

UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS

CLASE: AUDITORÍA DE SISTEMAS

MASTER: KENIA MATUTE

INTEGRANTES:

NIXON ALDAHIR MARADIAGA PERALTA

20192000497

WILBERT ENRRIQUE CASTILLO NOLASCO

20151004055

**Índice**

[**Introducción 2**](#_heading=h.bnpcs5jxuhe8)

[**Objeto y alcance de la auditoría 3**](#_heading=h.kb7kli46n0qm)

[**Justificación de la auditoría 4**](#_heading=h.pjusxad1oiej)

[**Competencia de la auditoría 6**](#_heading=h.k9hhkd6fst8r)

[**Áreas en que aplicará la auditoría 7**](#_heading=h.pubbrdrp24k)

[**Estructura organizativa de la empresa 8**](#_heading=h.ej9uol6gt4yj)

[**Duración de la auditoría de sistemas 9**](#_heading=h.ru6gu9f54w9c)

[**Aplicaciones de soporte 10**](#_heading=h.8ximul5ci8ow)

[**Formato plan de acción propuesto 11**](#_heading=h.c3elnud40z3h)

[**Elaboración de informes 14**](#_heading=h.o6ta30kbf54x)

[**Planeación 19**](#_heading=h.x3zeyx3qrv1u)

[**Organigrama del área 21**](#_heading=h.yntp274otubg)

[**Cuestionarios que identifican y miden el control interno 22**](#_heading=h.rrhz5m80ytww)

[**Formato debilidad encontrada, situación actual 24**](#_heading=h.qu6hg3qr1iwr)

[**Ejecución 28**](#_heading=h.giw039urp82e)

[**Hallazgos 30**](#_heading=h.nog7l5vf2heg)

[**Formato de antecedentes, hallazgos, tipos de evidencia 31**](#_heading=h.1s5tvpwpd7x9)

[**Formato de pruebas de auditoría 35**](#_heading=h.7em06wwr8lhr)

[**Seguimiento de recomendaciones 44**](#_heading=h.3k8kmgqaswh8)

[**Flujograma de procesos 45**](#_heading=h.gjdgxs)

[**Resultados de la auditoría 46**](#_heading=h.j5nd98sfcpn7)

[**Presentación Detallada de Resultados de Auditoría en el Área de Bases de Datos 46**](#_heading=)

[**Presentación Detallada de Resultados de Auditoría en el Área de Seguridad en La Red 48**](#_heading=)

[**Resultados Detallados de la Auditoría de Seguridad en la Red 48**](#_heading=)

[**Se recomienda al Banco BAC implementar las siguientes medidas correctivas para mitigar los riesgos identificados: 50**](#_heading=h.cz04wloncmak)

[**Glosario 52**](#_heading=h.9i0ff9nl3zur)

[**Conclusiones 54**](#_heading=h.uec52vz0yc3p)

[**Recomendaciones finales 55**](#_heading=h.7xhf7van6mqy)

## Introducción

El presente informe presenta los resultados de la auditoría realizada en las áreas de bases de datos y seguridad en la red de Banco BAC Credomatic. La auditoría se llevó a cabo con el objetivo de evaluar el nivel de cumplimiento de las normas y estándares de seguridad de la información establecidos por la organización, así como identificar posibles vulnerabilidades y riesgos que pudieran afectar la confidencialidad, integridad y disponibilidad de la información del banco.

## 

## Objeto y alcance de la auditoría

El objeto de esta auditoría es evaluar la eficiencia del departamento de IT, específicamente en las áreas de seguridad de red y bases de datos de la empresa financiera Bac Credomatic. La presente auditoría tiene como fin identificar vulnerabilidades y riesgos de seguridad con el fin de garantizar que se cumplan los estándares de seguridad en la red y las normas de seguridad y privacidad de los datos financieros e información confidencial de los clientes y empleados.

La auditoría se basará en revisar la infraestructura de red, configuraciones de los equipos de red, gestiones de seguridad y salvaguardar la privacidad de la información de la base de datos de la empresa.

El alcance de la auditoría se enfocará en revisar los procedimientos y las políticas relacionadas a la seguridad de red y datos dentro del banco, estos son algunos procesos que se analizaran:

**Arquitectura de red:** evaluación de la arquitectura de red del banco, segmentación, análisis de la topología y redundancias para poder identificar posibles puntos de fallo.

**Configuración de dispositivos:** revisión de las configuraciones de seguridad como firewalls, prevención de intrusiones en los dispositivos de red para verificar que estén correctamente configurados y actualizados.

**Conexiones de red:** evaluar los niveles de seguridad en conexiones internas y externas, incluyendo conexiones remotas como VPN para asegurar la confidencialidad y seguridad.

**Gestión de usuarios y privilegios:** evaluación de la gestión de usuarios y privilegios en las bases de datos para prevenir accesos no autorizados

**Políticas y procedimientos de respaldo**: asegurar la disponibilidad y la integridad de los datos en caso de algún fallo del sistema.

La auditoría no solo se basará en que se cumplan las medidas de seguridad, también se buscará que las áreas auditadas tengan la capacidad de adaptarse a los cambios constantes en el entorno empresarial del banco dándole una mejora continua a los procesos. Esto permitirá que el banco Bac Credomatic mantenga su lugar en el mercado financiero.

## Justificación de la auditoría

**Cumplimiento normativo**

**\* Regulaciones de protección de datos:**

   Ley de Protección de Datos Personales (Decreto No. 169-2019)

**\* Estándares de seguridad de la información:**

    ISO/IEC 27001:2013

    NIST Cybersecurity Framework

**Ámbito de la auditoría:**

* **Bases de datos:**
  + Evaluación de la seguridad, integridad, disponibilidad y confidencialidad de los datos.
  + Análisis de los controles de acceso, gestión de cambios y respaldos.
* **Seguridad de la red:**
  + Verificación de la eficacia de las medidas de seguridad perimetral, control de acceso a la red y protección contra malware.
  + Evaluación de la segmentación de la red y la gestión de vulnerabilidades.

**Objetivos de la auditoría:**

* **Cumplimiento normativo:**
  + Cumplimiento con la normativa aplicable al sector financiero y de las TI.
  + Verificación del cumplimiento de los estándares de seguridad de la información.
* **Gestión de riesgos:**
  + Identificación y evaluación de los riesgos asociados a las bases de datos y la seguridad de la red.
  + Implementación de medidas para mitigar los riesgos identificados.
* **Mejora continua:**
  + Optimización de los procesos y procedimientos relacionados con la gestión de bases de datos y la seguridad de la red.
  + Implementación de mejoras en la infraestructura tecnológica.

**Beneficios de la auditoría:**

* Mayor seguridad y protección de la información confidencial.
* Reducción del riesgo de incidentes de seguridad.
* Mejora en la disponibilidad y confiabilidad de los sistemas de información.
* Cumplimiento con las regulaciones vigentes.
* Optimización de los recursos de TI

## Competencia de la auditoría

La auditoría en las áreas de seguridad de red y bases de datos implica evaluar la seguridad, integridad y confidencialidad de la infraestructura de sistemas para almacenar y gestionar la información financiera y personal de los clientes. Estas son algunas competencias que se necesita para este tipo de auditoría:

**Conocimiento de normativas y estándares:** Un auditor de sistemas de red y bases de datos en un banco debe tener un profundo conocimiento de las normativas y estándares relevantes de la industria financiera, esto incluye comprender los requisitos de seguridad y privacidad de los datos y cómo se aplican al banco.

**Arquitectura de redes:** conocimientos de protocolos de red, topologías, dispositivos de red y sistemas de detección de instrucciones.

**Base de datos y sistemas de gestión de datos:** conocimiento en bases de datos relacionales y no relacionales para evaluar la seguridad y rendimiento de la base de datos del banco.

**Ética y profesionalismo:** Es esencial mantener altos estándares éticos y profesionales en todas las etapas de la auditoría, incluyendo la confidencialidad de la información sensible del banco y la imparcialidad en la evaluación de los controles de seguridad.

## Áreas en que aplicará la auditoría

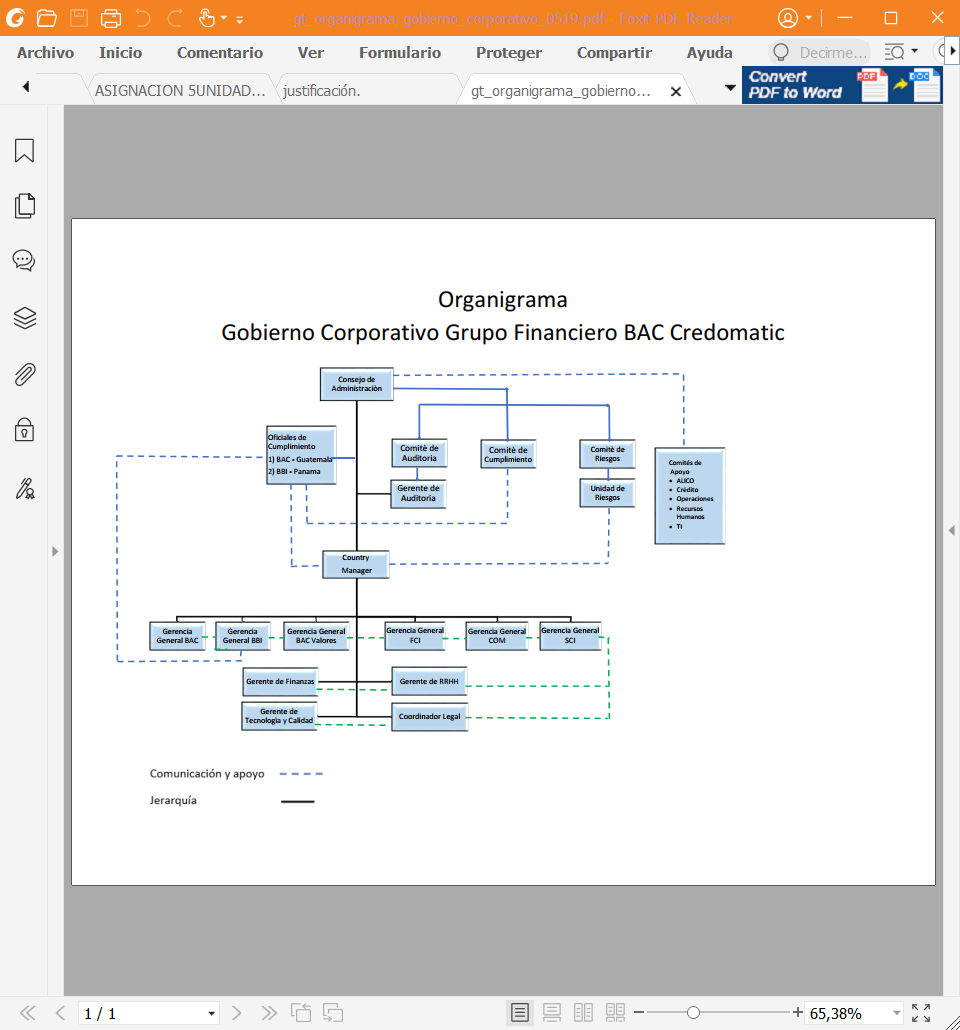
1. **Área de seguridad de red**

En el área de IT en la seguridad de la red los problemas de seguridad pueden ser muy graves debido a la sensibilidad de la información financiera y personal que manejan, algunos dispositivos de red como routers, switches y firewalls pueden estar mal configurados lo que puede permitir accesos no autorizados o dejar puertas abiertas para ataques, otros problemas pueden ser la falta de actualizaciones en los parches de seguridad y falta de segmentación de la red de Bac Credomatic.

**2) Área de base de datos**

En el área de IT se pueden encontrar una serie de problemas que pueden ser la calidad de los datos afectando así la integridad y la confiabilidad de la información, la seguridad de los datos ya que al ser una entidad bancaria tiene que cumplir con normas o regulaciones estrictas sobre la protección de los datos ya que maneja información sensible como ser la información financiera y personal de los clientes y problemas en los respaldos y recuperación de los datos.

## Estructura organizativa de la empresa



## Duración de la auditoría de sistemas

| **Auditoria de sistemas** | |
| --- | --- |
| Fecha de inicio: | 01 de mayo 2024 |
| Fecha de cierre: | 31 de julio 2024 |
| Duración: | 3 meses |

## Aplicaciones de soporte

(Licencias y software propios desarrollar los trabajos de programación)

| **Item** | **Cantidad** | **Descripción** | **Precio Unitario** | **Total** |
| --- | --- | --- | --- | --- |
| 1 | 5 | licencias de kaspersky antivirus | 1,230.00 | 6,150.00 |
| 2 | 1 | Disco duro externo SSD 1 Terabyte | 1,722.00 | 1,722.00 |
| 3 | 4 | Laptop HP | 16,990.00 | 67,960.00 |
| 4 | 1 | Laptop Dell Inspiron 3520 | 15,495.00 | 15,495.00 |
| 5 | 4 | Ups Forza | 3,000.00 | 12,000.00 |
| 6 | 2 | Licencia de SQL server Enterprise | 4,920.00 | 9,840.00 |
| 7 | 1 | Licencia office | 2,460.00 | 2,460.00 |
|  |  |  | **Sub-total** | **115,627.00** |
|  |  |  | **Isv** | **17,344.05** |
|  |  |  | **Total** | **132,971.05** |

## Formato plan de acción propuesto

## 

| **CRONOGRAMA DE ACTIVIDADES ÁREA DE RED** | | | | |
| --- | --- | --- | --- | --- |
| **Actividad** | **Fase** | **Responsable** | **Duración** |
| Revisión de políticas y procedimientos de seguridad | Examinar las políticas y los procedimientos de seguridad en la red y el sistema del banco. | Nixon Maradiaga | 10.5 días |
| Análisis de la topología de red | Identificar los posibles fallos en la topología del banco como la congestión de datos. | Wilbert | 4 días |
| Verificar los riesgos de seguridad relacionados a la conectividad de la red. | 5 días |
| Análisis de la arquitectura de red | Inspeccionar la arquitectura de red para identificar las posibles vulnerabilidades. | Nixon Maradiaga | 9 días |
| Revisar los puntos de entrada no autorizados. | 1.5 días |
| Revisión de controles de acceso remoto | Evaluar los controles de acceso remoto, como VPN y conexiones de acceso remoto. | Wilbert | 12 días |
| Revisión de seguridad wifi | Evaluar la seguridad de las redes inalámbricas que se utilizan en las instalaciones del banco. | Nixon Maradiaga | 10.5 días |
| Gestión de incidentes de seguridad | Evaluar la capacidad del banco para detectar, investigar y responder a los problemas de seguridad. | Wilbert | 9 días |
| Pruebas de seguridad física | Determinar la protección de los dispositivos de red contra acceso no autorizado. | Nixon Maradiaga | 10.5 días |
| Informe de resultados y recomendaciones. | Presentación del informe sobre los hallazgos a la gerencia general. | Nixon Maradiaga | 10 días |
| Presentar las recomendaciones a la gerencia general. | 2 días |

| **CRONOGRAMA DE ACTIVIDADES EN EL ÁREA DE BASE DE DATOS** | | | | |
| --- | --- | --- | --- | --- |
| **Actividad** | **Fase** | **Responsable** | **Duración** |
| Revisión de procedimientos en la gestión de datos | Revisar los procedimientos en la creación, almacenamiento, acceso y uso de datos y la eliminación de los mismos. | Nixon Maradiaga | 10.5 días |
| Análisis de la calidad de los datos | Evaluar la integridad y consistencia de los datos. | Wilbert | 7 días |
| Evaluar si el banco cumple con los estándares establecidos en la gestión de datos. | 2 días |
| Seguridad de los datos | Auditar los controles de seguridad para asegurar que solo empleados autorizados tengan acceso a los datos financieros. | Nixon Maradiaga | 10.5 días |
| Procesos de respaldo y recuperación de datos | Inspeccionar la frecuencia de las copias de seguridad y la capacidad para restaurar datos. | Nixon Maradiaga | 10 días |
| Verificar si se cuenta con respaldos de datos en la nube. | Wilbert | 2 días |
| Análisis de controles de acceso a los datos | Revisar los controles de acceso para verificar si se cumplen las políticas de seguridad. | Nixon Maradiaga | 10.5 días |
| Revisión de arquitectura de datos | Analizar la arquitectura de datos del banco para identificar áreas de mejora en escalabilidad y seguridad. | Wilbert | 9 días |
| Controles de privacidad de datos | Verificar que se apliquen los controles de privacidad de la información personal del cliente y empleados del banco. | Wilbert | 10.5 días |
| Monitoreo de datos | Identificación de intentos de acceso no autorizado. | Nixon Maradiaga | 12 días |

## Elaboración de informes

| **Informe semanal de auditoría De sistemas del área de bases de datos** |
| --- |
| **Empresa:** BAC CREDOMATIC |
| **Semana:** 8/06/24 – 15/06/24 |
| **Equipo responsable:** Auditor Wilbert Castillo |
| **Resumen :** La presente auditoría se llevó a cabo con el objetivo de evaluar la seguridad de las bases de datos del Banco BAC. Se identificaron diversas debilidades que podrían poner en riesgo la confidencialidad, integridad y disponibilidad de la información almacenada en las bases de datos. Se recomienda a la gerencia del banco implementar las medidas correctivas necesarias para mitigar estos riesgos. |
| **Actividades realizadas en la semana** |
| * Revisión de la política de seguridad de bases de datos. * Entrevistas con usuarios y administradores de bases de datos. * Análisis de permisos de acceso a las bases de datos. * Revisión de registros de acceso. * Análisis de configuraciones de registro. * Pruebas de penetración en las bases de datos. |
| **Hallazgos y recomendaciones** |
| Contraseñas débiles para usuarios de bases de datos: Algunos usuarios de bases de datos utilizan contraseñas débiles que no cumplen con los requisitos mínimos de complejidad establecidos en la política de seguridad. Esta debilidad representa un riesgo significativo para la seguridad de las bases de datos, ya que las contraseñas débiles pueden ser fácilmente adivinadas o descifradas por atacantes.  Falta de controles de acceso adecuados: Se observó que algunos usuarios tienen acceso a bases de datos que no necesitan para realizar sus tareas laborales. Esto aumenta el riesgo de accesos no autorizados y posibles fugas de datos.  Falta de registros de auditoría: No se encontraron registros de auditoría que permitan rastrear las actividades de los usuarios en las bases de datos. Esto dificulta la detección y la investigación de posibles incidentes de seguridad.  **Recomendaciones**  Adoptar la autenticación multifactor (MFA): Implementar MFA como capa adicional de seguridad para el acceso a las bases de datos, requiriendo no solo una contraseña, sino también un segundo factor de autenticación, como un código generado por una aplicación o dispositivo móvil.  Implementar el principio de mínimo privilegio: Otorgar a cada usuario solo los permisos de acceso estrictamente necesarios para realizar sus tareas laborales.  Implementar controles de acceso basados en roles (RBAC): Definir roles con permisos específicos y asignarlos a los usuarios en función de sus responsabilidades.  Establecer alertas y notificaciones: Configurar alertas y notificaciones para detectar comportamientos inusuales o accesos no autorizados en tiempo real. |

| **Informe mensual de auditoria de sistemas de gestión de calidad** |
| --- |
| **Empresa:** BAC CREDOMATIC |
| **Mes:** 8/07/24 – 08/08/24 |
| **Equipo responsable:** Auditor líder: Wilbert Castillo |
| **Resumen:** Este informe mensual resume los hallazgos y observaciones de la auditoría de seguridad en la red del Banco BAC realizada durante el mes de [Mes actual]. Se identificaron diversas debilidades en la configuración y gestión de la red que podrían poner en riesgo la seguridad de la información y la continuidad operativa del banco. Se recomienda a la gerencia del banco implementar las medidas correctivas necesarias para mitigar estos riesgos. |
| **Actividades realizadas en el mes** |
| * Revisión de las políticas de seguridad de red. * Entrevistas con administradores de red y personal de seguridad. * Análisis de configuraciones de seguridad de dispositivos de red. * Pruebas de vulnerabilidad en la red. * Análisis de registros de seguridad. |
| **Hallazgos y recomendaciones** |
| Configuraciones de seguridad del firewall no óptimas: Se identificaron configuraciones de seguridad en el firewall que no están alineadas con las mejores prácticas recomendadas por los fabricantes y expertos en seguridad. Esta debilidad podría permitir que los atacantes exploten vulnerabilidades en las configuraciones del firewall para acceder a la red interna del banco.  Falta de actualizaciones de software: Se detectó que algunos equipos de red no están actualizados con los últimos parches de seguridad. Esto los hace vulnerables a ataques conocidos que podrían ser explotados por los atacantes.  Falta de segmentación de red: La red no está segmentada en diferentes zonas de seguridad, lo que aumenta el riesgo de que un atacante que comprometa un segmento de la red pueda acceder a otros segmentos.  Monitoreo y registro insuficiente de la actividad de la red: No se está realizando un monitoreo y registro adecuado de la actividad de la red, lo que dificulta la detección y la investigación de posibles incidentes de seguridad.  **Recomendaciones**  Revisar y ajustar las configuraciones del firewall de acuerdo con las mejores prácticas recomendadas.  Implementar un proceso de actualización de software más riguroso para garantizar que todos los equipos de red estén actualizados.  Implementar una estrategia de segmentación de red para aislar diferentes zonas de seguridad.  Implementar un sistema de monitoreo y registro de la actividad de la red que permita identificar y responder a posibles incidentes de seguridad.  Realizar capacitaciones periódicas al personal de seguridad y administradores de red sobre las mejores prácticas de seguridad en la red.  Contratar a una empresa especializada en seguridad de redes para realizar auditorías de seguridad periódicas y brindar soporte en la implementación de medidas de seguridad. |

| **Informe trimestral de auditoría de sistemas de gestión de calidad** |
| --- |
| **Empresa:** BAC Credomatic |
| **Meses:** 8/06/24 – 8/09/24 |
| **Equipo Responsable:** Auditor: Wilbert Castillo |
| **Resumen:** Este informe trimestral resume los hallazgos y observaciones de la auditoría de seguridad en el área de bases de datos del Banco BAC realizada durante el trimestre. Se identificaron diversas debilidades en la gestión y seguridad de las bases de datos que podrían poner en riesgo la confidencialidad, integridad y disponibilidad de la información almacenada. Se recomienda a la gerencia del banco implementar las medidas correctivas necesarias para mitigar estos riesgos. |
| **Actividades realizadas en el trimestre** |
| * Revisión exhaustiva de las políticas de seguridad de bases de datos. * Entrevistas en profundidad con administradores de bases de datos y usuarios clave. * Análisis minucioso de los permisos de acceso a las bases de datos. * Revisión exhaustiva de los registros de acceso y auditoría. * Pruebas de penetración avanzadas en las bases de datos. |
| **Hallazgos y recomendaciones** |
| 1. Documentos de Calidad   Hallazgo: Complejidad persistente en la documentación, afectando la accesibilidad.   Observación: Se requiere un enfoque más simplificado y accesible para mejorar la eficacia.     1. Procesos Clave:   Hallazgo: Algunos procedimientos aún no están alineados con las mejores prácticas.  Observación: La actualización continua es necesaria para mantenerse al día con las mejores prácticas y estándares.     1. Indicadores de Desempeño   Hallazgo: Persisten discrepancias en la medición del desempeño.    Observación: Se sugiere una revisión integral para garantizar la coherencia y la relevancia de los indicadores. |

## Planeación

**(Descripción puestos existentes en el área de IT)**

La planeación de puestos en el área de IT es esencial para garantizar la eficiencia operativa de los sistemas y equipos de cómputo en una organización y a su vez garantizar la adaptación continua en un entorno tecnológico en constante cambio. Los siguientes puestos son:

**Jefe de Tecnología de la Información (CIO):**

* Responsable máximo del área de TI.
* Define la estrategia tecnológica de la empresa.
* Supervisa la implementación de proyectos y la operación de sistemas.

**Arquitecto de Sistemas:**

* Diseña la arquitectura de sistemas informáticos.
* Analiza y propone soluciones tecnológicas.
* Asegura la integración y compatibilidad entre sistemas.

**Administrador de Bases de Datos:**

* Responsable de la administración y mantenimiento de bases de datos.
* Gestiona el rendimiento, seguridad y respaldo de la información.
* Especialista en Seguridad de la Información:
* Protege la infraestructura tecnológica de amenazas y vulnerabilidades.
* Desarrolla políticas de seguridad y procedimientos para proteger los datos.

**Analista de Sistemas:**

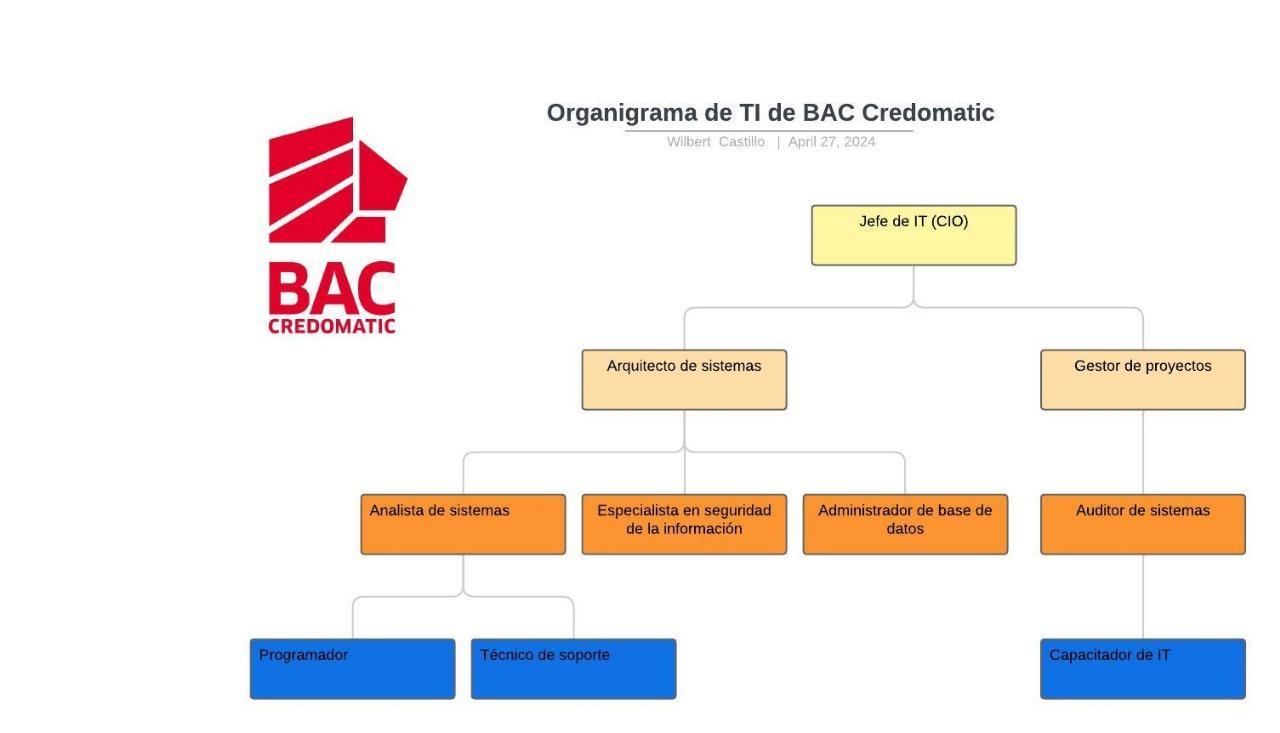
* Analiza los requisitos de los usuarios y diseña soluciones informáticas.
* Documenta los procesos y especificaciones de los sistemas.

**Programador:**

* Desarrolla y mantiene software según los requisitos especificados.
* Codifica, depura y prueba programas para garantizar su correcto funcionamiento.

## Organigrama del área

**(funciones asignadas del área)**



## Cuestionarios que identifican y miden el control interno

| **Formato de control interno para el área de seguridad en la red** |
| --- |
| Nombre de la empresa: |
| Fecha: |
| Responsable: |

| Actividad | Si | No | Observaciones |
| --- | --- | --- | --- |
| **Gestión de la seguridad de transmisión de los datos** |  |  |  |
| ¿Se ha implementado una política de seguridad de red formal y documentada? |  |  |  |
| ¿Se han realizado análisis de riesgos para identificar las amenazas y vulnerabilidades de la red? |  |  |  |
| ¿Se han implementado controles de seguridad de red adecuados, como firewalls, sistemas de detección de intrusiones y listas de control de acceso? |  |  |  |
| ¿Se realizan pruebas de penetración y otras evaluaciones de seguridad de la red de forma regular? |  |  |  |
| ¿Existe un plan de respuesta a incidentes de seguridad de red que se aprueba y actualiza periódicamente? |  |  |  |

| **Formato de control interno para el área de base de datos** |
| --- |
| Nombre de la empresa: |
| Fecha: |
| Responsable: |

| Actividad | Si | No | Observaciones |
| --- | --- | --- | --- |
| **Protección en los sistemas gestores de datos** |  |  |  |
| ¿Se ha implementado una política de seguridad de bases de datos formal y documentada? |  |  |  |
| ¿Se han realizado análisis de riesgos para identificar las amenazas y vulnerabilidades de las bases de datos? |  |  |  |
| ¿Se han implementado controles de seguridad de bases de datos adecuados, como control de acceso basado en roles, cifrado de datos y copias de seguridad? |  |  |  |
| ¿Se realizan auditorías de seguridad de las bases de datos de forma regular? |  |  |  |
| ¿Existe un plan de respuesta a incidentes de seguridad de bases de datos que se prueba y actualiza periódicamente? |  |  |  |

## Formato debilidad encontrada, situación actual

| **Formato de control situaciones encontradas para el área de bases de datos** |
| --- |
| Nombre de la empresa: Bac Credomatic |
| Fecha: 27/04/2024 |
| Responsable: Julio Sanchez |

| **Debilidad** | **Situación Actual** | **Comentario del grupo de trabajo de auditoría** | **Comentario de la gerencia de la empresa** |
| --- | --- | --- | --- |
| Se detectó que algunos usuarios de bases de datos utilizan contraseñas débiles que no cumplen con los requisitos mínimos de complejidad establecidos en la política de seguridad. | La política de seguridad de bases de datos establece requisitos mínimos de complejidad para las contraseñas, como longitud mínima, uso de caracteres especiales y mayúsculas/minúsculas | Es un riesgo significativo para la seguridad de las bases de datos, ya que las contraseñas débiles pueden ser fácilmente adivinadas o descifradas por atacantes. Se recomienda implementar medidas para garantizar que todos los usuarios cumplan con los requisitos de complejidad de las contraseñas. | Se reconoce la importancia de esta debilidad y se tomarán medidas para fortalecer la política de contraseñas e implementar mecanismos de control para garantizar su cumplimiento. |
| Se observó que algunos usuarios tienen acceso a bases de datos que no necesitan para realizar sus tareas laborales. Esto aumenta el riesgo de accesos no autorizados y posibles fugas de datos. | La política de control de acceso establece que los usuarios solo deben tener acceso a las bases de datos que necesitan para realizar sus tareas laborales. | Los usuarios no autorizados podrían acceder a información confidencial. Se recomienda revisar y actualizar los permisos de acceso a las bases de datos para garantizar que solo los usuarios autorizados tengan acceso a la información que necesitan. | Se revisarán los permisos de acceso a las bases de datos y se tomarán las medidas necesarias para restringir el acceso a la información confidencial. |
| No se encontraron registros de auditoría que permitan rastrear las actividades de los usuarios en las bases de datos. Esto dificulta la detección y la investigación de posibles incidentes de seguridad. | La política de seguridad de bases de datos establece que se deben generar registros de auditoría para todas las actividades de los usuarios. | La falta de registros de auditoría limita la capacidad del banco para identificar y responder a posibles incidentes de seguridad. Se recomienda implementar una solución de registro de auditoría que permita rastrear todas las actividades de los usuarios en las bases de datos. | Se implementará una solución de registro de auditoría para mejorar la visibilidad y el control sobre las actividades en las bases de datos. |

| **Formato de control situaciones encontradas para el área de seguridad en la red** |
| --- |
| Nombre de la empresa: Bac Credomatic |
| Fecha: 27/04/2024 |
| Responsable: Julio Sanchez |

| **Debilidad** | **Situación Actual** | **Comentario del grupo de trabajo de auditoría** | **Comentario de la gerencia de la empresa** |
| --- | --- | --- | --- |
| Se identificaron configuraciones de seguridad en el firewall que no están alineadas con las mejores prácticas recomendadas por los fabricantes y expertos en seguridad. | El firewall es un componente crítico de la seguridad de la red, y su configuración debe ser óptima para proteger la red contra amenazas externas. | Los atacantes podrían explotar vulnerabilidades en las configuraciones del firewall para acceder a la red interna del banco. Se recomienda revisar y ajustar las configuraciones del firewall de acuerdo con las mejores prácticas recomendadas. | Se revisarán las configuraciones del firewall y se realizarán los ajustes necesarios para fortalecer la seguridad de la red. |
| Se detectó que algunos equipos de red no están actualizados con los últimos parches de seguridad. Esto los hace vulnerables a ataques conocidos que podrían ser explotados por los atacantes. | La política de seguridad de la red establece que todos los equipos de red deben mantenerse actualizados con los últimos parches de seguridad. | Los atacantes podrían explotar vulnerabilidades conocidas en los equipos de red para acceder a la información confidencial del banco. Se recomienda implementar un proceso de actualización de software más riguroso para garantizar que todos los equipos estén actualizados. | Se implementará un proceso de actualización de software más riguroso para garantizar la seguridad de la red. |
| La red no está segmentada en diferentes zonas de seguridad, lo que aumenta el riesgo de que un atacante que comprometa un segmento de la red pueda acceder a otros segmentos. | La segmentación de la red es una práctica recomendada para aislar diferentes partes de la red y reducir el impacto de posibles incidentes de seguridad. | La falta de segmentación de la red aumenta el riesgo de que un incidente de seguridad pueda afectar a toda la red. Se recomienda implementar una estrategia de segmentación de red para aislar diferentes zonas de seguridad. | Se contratará a una empresa especializada en seguridad de redes para diseñar e implementar una estrategia de segmentación de red adecuada para las necesidades del banco. |

## Ejecución

**Área de base de datos**

**1. Contraseñas débiles:**

* No se aplican contraseñas robustas para los accesos a las bases de datos, esto expone de manera significativa la seguridad de la empresa ya que las contraseñas débiles pueden ser descifradas o adivinadas.

**2. Falta de actualizaciones de seguridad:**

* Se cuentan con parches de seguridad, pero se encuentran desactualizados y otros segmentos no cuentan con los parches, lo que deja a la empresa vulnerable a ataques.

**3. Políticas de seguridad:**

* No cumplen con las políticas de seguridad en la complejidad de las contraseñas.

**4. Permisos de acceso:**

* Algunos usuarios tienen acceso a todos los datos del banco, esto puede generar fugas de información sensible de empleados e información confidencial de los clientes.

**Área de seguridad en la red**

**1. Falta de actualizaciones de seguridad:**

* No se aplican con frecuencia los parches de seguridad a los dispositivos de red, dejando al banco vulnerable a ciberataques.

**2. Configuraciones inseguras:**

* Configuraciones débiles en firewalls, routers y switches, esto deja puertas traseras abiertas para ataques.

**3. Gestión de contraseñas:**

* Contraseñas débiles o compartidas en los dispositivos de red y faltas de políticas de cambio de contraseñas.

**4. Falta de capacitación:**

* No se capacitan a los empleados en prácticas de seguridad en los dispositivos de red.

**5. Software y hardware desactualizado:**

* Utilizan sistemas y dispositivos que ya no reciben soporte técnico y por ende se encuentran desactualizados.

**Pasos de mejora**

**1. Implementar nuevas tecnologías:**

El jefe de IT se debe encargar de implementar nuevas tecnologías y nuevos equipos informáticos en el banco para reducir los problemas de seguridad en la red y las bases de datos.

**2. Actualizaciones de sistemas y parches de seguridad:**

Mantener actualizados todos los sistemas y dispositivos de red con los parches de seguridad modernos para mitigar amenazas

**3. Auditorías internas:**

Realizar auditorías internas para identificar y corregir problemas.

**4. Capacitación del personal:**

Capacitar al personal de IT para mejorar la seguridad en las áreas auditadas.

**5. Establecer procedimientos:**

Establecer procedimientos para asegurar la eficacia en el área de red y base de datos para mitigar problemas de seguridad.

## Hallazgos

La presente auditoría se llevó a cabo para evaluar la seguridad de la red y sus registros en la base de datos del área de IT de Bac Credomatic. El objetivo de la auditoría fue identificar las posibles vulnerabilidades y riesgos de seguridad que puedan llegar a comprometer la confidencialidad y la integridad de los datos.

Estos hallazgos proporcionan una visión amplia de las áreas que requieren acciones de mejora para garantizar los servicios que brinda Bac Credomatic.

**Seguridad de la red**

**Configuraciones de firewall:** se identificaron puertos abiertos no autorizados en el firewall, lo que podría permitir el acceso no autorizado a la red interna del banco.

**Parches de seguridad:** varios dispositivos dentro de la infraestructura de red del banco no cuentan con los parches de seguridad actualizados.

**Dispositivos con versiones desactualizadas:** se encontraron múltiples dispositivos con versiones desactualizadas de firmware.

**Segmentación de la red:** La infraestructura de red no está adecuadamente segmentada, se observó que todos los dispositivos como servidores y estaciones de trabajo están ubicados en la misma red sin separaciones lógicas de seguridad.

**Base de datos**

**Contraseñas de seguridad:** se detectó que en las bases de datos carecían de políticas de contraseñas robustas, lo que puede facilitar el acceso no autorizado por contraseñas débiles.

**Controles de acceso:** se descubrieron permisos excesivos en algunas cuentas de usuarios de la base de datos, acceso a información que no necesitan para realizar sus labores diarias, lo que puede aumentar significativamente el uso indebido de datos.

**Parches de seguridad:** Algunas bases de datos se encuentran sin parches de seguridad o con parches desactualizados, dejando vulnerable a filtraciones de datos.

## Formato de antecedentes, hallazgos, tipos de evidencia

| **Formato de antecedentes para el área de bases de datos** |
| --- |
| Nombre de la empresa: Bac Credomatic |
| Fecha: 27/04/2024 |
| Responsable: Julio Sanchez |

| **Antecedente** | **Hallazgos** | **Tipo de Evidencia** | **No conformidad/Oportunidad** |
| --- | --- | --- | --- |
| Políticas de seguridad de bases de datos: El banco cuenta con una política de seguridad de bases de datos que establece los requisitos mínimos para la protección de las bases de datos. | Contraseñas débiles para usuarios de bases de datos: Algunos usuarios de bases de datos utilizan contraseñas débiles que no cumplen con los requisitos mínimos de complejidad establecidos en la política de seguridad. | Entrevistas con usuarios, análisis de registros de acceso. | Oportunidad para el sistema. |
| Controles de acceso a bases de datos: El banco implementa controles de acceso para restringir el acceso a las bases de datos a los usuarios autorizados. | Falta de controles de acceso adecuados: Algunos usuarios tienen acceso a bases de datos que no necesitan para realizar sus tareas laborales. | Análisis de permisos de acceso, revisión de registros de acceso. | Oportunidad para el sistema. |
| Registros de auditoría de bases de datos: El banco genera registros de auditoría para rastrear las actividades de los usuarios en las bases de datos. | Falta de registros de auditoría: No se encontraron registros de auditoría que permitan rastrear las actividades de los usuarios en las bases de datos. | Revisión de registros de auditoría, análisis de configuraciones de registro. | Oportunidad para el sistema. |

| **Formato de antecedentes para el área de seguridad en la red** |
| --- |
| Nombre de la empresa: Bac Credomatic |
| Fecha: 27/04/2024 |
| Responsable: Julio Sanchez |

| **Antecedente** | **Hallazgos** | **Tipo de Evidencia** | **No conformidad/Oportunidad** |
| --- | --- | --- | --- |
| Políticas de seguridad de red: El banco cuenta con una política de seguridad de red que establece los requisitos mínimos para la protección de la red. | Configuraciones de seguridad del firewall no óptimas: Se identificaron configuraciones de seguridad en el firewall que no están alineadas con las mejores prácticas recomendadas por los fabricantes y expertos en seguridad. | Análisis de configuraciones del firewall, revisión de manuales del fabricante. | Oportunidad para el sistema. |
| Gestión de parches de seguridad: El banco implementa un proceso de gestión de parches de seguridad para mantener los equipos de red actualizados con los últimos parches de seguridad. | Falta de actualizaciones de software: Algunos equipos de red no están actualizados con los últimos parches de seguridad. | Análisis de registros de actualizaciones, revisión de políticas de gestión de parches. | Oportunidad para el sistema. |
| Segmentación de red: La red no está segmentada en diferentes zonas de seguridad. | Falta de segmentación de red: La red no está segmentada en diferentes zonas de seguridad, lo que aumenta el riesgo de que un atacante que comprometa un segmento de la red pueda acceder a otros segmentos. | Análisis de la topología de la red, revisión de políticas de segmentación. | Oportunidad para el sistema. |

## Formato de pruebas de auditoría

| **Nombre de la auditoría:** Auditoría de Seguridad de Bases de Datos | |
| --- | --- |
| **Fecha:** 2024-07-28 | **Auditor:** Wilbert Castillo |
| **Área auditada:** Área de Bases de Datos | |
| **Objetivo:** Evaluar la seguridad de las bases de datos del Banco BAC. | |
| **Alcance:** La auditoría abarca las políticas de seguridad de bases de datos, los controles de acceso, la gestión de parches de seguridad, la segmentación de bases de datos, el monitoreo y registro de la actividad, y las prácticas de los usuarios. | |
| **Metodología:** La auditoría se realizó mediante una combinación de técnicas, incluyendo entrevistas, análisis de documentos, revisión de registros, y pruebas de penetración. | |

| **Prueba** | **Descripción** | **Resultado** | **Evidencia** |
| --- | --- | --- | --- |
| **Prueba 1:** Revisión de la política de seguridad de bases de datos | Se verificó si la política de seguridad de bases de datos está actualizada y es adecuada para proteger las bases de datos del banco. | La política de seguridad de bases de datos está actualizada, pero no cubre todos los aspectos de la seguridad de las bases de datos. Se recomienda revisar y actualizar la política para incluir todos los aspectos relevantes, como la gestión de contraseñas, el control de acceso, la gestión de parches de seguridad, la segmentación de bases de datos y el monitoreo de la actividad. | Entrevista con el administrador de bases de datos, copia de la política de seguridad de bases de datos. |
| **Prueba 2:** Análisis de los permisos de acceso a las bases de datos | Se verificó si los usuarios tienen acceso solo a las bases de datos que necesitan para realizar su trabajo. | Se detectó que algunos usuarios tienen acceso a bases de datos que no necesitan para realizar su trabajo. Se recomienda revisar y ajustar los permisos de acceso para garantizar que solo los usuarios autorizados tengan acceso a la información que necesitan. | Análisis de permisos de acceso a las bases de datos. |
| **Prueba 3:** Revisión de los registros de parches de seguridad | Se verificó si las bases de datos están actualizadas con los últimos parches de seguridad. | Se detectó que algunas bases de datos no están actualizadas con los últimos parches de seguridad. Se recomienda implementar un proceso de actualización de parches de seguridad más riguroso para garantizar que todas las bases de datos estén actualizadas y protegidas contra las últimas amenazas. | Revisión de los registros de parches de seguridad. |
| **Prueba 4:** Prueba de penetración en las bases de datos | Se simularon ataques a las bases de datos para identificar vulnerabilidades. | Se identificaron algunas vulnerabilidades en las bases de datos, como contraseñas débiles, configuraciones de seguridad inadecuadas y falta de segmentación de datos. Se recomienda implementar las medidas correctivas necesarias para mitigar estas vulnerabilidades. | Reporte de la prueba de penetración. |

**Recomendaciones:**

* Revisar y actualizar la política de seguridad de bases de datos para incluir todos los aspectos relevantes.
* Revisar y ajustar los permisos de acceso a las bases de datos para garantizar que solo los usuarios autorizados tengan acceso a la información que necesitan.
* Implementar un proceso de actualización de parches de seguridad más riguroso para garantizar que todas las bases de datos estén actualizadas.
* Implementar las medidas correctivas necesarias para mitigar las vulnerabilidades identificadas en las pruebas de penetración.
* Brindar capacitación a los usuarios sobre las mejores prácticas de seguridad en bases de datos.

**Observaciones:**

* La gerencia del banco debe tomar medidas urgentes para implementar las recomendaciones de esta auditoría.
* La seguridad de las bases de datos es un tema crítico para el banco y debe ser una prioridad para todos los empleados.

| **Nombre de la auditoría:** Auditoría de Seguridad de la Red | |
| --- | --- |
| **Fecha:** 2024-06-28 | **Auditor:** Wilbert Castillo |
| **Área auditada:** Área de Seguridad en la Red | |
| **Objetivo:** Evaluar la seguridad de la red del Banco BAC. | |
| **Alcance:** La auditoría abarca las políticas de seguridad de la red, la configuración de los dispositivos de red, la gestión de vulnerabilidades, el monitoreo de la red, la respuesta a incidentes y las prácticas de los usuarios. | |
| **Metodología:** La auditoría se realizó mediante una combinación de técnicas, incluyendo entrevistas, análisis de documentos, revisión de configuraciones, pruebas de vulnerabilidad y monitoreo de la red. | |

| **Prueba** | **Descripción** | **Resultado** | **Evidencia** |
| --- | --- | --- | --- |
| **Prueba 1:** Revisión de la política de seguridad de la red | Se verificó si la política de seguridad de la red está actualizada y es adecuada para proteger la red del banco. | La política de seguridad de la red está actualizada, pero no cubre todos los aspectos de la seguridad de la red. Se recomienda revisar y actualizar la política para incluir todos los aspectos relevantes, como la gestión de contraseñas, el control de acceso, la gestión de parches de seguridad, la segmentación de la red y el monitoreo de la actividad. | Entrevista con el administrador de red, copia de la política de seguridad de la red. |
| **Prueba 2:** Análisis de la configuración de los dispositivos de red | Se revisaron las configuraciones de los dispositivos de red para identificar posibles vulnerabilidades. | Se identificaron algunas configuraciones de seguridad inadecuadas en los dispositivos de red. Se recomienda revisar y ajustar las configuraciones para garantizar que cumplan con las mejores prácticas de seguridad. | Análisis de configuraciones de dispositivos de red. |
| **Prueba 3:** Pruebas de vulnerabilidad en la red | Se realizaron pruebas de vulnerabilidad para identificar vulnerabilidades en la red. | Se identificaron algunas vulnerabilidades en la red, como software desactualizado, puertos abiertos innecesarios y configuraciones de seguridad inadecuadas. Se recomienda implementar las medidas correctivas necesarias para mitigar estas vulnerabilidades. | Reporte de pruebas de vulnerabilidad. |
| **Prueba 4:** Monitoreo de la red | Se revisó el monitoreo de la red para identificar posibles actividades maliciosas. | Se detectó que el monitoreo de la red no es suficiente para detectar todas las posibles actividades maliciosas. Se recomienda implementar un sistema de monitoreo de la red más completo y eficaz. | Revisión de los registros de monitoreo de la red. |
| **Prueba 5:** Pruebas de respuesta a incidentes | Se realizaron pruebas de respuesta a incidentes para evaluar la capacidad del banco para responder a incidentes de seguridad en la red. | Se identificaron algunas deficiencias en la capacidad del banco para responder a incidentes de seguridad en la red. Se recomienda desarrollar un plan de respuesta a incidentes y capacitar al personal en la respuesta a incidentes. | Reporte de pruebas de respuesta a incidentes. |

**Recomendaciones:**

* Revisar y actualizar la política de seguridad de la red para incluir todos los aspectos relevantes.
* Revisar y ajustar las configuraciones de los dispositivos de red para garantizar que cumplan con las mejores prácticas de seguridad.
* Implementar las medidas correctivas necesarias para mitigar las vulnerabilidades identificadas en la red.
* Implementar un sistema de monitoreo de la red más completo y eficaz.
* Desarrollar un plan de respuesta a incidentes y capacitar al personal en la respuesta a incidentes.

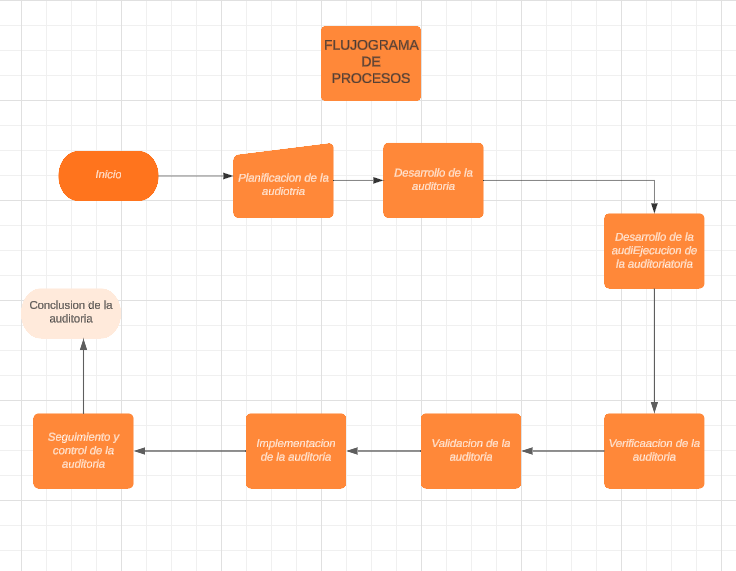
**Observaciones:**

* La gerencia del banco debe tomar medidas urgentes para implementar las recomendaciones de esta auditoría.
* La seguridad de la red es un tema crítico para el banco y debe ser una prioridad para todos los empleados.

## Seguimiento de recomendaciones

| **Seguimiento de Recomendaciones** |
| --- |
| **Empresa:** BAC CREDOMATIC |
| **Fecha:** 28/04/2024 |
| **Áreas:** Redes y base de datos |
| **Equipo Responsable:** Auditor Líder: Nixon Maradiaga |
| **Resumen Ejecutivo:** La auditoría de sistemas de seguridad de la red y base de datos se realizó con el objetivo de evaluar la seguridad en la infraestructura de red y en los dispositivos así como la eficiencia de las bases de datos del banco. |
| **Área de seguridad de red** |
| **Hallazgos:** Se identificó la falta de actualizaciones e implementación de procedimientos de seguridad en los dispositivos de red.  **Recomendaciones:** Se recomienda implementar medidas robustas de seguridad, como firewalls, sistemas de detección de intrusos, pero sin obstaculizar el rendimiento de los servicios bancarios.  **Seguimiento:** Monitorizaciones de seguridad que permitan supervisar el tráfico en la red, las actividades de los usuarios y las posibles intrusiones. |
| **Área de base de datos** |
| **Hallazgos:** Se pudo observar que los usuarios gozan de libertad de accesos en los datos y que utilizan contraseñas débiles.  **Recomendaciones:** Se recomienda implementar políticas de contraseñas robustas y políticas de cambio de contraseñas, así como asignar los accesos de acuerdo a las funciones de los empleados.  **Seguimiento:** Se realizan monitoreos de actividad en la base de datos y se supervisan el acceso de los usuarios. |
| **Observaciones Adicionales** |
| Gracias a las recomendaciones se observa un avance en las áreas auditadas. |
| **Próximos Pasos y Plan de Acción** |
| Realizar auditorías de seguimiento para evaluar si aplican las recomendaciones. |
| **Firma del responsable de Seguimiento:** |

## Flujograma de procesos



## Resultados de la auditoría

### Presentación Detallada de Resultados de Auditoría en el Área de Bases de Datos

**Fecha:** 25-12-2024

**Área Auditada:** Área de bases de datos

**1. Políticas de seguridad de bases de datos inadecuadas:**

* **Falta de actualización:** La política de seguridad de bases de datos no se ha actualizado desde  2020, lo que significa que no refleja las últimas amenazas y vulnerabilidades.
* **Cobertura incompleta:** La política no cubre todos los aspectos relevantes de la seguridad de las bases de datos, como la gestión de contraseñas, el control de acceso, la gestión de parches de seguridad, la segmentación de bases de datos y el monitoreo de la actividad.
* **Falta de mecanismos de cumplimiento:** No existen mecanismos para garantizar el cumplimiento de la política de seguridad de bases de datos. Esto significa que la política podría no estar siendo seguida por los usuarios y no estar protegiendo adecuadamente las bases de datos.

**2. Controles de acceso deficientes:**

* **Permisos excesivos:** Se detectó que algunos usuarios tienen acceso a bases de datos que no necesitan para realizar su trabajo. Esto aumenta el riesgo de que estos usuarios accedan accidental o intencionalmente a información confidencial o sensible.
* **Falta de segmentación:** No existe una segmentación adecuada entre diferentes tipos de datos sensibles. Esto significa que si un atacante obtiene acceso a una base de datos, podría potencialmente acceder a todos los datos almacenados en ella, independientemente de su sensibilidad.
* **Ausencia de RBAC:** No se utilizan controles de acceso basados en roles (RBAC) para limitar el acceso a las bases de datos. Esto significa que los usuarios tienen acceso a toda la información a la que están autorizados dentro de su grupo de usuarios, incluso si no la necesitan para realizar su trabajo.

**3. Gestión de parches de seguridad deficiente:**

* **Bases de datos no actualizadas:** Se detectó que algunas bases de datos no están actualizadas con los últimos parches de seguridad. Esto las expone a vulnerabilidades conocidas que podrían ser explotadas por atacantes para obtener acceso no autorizado a las bases de datos.
* **Falta de un proceso de actualización:** No existe un proceso de actualización de parches de seguridad riguroso y automatizado. Esto significa que las bases de datos no se actualizan de manera oportuna, lo que aumenta el riesgo de que sean explotadas por vulnerabilidades conocidas.

**4. Monitoreo y registro de actividad insuficiente:**

* **Monitoreo incompleto:** El monitoreo y registro de la actividad en las bases de datos no es suficiente para detectar accesos no autorizados o posibles incidentes de seguridad.
* **Dificultad para detectar anomalías:** La falta de monitoreo y registro completo dificulta la identificación de patrones anormales o comportamientos sospechosos en la actividad de las bases de datos.

**5. Prácticas inadecuadas de los usuarios:**

* **Uso de contraseñas débiles:** Se detectó que algunos usuarios utilizan contraseñas débiles o reutilizadas para acceder a las bases de datos. Esto facilita que los atacantes obtengan acceso no autorizado a las bases de datos mediante técnicas de fuerza bruta o ataques de diccionario.
* **Falta de conocimiento:** Se detectó que algunos usuarios no tienen el conocimiento adecuado sobre las mejores prácticas de seguridad en bases de datos. Esto aumenta el riesgo de que cometan errores que puedan comprometer la seguridad de las bases de datos.
* **Incumplimiento de procedimientos:** Se detectó que algunos usuarios no siguen los procedimientos de seguridad establecidos para el acceso y uso de las bases de datos. Esto aumenta el riesgo de que se produzcan errores o incidentes de seguridad.

**Impacto potencial de los hallazgos:**

Los hallazgos de esta auditoría indican que la seguridad de las bases de datos del Banco BAC está en riesgo. Las debilidades identificadas podrían ser explotadas por atacantes para obtener acceso no autorizado a las bases de datos, robar información confidencial o sensible, o incluso interrumpir las operaciones del banco.

**Recomendaciones:**

Se recomienda al Banco BAC implementar las siguientes medidas correctivas para mitigar los riesgos identificados:

* **Fortalecer las políticas de seguridad de bases de datos:** Actualizar la política de seguridad de bases de datos para que incluya todos los aspectos relevantes y establecer requisitos estrictos para la gestión de contraseñas, el control de acceso, la gestión de parches de seguridad, la segmentación de bases de datos y el monitoreo de la actividad.
* **Mejorar los controles de acceso:** Revisar y ajustar los permisos de acceso a las bases de datos para garantizar que solo los usuarios autorizados tengan acceso a la información que necesitan.
* **Implementar un proceso de gestión de parches de seguridad riguroso:** Establecer un proceso automatizado de actualización de parches de seguridad para garantizar que todas las bases de datos estén actualizadas con los últimos parches de seguridad.

### Presentación Detallada de Resultados de Auditoría en el Área de Seguridad en La Red

**Fecha:** 25-12-2024

**Área Auditada:** Área de seguridad en la red

## Resultados Detallados de la Auditoría de Seguridad en la Red

**1. Política de seguridad de la red incompleta:**

* **Falta de actualización:** La política de seguridad de la red no se ha actualizado desde 2019, lo que significa que no refleja las últimas amenazas y vulnerabilidades en la seguridad de la red.
* **Cobertura incompleta:** La política no cubre todos los aspectos relevantes de la seguridad de la red, como la gestión de contraseñas, el control de acceso, la gestión de parches de seguridad, la segmentación de la red, el monitoreo de la red y la respuesta a incidentes.
* **Falta de mecanismos de cumplimiento:** No existen mecanismos para garantizar el cumplimiento de la política de seguridad de la red. Esto significa que la política podría no estar siendo seguida por los usuarios y no estar protegiendo adecuadamente la red.

**2. Configuraciones de seguridad inadecuadas en los dispositivos de red:**

* **Contraseñas débiles:** Se detectó que algunos dispositivos de red utilizan contraseñas débiles o predeterminadas, lo que facilita que los atacantes obtengan acceso no autorizado a la red.
* **Servicios innecesarios habilitados:** Se detectó que algunos servicios innecesarios están habilitados en algunos dispositivos de red, lo que aumenta la superficie de ataque y el riesgo de vulnerabilidades.
* **Configuraciones de firewall deficientes**: Se detectó que las configuraciones de firewall en algunos dispositivos de red no son lo suficientemente restrictivas, lo que permite el acceso no autorizado a la red.
* **Falta de cifrado:** Se detectó que algunos dispositivos de red no utilizan cifrado para proteger las comunicaciones, lo que hace que la información sea vulnerable a la interceptación.

**3. Vulnerabilidades en la red:**

* **Software desactualizado:** Se detectó que algunos dispositivos de red están ejecutando software desactualizado que contiene vulnerabilidades conocidas.
* **Puertos abiertos innecesarios:** Se detectó que algunos puertos abiertos en la red no son necesarios, lo que aumenta el riesgo de ataques y vulnerabilidades.
* **Configuraciones de seguridad inadecuadas en aplicaciones web:** Se detectó que algunas aplicaciones web que se ejecutan en la red tienen configuraciones de seguridad inadecuadas que las hacen vulnerables a ataques.

**4. Monitoreo de la red insuficiente:**

* **Falta de monitoreo completo:** El monitoreo de la red no es suficiente para detectar todas las posibles actividades maliciosas, como intrusiones no autorizadas, intentos de ataque o malware.
* **Análisis de registros inadecuado:** No se realiza un análisis adecuado de los registros de la red, lo que dificulta la identificación de patrones anormales o comportamientos sospechosos.
* **Falta de herramientas de monitoreo especializadas:** No se utilizan herramientas de monitoreo especializadas para detectar ataques cibernéticos sofisticados o malware avanzado.

**5. Deficiencias en la respuesta a incidentes:**

* **Falta de un plan de respuesta a incidentes:** No existe un plan de respuesta a incidentes documentado que defina las acciones a tomar en caso de un incidente de seguridad en la red.
* **Falta de capacitación del personal:** El personal no está capacitado adecuadamente para responder a incidentes de seguridad en la red, lo que podría retrasar la respuesta y aumentar el impacto del incidente.
* **Falta de herramientas de respuesta a incidentes:** No se dispone de las herramientas necesarias para investigar y responder a incidentes de seguridad en la red de manera eficaz.

**Impacto potencial de los hallazgos:**

Los hallazgos de esta auditoría indican que la seguridad de la red del Banco BAC está en riesgo. Las debilidades identificadas podrían ser explotadas por atacantes para obtener acceso no autorizado a la red, robar información confidencial o sensible, interrumpir las operaciones del banco o incluso tomar el control de la infraestructura de red.

**Recomendaciones:**

## Se recomienda al Banco BAC implementar las siguientes medidas correctivas para mitigar los riesgos identificados:

* **Fortalecer la política de seguridad de la red**: Actualizar la política de seguridad de la red para que incluya todos los aspectos relevantes y establece requisitos estrictos para la gestión de contraseñas, el control de acceso, la gestión de parches de seguridad, la segmentación de la red, el monitoreo de la red y la respuesta a incidentes.
* **Revisar y ajustar las configuraciones de seguridad de los dispositivos de red**: Revisar las configuraciones de seguridad de todos los dispositivos de red para garantizar que cumplan con las mejores prácticas de seguridad.
* **Implementar un programa de gestión de vulnerabilidades:** Implementar un programa de gestión de vulnerabilidades para identificar y corregir las vulnerabilidades en la red de manera oportuna.

## Glosario

**1. Firewall:** Es un dispositivo que controla el tráfico entre redes, permitiendo o bloqueando ciertas comunicaciones basadas en un conjunto de reglas de seguridad.

**2.** **Sistema de detección de intrusiones:** herramienta de seguridad que monitorea el tráfico de red en busca de actividades maliciosas o inusuales y alerta a los administradores cuando se detecta una posible intrusión.

**3. Sistema de prevención de intrusión:** monitorea el tráfico de la red en busca de actividades sospechosas, pero también tiene la capacidad de tomar medidas para evitar o bloquear ataques.

**4. Listas de control de acceso:** son conjuntos de reglas que especifican qué usuarios o sistemas pueden acceder a recursos específicos en una red.

**5. Gestión de datos:** proceso de administrar y mantener una base de datos de manera eficiente y efectiva.

**6. Infraestructura de red:** Es el conjunto de componentes que permite la conectividad y el intercambio de información en una red.

**7. Protocolos de red:** conjunto de reglas y convenciones que dictan cómo los dispositivos en una red se comunican entre sí.

**8. Parches de seguridad:** son actualizaciones o correcciones de software diseñadas para cerrar brechas de seguridad, corregir vulnerabilidades y mejorar la protección contra amenazas cibernéticas.

**9. Política de cambio de contraseña:** es un conjunto de reglas y directrices que especifican cuándo y cómo los usuarios deben cambiar sus contraseñas en un sistema informático o una red.

**10. Política de seguridad de red:** conjunto de directrices y prácticas establecidas por una organización para proteger su información en la red.

**11. Puerta trasera:** en el contexto de la informática, es una vulnerabilidad no documentada en un sistema o software que permite el acceso no autorizado.

**12. Segmentación de la red:** consiste en dividir una red informática en segmentos más pequeños o subredes.

**13. Permisos de acceso:** se utilizan para controlar quién tiene acceso a qué recursos y en qué capacidad dentro de un entorno de IT. Son reglas que definen qué acciones pueden realizar los usuarios.

**14. Redundancia:** se refiere a la duplicación o repetición de elementos o funciones en un conjunto de datos.

## Conclusiones

La auditoría realizada a las áreas de seguridad en la red y base de datos nos revelan que existen vulnerabilidades tanto en la red como en la base de datos, ya que no cuentan con los niveles de seguridad mínimos y no cuentan con políticas de seguridad.

La falta de políticas y procedimientos adecuados para la gestión de accesos y la monitorización a la red puede resultar en una exposición a amenazas internas y externas.

Se observó que la infraestructura de base de datos carece de medidas de seguridad y se presentan deficiencias en la configuración que podrían comprometer la integridad y la confidencialidad de la información

La revisión en las bases de datos resalta la necesidad de asignar permisos a los usuarios en los controles de acceso a los datos para minimizar la fuga de información sensible.

Al implementar medidas y políticas de seguridad robustas, la seguridad en la red y en la base de datos aumentará muy satisfactoriamente y reducirá las vulnerabilidades en ataques dentro de la red y fugas de información de los clientes, esto permitirá que el banco aumente su popularidad como uno de los bancos más seguros para los clientes.

## 

## Recomendaciones finales

**Prioridades:**

* Implementar de manera urgente las medidas correctivas para las vulnerabilidades críticas y las malas prácticas.
* Desarrollar un plan de acción para implementar las demás medidas correctivas de manera gradual y ordenada.
* Asignar los recursos necesarios para la implementación y el mantenimiento continuo de las medidas de seguridad e integridad de datos.

**Responsabilidades:**

* La gerencia del banco debe asumir la responsabilidad general de la implementación de las recomendaciones finales.
* El departamento de TI debe liderar la implementación de las medidas técnicas y la capacitación del personal.
* Las demás áreas del banco deben colaborar en la implementación de las medidas que les correspondan.

**Monitoreo y Evaluación:**

* Establecer indicadores clave de rendimiento (KPIs) para medir la efectividad de las medidas implementadas.
* Realizar auditorías de seguimiento periódicas para evaluar el cumplimiento de las recomendaciones y la mejora continua.
* Mantenerse actualizado sobre las nuevas amenazas, vulnerabilidades y mejores prácticas para ajustar las medidas y políticas en consecuencia.

**Inversión en Seguridad:**

* Considerar la seguridad como una inversión fundamental para proteger los activos y la reputación del banco.
* Asignar un presupuesto adecuado para la implementación y el mantenimiento de las medidas de seguridad.
* Capacitar al personal sobre la importancia de la seguridad y las buenas prácticas para proteger la información.

Estas recomendaciones finales son un resumen general de las medidas necesarias para mejorar la seguridad de las bases de datos y la red del Banco BAC. Se recomienda desarrollar un plan de acción detallado que describa las acciones específicas, los plazos, los responsables y los recursos necesarios para implementar cada una de las recomendaciones.