Auditoría al proceso de gestión de acceso lógico en la Entidad Financiera ABC., mediante la metodología de auditoría basada en riesgos

Angie Lorena Rivera Vargas

Billy Joel Galvis Peña

Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Especialización en Proyectos Informáticos

Director: Edgar Jacinto Rincón Rojas

Bogotá D.C, 2022

Resumen

En las entidades financieras un problema recurrente es que no hay un procedimiento estructurado en los servicios de gestión de acceso lógico, lo cual, genera una serie de afectaciones para las entidades y para el usuario interno, se presentan reprocesos, mala experiencia del cliente interno y externo, problemas, incumplimientos con entes de control y baja productividad. Una de las herramientas que aportan a la solución frente a la mala ejecución de gestión de acceso lógico es la auditoría interna, porque permite buscar las debilidades del proceso para proponer mejoras. Por tanto, este proyecto tiene como objetivo realizar la auditoría de la gestión de acceso lógico de la entidad financiera ABC. para determinar ¿en qué partes de la gestión se encuentran los inconvenientes? y proponer ciertas recomendaciones, de esta manera se busca brindar a la organización un valor agregado que pueda ejecutar.

Palabras clave: Auditoría interna, auditoría basada en riesgo, acceso lógico.

Contenido

INTRODUCCIÓN 8
PARTE I. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN 9
CAPÍTULO 1. DESCRIPCIÓN DE LA INVESTIGACIÓN 9
1.1 Planteamiento del problema 9
1.2 Objetivos de la investigación 9
1.2.1 Objetivo general. 9
1.2.2 Objetivos específicos. 9
1.3 Justificación de la investigación 9
1.4 Hipótesis de la investigación 10
1.5 Marco Teórico 10
1.5.1. Origen de la gestión de acceso lógico. 11
1.5.2 ISO 27001. 12
1.5.3 Entidad Financiera. 14
1.5.4 Cliente Interno. 14
1.5.5 Acceso Lógico. 14
1.5.6 Importancia del acceso lógico. 14
1.5.7 Auditoría. 15
1.5.8 Auditoría interna. 15
1.5.9 Auditoría interna basada en riesgos. 15
1.5.10 Tecnologías de la información. 16
1.5.11 Archivo Permanente. 16
1.5.12 Archivo Corriente. 16
1.6 Metodología de la investigación 16
1.6.1 Tipo de investigación. 17
1.6.2 Fases de la metodología basada en riesgos. 17
1.6.3 Técnicas de recolección de información. 19
1.6.4 Tratamiento de la información. 20
1.7 Organización del trabajo de grado 20
PARTE II. DESARROLLO DE LA INVESTIGACIÓN 24
CAPÍTULO 2: DESARROLLO DE LA METODOLOGÍA DE AUDITORÍA BASADA EN RIESGOS 24
2.1 Fase 1: Conocimiento Global de la Organización 25

2.1.1 Información de la organización. 25
2.1.2 Razón social de la organización. 25
2.1.3 Servicios y Productos destacados de la entidad financiera ABC. 25
2.1.4 Filosofía institucional. 26
2.1.5 Objetivos de la organización. 26
2.1.6 Resultados económicos o estados financieros de los últimos años. 26
2.1.7 Identificación de competidores de la organización. 27
2.1.8 Principales proveedores. 27
2.1.9 Principales clientes y dependencia de los clientes. 28
2.1.10 Situación legal de la organización. 28
2.1.11 Manuales de procedimientos y funciones de la organización. 28
2.2 Fase 2: Definición del objeto a auditar y áreas auditables 28
2.2.1 Definición del objeto a Auditar. 29
2.2.2 Misión y visión del objeto a auditar. 29
2.2.3 Objetivos del objeto a Auditar. 29
2.2.4 Distribución de planta física del objeto a auditar. 29
2.2.5 Recurso humano del objeto a auditar. 30
2.2.6 Inventarios del Objeto a auditar. 30
2.2.7 Descomposición del objeto a auditar en áreas auditables 30
2.3 Fase 3: Evaluación de Riesgos 31
2.3.1 Lista de riesgos. 31
2.3.2 Matriz C-R-E. 31
2.3.3 Listas de controles. 31
2.3.4 Riesgos vs Riesgos. 31
2.3.5 Controles vs Riesgos. 32
2.3.6 Matriz Puntaje. 32
2.3.7 Priorización. 32
2.4 Fase 4: Planeación de la Auditoría 32
2.4.1 Riesgos más críticos del área. 33
2.4.2 Objetivo General de la auditoría. 33
2.4.3 Objetivos Específicos. 33
2.4.4 Cronograma. 34
2.4.5 Técnicas de Auditoría. 35
2.4.6 Procedimientos de Auditoría. 37

2.5 Ejecución de la Auditoría 39
2.6 Análisis de resultados 40
PARTE III. CIERRE DE LA INVESTIGACIÓN 41
CAPÍTULO 3: INFORME DE AUDITORÍA 41
3.1 Informe técnico. 41
3.2 45
CAPÍTULO 4. RESULTADOS Y DISCUSIÓN 41
CAPÍTULO 5. CONCLUSIONES 42
5.1 Verificación, contraste y evaluación de los objetivos 42
5.2 Síntesis del modelo propuesto 43
5.3 Aportes originales 43
CAPÍTULO 6. PROSPECTIVA DEL TRABAJO DE GRADO 43
6.1 Líneas de investigación futuras 43
6.2 Trabajos de investigación futuros 44
BIBLIOGRAFÍA 45

Listado de Tablas

Tabla 1. Objetivos del control de accesos según ISO 270001. Extraído de Norma ISO 27001-ICONTEC 15
Tabla 2. Nemotécnicos y referencias. Fuente: Auditoría e interventoría de proyectos informáticos-Luis Montenegro 26
Tabla 3. Recurso humano objeto a auditar. Fuente: Elaboración propia 32
Tabla 4. Lista de controles para el incumplimiento de protocolo de enrolamiento para nuevas aplicaciones. Fuente: Elaboración propia 36
Tabla 5. Lista de controles para Definición de roles incorrectos. Fuente: Elaboración propia 37
Tabla 6. Actividades para la auditoría 38
Tabla 7. Diagrama de Gantt de las actividades de la auditoría. 39

Lista de figuras

Figura 1. Matriz de priorización. Fuente: Elaboración propia 33
Figura 2. Matriz de puntajes. Fuente: Elaboración propia 34
Figura 3. Diagrama de Gantt de las actividades de la auditoría. 40

INTRODUCCIÓN

Generalmente se tiene la creencia de que el éxito de una entidad financiera radica en toda la administración de operaciones financieras como gestión de créditos, inversiones y expansión, desde que se busca el cliente, se ofrecen los productos, pasando al análisis de viabilidad financiera y concretando negocios, generando ingresos a la entidad y crecimiento económico, pero desde la experiencia se denota que no se le da la misma importancia a un área fundamental que influye en el futuro de las entidades financieras, el servicio de gestión de acceso lógico del cliente interno, un factor importante que soporta la operación de las empresas.

Es muy importante cuidar y motivar al cliente interno, dado que es uno de los primordiales elementos que generan valor al consumidor final, su gestión permite que el cliente final reciba un servicio o producto de calidad, que satisfaga sus necesidades. (Silva, 2021).

Para brindar un servicio al cliente interno de calidad, existen operaciones internas en las organizaciones que con su eficiente gestión permiten que esto ocurra, una de ellas es la gestión de acceso lógico, si el cliente interno tiene oportuna y fácilmente sus accesos, es un cliente interno satisfecho, que estará en la capacidad de atender adecuadamente al cliente externo.

Por medio de este proyecto se podrá determinar el modo en el que en la entidad financiera ABC. ha prestado el servicio de gestión de acceso lógico al cliente interno, identificando por medio de la metodología de auditoría interna basada en riesgos las debilidades, cuellos de botella y procedimientos para mejorar la calidad del servicio.

PARTE I. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

CAPÍTULO 1. DESCRIPCIÓN DE LA INVESTIGACIÓN

En el presente capítulo se describe la investigación a realizar, la cual es base para el desarrollo de este documento, se precisan temas como la definición del problema de investigación, objetivos y justificación.

1.1 Planteamiento del problema

Las entidades financieras usualmente enfocan sus esfuerzos a la creación y venta de diversos productos financieros, para dicho fin realizan múltiples análisis, diseño de estrategias de negocio y publicidad, la prioridad de las entidades financieras son los clientes externos, tienen comités y servicios especializados para mejorar la experiencia de estos, resolviendo las incidencias que reporten con el fin de fidelizarlos.

Este tipo de entidades tienen muchos componentes tecnológicos que apoyan su éxito y crecimiento, cuentan con sistemas de información para administrar toda la información financiera, innovan con aplicaciones más fáciles, oportunas, y seguras, hacen implementaciones que apalancan el mejoramiento de la gestión transaccional, la incursión en nuevos mercados y la gestión de pagos. (Ontiveros et al.,2012). Sin embargo, todo esto es de cara al cliente externo.

Con la transformación digital que se ha impulsado en los últimos años y que tomó más fuerza con la pandemia causada por el COVID 19, las entidades financieras tienen la necesidad de preocuparse más por sus labores internas, con el fin de ser empresas competitivas, adoptando componentes inteligentes y ágiles, es por ello que nace la necesidad de determinar la eficacia de toda gestión, identificar oportunidades de mejora y evaluar el cumplimiento de diversas regulaciones; para dichos fines, es fundamental analizar los procesos que son usados por el cliente interno y que contribuyen a que pueda realizar una gestión más ágil.

De acuerdo con la consultora EY Parthenon, la demanda de plataformas y canales de banca digital aumentó 59% en el último año en Colombia, en consecuencia, los bancos y entidades financieras requieren ofertar un servicio con componentes de innovación que este a la altura de esta era digital. (Forbes, 2022).

Uno de los puntos más relevantes para el cliente interno es la gestión de acceso lógico, que lo posibilita a obtener lo que requiere para el desarrollo de sus funciones. Por tanto, es importante hacer una gestión de accesos de forma oportuna y fácil, en donde el cliente interno realice el mínimo esfuerzo para obtener lo requerido y pueda realizar una labor eficiente, a tiempo y segura.

Los datos hoy en día son activos de información muy valiosos para las organizaciones y son el insumo principal para estas, la necesidad de cuidar los accesos a los datos es muy grande hoy en día, por lo que se deben proteger estos, un acceso no autorizado puede ocasionar pérdida de secretos comerciales, innovación y futuras rentabilidades. Así mismo, los clientes del día de hoy son más exigentes, se preocupan por salvaguardar la confiabilidad de la importación, si no está asegurada la confiabilidad no consumen. (IBM, 2021)

En el pasado, el área de gestión de acceso lógico era un área un poco descuidada en la mayoría de las entidades financieras, como tal, no representa un ingreso monetario instantáneo a la organización, se tiene la percepción de que es un área que demanda diversos recursos y no retorna inversión, sin embargo, realizar una gestión de acceso lógico ágil y segura apalanca el éxito de las organizaciones, por tanto, las empresas ya se están concientizando de esto y realizan múltiples implementaciones para evaluar dicha gestión con el propósito de encontrar puntos débiles y mejorarlos. Por esto, es importante determinar ¿por qué no se está realizando una buena gestión de acceso lógico?, y en caso de que se identifiquen falencias en el servicio, entrar a

proponer mejoras para mayor optimización de los recursos y una plena satisfacción del cliente interno en particular en lo referente al servicio prestado desde la gestión de acceso lógico.

Teniendo en cuenta lo planteado, se establece la pregunta de investigación: ¿La ejecución de una auditoría interna basada en riesgos en los procesos de servicio de gestión de acceso lógico del cliente interno de la entidad financiera ABC.?, contribuye a la identificación de los aspectos a mejorar y fortalecer?

1.2 Objetivos de la investigación

A continuación, se presentan los objetivos que enmarcan el desarrollo de este proyecto:

1.2.1 Objetivo general.

Realizar una auditoría mediante la metodología de auditoría interna basada en riesgos, que identifique los riesgos y controles que afectan negativamente en la gestión de acceso lógico para el cliente interno de la entidad financiera ABC.

1.2.2 Objetivos específicos.

- Establecer la metodología de auditoría basada en riesgos que será aplicada.
- Aplicar la metodología de auditoría basada en riesgos en el servicio de gestión de acceso lógico del cliente interno de la entidad financiera ABC.
- Definir y ejecutar procedimientos de auditoría para los dos riesgos más críticos del área auditable más expuesta.
- Generar los informes del resultado de la auditoría.

1.3 Justificación de la investigación

Las auditorías permiten evaluar a las empresas para emitir conceptos y recomendaciones que contribuyan con el buen desempeño de estas, dando valor agregado a la organización. Teniendo en cuenta los resultados se generan recomendaciones que contribuyen al crecimiento de la

compañía, además del aporte en temas de competitividad frente a las demás empresas (Leiva,2018).

La auditoría interna basada en riesgos es una herramienta integral y especializada, que puede aplicarse a cualquier organización, permite identificar si los controles internos aplicados a diferentes labores son adecuados y están exonerados de errores que afecten de forma negativa los objetivos de la organización. Cada vez son más las organizaciones que recurren a la auditoría interna basada en riesgos para identificar fraude interno, el cual se puede materializar en cualquier organización, la identificación de riesgos es fundamental para el control de estos, de tal forma se protege al negocio (Gutiérrez,2022).

Por lo anterior, la aplicación de auditoría interna basada en riesgos en el proceso de gestión de acceso lógico del cliente interno es algo muy benéfico para la entidad financiera ABC, dado que mediante esta labor se puede identificar puntos que están generando afectaciones que no permiten realizar una asignación de accesos seguras, oportunas y eficientes, con el fin de proponer una serie de recomendaciones que a la organización le permita optimizar recursos y dar un mejor servicio.

La justificación para este proyecto es de tipo práctico, su desarrollo ayudará a resolver un problema ya identificado que es la calidad de la prestación del servicio de gestión de acceso lógico del cliente interno, o por lo menos se propondrá un plan de mejora que estará disponible para que la organización lo pueda implementar si lo considera necesario.

1.4 Hipótesis de la investigación

Basados en la identificación del problema, se plantea la siguiente hipótesis:

La ejecución de una auditoría interna basada en riesgos en la gestión de acceso lógico del cliente interno de la entidad financiera ABC. contribuye a la identificación de los aspectos a mejorar y fortalecer.

1.5 Marco Teórico

A continuación, se relacionan conceptos esenciales para abordar el problema:

1.5.1. Origen de la gestión de acceso lógico.

En los años 80 's las primeras tecnologías por arrastre representaron una enorme mejora administrativa con relación a las cerraduras y llaves manuales en cuanto a la gestión, la trazabilidad y los reportes judiciales. Saber quién tenía privilegios de acceso a ciertas áreas, y poder controlar de manera eficiente dichos privilegios, eliminó la necesidad de volver a cambiar las claves de las cerraduras cuando los empleados se iban o cambiaban de función. La tecnología de contacto requiere realizar un deslizamiento manual para transferir la información no cifrada de la credencial a un lector. Cuando el usuario necesitaba ingresar a un área determinada, deslizaba una tarjeta, tal como lo haría con una tarjeta de crédito o débito en un establecimiento comercial. En cuanto al ingreso y gestión lógico en aplicaciones, en esta década se empezó a investigar sobre cómo gestionar digitalmente el control de directorios telefónicos, de esta manera se dio origen al Protocolo Ligero de Acceso a Directorios (LDAP), que es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una Base de datos a la que pueden realizarse consultas. Está basado en el estándar X.50 (IBM,2021)

Con el tiempo, al iniciar la década de los 90 se empezó a implementar la necesidad del contacto físico entre lectores y credenciales podía resultar incómoda e ineficaz para los usuarios, además del uso de tarjetas para ciertos accesos que en ese tiempo se necesitaba de manera netamente física,

se tenía en cuenta el uso de contraseñas para ingresar a las aplicaciones que se tenían, que por cierto eran bastante básicas y manejaban interfaces sencillas sin vinculación lógica por base de datos ni un sistema integrado.

Con el pasar del tiempo en el cambio de siglo se comenzó a tener en cuenta el concepto del directorio activo, que básicamente trata de una tecnología basada en un servidor que se utiliza para gestionar ordenadores y otros dispositivos en una red, construido sobre Windows 2000. Su diseño estaba fuertemente influenciado por el emergente Protocolo Ligero de Acceso a Directorios (LDAP) (Reimer, Mulcare. 2003).

1.5.2 ISO 27001.

La norma ISO 27001 es un estándar de información publicado como norma internacional en el año 2005 por la ISO, esta norma describe cómo gestionar la seguridad e integridad de los datos e información.

Las medidas de gestión de control de accesos están incluidas en esta norma y están orientadas a controlar los accesos a aplicaciones, bases de datos y otros medios de información de acuerdo con las políticas establecidas previamente por la organización. Los objetivos del control de acceso y sus respectivos controles según la ISO 27001 son:

Objetivo	Controles
Limitar el acceso a la información y a las instalaciones de procesamiento de información.	*Política de control de acceso * Acceso a las redes y a los servicios de red

Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información	* Registro de usuarios y cancelación del registro * Gestión de acceso a los usuarios * Gestión de derechos de acceso privilegiados * Gestión de la información de autenticación secreta de los usuarios * Revisión de derechos de acceso de usuario * Remoción o ajuste de los derechos de acceso
Hacer a los usuarios responsables de salvaguardar su información de autenticación	* Uso de la información de autenticación secreta
Impedir el acceso no autorizado a los sistemas y las aplicaciones.	* Restricción de acceso a la información * Procedimientos de conexión (log-on) seguros * Sistema de gestión de contraseñas * Uso de programas de utilidad privilegiados * Control de acceso al código de programas fuente

Tabla 1. Objetivos del control de accesos según ISO 270001. Extraído de Norma ISO 27001-ICONTEC

(ICONTEC, 2006)

De igual manera, la norma establece la asignación de roles según las políticas establecidas, estos roles informan acerca de los privilegios que tendrá un usuario en el sistema.

ISO 27001 define que un control de acceso debe incluir los eventos de:

- Identificación: métodos para proporcionar un sujeto (entidad que solicita acceso) con una identidad reconocible (por ejemplo, ID usuario o cuenta de usuario, IVA, número de seguro social, pasaporte, etc.).

- Autenticación: métodos para garantizar que un sujeto sea quien dice ser (por ejemplo, contraseña, token, huella digital, etc.). Autorización: métodos para controlar qué acciones puede realizar un sujeto en un objeto (entidad a la que se accede) (por ejemplo, lista de permisos de materia y lista de permisos de objetos) (IBM,2021).

1.5.3 Entidad Financiera.

Una entidad financiera es una asociación que tiene como objetivo ofrecer servicios financieros en el área de la banca, valores y seguros. Su oferta considera desde la intermediación, comercialización de seguros, créditos y asesoramiento, entre otros. (BBVA,2019).

1.5.4 Cliente Interno.

El cliente interno es aquel miembro de una organización, que obtiene el resultado o producto efectuado al interior de la organización previamente. (Silva,2021).

1.5.5 Acceso Lógico.

¿Qué es acceso lógico? Es la totalidad de métodos y controles lógicos integrados que se encargan de salvaguardar la confidencialidad e integridad de la información, posibilitando el ingreso a los usuarios autorizados por el negocio, requeridos para el desempeño de sus funciones (Solís, 2017).

1.5.6 Importancia del acceso lógico.

¿Por qué es tan importante el control de acceso lógico? El control de acceso lógico es un arma de seguridad fundamental en las entidades financieras, sirve como obstáculo para evitar accesos no autorizados a los sistemas de información, en la actualidad, un activo muy valioso son los sistemas de información, por ende, uno de los objetivos de las entidades financieras es cuidar el acceso a estos, un acceso no autorizado, puede generar graves consecuencias, se puede materializar fraude, divulgación de información no confidencial y esto repercute en la imagen de

la entidad, un incidente asociado a esto, puede afectar el negocio, es por esto, que las entidades financieras cada día se preocupan más por hacer un correo control de acceso lógico, para salvaguardar sus sistemas de información (Tecnitrán, 2016).

1.5.7 Auditoría.

¿Qué es auditoría? Procedimiento metódico con el fin de obtener y evaluar adecuadamente procedimientos e información revelada por empresas para determinar su veracidad con la intención de incrementar su utilización de forma positiva cumpliendo con los estándares definidos (Contadores Públicos, 2016).

1.5.8 Auditoría interna.

Según el IIA, la auditoría interna se define como "una actividad de aseguramiento y consultoría objetiva e independiente diseñada para agregar valor y mejorar las operaciones de una organización, ayudando a la organización a alcanzar sus objetivos aportando un enfoque sistemático y disciplinado con el fin de evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno" (Institute of Internal Auditors,2017).

1.5.9 Auditoría interna basada en riesgos.

La auditoría interna basada en riesgos es considerada como un mecanismo de mejora continua en las organizaciones, para la estabilidad en los mercados. Es un factor determinante que en la actualidad ha tomado mucha fuerza y a la que se le debe prestar mucha atención.

Su misión es analizar un elemento de punta a punta, con el fin de encontrar sus riesgos, deficiencias y proponer opciones de mejora y maximizar la calidad en el servicio, es un mecanismo evolutivo, dado que las personas, los procesos, las plataformas y el mundo cambia.

Contrario a la concepción de lo que la mayoría de las personas piensan sobre auditoría como un examen estricto para perjudicar negativamente a los evaluados, la auditoría basada en riesgos

es una herramienta que ofrece una oportunidad en donde todos los componentes se ven beneficiados, permitiendo el mejoramiento de la productividad para los empleados y velando por la calidad de los servicios o productos que son ofertados en la compañía, lo cual genera más ingresos económicos.

Al implementar una auditoría de servicio al cliente adecuada, se identifican, debilidades y fortalezas, aportando un gran valor a la toma de decisiones de manera informada, correcta y estratégica (Gobierno de Colombia,1993).

1.5.10 Tecnologías de la información.

Los autores Thompson y Strickland mencionan que las tecnologías de la información son el conjunto de dispositivos, herramientas, equipos, componentes electrónicos, con la capacidad de gestionar información que aportan al desarrollo del crecimiento económico de una organización (Vital,2007)

1.5.11 Archivo Permanente.

Es un elemento de la gestión documental de auditoría que consolida los documentos de la auditoría, como manuales, libros, normas etc.

En el caso de auditorías internas, son los documentos que contienen información de la empresa y se emplean para la auditoría.

1.5.12 Archivo Corriente.

Es el componente que contiene todos los papeles de trabajo que se emplean en la auditoría de punta a punta (Auditol, 2021)

1.6 Metodología de la investigación

A continuación, se aborda el tipo de investigación y todo el diseño metodológico a implementar con el fin de cumplir con los objetivos del proyecto.

1.6.1 Tipo de investigación.

Para este caso se aplicará la metodología de auditoría interna basada en riesgos que permitirá tener un espectro más amplio de lo que pueda estar ocurriendo en el área, teniendo en cuenta no solamente los riesgos sino también sus causas, efectos y controles existentes. Además, se ejecutará teniendo en cuenta el método de puntajes multidimensional porque da más herramientas para el análisis de riesgos suprimiendo la subjetividad, este método no deja todo al criterio de los auditores, sino que provee un paso a paso para llegar a un diagnóstico mucho más preciso. También se aplicará un método **analítico,** debido a que la información que resulte de la auditoría permitirá evaluar el impacto que pueda tener su implementación en la gestión de proyectos informáticos en la organización.

Así mismo, es importante mencionar que la metodología de riesgos a ejecutar fue tomada de la clase de auditoría e interventoría, que fue vista en el plan de estudios de la especialización en proyectos informáticos de la Universidad Francisco José de Caldas, por ende, las fases mencionadas a continuación son con exactitud las propuestas en tal materia.

Teniendo en cuenta que la metodología basada en riesgos es la secuencia de unas fases puntuales, esto permite implementar algunos de sus elementos o la totalidad de estos. Las siguientes fases componen el plan de trabajo asociado a la presente propuesta:

1.6.2 Fases de la metodología basada en riesgos.

- **Conocimiento Global de organización y del objeto a auditar:**

  Recopilación, entendimiento y análisis de la misión, visión, plan de desarrollo, objetivos, metas, regulación que rige la organización, estructura organizacional, situación financiera y legal, servicios que produce, posicionamiento en el mercado, competidores, cumplimiento de

normas, problemas jurídicos (En caso de que existan), manuales, procedimientos y funciones, planta física, talento humano, solidez, dependencia y calidad de los clientes.

- **Definición del objeto y áreas a auditar**

Determinación del objeto a auditar y descomposición del objeto en áreas auditables, mediante la estrategia divide y vencerás.

- **Evaluación de riesgos**

Priorización de las áreas auditable teniendo en cuenta su criticidad, con el propósito de identificar en qué se debe hacer hincapié y posibilitar la planeación de la auditoría, para la evaluación de riesgos, se tomará como referencia la evaluación de riesgos que aplique la organización, en caso de que no exista, se aplicarán los siguientes pasos:

- Elaboración de lista de riesgos.
- Construcción matriz de C-R-E.
- Identificación de posibles controles.
- Aplicación de la Matriz Riesgos vs Riesgos (RvsR), para obtener el valor del impacto de cada riesgo.
- Aplicación de la Matriz de Controles vs Riesgos (CvsR), para obtener el nivel de exposición de cada riesgo.
- Aplicación Matriz de puntaje con el resultado de las matrices anteriores.
- Aplicación Matriz de priorización, ordenando de mayor a menor criticidad.

- **Planeación de la auditoría**

Proposición de objetivos, procedimientos, técnicas de auditoría y pruebas desde el área más crítica a la menos crítica y también por los riesgos con mayor calificación.

- **Ejecución de la auditoría**

Aplicación de procedimientos con sus respectivas pruebas y técnicas diseñadas en la planeación. Registrar organizadamente las evidencias, soportes, en el archivo corriente.

- **Análisis de resultados**

Teniendo en cuenta que en fases previas posiblemente se identificaron hallazgos con sus evidencias, se deben concretar los resultados desarrollando las siguientes actividades:

- Revisión documental
- Precisar hallazgos
- Precisar evidencias.
- Validar resultados
- Evaluar resultados.

- **Construcción de Informes de auditoría**

- Informe ejecutivo
- Informe técnico.

1.6.3 Técnicas de recolección de información.

Tal como lo indica la metodología de auditoría interna basada en riesgos se tomarán las siguientes técnicas de recolección de información:

- **Cuestionarios y Encuestas:** Por medio de herramientas digitales se diseñarán cuestionarios que permitan recopilar la cantidad de información necesaria para el análisis de la gestión de acceso lógico de la entidad financiera ABC. con el fin de conocer sus opiniones y sentimientos con respecto al objeto auditado.
- **Observaciones:** Va más de la mano con la naturaleza del auditor, se trata de estar atento desde el primer contacto con los auditados a toda información que pueda resultar provechosa y que no haya sido capturada por medio de las demás técnicas.

- **Documentos:** Para realizar mejor la auditoría es primordial contar con la documentación en la que quedará registrada la evidencia de todo el proceso, se contará con documentos de auditoría, manuales, estándares, listas de chequeo, listas de riesgos, listas de controles, matrices, procedimientos, actas, informes, etc.

1.6.4 Tratamiento de la información.

La información que será obtenida por los distintos medios de recopilación se maneja para su completo análisis, por tanto, se verá sometida a las siguientes operaciones: Lectura, escritura, ordenación, clasificación, comparación, archivo, análisis.

De igual manera toda la información será procesada mediante herramientas de ofimática.

1.7 Organización del trabajo de grado

A continuación, se plantea los capítulos del contenido propuesto que conformará el documento del trabajo de grado a entregar:

INTRODUCCIÓN

PARTE I. CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

CAPÍTULO 1. DESCRIPCIÓN DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

1.2 Objetivos de la investigación

1.2.1 Objetivo general.

1.2.2 Objetivos específicos.

1.3 Justificación de la investigación

1.4 Hipótesis de la investigación

1.5 Marco Teórico

1.5.1. Origen de la gestión de acceso lógico.

1.5.2 ISO 27001.

1.5.3 Entidad Financiera.

1.5.4 Cliente Interno.

1.5.5 Acceso Lógico.

1.5.6 Importancia del acceso lógico.

1.5.7 Auditoría.

1.5.8 Auditoría interna.

1.5.9 Auditoría interna basada en riesgos.

1.5.10 Tecnologías de la información.

1.5.11 Archivo Permanente.

1.5.12 Archivo Corriente.

1.6 Metodología de la investigación

1.6.1 Tipo de investigación.

1.6.2 Fases de la metodología basada en riesgos.

1.6.3 Técnicas de recolección de información.

1.6.4 Tratamiento de la información.

1.7 Organización del trabajo de grado

1.8 Estudio de sistemas previos

PARTE II. DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO 2: DESARROLLO DE LA METODOLOGÍA DE AUDITORÍA BASADA EN RIESGOS

2.1 Fase 1: Conocimiento Global de la Organización

2.1.1 Información de la organización.

2.1.2 Razón social de la organización.

2.1.3 Servicios y Productos destacados de la entidad financiera ABC.

2.1.4 Filosofía institucional.

2.1.5 Objetivos de la organización.

2.1.6 Resultados económicos o estados financieros de los últimos años.

2.1.7 Identificación de competidores de la organización.

2.1.8 Principales proveedores.

2.1.9 Principales clientes y dependencia de los clientes.

2.1.10 Situación legal de la organización.

2.1.11 Manuales de procedimientos y funciones de la organización.

2.2 Fase 2: Definición del objeto a auditar y áreas auditables

2.2.1 Definición del objeto a Auditar.

2.2.2 Misión y visión del objeto a auditar.

2.2.3 Objetivos del objeto a Auditar.

2.2.4 Distribución de planta física del objeto a auditar.

2.2.5 Recurso humano del objeto a auditar.

2.2.6 Inventarios del Objeto a auditar.

2.2.7 Descomposición del objeto a auditar en áreas auditables

2.3 Fase 3: Evaluación de Riesgos

2.3.1 Lista de riesgos.

2.3.2 Matriz C-R-E.

2.3.3 Listas de controles.

2.3.4 Riesgos vs Riesgos.

2.3.5 Controles vs Riesgos.

2.3.6 Matriz Puntaje.

2.3.7 Priorización.

2.4 Fase 4: Planeación de la Auditoría

2.4.1 Riesgos más críticos del área.

2.4.2 Objetivo General de la auditoría.

2.4.3 Objetivos Específicos.

2.4.4 Cronograma.

2.4.5 Técnicas de Auditoría.

2.4.6 Procedimientos de Auditoría.

2.5 Ejecución de la Auditoría

2.6 Análisis de resultados

PARTE III. CIERRE DE LA INVESTIGACIÓN

CAPÍTULO 3: INFORME DE AUDITORÍA

3.1 Informe técnico.

3.2 Informe ejecutivo

CAPÍTULO 4. RESULTADOS Y DISCUSIÓN

CAPÍTULO 5. CONCLUSIONES

5.1 Verificación, contraste y evaluación de los objetivos

5.2 Síntesis del modelo propuesto

5.3 Aportes originales

CAPÍTULO 6. PROSPECTIVA DEL TRABAJO DE GRADO

6.1 Líneas de investigación futuras

6.2 Trabajos de investigación futuros

BIBLIOGRAFÍA

PARTE II. DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO 2: DESARROLLO DE LA METODOLOGÍA DE AUDITORÍA BASADA EN RIESGOS

En este capítulo se relaciona el paso a paso realizado durante la metodología basada en riesgos de la entidad financiera ABC. planteado en esta investigación, también conocido como archivo corriente.

Teniendo en cuenta que en la metodología que se va a ejecutar se hace uso de los papeles de trabajo archivo permanente y corriente, es necesario manejar una referenciación especial en el proyecto, por ende, a continuación, se relaciona la referenciación utilizada para el presente ejercicio de auditoría que se utilizará en las diferentes fases de la auditoría:

NIVELES	NEMOTÉCNICO
ARCHIVO PERMANENTE	**N/A**
ARCHIVO CORRIENTE	N/A
NIVEL 1 • GESTIÓN ACCESO LÓGICO MEDIANTE IM	-GALIDM
NIVEL 2 • INTEGRACIÓN • IDENTIDAD ÚNICA • GOBIERNO DE ROLES	 - IN - IU - GR
NIVEL 3 • MATRIZ • DOCUMENTO • LISTAS • PROCEDIMIENTO • ENCUESTA • CORREOS	 - MAT - DOC - LIST - PROC - ENC -CORR

Tabla 2. Nemotécnicos y referencias. Fuente: Auditoría e interventoría de proyectos informáticos-Luis Montenegro

RPT: Es importante mencionar que se hará uso de esta abreviación para referenciar el nombre de cada documento que repose en el archivo permanente o corriente.

Así mismo, se informa que el presente proyecto se utilizará como archivo maestro.

2.1 Fase 1: Conocimiento Global de la Organización

2.1.1 Información de la organización.

Teniendo en cuenta los principios de la metodología de auditoría basada en riesgos, se efectuó el levantamiento de información relacionado a continuación, la mayoría de la información es pública. Sin embargo, se realizan algunas ediciones, acatando el acuerdo de confidencialidad con la organización.

2.1.2 Razón social de la organización.

Entidad financiera ABC.

2.1.3 Servicios y Productos destacados de la entidad financiera ABC.

A continuación, se relaciona los servicios y productos principales que la organización ofrece:

- ***Tarjeta de crédito sin cuota de manejo.***

Tiene como fin mejorar el flujo de caja, dicha tarjeta permite el uso del total del cupo de la tarjeta para avances.

- ***Cuentas de Ahorro sin cuota de manejo***

Producto orientado a la línea de ahorro, la cual ofrece los siguientes beneficios: Liquidación y abono de intereses diariamente.

- ***Portal empresarial.***

Es una canal transaccional que permite la administración de productos empresariales brindando múltiples comodidades a las empresas y confort.

RPT: Archivo Permanente - Servicios y Productos destacados

2.1.4 Filosofía institucional.

A continuación, se relaciona visión y principios éticos de la organización.

- ***Visión.***

  Ser únicos, queridos y recomendados por nuestra gente.

- ***Principios éticos.***

El comportamiento de los empleados del ABC, deberá sujetarse a los siguientes principios éticos: lealtad, respeto, honestidad, responsabilidad y compromiso.

2.1.5 Objetivos de la organización.

- Ser una empresa sostenible con experiencias positivas.
- Apoyar y acompañar financieramente a los colombianos
- RPT: Archivo Permanente - Filosofía organizacional

2.1.6 Resultados económicos o estados financieros de los últimos años.

La organización maneja unos estados financieros públicos, desde el año 2018 – 2021, estos documentos, pueden ser consultados en la carpeta del archivo permanente anexo al presente proyecto.

RPT:

- Archivo Permanente - eeff-consolidados-bp-2018
- Archivo Permanente - informe-revelaciones-consolidado-diciembre-2019
- Archivo Permanente - Libro-2-EEFF-Consolidados-BP-2020-WEB-INDICEOK+28_4_2021
- Archivo Permanente - libro-iiggss-separados-2021

2.1.7 Identificación de competidores de la organización.

Con base al fomento interno de la entidad financiera, los competidores actuales son los bancos digitales o neo bancos:

- Nequi
- Movii
- Lulo Bank
- NuBank.
- Bancos tradicionales

RPT: Archivo Permanente - Entrevista con Portafolio agosto 2021

2.1.8 Principales proveedores.

Los siguientes proveedores, tienen una relación destacada con el objeto auditado.

- IBM
- Microfocus
- Atento
- EXxertos Consulting Outosourcing
- Project BPOP S.A.S
- Zurich International Brokes
- Serfyneg
- System Solution
- Epika

RPT: Archivo Permanente - Principales Proveedores

2.1.9 Principales clientes y dependencia de los clientes.

Por temas de confidencialidad, solo se relacionan los clientes más destacados:

- Policía Nacional de Colombia – Alta
- Universidad Nacional de Colombia-Alta

2.1.10 Situación legal de la organización.

Con base al estado financiero del año 2021, se identifica que el Banco cumple con las disposiciones legales que rigen el desarrollo de su objeto social, así como las exigencias de los organismos de control y los estatutos sociales. De igual manera, ha respetado las decisiones adoptadas por la Asamblea General de Accionistas y por la Junta Directiva. Por otra parte, el Banco presenta una situación jurídica y administrativa de normalidad en sus operaciones.

RPT: Archivo Permanente - libro-iiggss-separados-2021

2.1.11 Manuales de procedimientos y funciones de la organización.

En el informe de estados financieros 2021, se menciona que el Banco cuentan con manuales detallados de procedimientos y políticas con respecto al manejo del riesgo, los grupos de negocio y de riesgo del Banco mantiene reuniones periódicas de orientación con enfoques de riesgo que están en línea con la cultura de riesgo del mismo. Sin embargo, al tratarse de información confidencial, no es posible compartir esta información.

2.2 Fase 2: Definición del objeto a auditar y áreas auditables

2.2.1 Definición del objeto a Auditar.

Teniendo en cuenta la intención del presente proyecto, el objeto a auditar es la Gestión acceso lógico mediante IM de la entidad financiera ABC, dicha área se encarga del Aprovisionamiento de acceso lógico de diferentes aplicaciones de la organización que se encuentran integradas con Identity Managament para los funcionarios de la entidad financiera.

2.2.2 Misión y visión del objeto a auditar.

- Misión: Apalancar a las diferentes áreas del negocio para que puedan laborar y crecer de una forma segura y ágil, teniendo sus accesos a tiempo y sin traumas.

Visión: Aumentar la cobertura de gestión de acceso lógico de la entidad financiera ABC, realizando una labor ágil, segura, eficaz y eficiente, mediante la implementación de estándares, procesos y tecnologías que faciliten la labor del Banco. RPT: Archivo Permanente – Lema.

2.2.3 Objetivos del objeto a Auditar.

- Gestionar acceso lógico de forma oportuna y segura.
- Incrementar la cobertura de gestión.
- Disminuir el esfuerzo del usuario final para la obtención de acceso lógico.

  RPT: Archivo Permanente – Lema.

2.2.4 Distribución de planta física del objeto a auditar.

El objeto a auditar es un área que actualmente trabaja de forma distribuida a causa de lo ocurrido por pandemia del Covid 19, por ende, la entidad financiera ABC, tomó la decisión de editar el contrato de los colaboradores del área, pactando un contrato de teletrabajo al 100% de forma indefinida, por tanto, cada colaborador tiene sus equipos de cómputo en su respectivo domicilio. En la casa matriz de la organización se encuentran los servidores de las plataformas usadas y el acceso a estas se hace mediante una VPN.

2.2.5 Recurso humano del objeto a auditar.

Rol Organizacional	Perfil	Cantidad de recursos
Coordinador y supervisor	Profesional especializado	1
Operativo	Profesional	1
Operativo	Analista Operativo	1

Operativo	Aprendiz SENA	2
Administrativo	Director	3

Tabla 3. Recurso humano objeto a auditar. Fuente: Elaboración propia

2.2.6 Inventarios del Objeto a auditar.

Por efectos de confidencialidad de la organización no se puede obtener un inventario detallado para el objeto a auditar, pero se logra establecer un detalle general del inventario para esta sección:

- Hardware: Computadores portátiles.
- Software: Matrices de roles y perfiles, VPN e Identity Managament.

2.2.7 Descomposición del objeto a auditar en áreas auditables

- Gobierno de Roles: Brinda asesorías de construcción y oficialización de matrices de roles RBAC, se encarga de transformar los roles funcionales a técnicos para que IdM haga la gestión de accesos.
- Identidad Única: Se encarga ejecutar altas, bajas y cambios de accesos a los usuarios, una parte automática y la otra manual.
- Integraciones: Área que se encarga de realizar levantamiento de información, desarrollo y paso a producción de opciones de mejora para el área de gestión de acceso, así mismo, realiza integraciones con otras áreas para hacerse cargo de la gestión de acceso lógico.

2.3 Fase 3: Evaluación de Riesgos

Para una mayor organización se realizaron anexos para facilitar el análisis de riesgos, en consecuencia, a continuación, se referencian:

2.3.1 Lista de riesgos.

RPT:

- Listado de riesgos para el área a auditar de Gobierno de Roles: GALIDM-GR-LIST-001

- Listado de riesgos para el área a auditar de Integración QA: GALIDM-IN-LIST-001
- Listado de riesgos para el área a auditar de Identidad Única: GALIDM-IU-LIST-001

2.3.2 Matriz C-R-E.

RPT:

- Matriz C-R-E para el área a auditar de Gobierno de Roles: GALIDM-GR-MAT-001
- Matriz C-R-E para el área a auditar de Integración QA: GALIDM-IN-MAT-001
- Matriz C-R-E para el área a auditar de Identidad Única: GALIDM-IU-MAT-001

2.3.3 Listas de controles.

RPT:

- Listado de controles para el área a auditar de Gobierno de Roles: GALIDM-GR-LIST-002
- Listado de controles para el área a auditar de Integración QA: GALIDM-IN-LIST-002
- Listado de controles para el área a auditar de Identidad Única: GALIDM-IU-LIST-002

2.3.4 Riesgos vs Riesgos.

RPT:

- Matriz de RvsR para el área a auditar de Gobierno de Roles: GALIDM-GR-MAT-002
- Matriz de RvsR para el área a auditar de Integración QA: GALIDM-IN-MAT-002
- Matriz de RvsR para el área a auditar de Identidad Única: GALIDM-IU-MAT-002

2.3.5 Controles vs Riesgos.

RPT:

- Matriz de CvsR para el área a auditar de Gobierno de Roles: GALIDM-GR-MAT-003
- Matriz de CvsR para el área a auditar de Integración QA: GALIDM-IN-MAT-003

- Matriz de CvsR para el área a auditar de Identidad Única: GALIDM-IU-MAT-003

2.3.6 Matriz Puntaje.

RPT:

- Matriz de puntajes para el área a auditar de Gobierno de Roles: GALIDM-GR-MAT-004
- Matriz de puntajes para el área a auditar de Integración QA: GALIDM-IN-MAT-004
- Matriz de puntajes para el área a auditar de Identidad Única: GALIDM-IU-MAT-004

2.3.7 Priorización.

RPT: Archivo corriente - Matriz de priorización.

2.4 Fase 4: Planeación de la Auditoría

A partir de la matriz de priorización (Figura 1) se puede ver que el área que más está sufriendo impacto en el proceso de la gestión de acceso lógico es la de Gobierno de Roles:

ANALISIS DE RIESGOS		
MATRIZ DE PRIORIZACIÓN		
ORGANIZACIÓN: Universidad Distrital Francisco José de Caldas		
OBJETO A AUDITAR: Gestión acceso lógico mediante IM	**FECHA:** 14/04/2022	
EMPRESA AUDITORA: Universidad Francisco José de Caldas	**AUDITORES**: Angie Lorena Rivera Vargas - Billy Joel Galvis Peña	
#	**ÁREA**	**%**
1	Gobierno de Roles	396,58
2	Idenridad Única	380,08
3	Integración	335,9

Figura 1. Matriz de priorización. Fuente: Elaboración propia

En consecuencia, a lo anterior, debido al tiempo disponible para realizar la auditoría, se centrará en la planeación y ejecución sobre esta área, teniendo en cuenta los riesgos que menos están siendo mitigados y que la están afectando de acuerdo con lo identificado en la matriz de puntajes GALIDM-GR-MAT-004:

ANALISIS DE RIESGOS					
MATRIZ DE PUNTAJES					
ORGANIZACIÓN: Universidad Distrital Francisco José de Caldas			**OBJETO A AUDITAR:** Gestión acceso lógico mediante IM		
ÁREA AUDITABLE: Gestión de Roles			**FECHA:** 14/04/2022		
EMPRESA AUDITORA: Universidad Francisco José de Caldas			**AUDITORES:** Angie Lorena Rivera Vargas - Billy Joel Galvis Peña		
RIESGOS		**IMPACTO NEGATIVO**	**NIVEL DE EXPOSICIÓN**	**PORCENTAJE DEL RIESGO**	**TOTAL POR RIESGO**
AICM	Asesorías incorrectas para la construcción de	150,9	2,34	3,04	10,73
AIOM	Asesorías incorrectas para la oficialización de	145,2	3	2,93	12,76
PNUD	Proceso de nivel uno desactualizado	148,6	2,98	2,99	13,24
RMRT	Revisiones a matrices de roles tardía	140,7	2,96	2,84	11,83
AUMT	Autorización de matrices de roles tardía	141	3,2	2,84	12,81
ACMT	Actualización de matrices de roles tardía	143	2,75	2,88	11,33
IPOOAM	Incumplimiento del protocolo de oficialización o	145,8	3,47	2,94	14,87
NRMR	Notificación con retrasos de oficializaciones y	142,3	2,84	2,87	11,60
ARMR	Actualización con retrasos de las matrices	144,3	2,23	2,91	9,36
AIMR	Actualización incorrecta de las matrices	145,3	2,81	2,93	11,96
DMUR	Definición de la actualización de la matriz única con	149,7	2,94	3,02	13,29
DIAMU	Definición incorrecta de la actualización de la	152,7	2,69	3,08	12,65
IPMGR	Incumplimiento del protocolo de oficialización o	145,7	2,38	2,94	10,19
AIAM	Almacenamiento incorrecto de los archivos	145,1	1,94	2,92	8,22
MMRM	Mal manejo del repositorio de matrices	143,1	3,06	2,88	12,61
DRMR	Daño del repositorio de matrices	142,3	3,25	2,87	13,27
DRMU	Daño del repositorio de matriz única	151,5	3,18	3,05	14,69
AMRA	Ausencia de matrices de roles para aplicaciones	156,5	2,33	3,15	11,49
DRDNA	Definición de roles desactualizados a las	151,3	3,25	3,05	15,00
DRI	Definición de roles incorrectos	165	2,78	3,32	15,23
DRDI	Definición de roles duplicados innecesariamente	134,6	2,44	2,71	8,90
PRCCV	Permanencia de roles que ya cumplieron con su	133,9	2,99	2,7	10,81
DRNA	Definición de roles no autorizados	151,6	3,22	3,05	14,89
DNR	Difícil nomenclatura de roles	141,8	3,14	2,86	12,73
RTDR	Respuesta tardía de la definición de roles	145	3,15	2,92	13,34
RD	Roles desactualizados	148,9	3,16	3	14,12
IPEPN	Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones	151,4	3,28	3,05	15,15
ETMT	Elaboración tardía de matrices técnicas	148,3	2,13	2,99	9,44
AMRSA	Oficialización o actualización de matrices de roles	156,1	2,43	3,15	11,95
APNAM	Acceso a personal no autorizado a matrices de	146,9	1,66	2,96	7,22
MRDI	Matrices de roles duplicadas innecesariamente.	135,6	1,6	2,73	5,92
DUMR	Difícil ubicación de matrices	139,6	1,72	2,81	6,75
IMRD	Indexación de matrices de roles deficiente	138,8	2,44	2,8	9,48
ANAPM	Acceso no autorizado para modificación de	151,8	1,88	3,06	8,73
			SUMA TOTAL		396,58
			PROMEDIO		11,66

Figura 2. Matriz de puntajes. Fuente: Elaboración propia

2.4.1 Riesgos más críticos del área.

A continuación, se relacionan los riesgos más críticos del área de Gestión de Acceso Lógico de la entidad financiera ABC.

- Definición de roles incorrectos
- Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones

Partiendo de este par de riesgos, se tiene en cuenta la lista de controles definidos para mitigar cada uno respectivamente, junto a las calificaciones obtenidas:

Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones:

CONTROL	CALIFICACIÓN	APLICABILIDAD (T/P)
¿Están técnicamente definidas las cargas laborales?	4,1	T
¿Están claramente definidos los procesos de contingencia en caso de que el correo electrónico falle?	2	T
¿Se valida el cumplimiento de los ANS definidos para esta labor?	3	T
¿Se implementan controles de calidad de los casos atendidos?	4	T
¿Se han implementado mecanismos de contingencia para la atención a los clientes?	2	T
¿Se han implementado metodologías ágiles para aumentar la productividad de la organización?	3	T

Tabla 4. Lista de controles para el incumplimiento de protocolo de enrolamiento para nuevas aplicaciones. Fuente: Elaboración propia

Definición de roles incorrectos:

CONTROL	CALIFICACIÓN	APLICABILIDAD (T/P)
¿Se capacita al personal que imparte las asesorías para construcción de matrices de roles?	4,3	T
¿Existe un procedimiento riguroso para la selección de personal del área que asesora la construcción y oficialización de matrices de roles?	3,8	T
¿Se capacita al personal que imparte las asesorías para oficialización de matrices de roles?	3	T
¿El área funcional verifica los perfiles que están asignados cumplen con las necesidades del negocio?	3,2	T
¿Existe una implementación de certificación de accesos mediante herramientas de gobierno de accesos?	3,9	T
¿Se realiza mantenimiento de matrices de roles periódicamente?	3,5	T
¿Se implementan controles de calidad de los casos atendidos?	3,9	T
¿Se han implementado procesos de certificación de accesos autorizados?	3,8	T
¿Se han implementado procesos de certificación de accesos para retirar accesos no autorizados?	3,7	T
¿Existe una metodología para gestión de roles?	3,8	T

¿Periódicamente se realiza análisis del almacenamiento de matrices de roles?	3,8	T
¿Se capacita al personal que actualiza la matriz única?	3,8	T

Tabla 5. Lista de controles para Definición de roles incorrectos. Fuente: Elaboración propia

Viendo las calificaciones de los controles para cada uno de los riesgos críticos se tiene que algunos de estos controles fueron diseñados para una aplicabilidad total, sin embargo, no están siendo aplicados o si lo están, no han sido efectivos.

2.4.2 Objetivo General de la auditoría.

Evaluar los riesgos y controles más críticos del objeto a auditar Gestión acceso lógico mediante IdM de la entidad financiera ABC.

2.4.3 Objetivos Específicos.

- Verificar si los controles asociados a los riesgos más críticos de Gobierno de Roles existen.
- Evaluar si los controles asociados a los riesgos más críticos de Gobierno de Roles son efectivos.
- Sugerir recomendaciones de mejora para los controles actuales del área Gobierno de Roles.

2.4.4 Cronograma.

ACTIVIDAD	DURACIÓN (SEMANAS)
Levantamiento de riesgos y controles	3
Realizar matrices RvsR	2
Realizar matrices CvsR	2
Realizar matriz de priorización	1
Procedimiento GALIDM-GR-PROC-001	1
Procedimiento GALIDM-GR-PROC-002	1
Procedimiento GALIDM-GR-PROC-003	1
Procedimiento GALIDM-GR-PROC-004	1
Procedimiento GALIDM-GR-PROC-005	1
Procedimiento GALIDM-GR-PROC-006	1

Procedimiento GALIDM-GR-PROC-007	1
Procedimiento GALIDM-GR-PROC-008	1
Procedimiento GALIDM-GR-PROC-009	1
Procedimiento GALIDM-GR-PROC-010	1
Procedimiento GALIDM-GR-PROC-011	1
Procedimiento GALIDM-GR-PROC-012	1
Procedimiento GALIDM-GR-PROC-013	1
Procedimiento GALIDM-GR-PROC-014	1
Procedimiento GALIDM-GR-PROC-015	1
Procedimiento GALIDM-GR-PROC-016	1
Procedimiento GALIDM-GR-PROC-017	1
Procedimiento GALIDM-GR-PROC-018	1
Ejecución de la auditoría	2
Realización de informe ejecutivo	1
Realización de informe técnico	1

Tabla 6. Actividades para la auditoría

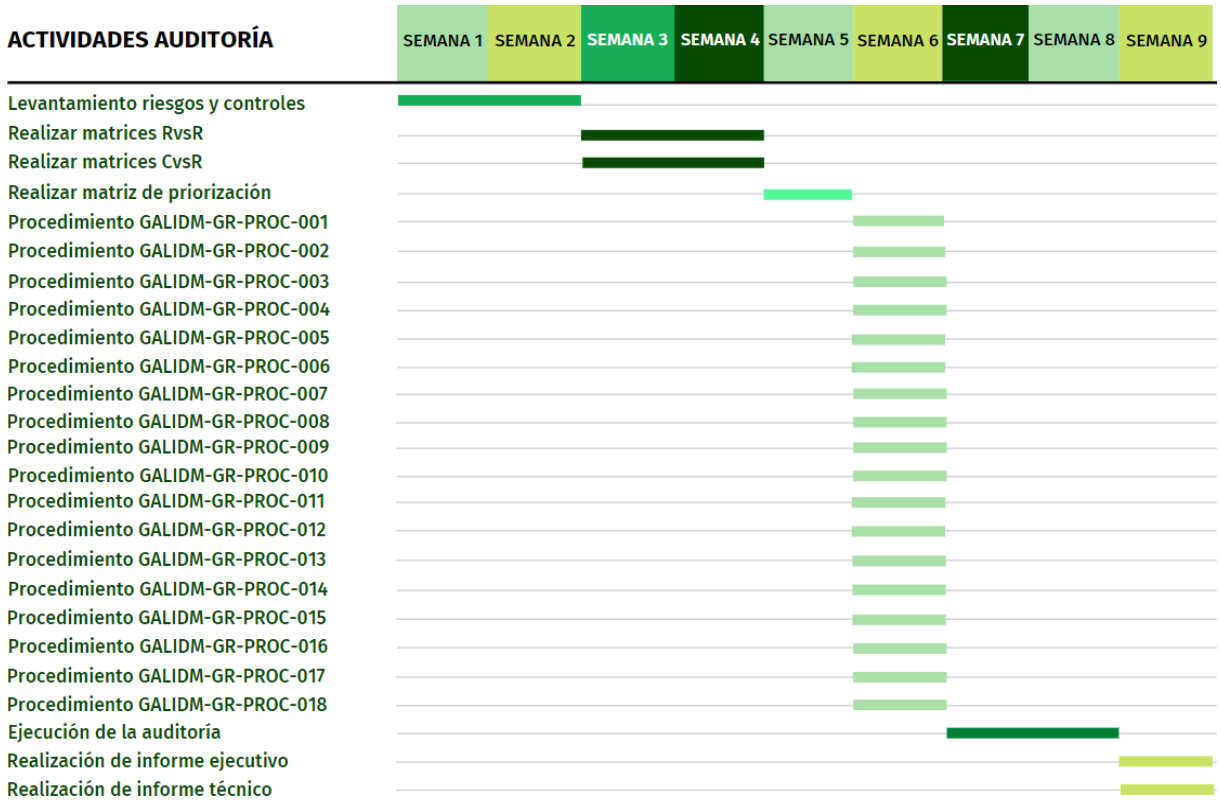

Tabla 7. Diagrama de Gantt de las actividades de la auditoría.

2.4.5 Técnicas de Auditoría.

Encuestas.

A continuación, se relaciona la información contenida en las respuestas de las encuestas de diagnóstico para los riesgos “Definición de roles incorrectos” (GALIDM-GR-ENC-001). “Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones” (GALIDM-GR-ENC-002) con el fin de determinar las conclusiones de las encuestas según la perspectiva de los integrantes del área de Gobierno de Roles dentro del objeto Gestión de Acceso Lógico.

Para comenzar se dará un breve contexto acerca de las encuestas:

Las presentes encuestas son guiadas a tener la opinión de los integrantes del área de Gobierno de Roles con el fin de hacer el contraste frente a lo obtenido en las matrices RvsC GALIDM-GR-MAT-003, de manera que, o confirme lo presenciado en cuanto a la deficiencia o eficiencia de controles, o dé una perspectiva completamente distinta a lo repasado en el estudio de los riesgos y controles.

Cabe recordar que se hace énfasis en los dos riesgos mencionados con anterioridad debido a que son los riesgos que mayor puntaje tienen en los estudios de riesgos y controles, por tanto, son los que más están impactando al área y al objeto de Gestión de Acceso Lógico de manera general.

Las preguntas están guiadas hacia los controles designados para ambos riesgos, de manera que se pueda tener una confirmación acerca de qué tan bien o mal implementados están siendo para mitigar los riesgos.

Por otra parte, vale destacar que el universo de la toma es de 6 personas, que es el total de integrantes del área de Gobierno de Roles, por tanto, la muestra debe ser de esos mismos 6 integrantes.

Preguntas diagnósticas para la definición de roles incorrectos:

- ¿Existe un procedimiento debidamente definido y documentado para la gestión de acceso lógico?
- ¿Qué tanta retroalimentación de sus labores recibe?
- ¿Qué tanto se realizan análisis y mantenimiento de las matrices de roles?
- ¿Qué tantos inconvenientes han tenido con los permisos de ingreso a alguna aplicación?
- ¿Qué tantos requerimientos se presentan por parte de los usuarios finales con respecto a la gestión de acceso lógico?
- ¿Qué tantas capacitaciones han recibido con respecto a la gestión de acceso lógico?
- ¿Qué tantas certificaciones/cursos/diplomados tiene, que sean enfocados a la gestión de acceso lógico?

Preguntas diagnósticas para el Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones:

- ¿Qué tantos planes de contingencia existen en momentos de fallos técnicos?
- ¿Qué tantos ANS conoce de la labor que lleva a cabo?
- ¿Qué tanto se realiza seguimiento de indicadores en la atención al usuario final?
- ¿Se implementan metodologías ágiles en los procesos del área?

Por último, la relación de las respuestas con análisis y conclusiones está incluido dentro del documento de encuestas GALIDM-GR-DOC-002

Observación:

Para este caso se tuvo en cuenta el tipo de observación participativa, ya que uno de los auditores actúa como integrante del objeto a auditar, por tanto, le ha permitido tener una visión mucho más amplia del mismo al igual que las áreas en las que se descompuso. Gracias a esta

observación y al trabajo conjunto con personas del área de calidad de la organización, fue posible realizar el levantamiento de información, riesgos, controles, documentación y demás datos pertinentes para el estudio pese a que, como ya se ha mencionado anteriormente, la entidad restringe el envío y divulgación de información confidencial.

2.4.6 Procedimientos de Auditoría.

RPT:

- Procedimiento área Gobierno de Roles, "**Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones**", control "¿Están técnicamente definidas las cargas laborales?" GALIDM-GR-PROC-01
- Procedimiento área Gobierno de Roles, "**Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones**", control "¿Están claramente definidos los procesos de contingencia en caso de que el correo electrónico falle?" GALIDM-GR-PROC-02
- Procedimiento área Gobierno de Roles, "**Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones**", control "¿Se valida el cumplimiento de los ANS definidos para esta labor?" GALIDM-GR-PROC-03
- Procedimiento área Gobierno de Roles, "**Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones**", control "¿Se implementan controles de calidad de los casos atendidos?" GALIDM-GR-PROC-04
- Procedimiento área Gobierno de Roles, "**Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones**", control "¿Se han implementado mecanismos de contingencia para la atención a los clientes?" GALIDM-GR-PROC-05
- Procedimiento área Gobierno de Roles, "**Incumplimiento del protocolo de enrolamiento para nuevas aplicaciones**", control "¿Se han implementado metodologías ágiles para aumentar la productividad de la organización?" GALIDM-GR-PROC-06
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Se capacita al personal que imparte las asesorías para construcción de matrices de roles?" GALIDM-GR-PROC-07

- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Existe un procedimiento riguroso para la selección de personal del área que asesora la construcción y oficialización de matrices de roles?" GALIDM-GR-PROC-08
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Se capacita al personal que imparte las asesorías para oficialización de matrices de roles?" GALIDM-GR-PROC-09
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿El área funcional verifica los perfiles que están asignados cumplen con las necesidades del negocio?" GALIDM-GR-PROC-10.
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Existe una implementación de certificación de accesos mediante herramientas de gobierno de accesos?" GALIDM-GR-PROC-11
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Se realiza mantenimiento de matrices de roles periódicamente?" GALIDM-GR-PROC-12
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Se implementan controles de calidad de los casos atendidos?" GALIDM-GR-PROC-13
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Se han implementado procesos de certificación de accesos autorizados?" GALIDM-GR-PROC-14
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Se han implementado procesos de certificación de accesos para retirar accesos no autorizados?" GALIDM-GR-PROC-15
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Existe una metodología para gestión de roles?" GALIDM-GR-PROC-16
- Procedimiento área Gobierno de Roles, "**Definición de roles incorrectos**", control "¿Periódicamente se realiza análisis del almacenamiento de matrices de roles?" GALIDM-GR-PROC-17
- Procedimiento área Gobierno de Roles, "Definición de roles incorrectos", control "¿Se capacita al personal que actualiza la matriz única?" GALIDM-GR-PROC-18.

2.5 Ejecución de la Auditoría

A medida que se realizó la ejecución de la auditoría según las técnicas y procedimientos descritos anteriormente se evidenció que hay carencias de metodologías y cierta documentación. Esto, además de las restricciones que impone el banco para suministrar información que es de tipo confidencial y a la que no fue posible acceder. Por otra parte, se notó falencias en los procesos del área ya que como lo mostraron las encuestas, análisis de riesgos y controles y la documentación suministrada por la organización, no se está siendo eficiente en la atención al usuario final y en la gestión de los accesos, aunque estas observaciones se abordarán de una manera un poco más profunda en el análisis de resultados e informe de auditoría.

Sin embargo, se debe destacar la buena disposición de los integrantes del área de gobierno de roles ya que gracias a su ayuda con las encuestas y observación se logró confirmar varios hallazgos realizados en el análisis de riesgos y controles.

A nivel general se recomienda adoptar alguna metodología que permita trabajar los procesos de una manera eficaz y eficiente, que involucre a toda el área bajo un mismo objetivo y bajo el mismo marco de trabajo para que todos estén “hablando el mismo idioma” y de ese modo dar una buena atención al usuario final. También es importante que los colaboradores estén lo suficientemente capacitados para cumplir a cabalidad con los objetivos del área y el objeto de investigación.

2.6 Análisis de resultados

El análisis de los resultados recogidos luego de la ejecución de auditoría pasa por lo destacado luego de las técnicas de auditoría (encuestas y observación), para terminar con toda la revisión documental de los procedimientos. Por parte de las técnicas de recolección de

información, más específicamente de las encuestas (GALIDM-GR-DOC-002), se tienen las siguientes conclusiones:

- La atención al usuario final no está siendo buena, no se tiene en cuenta las métricas para su resolución y satisfacción
- No se cuenta con personal lo suficientemente capacitado para las labores del área
- Se están presentando bastantes requerimientos por parte del usuario final, lo que deja ver que no se está haciendo muy bien la gestión de acceso lógico, presentando demoras en procesos del área propia y del banco en general.
- No hay uniformidad en los procesos, ya que cada integrante del área maneja información distinta y/o tiene una percepción muy diferente de cómo se manejan los procesos dentro del área.
- No se implementa algún tipo de metodología que ayude a realizar los procesos de mejor manera y enfocados al usuario final.

Por parte de la gestión documental se pudo apreciar que en su mayoría se cuenta con la documentación requerida y se encuentra completa pero no está siendo del todo aplicada, sin embargo, en varios casos como los planes de contingencia ante fallas, las metodologías aplicadas en el área, certificaciones de accesos, almacenamiento de repositorio, no se cuenta con la documentación, por tanto, son procesos que no se están teniendo en cuenta en el área y están afectando su operación.

PARTE III. CIERRE DE LA INVESTIGACIÓN

CAPÍTULO 3: INFORME DE AUDITORÍA

3.1 Informe técnico.

En la siguiente referencia se ubica el informe técnico asociado a la auditoría.

RPT: GALIDM-Informe técnico

3.2 Informe ejecutivo

En la siguiente referencia se ubica el informe técnico asociado a la auditoría.

RPT: GALIDM-Informe ejecutivo

CAPÍTULO 4. RESULTADOS Y DISCUSIÓN

Teniendo en cuenta lo recopilado en el apartado 2.6 *Análisis de resultado,* se procede a explicar un poco más a fondo los resultados encontrados luego de la ejecución de la auditoría:

- Los empleados en su mayoría no están lo suficientemente capacitados para llevar a cabo las labores propias del área, también tienen sobrecarga laboral ya que, aunque tienen un manual de funciones ya estipulado, este no se está respetando y se les está asignando labores que no son propias de ellos y para las cuales tampoco están capacitados.
- Los procesos están siendo improvisados ya que no se sujetan a alguna metodología o estándar, sólo se están realizando de manera intuitiva lo cual está llevando a que haya malentendidos, retrasos, desunión del equipo, baja calidad de producto y afectaciones no solamente a los procesos del área, sino del banco en general.
- No se tienen planes de contingencia ante distintas fallas que puedan ocurrir, principalmente del servicio de correo electrónico.
- No existen métricas lo suficientemente claras para la atención al cliente, existen algunas y ANS pero no se están aplicando, en parte, por el desconocimiento de las mismas por parte de los colaboradores
- No se están realizando procesos de certificación de accesos lo que lleva a incrementar bastante el margen de error a la hora de asignar accesos lógicos a los empleados del banco.

CAPÍTULO 5. CONCLUSIONES

En el presente capítulo se relacionan las conclusiones obtenidas a través del desarrollo de la presente investigación.

5.1 Verificación, contraste y evaluación de los objetivos

En el proyecto de grado se planteó como objetivo general el realizar una auditoría mediante la metodología de auditoría interna basada en riesgos, que identifique los riesgos y controles que afectan negativamente en la gestión de acceso lógico para el cliente interno de la entidad financiera ABC. Este objetivo se cumplió, dado que como resultado del presente trabajo se obtuvo el listado de los controles y riesgos que afectan negativamente la gestión de acceso lógico de para el cliente interno de dicha organización.

Respecto al primer objetivo específico; establecer la metodología de auditoría basada en riesgos que será aplicada, se comprueba que fue alcanzado, debido a que se estudió y aplicó una metodología puntual.

El segundo objetivo específico propone: aplicar la metodología de auditoría basada en riesgos en el servicio de gestión de acceso lógico del cliente interno de la entidad financiera ABC., lo cual también se llevó a cabo, en las evidencias registradas en el presente proyecto.

En el tercer objetivo específico propuso: Definir y ejecutar procedimientos de auditoría para los dos riesgos más críticos del área auditable más expuesta, dicho objetivo también fue cumplido.

Como cuarto objetivo específico se mencionó: Generar los informes del resultado de la auditoría, lo cual fue cumplido exitosamente, en dichos documentos se encuentran los hallazgos, conclusiones.

5.2 Síntesis del modelo propuesto

Dentro del modelo aplicado se efectuó la ejecución de las siguientes fases y en el orden relacionado:

1. Conocimiento global de la entidad.
2. Definición de los objetivos y las áreas auditables.
3. Evaluación de riesgos.
4. Planeación de la auditoría.
5. Ejecución de la auditoría.
6. Análisis de resultados.
7. Informe de auditoría.

5.3 Aportes originales

El principal aporte original producto de este trabajo de grado, se propone el resultado de la auditoría efectuada, los informes correspondientes, que contienen los hallazgos a mitigar y recomendaciones, para aplicar estas y mejorar el servicio de gestión de acceso lógico de la Entidad Financiera ABC., de acuerdo a las validaciones realizadas este tipo de auditorías interna basada en riesgos no se han realizado para dicha área, lo cual hace único el producto mencionado.

CAPÍTULO 6. PROSPECTIVA DEL TRABAJO DE GRADO

6.1 Líneas de investigación futuras

En esta parte del documento, se mencionan algunas líneas de investigación derivadas del presente trabajo.

6.2 Trabajos de investigación futuros

Con base al resultado de este trabajo, se identificó que es un campo muy amplio para desarrollar este tipo de investigación, por lo que se plantea como trabajos futuros de investigación:

• Potencializar los controles, procedimientos y recomendaciones propuestas.

• Ejecutar la fase de seguimiento propuesta por la metodología.

• Replicar el tipo de auditoría para otros procesos de la organización.

BIBLIOGRAFÍA

John Tschohl. "Servicio al cliente: el arma secreta de la empresa que alcanza la excelencia". Reporte especial. Capítulo 1 del libro. Miami, Florida.2006.

Juan Ramón Santillana González. Auditoría interna integral: administrativa, operacional y financiera. Edición 2. Mexico.2002.

The Institute of Internal Auditors, Perspectivas y Percepciones Globales Auditoría Interna y Auditoría externa. Funciones distintivas para la administración de una organización. Edición 8, 2017.

Grossberg Kenneth Alan, The Origins of Customer Service as Concept and Strategy. WASEDA BUSINESS & ECONOMIC STUDIES 2011 NO.47, 2012 Graduate School of Commerce Waseda University.

REFERENCIAS

Silva, D. (29 de marzo de 2021). *¿Qué es un cliente interno y cómo mejorar su satisfacción?* Blog de Zendesk. https://n9.cl/4iaif

Ontiveros, E., Martín, A., Navarro, M. y Rodríguez, E. (2012). *Las TIC y el sector financiero del*

*futuro.*Ariel. https://n9.cl/ouygw

Forbes. (28 de marzo de 2022). *La tecnología financiera que permite la innovación de la banca en Colombia.* https://n9.cl/07tnz

IBM. (7 de diciembre de 2021).*¿Qué es la seguridad de datos?* https://www.ibm.com/coes/topics/data-security

Leiva, J. (2018). *Auditoría interna sus ventajas y valores agregados.* [Tesis de seminario, Unicatólica. Archivo digital. https://n9.cl/y8vda

Gutiérrez, J (2022). *Auditoría basada en riesgos: la organización como un todo.* Universidad de Antioquia. https://n9.cl/o7nwl

Reimer y Mulcare. Active Directory for Windows, WINDOWS SERVER 2003, Technical

ICONTEC.(2006).NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. https://n9.cl/0vsen

IBM.(20 de abril de 2021). *Identificación y autenticación. https://n9.cl/rj0we*

BBVA. (2019). *Entidad Financiera*. BBVA. https://n9.cl/sj9gd

Solís, S.(2017). *Fundamentos de la ciberseguridad: Redes Controles de accesos físicos y lógicos.* LinkedIn. https://n9.cl/cnmo4

Tecnitrán. (2016). *La importancia de contar con un control de accesos*. Tecnitrán Telecomunicaciones. https://n9.cl/s99yi

Contadores Públitos Ltda. (2016). *Auditoría y Nomas Internacionales*. https://contabilidadparatodos.com/libro-auditoria-y-normas-internacionales/

The Institute of Internal Auditors. (2017). *Perspectivas y Percepciones Globales Auditoría Interna y auditoría externa*. Funciones distintivas para la administración de una organización Edición 8. Theiia.

Ley 87 de 1993. (1993,29 de noviembre). Gobierno de Colombia. Gestor Normativo. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=300

Vita Montiel, N. (2007). Tecnologías de información y comunicación para las organizaciones del siglo XXI. *CICAG, 5(1),77-86.*

Auditol.(2021). *Papeles de trabajo en auditoría. https://www.auditool.org/index.php?option=com_content&view=article&id=306:papeles-de-*