013), "los controles efectivos deben estar diseñados para mitigar los riesgos relevantes en todos los niveles de la organización, alineándose con sus objetivos estratégicos y operativos". Esto destaca la necesidad de un enfoque integral y estratégico en el diseño y funcionamiento de controles. En lugar de implementar controles genéricos o de forma reactiva ante problemas específicos, el enfoque debe ser preventivo y proactivo. Los controles deben identificar los riesgos relevantes para la organización, tanto financieros como operacionales, y alinearse con los objetivos a largo plazo. De esta manera, se asegura que los controles no solo sean efectivos para abordar los problemas inmediatos, sino que también apoyen la consecución de los objetivos estratégicos de la organización.

La alineación de los controles con los objetivos estratégicos de la organización es crucial para garantizar que no solo se mitiguen los riesgos, sino que también se promueva el desarrollo de la organización en su conjunto. Un sistema de control que esté alineado con los objetivos estratégicos permite a la organización mantenerse en el camino hacia su visión a largo plazo, a la vez que le brinda la flexibilidad necesaria para adaptarse a los cambios del entorno competitivo. Además, los controles deben ser escalables, de modo que puedan adaptarse a diferentes niveles de operación dentro de la organización. Esto significa que las áreas operativas, administrativas y de gestión deben estar igualmente cubiertas por un sistema de control coherente y eficaz que se ajuste a sus necesidades específicas.

Para lograr la efectividad de los controles, es esencial un proceso de monitoreo constante y retroalimentación, de manera que los controles sean evaluados periódicamente para identificar debilidades y oportunidades de mejora. El monitoreo permite detectar rápidamente fallos en el sistema de control, lo que posibilita una corrección rápida antes de que se convierta en un problema mayor. Esta evaluación continua y el ajuste proactivo de los controles permiten a la organización mantener una ventaja competitiva frente a cambios imprevistos en el mercado, en la normativa o en los riesgos emergentes.

Diseño de controles efectivos.

El diseño de controles efectivos requiere un enfoque proactivo que combine la identificación de riesgos y la asignación de responsabilidades claras. En mi opinión, este proceso debe incluir la participación de equipos multidisciplinarios para garantizar que los controles sean prácticos, viables y acordes con los recursos disponibles. La colaboración entre diferentes áreas de la organización, como las de TI, finanzas, operaciones y recursos humanos, permite que se consideren diversas perspectivas y se

aborden los riesgos desde diferentes ángulos. Además, la integración de expertos con distintos conocimientos asegura que los controles sean no solo adecuados para mitigar riesgos, sino también realistas en su implementación y sostenibilidad a largo plazo.

Según Hernández y Mendoza (2018), "el diseño de controles debe basarse en un análisis detallado de riesgos y considerar las particularidades de cada organización, con el fin de implementar soluciones prácticas y efectivas". Este enfoque resalta la importancia de comprender las características únicas de cada organización antes de diseñar los controles. Las soluciones no deben ser universales, sino que deben adaptarse a las particularidades del entorno operativo, los procesos específicos y la cultura organizacional. Esto requiere una evaluación profunda de los riesgos inherentes a cada área, identificando tanto los riesgos externos como internos que podrían afectar la operatividad de la entidad.

Además, el proceso de diseño debe ir más allá de la identificación de riesgos y la asignación de responsabilidades. Debe incluir un plan detallado de implementación, seguimiento y ajustes periódicos. Para que los controles sean efectivos, no basta con diseñarlos; también es crucial contar con una estrategia de comunicación clara para asegurar que todos los miembros de la organización comprendan sus roles en el proceso. De igual forma, los controles deben ser ajustados y evaluados regularmente para asegurarse de que continúen siendo relevantes y efectivos ante nuevos riesgos o cambios en el entorno de trabajo. Este ciclo continuo de evaluación y ajuste contribuye a la sostenibilidad y a la mejora continua de los controles, fortaleciendo así la organización frente a potenciales amenazas.

Tipos de controles internos: preventivos, detectivos y correctivos.

La combinación de controles preventivos, detectivos y correctivos fortalece el sistema de control interno, ya que aborda riesgos desde diferentes perspectivas. En mi

opinión, los controles preventivos son los más valiosos, ya que evitan errores desde el principio, pero no deben excluirse los demás tipos, ya que todos cumplen un propósito crítico en la mitigación de riesgos.

De acuerdo con Harmui y Varela (2013), "los controles preventivos buscan evitar que ocurran fallos, los detectivos identifican irregularidades en tiempo real, y los correctivos se enfocan en mitigar el impacto de los errores una vez detectados".

Procedimientos y políticas internas

El desarrollo y documentación de políticas internas para el banco es un proceso que refuerza la formalidad y consistencia de los controles internos. Considero que una correcta documentación facilita la capacitación, el monitoreo y la continuidad de las operaciones, especialmente en escenarios de cambios organizacionales.

Según COSO (2013), "los procedimientos y políticas internas deben ser claros, accesibles y revisados periódicamente, ya que proporcionan una base sólida para la implementación de controles consistentes y eficaces".

Normativas y estándares

Las normativas y estándares internacionales son guías indispensables para establecer sistemas de control interno que respondan a las mejores prácticas. En mi opinión, su relevancia aumenta en el sector bancario, donde el cumplimiento normativo es crucial para evitar sanciones y garantizar la confianza del público.

Según Hernández y Mendoza (2018), "las normativas y estándares internacionales, como las emitidas por COSO y COBIT, establecen principios fundamentales que las organizaciones deben considerar para el diseño y evaluación de sus controles internos".

Normas internacionales y locales sobre control interno.

Las normas internacionales, como COSO y COBIT, y las normativas locales, proporcionan un marco sólido para implementar controles internos eficaces. En mi opinión, estas normas no solo promueven la transparencia y la rendición de cuentas, sino que también contribuyen a la armonización de las prácticas globales, permitiendo a las instituciones adaptarse a un entorno dinámico y competitivo.

De acuerdo con COSO (2013), "el objetivo de las normas internacionales de control interno es proporcionar un marco integral para que las organizaciones evalúen, mejoren y mantengan la efectividad de sus controles".

Relevancia de estas normativas en el sector bancario.

En el sector bancario, las normativas sobre control interno son esenciales para proteger la estabilidad financiera y evitar riesgos sistémicos. Desde mi perspectiva, estas normas garantizan que las instituciones bancarias operen de manera ética y transparente, reduciendo la probabilidad de fraudes y malas prácticas que puedan poner en peligro los intereses de los depositantes.

Según Hernández y Mendoza (2018), "en el sector bancario, el cumplimiento de normativas como las de Basilea III y las emitidas por entes locales fortalece la gestión de riesgos y garantiza la sostenibilidad financiera".

Controles generales de tecnología de información (CGTI)

Los CGTI son una herramienta vital para gestionar los riesgos tecnológicos que enfrentan las organizaciones modernas. En mi opinión, estos controles deben estar alineados con los objetivos estratégicos y los sistemas de información de la entidad, asegurando que la tecnología respalde de manera segura y eficiente las operaciones diarias.

En la presente investigación nos baseremos en la evaluación de cuatro áreas: Control de Cambios, Controles de Accesos, Controles de Operaciones y la Red

De acuerdo con COBIT (2019), "los controles generales de tecnología de información son un conjunto de procesos y mecanismos diseñados para garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos de la organización".

Importancia de los CGTI en el control interno

Los CGTI juegan un papel crucial en el control interno, ya que protegen los sistemas contra vulnerabilidades y garantizan la continuidad operativa. Considero que su relevancia radica en su capacidad para prevenir ciberataques, mantener la integridad de la información y facilitar auditorías más eficientes.

Según Harmui y Varela (2013), "los CGTI aseguran que las operaciones tecnológicas estén alineadas con los objetivos estratégicos de la organización, minimizando riesgos y promoviendo la eficiencia operativa".

Componentes de los CGTI

Los componentes de los CGTI, como la gestión de acceso, los controles de cambio y los planes de recuperación, son fundamentales para el buen funcionamiento de los sistemas de información. En mi opinión, una adecuada implementación de estos componentes asegura que las organizaciones puedan responder rápidamente a incidentes tecnológicos, mitigando su impacto.

De acuerdo con COBIT (2019), "los componentes clave de los CGTI incluyen la seguridad de acceso, la gestión de cambios, la disponibilidad de sistemas y los planes de contingencia, todos diseñados para garantizar la continuidad y confiabilidad de los sistemas".

Evaluación y pruebas de los controles generales de tecnología de información (CGTI)

En la presente investigación evaluar y probar los CGTI es fundamental para garantizar la eficacia operativa de los controles que tiene diseñados el banco. Desde mi perspectiva, este proceso permite identificar vulnerabilidades y áreas de mejora, ayudando a las organizaciones a reforzar su postura frente a riesgos tecnológicos.

Según COSO (2013), "las pruebas de controles tecnológicos son un proceso clave para determinar su efectividad y para asegurar que cumplan con los objetivos operativos y de seguridad de la organización".

Marcos para la evaluación de CGTI

Los marcos como COBIT, ISO 27001 y NIST proporcionan directrices claras y estructuradas para evaluar los CGTI. En mi opinión, su adopción asegura que las organizaciones utilicen un enfoque estandarizado, fomentando la mejora continua y la alineación con las mejores prácticas internacionales.

De acuerdo con ISO 27001 (2013), "los marcos de evaluación permiten a las organizaciones implementar controles tecnológicos efectivos, alineados con estándares globales y adaptados a sus necesidades específicas".

Riesgo tecnológico y su gestión

El riesgo tecnológico representa una amenaza significativa en el entorno actual, especialmente en industrias altamente dependientes de sistemas digitales, como la bancaria. Desde mi perspectiva, gestionar estos riesgos de manera proactiva no solo protege los activos tecnológicos, sino que también fomenta la confianza de los clientes y los reguladores.

Según COSO (2013), "la gestión de riesgos tecnológicos implica la identificación, evaluación y mitigación de posibles amenazas relacionadas con el uso de la tecnología para garantizar la continuidad operativa y la Seguridad de la Información".

Identificación y evaluación de riesgos tecnológicos.

Identificar y evaluar riesgos tecnológicos requiere un enfoque meticuloso y basado en datos. En mi opinión, el uso de herramientas como mapas de riesgos y análisis de impacto es esencial para priorizar amenazas y diseñar estrategias efectivas de mitigación.

De acuerdo con COBIT (2019), "la identificación y evaluación de riesgos tecnológicos permiten a las organizaciones comprender su exposición a amenazas y priorizar acciones correctivas en función del impacto potencial".

Estrategias para mitigar riesgos tecnológicos en el entorno bancario

En el sector bancario, las estrategias de mitigación de riesgos tecnológicos deben ser robustas y adaptables, incluyendo medidas como la encriptación de datos, la autenticación multifactor y la capacitación del personal. Considero que estas estrategias no solo reducen vulnerabilidades, sino que también fortalecen la resiliencia frente a incidentes cibernéticos.

Según Hernández y Mendoza (2018), "las estrategias de mitigación, como los planes de contingencia y las pruebas de recuperación, son fundamentales para minimizar el impacto de los riesgos tecnológicos en las operaciones bancarias".

Deficiencias de control.

Las deficiencias de control son fallos o debilidades en los sistemas de control interno que pueden comprometer la efectividad de los procesos y aumentar los riesgos organizacionales. En mi opinión, su detección temprana es crucial para garantizar la integridad y la transparencia en la gestión empresarial.

De acuerdo con COSO (2013), "una deficiencia de control interno existe cuando el diseño o el funcionamiento de un control no permite a la dirección o a los empleados prevenir, detectar o corregir errores oportunamente".

Tipo de deficiencias control.

Las deficiencias de control pueden ser deficiencias, deficiencia material o deficiencia significativas, dependiendo del nivel de riesgo que representan. Considero que es fundamental clasificar estas deficiencias de forma adecuada para priorizar su corrección y evitar impactos negativos mayores en la organización.

Según Harmui y Varela (2013), "los tipos de deficiencias incluyen fallos en el diseño, la implementación o el monitoreo de los controles internos, lo que puede llevar a riesgos significativos si no se corrigen a tiempo".

Impacto de las deficiencias de control.

El impacto de las deficiencias de control puede manifestarse en pérdidas financieras, daños reputacionales o sanciones regulatorias. En mi opinión, las organizaciones deben adoptar una cultura de mejora continua para minimizar estos riesgos y fortalecer sus sistemas de control.

De acuerdo con Hernández y Mendoza (2018), "las deficiencias de control pueden comprometer la credibilidad y la estabilidad de una organización, especialmente en sectores sensibles como el financiero".

Informe y corrección de deficiencias.

El informe de deficiencias debe ser claro y detallado, destacando las áreas críticas y proponiendo soluciones concretas. Desde mi perspectiva, un enfoque estructurado en la corrección de deficiencias mejora la eficiencia operativa y fortalece la confianza de las partes interesadas.

Según COSO (2013), "el reporte oportuno y la corrección de deficiencias son fundamentales para mitigar riesgos y mantener la integridad de los controles internos".

Capitulo III: Marco metodológico

Para la investigación del presente tema se implementará el análisis de evidencia, ya que el tema en estudio se desarrollará con fuentes propias del banco como: de políticas, procedimientos, reportes de información, universos de usuarios, roles, cambios a los sistemas. Además, se utilizará investigación de campo mediante entrevistas a expertos y dueños de controles.

Enfoque de la investigación

El enfoque por utilizar para el desarrollo de este estudio es el cualitativo. Para Hernández, Baptista y Fernández (2014, citando a Hernández y Mendoza, 2008), definen el método de investigación cualitativo como un conjunto de procesos sistemáticos, empíricos y críticos, que implican la recolección y el análisis de datos cualitativos con el objetivo de obtener deducciones producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio.

Por lo anterior, el enfoque cualitativo se ajusta a la investigación en curso, porque el protagonismo se orienta en las políticas y procedimientos y reportes de información. En esta investigación el análisis de las oportunidades de mejora que tiene cada control es muy importante, para identificar los riesgos a los que está expuesto le banco y que controles generales del computador se deben robustecer.

Métodos de Investigación

Dentro de la presente investigación se utilizará el método deductivo, el cual Tena y Rivas (1995) lo definen como un método de razonamiento teórico, que parte del estudio de hechos prácticos y concretos, formando un sistema axiomático (que pretende ir más allá de las mismas disciplinas formales que le han dado origen) totalmente ideal, que no corresponde a una realidad, que permite manejarla y calcularla.

Así mismo, Rodríguez (2005) explica que es un proceso que consiste en obtener conclusiones particulares a partir de una ley universal. Este método consta en determinar los hechos más importantes, deducir las relaciones constantes de naturaleza uniforme que dan lugar al fenómeno, con base en las anteriores se formula la hipótesis, se observa la realidad para comprobarla y de esto, se deducen leyes. Este método parte de verdades generales y progresa por el razonamiento.

Por lo tanto, el método deductivo es el que se adecua al ensayo. Esto porque se analizará desde lo general de las políticas, procedimientos y controles hasta poder llegar a las conclusiones, acerca de las deficiencias que se pueden presentar en los controles a evaluar.

Tipos de investigación

El tipo de investigación a utilizar es el Fenomenológico. Taylor y Bodgan (1984) mencionan que "el fenomenólogo busca comprensión por medio de métodos cualitativos tales como la observación participante, la entrevista en profundidad y otros, que generan datos descriptivos" (p.16).

El método fenomenológico se ajusta a la investigación ya que permite observar los diferentes políticas y procedimientos en profundidad. Al respecto, Hernández et al. (2014) señala que: "Su propósito principal es explorar, describir y comprender las experiencias de las personas con respecto a un fenómeno y descubrir los elementos en común de tales vivencias" (p. 493).

Fuentes de información.

Para López (2017) las fuentes de información de acuerdo con la literatura clásica se clasifican dependiendo de la perspectiva desde la que se traten, pero las más reconocidas son de acuerdo con el nivel de información, y se clasifican en primarias, secundarias, terciarias y obras de consulta y referencia. Para la presente investigación se

obtendrán fuentes como listados de usuarios, listados de cambios, información de configuraciones de la base de datos, del sistema operativo y de la aplicación en alcance.

Primarias

Las fuentes de información primarias según López (2017) son "aquellos que tienen un carácter original, que no han sufrido ningún proceso de transformación o cambio, por ejemplo, un libro, un periódico, una revista" (p. 27).

Para la presente investigación se utilizarán como fuentes primarias: normas, marcos de referencia, , expertos en el tema presentados en conferencias o seminarios virtuales a través de la internet, así como entrevistas físicas al personal del banco que son relevante para la obtención de la información elemental para la investigación, entre los sujetos a entrevistar se acudirá a: Administrativos de TI, jefaturas, director de TI, encargado de la infraestructura tecnológica, encargados de la red y área de Seguridad de la Información.

Secundarias

Como fuentes de información secundarias Cordón et al., citado por López (2017), las define como "aquellos que resultan del análisis y del tratamiento de los documentos primarios y dan lugar a un documento diferente, por ejemplo, una bibliografía, una base de datos de resúmenes" (p. 28).

Las fuentes secundarias por utilizar en la investigación consistirán en: Análisis de tesis, artículos.

Terciarias

Así mismo, las fuentes documentales terciarias para Cordón et al., citado por López (2017), son "aquellos que someten a revisión los materiales primarios y

secundarios, por ejemplo, una bibliografía de bibliografías o un índice bibliográfico" (p. 28).

Sujetos de información

Población

De acuerdo con Hernández y Mendoza (2018, citando a Chaudhuri, 2018 y Lepkowski, 2008) la población es el conjunto de todos los casos que coinciden en una serie de especificaciones. Para la presente investigación se identificará la población de cada uno de los controles que van a ser evaluados.

Muestra

Según Gómez (2006) la muestra es una unidad de análisis o un grupo de ellas, sobre las que se recolectan datos, sin que sean necesariamente representativas de la población que se estudia. Para la presente investigación se identificará la población de cada uno de los controles que van a ser evaluados para poder seleccionar una muestra para poder concluir sobre cada control.

Tipo de muestra.

Las muestras se clasifican en dos grandes ramas: las no probabilísticas y las probabilísticas, para efectos de esta investigación se trabaja con la primera, la cual se define de la siguiente manera.

En las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace la muestra. Aquí el procedimiento "no es mecánico, ni con base en fórmulas de probabilidad" (Gómez, 2006, p. 111).

Dentro del muestreo no probabilístico tenemos el intencional y el accidental, entre otros. Para los fines de esta teoría se utiliza el muestreo intencional, que según Flores (2014): “es un procedimiento que permite seleccionar los casos característicos de la población limitando la muestra a estos casos” (p. 113).

Consideraciones éticas

Para Galeano (2004) las consideraciones éticas en la investigación social cualitativa son frecuentemente menos vistas y más sutiles que cuando se hacen en los métodos cuantitativos. Se asume la ética como práctica, modo de vida, y se presentan como los ejes éticos básicos la integridad del proceso, responsabilidad hacia los informantes (consentimiento informado, confidencialidad, anonimato y derechos de autor), pertinencia de las técnicas de recolección y registro de la información, manejo del riesgo y reciprocidad.

Técnicas

Tal como lo indica Ramírez (2018), las técnicas en la metodología cualitativa son los recursos que se pueden utilizar que permiten obtener información que ayude a identificar y describir las cualidades del objeto en estudio. Así mismo, existen diferentes técnicas para recolectar información cualitativa; sin embargo, las más utilizadas son la observación, la entrevista, la historia de vida, el grupo focal, el grupo de discusión y la información documental.

De las anteriores, la observación se define según Ramírez (2018, citando a Hernández, Fernández y Baptista, 2010) como el registro sistemático de comportamientos y situaciones, realizadas a partir de los sentidos, para buscar información específica. La observación se subdivide en: directa, indirecta, no participante, participante, no estructurada, estructurada, de campo, de laboratorio, individual y grupal.

Por otro lado, la entrevista según Ramírez (2018, citando a Hernández, Fernández y Baptista, 2010) es una conversación entre dos o más personas, donde el entrevistador hace preguntas para comprender las perspectivas, situaciones, problemas y soluciones de los consultados con sus propios términos. Esta se puede realizar mediante una guía estructurada, semiestructurada o abierta.

Así mismo, la otra técnica de importancia para la realización de esta investigación es la información documental, que de acuerdo con Ramírez (2018, citando a Ramírez, s.f.) señala que es una recopilación de datos hecha a partir de fuentes bibliográficas, iconografías, entre otros, que permiten explicar como sucedió un acontecimiento y orientar hacia otras fuentes de investigación. Esta se divide en dos tipos, los documentos escritos y los materiales audiovisuales.

Instrumentos

La elaboración de instrumentos para la obtención de información sobre una determinada construcción teórica exige una fundamentación técnica sobre aquello que queremos medir, y una construcción de instrumentos contrastados con la opinión de expertos y con la plausibilidad de que sea aplicable realmente en la recopilación de datos, comprobable mediante su aplicación y valoración de efectividad en lo pretendido (Martínez, 2014).

Para la presente investigación se utilizarán los siguientes instrumentos de medición:

Información documental

La información documental consiste en la lectura y comprensión de las diferentes fuentes de información primarias escritas, como lo son el análisis de normativa y Jurisprudencia a profundidad. Para la investigación que se va a desarrollar

Entrevistas no estructuradas

Es una de las fuentes más utilizadas en la investigación. Mediante esta una persona (entrevistador) solicita información a otra (entrevistado). Puede ser uno de los instrumentos más valiosos para conseguir información, se puede definir como: El arte de escuchar y captar información. Se realizarán entrevistas con las diferentes dependencias de TI con el fin de obtener el entendimiento de los controles a evaluar.

Proceso para la Recolección y Análisis de Datos

Una de las formas de procesar los acontecimientos es mediante la triangulación de datos, y según Martínez (2014) esta se define como:

La triangulación es una técnica que utiliza diferentes tipos de fuentes para asegurar las evidencias. El principio que subyace es el de recoger observaciones de una situación desde una variedad de perspectivas para después compararlas y contrastarlas. La investigación cualitativa utiliza diversidad de fuentes y técnicas de recogida de datos para evitar sesgos y asegurar la exactitud. (p. 95)

La recopilación de datos mixta es de naturaleza exploratoria, implica un análisis e investigación a profundidad. Los métodos de recolección de datos mixto no se enfocan en un método especifico, se profundiza de diversas formas para su recopilación.

Dado que la investigación es limitada a una población particular sea esta el Banco, identificando los Controles generales de TI se procede a establecer un mecanismo de investigación científica a través del uso del muestreo por conveniencia no probabilístico y no aleatorio.

Para la presente investigación se hará uso de la entrevista no estructurada y del muestreo por conveniencia, el cual según los autores Hernández, Baptista y Fernández (2014) se trata de una técnica de muestreo no probabilístico y no aleatorio utilizada para crear muestras de acuerdo con la facilidad de acceso, la disponibilidad de las personas de

formar parte de la muestra en un intervalo de tiempo dado o cualquier otra especificación práctica de un elemento particular.

El investigador elige a los miembros solo por su conveniencia y no considera si realmente estos representan muestra representativa de toda la población o no. Cuando se utiliza esta técnica, se pueden observar hábitos, opiniones y puntos de vista de manera más fácil.

De acuerdo con Hernández, Baptista y Fernández (2014), los investigadores utilizan técnicas de muestreo en situaciones en las que hay grandes poblaciones para ser evaluadas, ya que, en la mayoría de los casos, es casi imposible realizar pruebas a toda una población, incluso aunque muchos evitan implementar esta técnica, el muestreo por conveniencia es clave en situaciones en las que un investigador pretende obtener información en un lapso más corto y sin invertir demasiado dinero.

Capitulo IV: Análisis de resultados

En el contexto actual del sector bancario, la eficacia operativa de los controles generales de Tecnología de la Información (TI) es un factor crítico para garantizar la seguridad, integridad y confiabilidad de las operaciones financieras. La presente investigación se enfocará en la evaluación de la eficacia operativa de los controles generales de TI para el Core Bancario Oracle E-Business Suite (EBS) y su infraestructura tecnológica: base de datos y sistema operativo, principalmente en las siguientes áreas: control de cambios y control de acceso.

Aplicación	**Método de autenticación de los usuarios**	**Base de datos**	**Sistema Operativo**

Oracle eBusiness Suite	Método de Autenticación Propio de la aplicación	Oracle Database 12c	AIX 7.1

Según González y Ramírez (2020), la implementación de controles generales de TI no solo reduce riesgos operacionales, sino que también optimiza la eficiencia y la resiliencia del sistema bancario.

Historia de la entidad

La entidad bancaria objeto de estudio fue fundada en el año 1974 y ha desarrollado fundamentos sólidos que han impulsado su crecimiento y sostenibilidad a lo largo del tiempo. Su visión estratégica ha permitido consolidarse como una institución financiera de referencia, caracterizada por la prudencia en su administración y un enfoque orientado a la excelencia en el servicio. La institución tiene como misión comprender las necesidades de las empresas y personas, ofreciendo un servicio ágil y personalizado con condiciones competitivas. Su visión es ser el banco que satisface a sus clientes integralmente, generando una rentabilidad razonable mientras mantiene altos valores como la honestidad, responsabilidad, integridad y pasión por sus clientes.

En las últimas décadas, el crecimiento y modernización del banco han llevado a una creciente dependencia de los sistemas de información, particularmente de su Core Bancario Oracle E-Business Suite. Este sistema es fundamental para la ejecución de procesos financieros clave, como el ciclo de ingresos y el ciclo contable. Dada esta dependencia, es imperativo contar con controles robustos que garanticen la seguridad, confiabilidad y eficiencia operativa del sistema. La evaluación de los controles generales de TI permitirá determinar la fortaleza de los mecanismos actuales y la necesidad de implementar mejoras en la protección y gestión de los recursos tecnológicos del banco.

Alcance de la investigación

Alcance del sistema a evaluar en la investigación

Aplicación	Método de autenticación de los usuarios	Base de datos	Sistema Operativo
Oracle eBusiness Suite	Método de Autenticación Propio de la aplicación	Oracle Database 12c	AIX 7.1

Controles a evaluar y riesgos a la aplicación en alcance y su infraestructura tecnológica

Componente a evaluar	Descripción del control a evaluar	Riesgo Asociado
Base de datos Oracle 12c	El acceso a la base de datos a nivel privilegiado está autorizado y adecuadamente restringido.	Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus tareas asignadas, lo que puede crear una segregación de funciones inapropiada.
	El acceso se autentica mediante identificaciones de usuario y contraseñas únicas u otros métodos como mecanismo para validar que los usuarios están autorizados para acceder al sistema. Los parámetros de las contraseñas cumplen con las políticas y estándares de la empresa y/o profesionales (por ejemplo, longitud mínima y complejidad de la contraseña, caducidad, bloqueo de cuenta).	Los sistemas no están adecuadamente configurados ni actualizados para restringir el acceso al sistema a usuarios debidamente autorizados y apropiados.
	Los cambios en la base de datos son probados y aprobados adecuadamente antes de ser trasladados al entorno de producción.	Se realizan cambios inapropiados en la estructura de la base de datos y en las relaciones entre los datos.

	La capacidad de crear o modificar trabajos programados en Oracle está restringida a unos pocos individuos autorizados.	Los sistemas de producción, programas y/o trabajos resultan en un procesamiento de datos inexacto, incompleto o no autorizado.
	El estado de los trabajos en cola en Oracle se monitorea regularmente y se toman las acciones apropiadas.	
Aplicación Oracle eBusiness Suite	La gerencia aprueba la naturaleza y el alcance de los privilegios de acceso de los usuarios para el acceso de nuevos y modificados usuarios, incluyendo perfiles/roles estándar de aplicaciones, transacciones críticas de informes financieros y la segregación de funciones.	Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus tareas asignadas, lo que puede crear una segregación indebida de funciones.
	El acceso para usuarios que han sido terminados y/o transferidos se elimina o modifica de manera oportuna.	
	El acceso de los usuarios se revisa periódicamente.	
	La segregación de funciones se monitorea y el acceso conflictivo se elimina o se asigna a controles de mitigación, los cuales están documentados y probados.	
	El acceso a nivel privilegiado (por ejemplo, administradores de seguridad) está autorizado y adecuadamente restringido.	
	El acceso a través de la opción de perfil "Utilities: Diagnostics" está restringido	Se realizan cambios inapropiados directamente en los datos financieros mediante métodos distintos a las transacciones de la aplicación.
	El acceso se autentica mediante IDs de usuario y contraseñas únicas u otros métodos como mecanismo para validar que los usuarios están autorizados para acceder al sistema. Los parámetros de las contraseñas cumplen con las políticas y estándares de la empresa y/o profesionales (por ejemplo, longitud y	Los sistemas no están configurados o actualizados adecuadamente para restringir el acceso del sistema a usuarios debidamente autorizados y apropiados.

	complejidad mínima de la contraseña, expiración, bloqueo de la cuenta).	
	Los cambios en la aplicación se prueban y aprueban adecuadamente antes de ser trasladados al entorno de producción.	Se realizan cambios inapropiados en los sistemas o programas de aplicación que contienen controles automatizados relevantes (es decir, configuraciones configurables, algoritmos automatizados, cálculos automatizados y extracción automática de datos) y/o lógica de informes.
	El acceso para implementar cambios en el entorno de producción de la aplicación está adecuadamente restringido y segregado del entorno de desarrollo.	
	El acceso para programar y ejecutar programas concurrentes está restringido a individuos autorizados.	Los sistemas, programas y/o trabajos de producción resultan en el procesamiento inexacto, incompleto o no autorizado de datos.
Sistema Operativo AIX 7.1	Los sistemas críticos, programas y/o trabajos son monitoreados, y los errores de procesamiento se corrigen para asegurar su finalización exitosa.	
	El acceso de nivel privilegiado (por ejemplo, administradores de configuración y seguridad) está autorizado y restringido adecuadamente.	Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus tareas asignadas, lo que puede crear una segregación inadecuada de funciones.
	El acceso se autentica mediante identificaciones de usuario y contraseñas únicas u otros métodos como un mecanismo para validar que los usuarios están autorizados a acceder al sistema. Los parámetros de las contraseñas cumplen con los estándares de la empresa y/o de la industria (por ejemplo, longitud mínima y complejidad de la contraseña, caducidad, bloqueo de cuenta).	Los sistemas no están configurados o actualizados adecuadamente para restringir el acceso del sistema a usuarios debidamente autorizados y apropiados.
	Los atributos clave de la configuración de seguridad están implementados adecuadamente.	
	Los cambios en el sistema operativo se prueban y aprueban adecuadamente	Se realizan cambios inapropiados en el software del sistema (por ejemplo, sistema

	antes de ser trasladados al entorno de producción.	operativo, red, software de gestión de cambios, software de control de acceso).
	El acceso a los procesos laborales que manejan datos financieros clave está restringido al personal autorizado.	Los sistemas, programas y/o trabajos de producción resultan en un procesamiento de datos inexacto, incompleto o no autorizado.
	Los sistemas, programas y/o trabajos críticos son monitoreados, y los errores de procesamiento se corrigen para asegurar una finalización exitosa.	

Entendimiento de controles de la organización

Control de aprovisionamiento de usuarios

Fuente: Gerente y Supervisor de Seguridad de Tecnología de Información.

Durante la sesión de entendimiento con el Supervisor de Seguridad de Tecnología de Información, se corroboró que el área de Seguridad de Tecnología de Información es la encargada del ciclo de vida del acceso de usuarios en el sistema Oracle EBS, desde el alta en sistema hasta el borrado de usuarios que ya no requieran acceso, se utiliza la herramienta IVANTI para la administración de tickets relacionados al ABC de usuarios.

La entidad cuenta con los documentos “Manual de Seguridad de la Información” y “Política de Seguridad de la Información” donde se establece lo siguiente:

Altas de usuario

La oficina de Recursos Humanos deberá notificar con antelación al Departamento de Seguridad de la Información, y haciendo uso de correo electrónico o de las plataformas tecnológicas habilitadas para tal sentido, toda novedad o movimiento de personal asociado a procesos de vinculación, desvinculación, traslados, licencias, ausencias prolongadas o cualquier otro relacionado con la gestión del recurso humano (personal regular, personal temporal con contrato laboral de la entidad y de programas especiales,

jóvenes profesionales y practicantes) que pudiese requerir una creación, modificación o cancelación de privilegios de acceso de algún usuario, incluyendo la creación o eliminación de áreas o estructuras organizacionales, a fin de que dicha dependencia realice los cambios necesarios en la plataforma tecnológica. La oficina de Recursos Humanos debe informar al Departamento de Seguridad de la Información, haciendo uso de las herramientas formales que en tal sentido se establezcan, todas las novedades de personal, a más tardar el día efectivo de aplicación de la novedad.

La oficina de Recursos Humanos deberá notificar con antelación al Departamento de Seguridad de la Información, y haciendo uso de correo electrónico o de las plataformas tecnológicas habilitadas para tal sentido, toda novedad o movimiento de personal asociado a procesos de vinculación, desvinculación, traslados, licencias, ausencias prolongadas o cualquier otro relacionado con la gestión del recurso humano (personal regular, personal temporal con contrato laboral de la entidad y de programas especiales, jóvenes profesionales y practicantes) que pudiese requerir una creación, modificación o cancelación de privilegios de acceso de algún usuario, incluyendo la creación o eliminación de áreas o estructuras organizacionales, a fin de que dicha dependencia realice los cambios necesarios en la plataforma tecnológica. La oficina de Recursos Humanos debe informar al Departamento de Seguridad de la Información, haciendo uso de las herramientas formales que en tal sentido se establezcan, todas las novedades de personal, a más tardar el día efectivo de aplicación de la novedad, para que Recursos Humanos pueda llevar registro de dicho personal.

Posteriormente, el jefe de la dependencia deberá solicitar al departamento de Seguridad de la Información la creación de privilegios de acceso que corresponda, para lo cual deberá adjuntar copia de la notificación e información enviada a Recursos Humanos.

Recursos Humanos debe notificar al departamento de Seguridad de la Información la información del personal que vaya a gozar de licencias ininterrumpidas de más de seis meses, a fin de que les sean deshabilitados los accesos a la red y sistemas del Banco. Cualquier excepción a esta regla deberá ser autorizada por el superior inmediato de la persona que goza la licencia y por la oficina de Recursos Humanos. La notificación de estas licencias deberá hacerse, en la medida de lo posible, a más tardar el día de inicio de la licencia.

Los usuarios que requieran accesos a las plataformas aplicativas deben obtener las autorizaciones respectivas del jefe del área solicitante y del jefe del área dueña de la información del sistema, previo a enviar la solicitud de acceso al departamento de Seguridad de la Información, debiendo indicar fecha de inicio, fecha de finalización y justificación del acceso solicitado. El departamento de Seguridad de la Información no debe brindar acceso a ningún sistema de información si no se cuenta con las aprobaciones de manera expresa.

Control de bajas de usuarios

La Oficina de Recursos Humanos debe notificar al departamento de Seguridad de la Información cada vez que personal regular, personal temporal con contrato, jóvenes profesionales o practicantes finalicen su relación de trabajo con el Banco, con el fin de que todos los accesos lógicos y físicos otorgados sean deshabilitados. La oficina de Recursos Humanos debe informar al departamento de Seguridad de la Información todas las desvinculaciones de personal, a más tardar el día efectivo de desvinculación, haciendo uso de las herramientas que en tal sentido se establezcan para la comunicación de estas novedades de personal. No obstante, el departamento de Seguridad de la Información se reserva el derecho de revocar los accesos de forma automática al vencimiento de las relaciones que tengan un vencimiento establecido, (por ejemplo, contratistas, consultores,

etc.). Lo anterior no exime la responsabilidad de la oficina de Recursos Humanos de realizar la notificación al departamento de Seguridad de la Información en tiempo y forma.

Para el caso de consultores o personal de proveedores que presten servicios profesionales o de outsourcing, la dependencia que solicitó sus servicios será la responsable de notificar a Recursos Humanos cualquier desvinculación asociada con el personal que presta estos servicios, identificando la fecha de finalización efectiva de la relación y a más tardar la fecha efectiva de desvinculación, a fin de que la oficina de Recursos Humanos pueda actualizar el registro que lleva de dicho personal.

Control de parámetros de Contraseña

Fuente: Gerente y Supervisor de Seguridad de Tecnología de Información.

Durante una sesión de entendimiento con el Supervisor de Seguridad de Tecnología de Información, se corroboró que los parámetros de contraseña están basados en mejores prácticas de TI, adicionalmente que se cuenta con los documentos “Manual de Seguridad de la Información” e “Instructivo Gestión de Usuarios y Contraseñas” donde se establece lo siguiente:

A fin de procurar un adecuado uso de las contraseñas, todas las contraseñas deben ser tratadas como información confidencial, por lo que los usuarios deben cumplir con los siguientes aspectos:

No revelar o compartir las contraseñas a terceras personas.

No revelar o compartir la contraseña a compañeros de trabajo o superiores.

No revelar contraseñas en cuestionarios o formatos de seguridad que reciba.

No compartir las contraseñas con familiares o amigos.

Las contraseñas no deben ser escritas en agendas, calendarios, post-it o lugares visibles, ni almacenarlas en sistemas electrónicos personales.

Las contraseñas no deben ser transmitidas mediante servicios de redes sociales, mensajería instantánea ni vía telefónica.

Evitar en la medida de lo posible, teclear las contraseñas frente a otras personas

En aquellas plataformas que así lo permitan, los usuarios deberán auto gestionar el cambio de contraseña o desbloqueo de cuentas, de manera que se cuente con mayor agilidad para dicho proceso.

A fin de mantener altos controles de seguridad, en aquellas plataformas de sistemas que permitan establecer políticas de seguridad de contraseñas y acceso, Seguridad de la Información deberá configurar al menos las siguientes características:

- Longitud mínima de 8 caracteres.
- Complejidad por medio de la utilización de letras, mayúsculas, minúsculas, números y opcionalmente la utilización de caracteres especiales o símbolos.
- Cinco intentos de accesos fallidos, tras lo cual se bloqueará la cuenta.
- Período de caducidad variable, a ser establecido en días.
- Historia de las cuatro últimas contraseñas, para evitar la reutilización de las mismas.
- Los equipos y sistemas que no permitan establecer estas políticas deben emplear el máximo nivel de longitud de clave soportada, y los parámetros de expiración y caducidad máximos con los que cuenten internamente.

Las contraseñas de cuentas de usuario con altos privilegios o privilegios administrativos tales como: root, sysadmin, orcladmin, system y administrator entre otras, deben ser construidas con al menos 14 caracteres de longitud y diferentes entre los sistemas o aplicativos del Banco y limitados a unos pocos usuarios, quienes deberán velar

por su confidencialidad; estas cuentas privilegiadas se administrarán a través de una aplicación adquirida para tal fin, actualmente se utiliza la herramienta CyberArk.

Manual de Seguridad de la Información (Contraseñas).

Instructivo para la gestión de usuarios y contraseñas.

Control de gestión de cuentas privilegiadas

Fuente: Gerente y Supervisor de Seguridad de la Información.

Por norma, no se deben utilizar las cuentas privilegiadas que por defecto traen las diferentes plataformas (ej. usuario Root, admin, etc.) para el desarrollo de actividades habituales. El acceso a dichas cuentas debe ser autorizado por Seguridad de la Información y está restringido exclusivamente a personal de Seguridad de la Información y Aplicaciones cada uno dentro de su ámbito de competencia, la entidad utiliza la herramienta CyberArk para la gestión y uso de cuentas privilegiadas con el fin de prevenir acciones no autorizadas en los sistemas de información.

En la investigación se identificó que se cuenta con el documento "Manual de Seguridad de la Información" en donde se establece lo siguiente:

Se permite el acceso temporal a cuentas privilegiadas a personal de outsourcing o de servicios tecnológicos, solo en aquellas plataformas que provean mecanismos de trazabilidad sobre las acciones realizadas y siempre bajo la supervisión de alguna de las áreas tecnológicas de la Subgerencia de Tecnología e Innovación.

El Departamento de Tecnología y Comunicaciones debe asegurar que todos los equipos de la plataforma de procesamiento central estén integrados a la herramienta establecida por el Departamento de Seguridad de la Información para el control de cuentas privilegiadas, de tal forma que, a través de la misma, se pueda guardar la trazabilidad de las acciones realizadas en la plataforma tecnológica del Banco con este tipo de cuentas por parte del personal tecnológico de la Subgerencia de Tecnología e Innovación.

El Departamento de Tecnología y Comunicaciones debe asegurar que todos los equipos de la plataforma de procesamiento central estén integrados a la herramienta establecida por el Departamento de Seguridad de la Información para el control de cuentas privilegiadas, de tal forma que, a través de la misma, se pueda guardar la trazabilidad de las acciones realizadas en la plataforma tecnológica del Banco con este tipo de cuentas por parte del personal tecnológico de la Subgerencia de Tecnología e Innovación.

Control de recertificación de usuarios y segregación de funciones

Fuente: Gerente y Supervisor de Seguridad de la Información.

La administración realiza un ejercicio de recertificación de usuarios para las aplicaciones EBS, de manera anual, adicionalmente la entidad cuenta con una matriz donde realizan la identificación de privilegios adicionales asignados a usuarios con el mismo puesto, dichos privilegios fueron validados con el jefe directo para confirmas que no existiera algún conflicto de Segregación de Funciones.

Adicionalmente se cuenta con el documento “Manual de Seguridad de la Información” en donde se establece lo siguiente:

Para gestionar adecuadamente el acceso a las plataformas aplicativas del Banco, los responsables de la información deben revisar anualmente o cuando se requiera, los privilegios, roles y funciones otorgados a los usuarios de sus respectivas dependencias validando y asegurando la debida segregación funcional al interior de sus áreas, así como de modificar o revocar los privilegios que no sean requeridos o no estén alineados a las necesidades de cada área del Banco. Para ello, el departamento de seguridad de la información debe brindar los reportes necesarios a los dueños de los aplicativos para la revisión de los accesos.

Al menos con una periodicidad anual, genera los reportes de usuario de la aplicación eBusiness, clasificando los usuarios por dependencia, y especificando

usuarios, roles y permisos, incluyendo dentro del alcance los usuarios de la herramienta de gestión de cuentas privilegiadas. Estos reportes se obtienen de aquellos sistemas aplicativos que proveen la funcionalidad de emisión de reportes. Igualmente valida que toda la información de los reportes generados sea comunicada a las áreas usuarias, conforme la siguiente actividad, a fin de que no quede ningún usuario definido en el alcance que se quede sin ser validado.

En el evento de que existan conflictos de segregación funcional que deban ser mantenidos, identificará el motivo por el cual se requiere mantener los accesos y documenta controles supletorios existentes.

Manual de Seguridad de la Información (Control de accesos a sistemas de información).

Política de Seguridad de la Información (Control de accesos a sistemas de información)

Control de aprovisionamiento de usuarios en CyberArk

Fuente: Gerente y Supervisor de Seguridad de la Información.

CyberArk es un Software de Seguridad para las cuentas privilegiadas a nivel de Infraestructura (Base de Datos y Sistema Operativo), dedicada a detener y proteger de forma proactiva las amenazas cibernéticas, el monitoreo y el control de los accesos privilegiados.

El Proceso de aprovisionamiento de usuarios, comienza a través de la creación de un ticket por medio de la Herramienta IVANTI del área correspondiente (departamento de Aplicaciones, Departamento de Tecnología), hacia el departamento de Seguridad de la Información, con el objetivo de agregar alguna cuenta privilegiada dentro de alguna de las bóvedas de la Herramienta que debe de contener: Tipo de Dispositivo (Sistema Operativo o Base de Datos), Plataforma, Nombre de Usuario y Dirección. Posterior al

resguardo de la cuenta dentro de CyberArk, para dominio, gestión y custodia del departamento de Seguridad de la Información.

Control de gestión de usuarios privilegiados en CyberArk

Fuente: Entrevista Gerente y Supervisor de Seguridad de la Información.

CyberArk se encuentra configurado para realizar las tareas de administración por medio de las siguientes Cuentas de Usuario:

Master: Cuenta nativa de la Herramienta, sin embargo, no se utiliza para la administración de CyberArk.

Administrator: Cuenta nativa de la Herramienta que se utiliza para la administración de CyberArk, y la cual es custodiada y monitoreada por el departamento de Seguridad de la Información.

Batch: Cuenta nativa de la Herramienta que funge para realizar las tareas de monitoreo y grabado del uso de las cuentas privilegiadas, la cual es custodiada y monitoreada por el departamento de Seguridad de la Información.

Lcastro: Única cuenta de usuario final que tiene como objetivo realizar las tareas de administración dentro de la Herramienta (Se realizó este tipo de configuración para no utilizar las cuentas nativas (Master & Administrator), y la cual se encuentra autorizada, custodiada y monitoreada por el departamento de Seguridad de la información.

Control de parámetros de contraseña en Cyber Ark

Fuente: Gerente y Supervisor de Seguridad de la Información.

CyberArk se encuentra configurado para heredar las contraseñas directamente del Controlador de Dominio para los usuarios que existen y administran la Herramienta (Método de autenticación LDAP), adicionalmente utiliza un doble factor de autenticación para permitir el acceso (MFA).

Control de cambios: desarrollo y mantenimiento de sistemas

Fuente: Gerente de Aplicaciones

Se cuenta con cambios estándar y de emergencia para la plataforma tecnológica, plataforma aplicativa e Inteligencia de Negocios, IVANTI es la herramienta para realizar la petición de cambios.

La entidad cuenta con el documento “Instructivo para la Gestión de Cambios” en donde se establece lo siguiente:

Cambios de Emergencia

Para cualquier solicitud de emergencia en la plataforma tecnológica, se debe documentar en el aplicativo de gestión de cambios la solicitud con la siguiente documentación:

Correo generado por el Administrador de Sistemas, el Administrador de Base de Datos o el Administrador de Redes, documentando la solicitud de cambio y solicitando la autorización del Coordinador de Tecnología y del Subgerente de Tecnología de Información, copiando al jefe de Aplicaciones y al Coordinador del Departamento de Seguridad de la Información y Aseguramiento de la Calidad.

Autorización de cambio de emergencia dado por el Coordinador de Tecnología. En caso de cambios a la plataforma de seguridad, se requiere la autorización del jefe de Seguridad de la Información.

Autorización de cambio de emergencia dado por el Subgerente de Tecnología de Información.

Script y demás archivos con programas que se ejecutaron en producción, en los casos que aplique.

Documentación técnica y funcional del cambio en los casos que aplique.

Para cualquier solicitud de emergencia en la plataforma aplicativa, se debe documentar en el aplicativo la gestión de cambios (al momento de normalizar el cambio de emergencia) la solicitud con la con la siguiente documentación:

- Correo generado por el responsable del Cambio documentando la solicitud de cambio y solicitando la autorización del Jefe de Aplicaciones y del Subgerente de Tecnología de Información y copiando al Coordinador de Tecnología y al Coordinador del departamento de Seguridad de la Información y Aseguramiento de la Calidad. En los casos en que el cambio no sólo sea de índole técnico, sino que sea funcional, se deberá copiar a los jefes de las áreas usuarias involucradas con la solicitud de cambio.
- Correo de autorización de cambio de emergencia dado por el Jefe de Aplicaciones.
- Correo de autorización de cambio de emergencia dado por el Subgerente de Tecnología de Información.
- Script y archivos con programas a ejecutar en producción en los casos que aplique.
- Documentación técnica y funcional del cambio en los casos que aplique.

Para el caso de cambios de emergencia de Datos (datapatch)o cambios generados por solución de errores funcionales, se incluirá en el aplicativo de gestión de cambios el correo con la documentación donde el área usuaria reporta el error identificado y el correo donde el departamento de aplicaciones envía la solución a implementar. En estos correos debe estar copiados los jefes de áreas usuarias afectadas por el cambio.

Para el caso de cambios de emergencia, la validación y aceptación de la solución implementada es realizada por el usuario solicitante, en el ambiente productivo, luego que se le informa la aplicación de la solución.

Cambios estándar.

Para cualquier solicitud estándar en la plataforma tecnológica, se debe documentar en el aplicativo de gestión de cambios la solicitud con la siguiente documentación:

- Solicitud de cambio requerida por el Administrador de Sistemas, el Administrador de Base de Datos o el Administrador de Redes.
- Autorización del Coordinador de Tecnología.
- Autorización del Subgerente de Tecnología de Información del paso a producción en los casos de solicitudes de cambio cuya valoración de riesgo sea Alta. En estos casos, el jefe de Aplicaciones debe estar informado y en los casos necesarios, el jefe del área usuaria.
- Script y archivos con programas a ejecutar en producción en los casos que aplique.
- Documentación técnica y funcional del cambio en los casos que aplique.

Para cualquier solicitud estándar en la plataforma aplicativa, se debe documentar en el aplicativo de gestión de cambios la solicitud con la siguiente documentación:

Solicitud de cambio requerida por el usuario.

Autorización del Gerente de Aplicaciones.

Autorización del Jefe del área usuaria en los casos aplicables, o del Gerente del área usuaria o su delegado oficial en los casos aplicables.

Autorización del Subgerente de Seguridad de la Información del paso a producción en los casos de solicitudes de cambio cuya valoración de riesgo sea Alta.

Igualmente, en estos casos de cambios de riesgo Alto, se requerirá que el jefe del área usuaria esté informado.

Instrucciones para el despliegue de la solución:

- Scripts y/o ejecutables (en los casos que aplique)
- Manual de instalación.
- Parámetros SQL (en los casos que aplique).
- Si se modificó el esquema de seguridad, actualización de la documentación de seguridad (matriz de roles y permisos)
- Evidencia de realización de las pruebas realizadas por el usuario, en ambientes de prueba, aceptando los cambios efectuados a la aplicación de acuerdo con la solicitud (en caso de modificaciones aplicativas). Para el caso de cambios a Datos (datapatch) o cambios generados para solucionar errores funcionales (datos), la validación y aceptación de la solución implementada es realizada por el usuario solicitante, en el ambiente productivo, luego que se le informa la aplicación de la solución.

Desarrollo de la investigación

La presente investigación se enfocará en la evaluación de la eficacia operativa de los controles generales de TI para el Core Bancario Oracle E-Business Suite (EBS) y su infraestructura tecnológica: base de datos y sistema operativo, principalmente en las siguientes áreas: control de cambios y control de acceso.

Controles de cambios en la aplicación, base de datos y sistema operativo:

1. Los cambios en la aplicación, base de datos y sistema operativo se prueban y aprueban adecuadamente antes de ser trasladados al entorno de producción.

Diseño del control:

La entidad cuenta con cambios estándar y de emergencia para la plataforma tecnológica (Infraestructura), plataforma aplicativa, IVANTI es la herramienta para realizar la petición y documentación de cambios.

El documento “Instructivo para la Gestión de Cambios” en donde se establece lo siguiente:

Cambios de Emergencia

Para cualquier solicitud de emergencia en la plataforma tecnológica, se debe documentar en el aplicativo de gestión de cambios la solicitud con la documentación correspondiente según el Instructivo de gestión de cambios.

Para cualquier solicitud de emergencia en la plataforma aplicativa, se debe documentar en el aplicativo la gestión de cambios (al momento de normalizar el cambio de emergencia) la solicitud con la documentación correspondiente segun el Instructivo de gestión de cambios.

Correo generado por el responsable del Cambio documentando la solicitud de cambio y solicitando la autorización del Jefe de Aplicaciones y del Subgerente de Tecnología de Información y copiando al Coordinador de Tecnología y al Coordinador del Departamento de Seguridad de la Información y Aseguramiento de la Calidad. En los casos en que el cambio no sólo sea de índole técnico, sino que sea funcional, se deberá copiar a los jefes de las áreas usuarias involucradas con la solicitud de cambio.

Correo de autorización de cambio de emergencia dado por el Jefe de Aplicaciones.

Correo de autorización de cambio de emergencia dado por el Subgerente de Seguridad de Información.

Script y archivos con programas a ejecutar en producción en los casos que aplique.

Documentación técnica y funcional del cambio en los casos que aplique.

Para el caso de cambios de emergencia de Datos (datapatch)o cambios generados por solución de errores funcionales, se incluirá en el aplicativo de gestión de cambios el correo con la documentación donde el área usuaria reporta el error identificado y el correo donde el departamento de aplicaciones envía la solución a implementar. En estos correos debe estar copiados los jefes de áreas usuarias afectadas por el cambio.

Para el caso de cambios de emergencia, la validación y aceptación de la solución implementada es realizada por el usuario solicitante, en el ambiente productivo, luego que se le informa la aplicación de la solución.

Cambios estándar.

Para cualquier solicitud estándar en la plataforma tecnologica, se debe documentar en el aplicativo de gestión de cambios la solicitud con la documentación correspondiente según el Instructivo de gestión de cambios.

Para el caso de implementación de nuevas soluciones, correo de notificación a Seguridad de la Información confirmando si existen o no nuevas cuentas privilegiadas en el paso a producción, en cuyo caso deben confirmar la debida actualización del repositorio centralizado de cuentas privilegiadas y su enrolamiento en Cyberark.

Para cualquier solicitud estándar en la plataforma aplicativa, se debe documentar en el aplicativo de gestión de cambios la solicitud con la siguiente documentación:

1. Solicitud de cambio requerida por el usuario.

2. Autorización del Jefe de APLI.

3. Autorización del Jefe del área usuaria en los casos aplicables, o del Gerente del área usuaria o su delegado oficial en los casos aplicables conforme a lo establecido en el lineamiento 1.14.

Autorización del Subgerente de Tecnología de Información del paso a producción en los casos de solicitudes de cambio cuya valoración de riesgo sea Alta. Igualmente, en

estos casos de cambios de riesgo Alto, se requerirá que el jefe del área usuaria esté informado. Instrucciones para el despliegue de la solución:

Scripts y/o ejecutables (en los casos que aplique)

Manual de instalación

Parámetros SQL (en los casos que aplique)

Si se modificó el esquema de seguridad, actualización de la documentación de seguridad (matriz de roles y permisos)

Evidencia de realización de las pruebas realizadas por el usuario, en ambientes de prueba, aceptando los cambios efectuados a la aplicación de acuerdo con la solicitud (en caso de modificaciones aplicativas). Para el caso de cambios a Datos (datapatch) o cambios generados para solucionar errores funcionales (datos), la validación y aceptación de la solución implementada es realizada por el usuario solicitante, en el ambiente productivo, luego que se le informa la aplicación de la solución.

Prueba de la Implementación y Eficacia Operativa:

Validación de los cambios documentados

Se obtuvo una lista de cambios generada por el sistema para el período de auditoría, se probaron los siguientes atributos:

El cambio se probó antes de pasar a la producción y parece apropiado según la naturaleza del cambio: Para una muestra, se corroboró que se realizaron pruebas para el total de la muestra, exceptuando los cambios de emergencia y/o datapatch, que están excluídos por su naturaleza.

El cambio fue aprobado por la gerencia correspondiente: Todos los cambios de la muestra fueron debidamente aprobados por la gerencia correspondiente.

Se mantuvo la segregación de funciones en el proceso de cambio: Se mantuvo la segregación de funciones entre quienes ejecutan, prueban y aprueban el cambio para todas las muestras.

Conclusión: El control es efectivo.

Validación de objetos / Ejecutables:

Se realizó una prueba previa a la de control de cambios, que consiste en validar que los objetos/ejecutables del aplicativo ORACLE EBS se encontrasen documentados por la Entidad en los tickets que se levantan por cada modificación a estos. Para tal actividad se procedió a obtener un listado completo de ejecutables y objetos modificados se realizó una muestra.

De acuerdo con la frecuencia con la que operó el control durante el, se identificó una frecuencia de operación "muchas veces al día", se solicitó una muestra para validar que estos se encontrasen documentados.

Se corroboró que para todos los ítem de la muestra, cada uno poseía un ticket asociado, sobre el cual se validó que el objeto/rutina se documentó. Por lo tanto, se considera esta actividad como efectiva, lo que da la pauta para revisar los cambios registrados.

Conclusión: El control es efectivo.

Validación de parches en el sistema operativo:

Se solicito el 'software history' y se obtuvo la población de parches/cambios realizados al servidor, donde se identificó lo siguiente:

Se validaron los siguientes atributos:

- El cambio se probó y/o planes de retroceso se crearon antes de la implementación.

- El cambio fue aprobado por la administración antes de instalarse en la base de datos y/o el servidor.

Conclusión: El control es efectivo.

2. El acceso para implementar cambios en el entorno de producción de la aplicación está adecuadamente restringido y segregado del entorno de desarrollo.

Diseño del control:

La entidad cuenta con cambios estándar y de emergencia para la plataforma tecnológica (Infraestructura), plataforma aplicativa, IVANTI es la herramienta para realizar la petición y documentación de cambios.

La entidad cuenta con el documento “Instructivo para la Gestión de Cambios” en donde se establece lo siguiente:

Cambios de emergencia

• Para cualquier solicitud de emergencia en la plataforma tecnológica, se debe documentar en el aplicativo de gestión de cambios la solicitud con la documentación correspondiente según el Instructivo de gestión de cambios.

• Para cualquier solicitud de emergencia en la plataforma aplicativa, se debe documentar en el aplicativo la gestión de cambios (al momento de normalizar el cambio de emergencia) la solicitud con la documentación correspondiente según el Instructivo de gestión de cambios.

Cambios estándar.

• Para cualquier solicitud estándar en la plataforma tecnológica, se debe documentar en el aplicativo de gestión de cambios la solicitud con la documentación correspondiente según el Instructivo de gestión de cambios.

• Para cualquier solicitud estándar en la plataforma aplicativa, se debe documentar en el aplicativo de gestión de cambios la solicitud con la documentación correspondiente según el instructivo de gestión de cambios.

Durante la entrevista la administración de TI comenta que:

Los usuarios desarrolladores no tienen acceso a los ambientes productivos.

Los ambientes de QA, desarrollo y producción se encuentra segregados.

El área de aplicaciones es la encargada y autorizada para implementar cambios en el ambiente productivo.

El pasaje a producción es realizado de forma manual, no se requiere de herramientas para realizar este proceso.

Prueba de la Implementación y Eficacia Operativa:

La entidad suministró los listados de usuario con acceso a implementar cambios en el ambiente productivo, se identificó que se utilizan las cuentas de SYS y SYSTEM para implementar cambios en el ambiente productivo de Oracle EBS, para las cuentas corroboró que:

Son reconocidas y autorizadas por el Jefe de aplicaciones

La gestión y utilización de estas cuentas se realiza mediante la herramienta CyberArk.

En el aplicativo EBS corroboró la existencia de 6 cuentas de usuario con acceso a:

1. Create/Modify Menus
2. Define System Profile Option Values
3. Create/Modify Functions
4. Create/Modify Responsibilities

Se identifico un usuario con acceso a "Creación/modificación de roles" y 10 usuarios con acceso a "Create/Modify Configurations", para cada una de las cuentas identificadas se validó que:

Las cuentas son reconocidas y autorizadas por el jefe de aplicaciones.

Los usuarios cuentan con los accesos son apropiados con base a sus funciones.

Conclusión: El control es efectivo.

Controles de seguridad de accesos:

1. La gerencia aprueba la naturaleza y el alcance de los privilegios de acceso de los usuarios, para accesos nuevos y modificados, incluyendo perfiles/roles estándar de aplicaciones, transacciones críticas y la segregación de funciones

Diseño del control:

El área de Seguridad de la Información es la encargada del ciclo de vida del acceso de usuarios a los sistemas de información que conllevan desde el alta en sistema hasta el borrado de usuarios que ya no requieran acceso, actualmente se utiliza la herramienta IVANTI para la administración de tickets relacionados al ABC de usuarios en los sistemas de información.

La entidad cuenta con los documentos “Manual de Seguridad de la información” y “Política de Seguridad de la Información” donde se establece lo siguiente:

El Analista / Asistentes Administrativas / Secretarias /Jefe de la Dependencia Solicitante solicita accesos permanentes o temporales a los aplicativos del Banco para su colaborador. Este envía solicitud a través del CUAT (Centro Unificado de Atención) para su registro en el Aplicativo de Mesa de Servicio, detallando lo siguiente:

Correo de solicitud por parte del Jefe de área, si es un analista quien envía la solicitud, debe indicar en el correo que la solicitud se hace por instrucciones de su jefe y debe copiar a este.

Nombre del colaborador, sistema aplicativo y tipo de acceso requerido, pudiendo mencionar como parámetro los accesos otorgados a otro colaborador y la justificación del mismo.

Notificación del área usuaria indicando que los accesos solicitados no contravienen la normativa existente y que los mismos no generan concentración de funciones o inadecuada segregación funcional en el área.

Para creación de accesos por delegaciones temporales: nombre del titular, nombre del Encargado Temporal designado, notificación oficial del área informando a todo el personal sobre la delegación temporal o que el titular del puesto estará temporalmente fuera del Banco, sistema aplicativo, período del encargo.

Para creación de accesos temporales no derivados de una delegación temporal: nombre y cargo del colaborador, sistema aplicativo.

El Supervisor de Seguridad de la Información o Analista SOC de Seguridad de la información revisa la solicitud de accesos permanentes o temporales a los aplicativos y verifica lo siguiente:

La fecha de ingreso y finalización en el caso de que sea un personal temporal.

La completitud de toda la información requerida.

Que la dependencia solicitante haya manifestado que desde la perspectiva funcional, la solicitud no genera concentración de funciones e inadecuada segregación funcional, en el aplicativo eBusiness.

Que no exista incumplimiento de la política de la seguridad de información y su manual de aplicación.

Que existan licencias suficientes en el sistema aplicativo respectivo para poder otorgarle acceso.

Una vez que el Jefe del Área autoriza la creación del usuario, ingresa la información básica del usuario, asigna los roles solicitados en los sistemas y asigna una contraseña temporal. En caso de que el usuario ya esté creado en el sistema y que la solicitud corresponda a la asignación de un rol específico, actualiza su información.

Toda solicitud de acceso (Alta, baja, cambio de usuario), deberá de contar con:

- Ticket de solicitud (Helppeople)
- Especificar nombre, cargo, aplicación, tipo de acceso y justificación.
- Para altas de usuario - VoBo's de autorización de área dueña de la app (en caso de que el área dueña sea distinta al de la solicitud).

Prueba de la Implementación y Eficacia Operativa:

Se obtuvo la población de usuarios creados y modificados. Se probaron los siguientes atributos:

- La solicitud de acceso del usuario fue aprobada por la gerencia correspondiente: Según la inspección de la solicitud de acceso, se observó que la solicitud de acceso está aprobada por la gerencia correspondiente para todos los elementos de la muestra.
- El acceso solicitado es consistente con el acceso otorgado en el sistema: Según la inspección se identificó que el acceso en el formulario de solicitud coincide con lo que se concedió en el sistema para todos los elementos de la muestra.
- El acceso otorgado es proporcional a las funciones asignadas del usuario y hace cumplir la separación adecuada de funciones: Según la inspección

de la solicitud de acceso y el título del trabajo de los usuarios, el acceso otorgado se alinea con las responsabilidades laborales del usuario.

- Se mantiene la segregación de funciones entre el aprobador y la persona que otorga el acceso en el sistema: Según la inspección de la solicitud de acceso, se validó que el aprobador no es la persona que otorgó el acceso para todos los elementos de la muestra.

Conclusión: El control es efectivo.

2. El acceso para usuarios que han sido terminados y/o transferidos se elimina o modifica de manera oportuna.

Diseño del control:

Área de Seguridad de la Información es la encargada del ciclo de vida del acceso de usuarios a los sistemas de información que conllevan desde el alta en sistema hasta el borrado de usuarios que ya no requieran acceso, actualmente se utiliza la herramienta IVANTI para la administración de tickets relacionados al ABC de usuarios en los sistemas de información.

Se cuenta con los documentos “Manual de Seguridad de la información” y “Política de Seguridad de la Información” donde se establece lo siguiente:

El Analista de Recursos Humanos o Jefe de la Dependencia solicitante solicita la deshabilitación de usuarios de servicios de red y aplicativos. Ingresa la solicitud de retiro permanente (terminación de relación laboral con colaboradores permanentes o finalización contractual anticipada con empleados temporales u otras modalidades) o retiro temporal de usuario (licencias superiores a 6 meses), completando todos los campos necesarios e indicando el colaborador y la fecha efectiva del retiro, la cual no puede ser anterior a la fecha de la solicitud.

Para el caso de consultores o personal de proveedores que presten servicios profesionales o de outsourcing, el jefe de cada área que administre servicios de terceros, o un colaborador de dicha dependencia, copiando al jefe e indicando que es por solicitud del jefe de la dependencia, solicita al CUAT vía correo electrónico la deshabilitación de accesos, a fin de que el CUAT ingrese la solicitud al aplicativo de la mesa de servicio relacionada. En el caso que la Oficina de Recursos Humanos o el área que administre los servicios de terceros no especifique la hora de finalización de permisos se tomará la última hora hábil en Edificio Sede. Si el día de culminación cae en un día no laborable, se tomará como referencia el día hábil previo a la finalización.

Para el caso de ausencias prolongadas (licencias ininterrumpidas de más de 6 meses) indica el período de vigencia de esta (fecha de inicio y fecha de finalización) a fin de que se otorguen por defecto durante ese periodo los privilegios mínimos.

Supervisor de Seguridad de la Información o Analista deshabilita los accesos de correo, red y aplicativos en producción: Una vez que se revisa la solicitud de retiro del colaborador se deshabilitan los accesos a las diferentes plataformas a las cuales ingresaba el usuario y actualiza las tareas en el Aplicativo de Mesa de Servicio.

El administrador de Sistemas o Administrador de Base de Datos deshabilita accesos a nivel de Bases de Datos de los diferentes ambientes computacionales. Igualmente actualiza la tarea en el Aplicativo de Mesa de Servicio.

• El acceso es removido de forma manual

• El proceso de desvinculación aplica a usuarios externos e internos.

• Las cuentas no son eliminadas, únicamente pasan a un estatus inactivo o deshabilitado.

• Los accesos son eliminados una vez recibido la solicitud de baja.

Prueba de la Implementación y Eficacia Operativa:

Se obtuvo una lista de despidos de empleados y contratistas durante prevista por Recursos Humanos. Con base en la frecuencia se hizo una selección de los usuarios que fueron despedidos. Para cada usuario seleccionado, se probaron los siguientes atributos:

Los privilegios de acceso para el usuario cancelado ya no están activos en el sistema. Dicho acceso fue eliminado, eliminado o inhabilitado de manera oportuna (según la fecha de vigencia de la terminación): Según la inspección del ORACLE EBS, el acceso de los exempleados fue removido de manera oportuna.

Para cada caso se obtuvo de evidencia lo siguiente:

Ticket de solicitud (Correo - Ivanti) donde se pudo corrobar la confirmación de la baja, con la fecha oportuna.

Se realizó un cruce del total de usuarios con estatus de "EGRESO" por parte de RH vs el listado de usuarios activos de EBS, se validó que no existen usuarios dados de baja de la entidad con algún privilegio activo en los sistemas.

Se obtuvo una lista de transferencias de empleados y contratistas prevista por Recursos Humanos. Con base en la frecuencia se hizo una selección de los usuarios que fueron despedidos. Para cada usuario seleccionado, se probaron los siguientes atributos:

Los privilegios de acceso que ya no eran necesarios como resultado de la transferencia del empleado se eliminaron de manera oportuna.

Según la inspección en el sistema ORACLE EBS, el acceso de los empleados que tuvieron traslados fue removido de manera oportuna.

Conclusión: El control es efectivo.

3. El acceso de los usuarios se revisa periódicamente.

Diseño del control:

Se obtuvo una comprensión de los siguientes atributos:

Políticas, procedimientos, estándares y orientación para revisar el acceso de los usuarios; Se identificó que la entidad posee el procedimiento "Administración de la Seguridad de los Sistemas", donde se detalla el proceso de recertificación de los sistemas.

Procedimientos y personas responsables para revisar el acceso de los usuarios; Responsabilidades y responsables en el procedimiento de revisión de accesos:

Supervisor de Seguridad de la Información: Genera los reportes de usuarios y valida completitud de estos. Solicita revisión de accesos de usuarios de cada dependencia.

Gerente o jefe de dependencia usuaria valida los privilegios de acceso asignados a los usuarios de su dependencia. Acepta accesos y notifica a Seguridad de la Información o solicita

modificación de accesos.

Supervisor de Seguridad de la Información revisa listados de acceso de aplicativos y realiza las modificaciones correspondientes.

Supervisor de Seguridad de la Información realiza el cambio o modificación en los sistemas, siguiendo los procedimientos de aprovisionamiento o desaprovisioamiento definido por la Entidad.

Frecuencia de la revisión de acceso; La revisión de accesos es efectuada de forma anual.

Alcance de la revisión (por ejemplo, empleados, proveedores, contratistas, invitados y cuentas genéricas/de sistema) y lo que se considera una excepción; Para este control se contemplan todas las cuentas de usuarios y cuentas de servicio e interfaces creadas en los sistemas revisados, pertenecientes a personal interno y/o externo de la Entidad.

Si la revisión incluye a los usuarios y sus derechos/privilegios de acceso asociados, incluida la segregación de funciones basada en roles y el acceso privilegiado;

La revisión de accesos incluye a todos los usuarios de los sistemas con sus privilegios asociados. Todos los usuarios contenidos en el aplicativo se cruzan con los reportes de empleados de RRHH, para determinar el puesto del usuario, y que el revisor sea el Gerente o Jefe de dependencia de cada área para asegurar que haya una debida segregación de funciones entre el revisor y el dueño de la cuenta.

Con qué nivel de detalle se realiza la revisión; El equipo de Seguridad de la Información procede a solicitar al TEC la extracción del listado de usuarios activos del sistema en revisión. De igual manera, solicita a Talento Humano el personal activo e inactivo del Banco, mismo que utilizará para realizar cruces con el de usuarios activos, para validar el puesto del personal a revisar, e igual validar si existen inconsistencias en base a usuarios que ya salieron de la Entidad y no requieren tener su cuenta activa en los sistemas o bien, que cambiaron de puestos en cierto tiempo y hay roles que ya no deberían poseer. Una vez obtenido un match entre usuarios y puestos, se procede a enviar vía correo electrónico en formato pdf a las diferentes áreas el listado de usuarios que corresponde a las gerencias correspondientes, mismos que tendrán que validar que los usuarios a su cargo posean el privilegio que corresponde en base a las actividades que debería realizar según su perfil de puesto.

Las gerencias responden a Seguridad de la Información de la siguiente manera en caso de no identificar ningún tipo de inconsistencia:

Los accesos existentes corresponden a los requeridos por el área y los mismos están correctamente asignados.

Los accesos existentes no contravienen la normativa existente.

Los accesos son consistentes con las responsabilidades laborales actuales de cada usuario.

Los accesos existentes no generan concentración de funciones o inadecuada segregación funcional al interior del área.

En el caso que se identifique que el usuario posee accesos que no debería, o bien, se identifica que requiera de nuevos accesos, este sigue lo detallado en los procedimientos de aprovisionamiento y desaprovisionamiento definidos por la entidad.

Cómo se documenta la revisión; La evidencia del control queda en correos, por este medio se envía a las gerencias el listado de usuarios con sus permisos y se retienen los insumos utilizados en el proceso (listados de usuarios de sistemas, RRHH y las extracciones de estos) por temas de auditorías.

Si se utiliza una herramienta para realizar la revisión de acceso y, de ser así, cómo se controla esa herramienta; No se utiliza una herramienta para la revisión de accesos, todo el proceso es realizado de forma manual.

Si la revisión incluye pasos para garantizar que los cambios de acceso solicitados se completen oportunamente.

En el caso de identificarse inconsistencias, se sigue lo detallado en los procedimientos de aprovisionamiento y desaprovisionamiento definidos por la entidad, de forma inmediata.

Prueba de la Implementación y Eficacia Operativa:

La revisión del acceso de usuarios incluyó una población completa y precisa de usuarios: se realizaron validaciones de exactitud de usuarios mediante la generación de diferentes reportes para validar que se están enviando a revisar la totalidad de usuarios, los usuarios que se marcan en amarillo son los que tienen inconsistencias en la comparativa de los reportes, dichas inconsistencias se detallan en el formulario de inconsistencias, donde se deja el detalle del porque existe esa diferencia de usuarios entre reportes, por lo que con esta validación concluimos que se revisó la totalidad de usuario

de los sistemas a pesar de no haber dejado capturas de pantalla del proceso de generación, se brindará la recomendación a la administración que realice la documentación de todo el proceso de extracción de usuarios para dejar un detalle más completo y sea más certero la validación de integridad y exactitud.

La revisión se documentó correctamente y se realizó con el nivel de detalle apropiado para determinar si el acceso era consistente con las responsabilidades laborales actuales de cada usuario: Se hizo envío de cuentas contenidas en el aplicativo, tomando datos como la gerencia, dependencia, usuario, nombre, cargo, aplicación a la que tiene acceso, rol y descripción del rol asociado. De igual manera se hizo un cruce con el listado empleados, para poder determinar el puesto del colaborador y el jefe inmediato (Adicional, los reportes en el sistema poseen una columna con dicho campo para validar la dependencia a la que corresponde). Al certificador se le envía el paquete de usuarios en formato pdf y se detallan dentro de las instrucciones la confirmación de los accesos que deben realizar en caso de que todo esté bien, o indicar que usuarios requieren una modificación según corresponda.

La revisión fue realizada por el personal de administración apropiado con la segregación adecuada de funciones aplicadas :De una muestra aleatoria de 20 recertificadores se identificó que 18 colaboradores parece como que se certifican ellos mismos, sin embargo se validó con administración y estos aparecen dentro de sus propios listados ya que tableau genera los usuarios de dependencias sin excluir a los lideres de cada dependencia, sin embargo estos fueron revisados por cada jefe superior.

El acceso al sistema se modificó adecuadamente de manera oportuna para los usuarios marcados como excepciones durante la revisión : Se identificó derivado del ejercicio que de 69 dependencias, únicamente se solicitaron 5 movimientos, que consiste en 2 bajas y 2 modificaciones de acceso para ORACLE EBS. Para cada uno de los casos

existe una gestión (por correo o Ivanti) donde se validó que el acceso fue modificado de forma oportuna para estas excepciones, siguiendo los controles de aprovisionamiento y desaprovisionamiento definidos por la Entidad.

Conclusión: El control es efectivo.

4. La segregación de funciones se monitorea y el acceso conflictivo se elimina o se asigna a controles de mitigación, los cuales están documentados y probados.

Diseño del control:

La administración realiza lo siguiente relacionado con el Análisis de Segregación Funcional:

Se realiza una depuración de los accesos para identificar a que dependencia/gerencia corresponde cada usuario.

Se sostienen sesiones virtuales por medio de Microsoft Teams con cada uno de los responsables de la dependencia/gerencia.

En conjunto con el área de Seguridad de la Información, el área de Aplicaciones y los responsables de cada área, realiza la revisión de cada rol/responsabilidad. Para el sistema eBS se construye una matriz de revisión donde se detallan cada responsabilidad que tiene los usuarios y se detalla si los acceso deben ser removidos por algún conflicto de segregación de funciones o en su caso deben permanecer, para los accesos que no son removidos se debe dejar un detalle completo en la misma matriz del motivo por el cual los accesos no deberán ser removidos.

Al finalizar se realiza un informe detalla con las actividades llevadas a cabo, donde se deja el detalle de todos los accesos que fueron revisados, así como los que fueron removidos o a los cuales se les debe mantener los accesos, al final de este se deben dejar las firmas con fecha y hora de los responsables de la revisión, así como los responsables de cada dependencia/gerencia.

Adicionalmente se cuenta con el documento “Manual de Seguridad de la información” en donde se establece lo siguiente:

Para gestionar adecuadamente el acceso a las plataformas aplicativas del Banco, los responsables de la información deben revisar anualmente o cuando se requiera, los privilegios, roles y funciones otorgados a los usuarios de sus respectivas dependencias validando y asegurando la debida segregación funcional al interior de sus áreas, así como de modificar o revocar los privilegios que no sean requeridos o no estén alineados a las necesidades de cada área del Banco. Para ello, el Departamento de Seguridad de la información debe brindar los reportes necesarios a los dueños de los aplicativos para la revisión de los accesos.

Al menos con una periodicidad anual, genera los reportes de usuario de la plataforma eBusiness, así como de cualquier otra plataforma considerada crítica, clasificando los usuarios por dependencia, y especificando usuarios, roles y permisos, incluyendo dentro del alcance los usuarios de la herramienta de gestión de cuentas privilegiadas. Estos reportes se obtienen de aquellos sistemas aplicativos que proveen la funcionalidad de emisión de reportes, para los usuarios con el mismo puesto y en donde se identifiquen privilegios adicionales será necesario validar que no exista segregación de funciones con el área correspondiente.

En el evento de que existan conflictos de segregación funcional que deban ser mantenidos, identificará el motivo por el cual se requiere mantener los accesos y documenta controles supletorios existentes.

Prueba de la Implementación y Eficacia Operativa:

Validamos que por medio de la herramienta GRC Monitor el área de Seguridad de la Información generó los diferentes conflictos identificados, los mismos fueron compartidos a las áreas del negocio, sin embargo la matriz actual de EBS no aborda el

riesgo asociado "Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus funciones asignadas, lo que puede crear una segregación inadecuada de funciones"

Solicitamos roles críticos para validar si existe un incumplimiento de segregación de funciones y se identificó que existen usuarios que pueden crear y registrar asiento de diario en el General Leger.

Conclusión: El control es Inefectivo.

Análisis del impacto de las deficiencias

Control de TI	Área de control de TI	Riesgo asociado al control	Descripción de la deficiencia	Causa raíz de la deficiencia	Mitigación del hallazgo	Impacto
La segregación de funciones se monitorea y el acceso conflictivo se elimina o se asigna a controles de mitigación, los cuales están documentados y probados.	Seguridad de accesos	Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus tareas asignadas, lo que puede crear una segregación indebida de funciones.	Usuarios administradores en las aplicaciones. El departamento de Seguridad de la Información es el responsable de gestionar y administrar las cuentas privilegiadas en la herramienta CyberArk por lo que se identificó lo siguiente durante la investigación: según el “Instructivo Para La Gestión De Cuentas Privilegiadas De La Plataforma Tecnológica, en el inciso 1.3: Todos los administradores de tecnologías y personal de soporte deben utilizar la solución de Cyberark para el uso de cuentas privilegiadas”, sin embargo, durante la evaluación realizada	Se identificó una deficiencia en la eficacia operativa del control de usuarios de nivel privilegiado en el sistema eBS. La deficiencia fue originada debido a que la administración por la naturaleza de las cuentas y la complejidad de enlorar de las aplicaciones. El control es de naturaleza manual para la gestión de usuarios privilegiados y aborda el riesgo de que los sistemas no están configurados de	Se revisó con ayuda de la administración las bitácoras de auditoría habilitadas para las cuentas ORACLE y SYSADMIN, confirmando que la cuenta ORACLE no poseyó acceso interactivo durante el 2023 y la cuenta SYSADMIN tuvo acceso, sin embargo, las actividades son persé del tipo de cuenta como tal (administración del sistema) Además, se logra validar que las activades de configuración en los sistemas están soportadas por controles de cambios, por lo que consideramos que el riesgo relacionado con la observación está siendo abordado por la compañía. Se evaluaron los	Alto

			se identificaron 2 cuentas que pertenecen al sistema Oracle EBS (Oracle, SYSADMIN) que no se encuentran enroladas en la herramienta CyberArk.	manera adecuada para restringir el acceso al sistema a los usuarios no apropiados y debidamente autorizados, lo que puede crear una segregación inadecuada de funciones.	siguientes controles de la aplicación los cuales mitigan el riesgo de que los usuarios tienen privilegios de acceso más allá de los necesarios para realizar las tareas asignadas, lo que puede crear una segregación inadecuada de función y fueron concluidos de forma efectiva: Aprovisionamiento de usuarios Control de cambios Control se segregación de ambientes.	
El acceso a nivel privilegiado (por ejemplo, administradores de seguridad) está autorizado y adecuadamente restringido.	Seguridad de accesos	Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus tareas asignadas, lo que puede crear una segregación indebida de funciones.	Análisis de Segregación de funciones. Análisis de segregación de funciones EBS: por medio de la herramienta GRC Monitor el área de Seguridad de la Información generó los diferentes conflictos identificados, los mismos fueron compartidos a las áreas del negocio, sin embargo, no se pudo corroborar que se cuente con la	Se identificó una deficiencia en el diseño del control de segregación de funciones en los accesos de los sistemas relevantes de la entidad. La deficiencia fue originada debido a que el control fue ejecutado fuera del periodo de evaluación. Este control es de naturaleza manual, pertenece al	Se evaluaron los siguientes controles de la aplicación los cuales mitigan el riesgo de que los usuarios tienen privilegios de acceso más allá de los necesarios para realizar las tareas asignadas, lo que puede crear una segregación inadecuada de función y fueron concluidos de forma efectiva: Aprovisionamiento de usuarios Desaprovisionamiento de usuarios Revisión periódica de	Alto

			documentación del análisis de la configuración y asignación de las responsabilidades que en combinación con otras responsabilidades causan un conflicto de segregación de funciones en la aplicación EBS, dicho análisis debe ser realizado en conjunto con el área de negocio para identificar los conflictos de segregación de funciones, análisis para remover los conflictos potenciales identificados así como la definición de controles compensatorios a asignar para conflictos cuyos existencia se haya considerado como necesaria para la operación. La matriz actual de EBS no aborda el riesgo asociado "Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus funciones asignadas, lo que puede crear una segregación inadecuada de funciones".	área de seguridad de accesos y aborda el riesgo de que los usuarios tenga privilegios de acceso más allá de los necesarios.	usuarios Accesos privilegiados	

Capitulo V: Conclusiones y recomendaciones

El presente estudio ha permitido evaluar de manera integral la efectividad de los controles implementados en la aplicación Oracle EBS, identificando tanto sus fortalezas como sus debilidades en la mitigación de riesgos tecnológicos. Se evidenció que, si bien existen políticas y procedimientos diseñados para proteger la integridad, confidencialidad y disponibilidad de los datos, la aplicación de estos mecanismos no siempre es uniforme ni eficiente.

Hallazgo 1

El departamento de Seguridad de la Información es el responsable de gestionar y administrar las cuentas privilegiadas en la herramienta CyberArk por lo que se identificó lo siguiente durante la investigación: según el "Instructivo Para La Gestión De Cuentas Privilegiadas De La Plataforma Tecnológica, en el inciso 1.3: Todos los administradores de tecnologías y personal de soporte deben utilizar la solución de Cyberark para el uso de cuentas privilegiadas", sin embargo, durante la evaluación realizada se identificaron 2 cuentas que pertenecen al sistema Oracle EBS (Oracle, SYSADMIN) que no se encuentran enroladas en la herramienta CyberArk.

Recomendación 1

El departamento de Seguridad de la Información debe realizar la inclusión de estas cuentas (Oracle, SYSADMIN) en la plataforma CyberArk, para que sean administradas por medio de la herramienta y esto permita la rotación de contraseña, la custodia y el monitoreo.

Se recomienda la inhabilitación de las cuentas genéricas actualmente en uso (Oracle, SYSADMIN) y la adopción de un enfoque que involucre la creación de usuarios específicos y nombrados para cada usuario.

Impacto: Alto

Causa raíz 1

Se identificó una deficiencia en la eficacia operativa del control de usuarios de nivel privilegiado en el sistema eBS. La deficiencia fue originada debido a que la administración por la naturaleza de las cuentas y la complejidad de enlorar de las aplicaciones. El control es de naturaleza manual para la gestión de usuarios privilegaidos y aborda el riesgo de que los sistemas no están configurados de manera adecuada para restringir el acceso al sistema a los usuarios no apropiados y debidamente autorizados, lo que puede crear una segregación inadecuada de funciones.

Plan de acción de la administración 1

Se atenderá la inclusión de las cuentas Oracle y SYSADMIN en la solución de CYBERARK.

Responsable: Seguridad de la información

Hallazgo 2

Análisis de segregación de funciones EBS: por medio de la herramienta GRC Monitor el área de Seguridad de la Información generó los diferentes conflictos identificados, los mismos fueron compartidos a las áreas del negocio, sin embargo, no se pudo corroborar que se cuente con la documentación del análisis de la configuración y asignación de las responsabilidades que en combinación con otras responsabilidades causan un conflicto de segregación de funciones en la aplicación EBS, dicho análisis debe ser realizado en conjunto con el área de negocio para identificar los conflictos de segregación de funciones, análisis para remover los conflictos potenciales identificados así como la definición de controles compensatorios a asignar para conflictos cuyos existencia se haya considerado como necesaria para la operación.

La matriz actual de EBS no aborda el riesgo asociado "Los usuarios tienen privilegios de acceso más allá de los necesarios para realizar sus funciones asignadas, lo que puede crear una segregación inadecuada de funciones".

Recomendación 2

El departamento de Seguridad de la información, Aplicaciones y los jefes de área deberán realizar el ejercicio de identificación de posibles conflictos de segregación de funciones, así como la documentación del análisis de la configuración y asignación de roles para cada uno de los usuarios existentes en la aplicación Oracle donde se estan identificando los posibles conflictos de segregación de funciones derivados del uso o combinación de uno o más roles en el sistema, validar la posibilidad de remover los privilegios y/o en caso de identificar la necesidad de contar con algún conflicto, es recomendable documentar el análisis, riesgo y formalizar controles compensatorios por cada posible conflicto con el objetivo de poder identificar y monitorear cualquier actividad no autorizada que sea ejecutada con estos accesos.

Realizar actualizaciones periódicas y continua de cualquier actualización de dicha matriz para asegurar que las mismas cuenten con la información más relevante actual derivado de nuevas creaciones y modificaciones a responsabilidades y conflictos de segregación de funciones a partir de cambios en la estructura o necesidades del negocio.

Impacto: Alto

Causa raíz 2

Se identificó una deficiencia en el diseño del control de segregación de funciones en los accesos de los sistemas relevantes de la entidad. La deficiencia fue originada debido a que el control fue ejecutado fuera del periodo de evaluación. Este control es de naturaleza manual, pertenece al área de seguridad de accesos y aborda el riesgo de que los usuarios tenga privilegios de acceso más allá de los necesarios.

Plan de acción de la administración 2

Se analizará la contratación de una consultaría que nos ayude a desarrollar un proyecto para la revisión de cada unos de los roles creados asegurando que no queden accesos que incumplan la segregación.

Responsable: Seguridad de la Información, Gerencia de Aplicaciones y Gerencias del negocio.

Referencias

- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Marco integrado de control interno*. Recuperado de https://www.coso.org.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2020). *Guía de gestión de riesgos empresariales*. Recuperado de https://www.coso.org.
- Harmui, G., & Varela, L. (2013). Control interno: Conceptos, estrategias y aplicaciones prácticas. Editorial Contemporánea.
- Hernández, R., & Mendoza, C. (2018). Control interno y gestión de riesgos en organizaciones financieras. Editorial Financieros.
- Information Systems Audit and Control Association (ISACA). (2019). *COBIT: Marco de control para la gobernanza y gestión de las tecnologías de la información*. Recuperado de https://www.isaca.org.
- International Organization for Standardization (ISO). (2013). *ISO/IEC 27001: Sistemas de gestión de la Seguridad de la Información: Requisitos*. Recuperado de https://www.iso.org.

- International Federation of Accountants (IFAC). (2018). *Manual de normas internacionales de auditoría y control de calidad*. Recuperado de https://www.ifac.org.
- Ley de Control Interno, Ley No. 8292. Asamblea Legislativa de Costa Rica. (2002). *Ley General de Control Interno*. Recuperado de https://www.pgr.go.cr.
- Superintendencia General de Entidades Financieras (SUGEF). (2019). *Normas de control interno en entidades financieras*. Recuperado de https://www.sugef.fi.cr.
- International Auditing and Assurance Standards Board (IAASB). (2021). *Norma Internacional de Auditoría 315: Identificación y valoración de riesgos de incorrección material*. Recuperado de https://www.iaasb.org.
- Instituto Nacional de Estadística y Censos (INEC). (2020). *Estadísticas financieras en Costa Rica 2020*. Recuperado de https://www.inec.cr.
- International Financial Reporting Standards (IFRS). (2018). *Norma Internacional de Información Financiera 9: Instrumentos financieros*. Recuperado de https://www.ifrs.org.
- Calderón, J., & Martínez, P. (2017). Auditoría y control interno: Estrategias para la gestión empresarial. Ediciones Empresariales.
- Fernández, M., & López, A. (2019). Gestión del riesgo operativo en entidades financieras: Teoría y práctica. Editorial Actualidad.
- Universidad de Costa Rica (UCR). (2021). *Análisis del control interno en organizaciones bancarias costarricenses*. Recuperado de https://www.ucr.ac.cr.
- Calderón, G., & Rivera, J. (2016). Riesgo tecnológico en la industria financiera: Enfoques y soluciones. Editorial Innovación.

- Organización Internacional de Trabajo (OIT). (2018). *Buenas prácticas en gobernanza y gestión de riesgos empresariales*. Recuperado de https://www.ilo.org.
- Oficina Nacional de Auditoría de Reino Unido (NAO). (2019). *Guía práctica para la identificación y mitigación de riesgos operativos*. Recuperado de https://www.nao.org.uk.
- American Institute of Certified Public Accountants (AICPA). (2017). *Guía de control interno para empresas pequeñas y medianas*. Recuperado de https://www.aicpa.org.
- Albrecht, W. S., & Albrecht, C. O. (2017). *Fraud examination and prevention*. Cengage Learning.
- Goodwin, M., & Manz, C. (2020). *Gestión del riesgo y control interno en instituciones bancarias*. Journal of Banking Regulation, 22(4), 246-259. https://doi.org/10.1057/s41261-020-00099-7
- Deloitte. (2021). *Global risks and compliance report: Internal controls and operational effectiveness*. Recuperado de https://www.deloitte.com.
- KPMG. (2019). *KPMG's Internal Control Framework*. Recuperado de https://home.kpmg.
- PricewaterhouseCoopers (PwC). (2019). *Internal control and risk management practices in the financial sector*. Recuperado de https://www.pwc.com.
- González, L., & Rodríguez, M. (2018). Normas internacionales de control interno y su aplicación en las entidades financieras costarricenses. Revista de Derecho y Finanzas, 32(1), 103-120.
- International Monetary Fund (IMF). (2019). *Informe sobre control interno y gestión de riesgos en el sector bancario*. Recuperado de https://www.imf.org.

- Allen, R., & Cuthbertson, R. (2019). Riesgo operativo y su gestión en los sectores financieros: Un análisis global. Wiley & Sons.
- Hall, S., & Mitchell, K. (2020). Global risk management strategies for financial institutions. Oxford University Press.
- World Bank. (2019). *Evaluación de controles internos y gestión de riesgos en el sector bancario global*. Recuperado de https://www.worldbank.org.
- International Federation of Accountants (IFAC). (2020). *Recomendaciones sobre la gestión del riesgo en el sector financiero*. Recuperado de https://www.ifac.org.
- Rodríguez, S., & Poveda, M. (2017). Evaluación y control en la gestión de riesgos: Estrategias para el sector financiero. Editorial Business Press.
- Banco Central de Costa Rica. (2021). *Regulación de control interno en el sector bancario costarricense: Normativas y mejores prácticas*. Recuperado de https://www.bccr.fi.cr.
- Fundación para la Gestión del Riesgo (2020). Gestión de riesgos operativos en entidades bancarias: Casos y mejores prácticas. Editorial Fundación Gestión.
- García, J., & Navarro, F. (2016). Control interno y auditoría en instituciones financieras: Un enfoque práctico. Ediciones Financieras.
- Business Continuity Institute. (2023). *Guía de mejores prácticas en continuidad del negocio*. Business Continuity Institute.
- Comité de Basilea. (2022). *Principios para la gestión y supervisión del riesgo operativo*. Bank for International Settlements.
- Deloitte. (2023). Informe sobre la seguridad en la banca digital y la experiencia del cliente. Deloitte Insights.
- European Union Agency for Cybersecurity. (2023). *Annual threat landscape report*. ENISA. https://www.enisa.europa.eu

- Gartner. (2022). Key metrics for IT risk management in financial institutions. Gartner Research.
- ISACA. (2021). Auditoría y control de los sistemas de información: Manual de referencia para la evaluación de TI. ISACA.
- International Organization for Standardization. (2022). *ISO/IEC 27001: Norma sobre gestión de Seguridad de la Información*. ISO.
- IT Governance Institute. (2020). *Enterprise governance of IT: Framework and best practices*. IT Governance Publishing.
- National Institute of Standards and Technology. (2022). *Risk management framework for information systems and organizations*. U.S. Department of Commerce. https://www.nist.gov
- Organización para la Cooperación y el Desarrollo Económicos. (2023). *Recomendaciones sobre seguridad digital para el sector financiero*. OCDE.

Apéndices

Entrevistas

¿Qué políticas y procedimientos tiene la entidad relacionados con el aprovisionamiento de usuarios?

¿Quiénes son los responsables de aprobar los accesos solicitados?

¿Quiénes son las personas responsables de administrar y otorgar los accesos?

¿Cómo se presentan, aprueban y documentan las solicitudes de acceso de los usuarios?

¿Se utiliza una herramienta para otorgar nuevos accesos y cómo se controla dicha herramienta?

¿Existe una segregación de funciones entre la persona que aprueba y la persona que otorga el acceso en el sistema?

¿Qué procesos se tienen implementados relacionados con la segregación de funciones durante la creación de un usuario?

¿Qué políticas y procedimientos tiene la entidad relacionados con el desaprovisionamiento de usuarios?

¿Cómo se notifica a Seguridad de la Información sobre los usuarios despedidos y/o transferidos?

¿Cómo se elimina o ajusta el acceso tras una terminación o transferencia y si se utiliza el mismo proceso para empleados y no empleados (como proveedores, contratistas, etc.)?

¿El proceso para eliminar el acceso es manual o automatizado?

¿Los usuarios se eliminan o se deshabilitan?

¿Quién tiene la responsabilidad de la administración de seguridad y de cambiar el acceso de los usuarios cuando ocurren despidos o transferencias?

¿Cuáles son las expectativas para la eliminación oportuna del acceso de usuario (es decir, desde la fecha de separación o transferencia hasta la fecha efectiva de modificación del acceso)?

¿Qué políticas y procedimientos tiene la entidad relacionados con la revisión de accesos de usuarios?

¿Quiénes son las personas responsables de revisar los accesos de los usuarios?

¿Con qué frecuencia se ejecutan las revisiones de accesos de los usuarios?

¿Cuál es el alcance de la revisión (por ejemplo, empleados, proveedores, contratistas, invitados y cuentas genéricas/sistema) y qué se considera una excepción para no ser tomado como parte de la revisión de accesos?

¿La revisión incluye a los usuarios y sus privilegios/accesos asociados, incluyendo la segregación de funciones basada en roles y el acceso privilegiado?

¿Con qué nivel de detalle se realiza la revisión y que documentación queda de esta revisión?

¿Qué políticas y procedimientos tiene la entidad relacionados con la segregación de funciones, incluyendo las combinaciones de acceso conflictivos relevantes que se monitorean?

¿Cómo la gerencia monitorea los conflictos de segregación de funciones, incluyendo la frecuencia de la revisión?

¿Cuál es el proceso para resolver conflictos cuando se identifican?

¿Quién es responsable de las actividades de monitoreo de segregación de funciones y de la ejecución de controles mitigantes?

¿Qué políticas relacionadas con la seguridad de la información y la protección del acceso a nivel privilegiado tiene la entidad?

¿Quiénes cuenta con la autoridad para utilizar el acceso a nivel privilegiado?

¿La entidad cuenta con políticas o procedimientos para la administración de los diferentes cambios en las aplicaciones, bases de datos y Sistemas Operativos?

¿Como es el proceso de gestión de cambios para los diversos tipos de cambios en la aplicación, como cambios de programas, cambios de configuración, cambios en informes y parches de proveedores?

¿La entidad cuenta con un entorno de pruebas/desarrollo y producción?

¿Los usuarios participan en el proceso de pruebas a los cambios?

¿Se realiza la retención de documentación formal de las pruebas realizadas?

¿ Se cuenta con criterios para el éxito de las pruebas (es decir, 100% = aprobado o 90% = aprobado, 50= no aprobado)

¿Cómo la gerencia determina que la versión migrada a producción es la misma que fue probada por aseguramiento de calidad (QA)?

¿Qué personas que tienen la autoridad y responsabilidad para aprobar cambios?

¿Existen herramientas para documentar la aprobación, pruebas y cambios, y cómo se controlan estas herramientas?

¿Existen herramientas para realizar el pase a producción de un cambio?