Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Trabajo Final de Maestría

Título

Diseño e implementación de controles internos de seguridad de la información en el dominio de gestión de accesos con base a la Ley SOX

Autora

Leticia Elena Ferreira González

Director

Hugo Pagola

Año de presentación 2024

Cohorte 2017

Declaración jurada de origen de los contenidos

“Por medio de la presente, la autora manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

FIRMADO

Leticia Elena Ferreira González

DNI: 95.736.835

Resumen

El presente trabajo final de maestría tiene el propósito de relatar el trabajo realizado por el área de auditoría y seguridad de la información una compañía sobre el diseño e implementación de controles internos de gestión de acceso de usuarios en los sistemas de tecnología de información con base en la Ley Sarbanes Oxley. La compañía ofrece servicios de conectividad y entretenimiento digital en varios países de Latinoamérica, y cotiza sus acciones en la Bolsa de Nueva York, Estados Unidos.

La Ley SOX establece estrictos requisitos para mejorar la precisión y fiabilidad de las divulgaciones corporativas. En este contexto, la gestión de accesos de usuarios se convierte en un elemento crítico para asegurar que solo las personas autorizadas tengan acceso a los sistemas y datos sensibles, reduciendo así los riesgos de accesos indebidos, brechas de seguridad, e incumplimiento normativo.

El trabajo se estructura en varios puntos, inicia describiendo una visión general de la Ley Sarbanes Oxley, incluyendo su importancia y beneficios para las organizaciones, así como los impactos del incumplimiento tanto a nivel organizacional como individual. Seguidamente se aborda la política de gestión de accesos del usuario, describiendo las directrices y procedimientos establecidos para regular el acceso a los sistemas de información, así como los riesgos asociados y las medidas para mitigarlos.

Luego, se explora el marco regulatorio, destacando normativas como la ISO/IEC 27002 y el marco COSO, que proporcionan estándares y mejores prácticas para la seguridad de la información y el control interno. La siguiente sección se centra en los controles corporativos, detallando la definición de riesgos y controles específicos para la gestión de acceso, así como la implementación de estos controles.

Seguidamente, se resalta los resultados obtenidos tras la implementación y ejecución de los controles, evaluando su impacto en la seguridad y cumplimiento regulatorio de la organización. También, se describe el papel crucial de la auditoría interna y externa en la supervisión y validación de estos controles, asegurando su correcta aplicación y eficiencia. Posteriormente, se incluye un ejemplo práctico que ilustra la ejecución del control sobre bajas de usuarios, y se presente un control complementario del proceso.

Finalmente, se proporciona un breve resumen y discusión sobre las limitaciones y los desafíos encontrados durante la implementación de los controles, así como las estrategias adoptadas para superarlos, y como último punto se ofrece las conclusiones del trabajo. Este análisis ofrece valiosas lecciones y recomendaciones para mejorar la seguridad y cumplir con regulaciones actuales.

Palabras claves: Auditoría, Seguridad, Control, Gestión de accesos, Identidad, Riesgo, Marco regulatorio, SOX, Proceso.

Índice General

Índice de Ilustraciones

Índice de Tablas

Agradecimientos

A mi familia quien me acompaña y apoya incondicionalmente en mi crecimiento personal y profesional.

A los docentes y compañeros de la maestría por los conocimientos y las experiencias compartidas durante la cursada.

Al Programa Nacional de Becas de Postgrado en el Exterior “Don Carlos Antonio López” por otorgarme la oportunidad de formarme y especializarme para fortalecer y afianzar mis capacidades profesionales.

1- Introducción

En el entorno empresarial actual, la información se ha convertido en un activo fundamental para el éxito y la competitividad de las organizaciones. Sin embargo, este valioso activo se encuentra constantemente expuesto a diversas amenazas, tanto internas como externas, que pueden comprometer su confidencialidad, integridad y disponibilidad. La Ley Sarbanes Oxley (SOX), promulgada en los Estados Unidos en 2002, busca fortalecer la confianza de los inversores en la información financiera de las empresas públicas mediante la implementación de controles internos efectivos.

En el contexto de la gestión de accesos, la seguridad de la información es particularmente crítica. Los sistemas de control de acceso permiten determinar quién puede acceder a qué recursos y cuándo, siendo crucial para proteger la información sensible y garantizar el cumplimiento de las regulaciones. Sin embargo, la complejidad de los entornos informáticos actuales, la proliferación de dispositivos y la creciente sofisticación de las amenazas hacen que el diseño e implementación de controles internos de seguridad de la información en el dominio de gestión de accesos sea un desafío significativo.

1.1- Objetivo general

Proponer un diseño de controles internos y su implementación para mitigar riesgos de gestión de acceso de usuarios.

1.2- Objetivos Específicos

I. Analizar la Ley SOX y los requerimientos a cumplir en materia de control para la gestión de seguridad en acceso de usuario.
II. Proponer controles para que la información se encuentre correctamente resguardada.
III. Minimizar el riesgo de acceso a la información de los activos de la organización por personas no autorizados.
IV. Identificar el impacto en los pilares de la seguridad, Confidencialidad, Integridad y Disponibilidad, al no aplicar los controles internos con el proceso de gestión de accesos.

2- Ley Sarbanes Oxley

2.1- ¿Qué es SOX?

La Ley Sarbanes-Oxley (SOX) es parte de la legislación de los Estados Unidos que entró en vigor en 2002 y fue aprobada por el Congreso en respuesta a varios de los siguientes escándalos corporativos:

Fraude contable institucionalizado, sistemático y creativamente planificado.

Utilidades sobreestimadas y gastos subestimados que permitieron a la empresa cumplir artificialmente con las proyecciones de ganancias en más de 5 trimestres.

El ex presidente de la Junta Directiva, Director Ejecutivo y el Director Financiero defraudaron a la compañía por más de $150 millones a través de supuestos pagos por prestación de servicios.

2.2- ¿Por qué SOX es tan importante?

El incumplimiento de la Ley SOX puede tener un impacto significativo en una organización y en todas las personas que trabajan allí.

2.2.1- Impacto del incumplimiento en las organizaciones

- Pérdida del registro de la cotización de los títulos valores en la Bolsa.
- Multas que puedan alcanzar millones de dólares.
- Daños reputacionales.
- Disminución/pérdida de inversión.
- Mayores esfuerzos en auditorías y por lo tanto incremento en sus honorarios.

2.2.2- Impacto del incumplimiento en los individuos

Si la certificación es emitida y posteriormente se identifica que los informes financieros carecen de integridad y exactitud, se podría considerar que el Director Ejecutivo y el Director Financiero tienen responsabilidad penal.

- Encarcelamiento por 10-20 años.
- Sanciones civiles incluyendo multas que pueden ascender hasta US$ 5 millones.

2.3- ¿Cómo beneficia SOX?

Cumplir con SOX es más que marcar simplemente una casilla. Puede utilizarse para agregar una enorme cantidad de valor al negocio. Éstos son sólo algunos de los beneficios que se pueden esperar:

2.3.1- Beneficios en informes financieros

- Mayor credibilidad de la información financiera proporcionada a las partes interesadas.
- Mejor integridad y exactitud de la información utilizada para gestionar el negocio.
- Reducir riesgo de errores y tiempo dedicado a resolverlos.

2.3.2- Beneficios comerciales

- Mayor inversión de capital debido a cotización de títulos valores en la Bolsa de los Estados Unidos.

- Disminución del riesgo de litigios legales o interrupción del negocio.
- Mayor credibilidad ante los organismos reguladores.
- Más credibilidad cuando se establecen nuevas relaciones con proveedores y clientes.

2.3.3- Beneficios operacionales

- Responsabilidad claramente definida sobre controles y el cumplimiento de estos en toda la organización.
- Oportunidades para estandarizar, optimizar y automatizar procesos.
- Facilitará la identificación y corrección de las debilidades en los procesos, así como los riesgos de negocio que podrían haberse pasado por alto anteriormente.
- Generará una cultura de cumplimiento y responsabilidad más sólida.

3- Política de gestión de acceso del usuario

3.1- Propósito

Para proteger los datos y recursos del acceso o divulgación no autorizados, la organización requiere mecanismos específicos de identificación, autenticación, y autorización donde se incluye el uso de contraseña, para controlar el acceso a todos los sistemas de la compañía y los datos que contienen, reduciendo así la materialización de riesgos.

La política de gestión de acceso se implementa en la compañía para aplicar reglas comerciales, tipos de datos y criterios y procesos de autorización de acceso para garantizar que el acceso se pueda aprovisionar y controlar de manera adecuada. Esto incluye la identificación de requisitos de acceso a datos y recursos del sistema.

La política define los requisitos para la administración y gestión del acceso lógico tanto de empleados directos como de terceros para todas las aplicaciones, sistemas y plataformas del ecosistema de la compañía. Además, aborda los siguientes riesgos:

- Protección de datos y recursos del sistema de información contra accesos no autorizados.
- Amenazas y vulnerabilidades a los sistemas de seguridad de la información que pueden resultar en pérdida, daño o destrucción de sistemas, aplicaciones o datos.

3.2- Requisitos de la política

La política cuenta con requisitos que están relacionados con los procesos de gestión de acceso de usuarios para mitigar adecuadamente los riesgos.

3.2.1- Control de acceso

3.2.1.1- Requerimientos generales

a. Todos los actores, como ser recursos humanos, gerentes de línea, supervisores, administradores y todos los colaboradores, que son responsables de los procesos de gestión de usuarios y control de acceso, deben cumplir con las políticas y estándares de gestión de

acceso de usuarios que respaldan el ciclo de vida del acceso de usuarios (registro, modificación, suspensión, y terminación del acceso) para cualquier acceso de usuario local o remoto.

3.2.1.2- Acceso autorizado y autenticado

a. Todas las cuentas sobre sistemas y componentes de información deben estar autorizadas antes de ser otorgadas y utilizadas.
b. Los dueños del sistema y/o el administrador del sistema deben implementar mecanismos de autenticación y autorización en todos los sistemas y componentes de información.
c. Se deben implementar controles de acceso basados en roles en los sistemas de información.
d. Se deben implementar mecanismos centralizados de autenticación y autorización, por ejemplo, SAML[1], SSO[2], LDAP[3].

3.2.1.3- Autorización de acceso

a. Se debe establecer un proceso estandarizado de solicitud y autorización de acceso para regular la concesión de acceso local o remoto a los sistemas y recursos de información y para garantizar que se conserve la documentación adecuada.
b. Se debe establecer un proceso estandarizado de solicitud y autorización para regir la modificación de acceso, derechos o permisos.
c. El proceso de autorización debe completarse antes de otorgar acceso o modificar el acceso y los permisos para cualquier usuario o cuenta.
d. Los procesos de autorización y todos los flujos de trabajo asociados deben estar completamente documentados.
e. Sólo el personal específicamente designado debe autorizar y aprobar el acceso de usuarios o cuentas.

3.2.1.4- Mínimo privilegio y acceso mínimo

a. Los dueños del sistema deben limitar los derechos y permisos de acceso de la cuenta al mínimo necesario para satisfacer las necesidades del rol o función.
b. Se deben desarrollar y documentar prácticas de privilegios mínimos para todos los sistemas y componentes.

3.2.1.5- Segregación de deberes

a. Los derechos de acceso deben alinearse con el principio de separación de funciones.

---

[1] SAML (*Security Assertion Markup Language*) es un lenguaje basado en XML para autenticar mediante identidades federadas.

[2] SSO (Single Sign-On) el inicio de sesión único es una tecnología que combina varias pantallas de inicio de sesión de aplicaciones diferentes en una sola.

[3] LDAP (*Lightweight Directory Access Protocol*) es un protocolo de acceso que permite acceder a los recursos de la red local, sin necesidad de crear los diferentes usuarios en el sistema operativo. [5]

b. La justificación de las decisiones de segregación de funciones debe documentarse para cada sistema de información y cualquiera de sus componentes.

3.2.1.6- Cuentas de usuario únicas

a. Todas las cuentas de usuario deben ser únicas y cumplir con la convención de nomenclatura aprobada.
b. Todas las cuentas de usuario deben asignarse a una sola persona.
c. Se deben evitar las cuentas de usuario no nominativas.
d. Las cuentas de usuario no deben reutilizarse ni reasignarse.
e. El personal sólo debe tener una cuenta de usuario.

3.2.1.7- Cuentas de usuarios privilegiados

a. Los dueños del sistema deben limitar las cuentas privilegiadas, por ejemplo, administrador, cuentas con derechos o permisos elevado, a lo mínimo necesario.
b. El acceso privilegiado debe limitarse al personal con tareas administrativas explícitas o requisitos funcionales críticos.
c. A las cuentas de usuario básicas no se les pueden asignar privilegios de administrador ni otros privilegios elevados.
d. Todas las cuentas privilegiadas deben ser únicas y separadas de las cuentas de usuario básicas.
e. Las cuentas privilegiadas solo deben usarse para realizar actividades que requieren derechos elevados y no para realizar actividades y funciones generales del usuario.
f. Se debe establecer y mantener proactivamente un inventario de cuentas privilegiadas.
g. No se debe otorgar a los usuarios acceso a bases de datos y sistemas operativos para servidores de producción para la ejecución de servicios y procesos en dichos sistemas.
h. De forma predeterminada, a los desarrolladores y arquitectos no se les debe conceder acceso al entorno de producción.

3.2.1.8- Otros tipos de cuenta

a. Las cuentas de administrador no nominativas/compartidas deben ser propiedad y estar bajo la responsabilidad de personas únicas identificadas.
b. Las cuentas de servicio no se deben utilizar para actividades interactivas.

3.2.1.9- Denominación de cuentas e identificadores

a. Se debe establecer un enfoque estandarizado y consistente para nombrar cuentas u otros identificadores.
b. Todos los nombres de cuentas de usuario deben cumplir con los estándares de nomenclatura definidos en el procedimiento de la compañía.

3.2.1.10- Aprovisionamiento, gestión y cancelación de cuentas

a. Se deben establecer procesos estandarizados, oportunos y documentados para todas las actividades de gestión de cuentas, incluido el aprovisionamiento, la modificación y la eliminación.
b. Siempre que sea posible, las actividades de gestión de cuentas deben utilizar mecanismos automatizados y centralizados.
c. Las cuentas deben desactivarse y/o eliminarse cuando ya no sean necesarias.
d. Los niveles de acceso y permisos de la cuenta deben modificarse o eliminarse cuando ya no sean necesarios.
e. El acceso del personal revocado debe eliminarse dentro de los plazos establecidos por la compañía.
f. En los sistemas de información críticos, todas las cuentas de usuario, roles, grupos y privilegios deben ser revisados para determinar su idoneidad y necesidad al menos una vez al año.
g. En los sistemas de información críticos, todas las cuentas, roles, grupos y privilegios del sistema y privilegiados deben revisarse para determinar su idoneidad y necesidad al menos cada seis meses.
h. Las acciones correctivas identificadas deben realizarse dentro de los plazos establecidos por la organización y cualquier acción correctiva debe estar completamente documentada.

3.2.1.11- Inactividad de la cuenta

a. En los sistemas de información críticos, se debe establecer un proceso de inactividad de cuenta en todos los componentes, es decir, aplicaciones, bases de datos, sistemas operativos, infraestructura de red, para los siguientes tipos de usuarios:
    i. Usuarios nominales
    ii. Usuarios privilegiados
b. Las cuentas inactivas en los componentes del sistema dentro del alcance deben identificarse, deshabilitarse, eliminarse o administrarse de otro modo dentro de los plazos establecidos por la compañía.
c. Se deberán utilizar mecanismos automatizados para facilitar el proceso de inactividad.
d. Tipos específicos de cuentas pueden permanecer inactivos con la revisión y aprobación adecuada.

3.2.1.12- Acceso de emergencia

a. El acceso de emergencia es para soportar incidentes de producción y resolución de problemas, debe registrarse y debe seguir los procedimientos documentados de la compañía.
b. Los accesos de emergencia deben concederse de forma temporal.
c. El acceso temporal de emergencia a los entornos de producción debe ser solicitado tanto por el dueño del negocio como por el dueño del sistema y el gerente de línea, y requiere aprobación del oficial de seguridad de la información.

d. El acceso temporal debe revocarse inmediatamente al finalizar las actividades de emergencia requeridas.

3.2.2- Autenticación y contraseña

3.2.2.1- Identificación y autenticación

a. Los sistemas y componentes de información deben autenticar todas las cuentas antes de otorgarles acceso.
b. Los sistemas y componentes de información deben implementar mecanismos de autenticación para identificar de forma única todas las cuentas.
c. Se debe definir un conjunto de mecanismos de autenticación aprobados y configuraciones asociadas.
d. Los mecanismos de autenticación aprobados deben cumplir con todos los requisitos técnicos y operativos relacionados.
e. Los mecanismos de autenticación deben implementar protecciones contra intentos de fuerza bruta, por ejemplo, bloqueos de cuentas.

3.2.2.2- Autenticación basada en contraseña

a. Debe implementarse en todos los componentes del sistema de información y capas tecnológicas.
b. Los parámetros de contraseña y los estándares de configuración que se derivan de los estándares de la industria deben establecerse y describirse en los procedimientos de contraseñas.
c. Los componentes del sistema de información y las capas tecnológicas deben configurarse para hacer cumplir técnicamente los estándares de contraseña definidos.
d. Las contraseñas deben cumplir con todos los requisitos de construcción detallados en la línea base de configuración de seguridad.

3.2.2.3- Gestión y manejo de contraseñas

a. Las contraseñas se consideran datos confidenciales y nunca deben enviarse en texto plano y, por lo tanto, deben estar protegidos según lo definido en los procedimientos de contraseñas.
b. Las contraseñas nunca deben compartirse ni revelarse a personal que no sea el dueño de la cuenta.
c. Si el dueño de la cuenta no genera una contraseña, la contraseña debe cambiarse después del primer uso.
d. La identidad del personal que recibe las credenciales debe verificarse durante:
    i. Distribución inicial de credencial.
    ii. Restablecimiento de credencial.
    iii. Cambio de credencial.
    iv. Restauración o reactivación de credencial.

3.2.2.4- Cambios de contraseña

a. Se deben cambiar las contraseñas:
   i. Cuando el autenticador ha sido comprometido o se sospecha que ha sido comprometido.
   ii. Cuando el personal con conocimiento de credenciales grupales o basadas en roles de cuentas privilegiadas cambia de roles o abandona la compañía.
   iii. Al volver a habilitar cuentas.

3.3- Desviaciones y excepciones

Cualquier desviación o solicitud de excepción a la política de gestión de acceso de usuario debe realizarse mediante el proceso de documentación de aceptación de riesgos y debe aprobarse antes de ejecutarse.

4- Marco regulatorio

4.1- Directivas de la organización a sus filiales

Las obligaciones asociadas con ser una organización pública en los Estados Unidos requieren importantes recursos y atención administrativa. La organización se encuentra sujeto a los requisitos de presentación de informes de la Ley de Bolsa de Valores de 1934, según enmendada (la “Ley de Bolsa”), la Ley Sarbanes-Oxley, los requisitos de cotización del Mercado de Valores Nasdaq[4] y otras normas y regulaciones de valores aplicables. La Ley de Bolsa requiere presentar informes anuales y actuales con respecto al negocio, situación financiera y resultados de operaciones. La Ley Sarbanes-Oxley exige, entre otras cosas, establecer y mantener controles y procedimientos internos eficaces para la presentación de informes financieros. [2]

Los controles y procedimientos aplicados en las filiales, tiene como objetivo garantizar que todas las operaciones realizadas dentro de la organización cumplan con los principios y la estrategia de gestión global, y las leyes y regulaciones vigentes.

Al implementar y contar con un sistema de control interno en todas las actividades de la organización se pretende obtener una seguridad razonable de que la organización ha implementado las actividades necesarias para gestionar los riesgos que enfrenta:

- Garantizar la exactitud y confiabilidad de su información financiera.
- Gestionar sus operaciones de manera eficiente y eficaz.
- Garantizar el cumplimiento de las leyes y regulaciones aplicables.

De esta forma, pretende proteger el valor de la organización para sus accionistas y empleados. Estas prácticas estándar deben adaptarse a las actividades y organizaciones locales.

[4] Nasdaq (*National Association of Securities Dealers Automated Quotations*): Asociación Nacional de Cotizaciones Automatizadas de Distribuidores de Valores

4.2- ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad

La norma ISO/IEC 27002:2022 es una norma internacional que proporciona directrices y buenas prácticas para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información en una organización. Esta norma se centra en la seguridad de la información y brinda orientación detallada sobre los controles de seguridad que una organización puede implementar para proteger sus activos de información y gestionar los riesgos relacionados con la seguridad de la información.

Cuando una organización está sujeta a la Ley Sarbanes-Oxley, que establece requisitos rigurosos en cuanto a la transparencia financiera y la protección de la información, los controles establecidos en la ISO/IEC 27002:2022 juegan un papel crucial en los procesos de gestión de acceso. Aquí hay una explicación de cómo colaboran en esos procesos:

a. Establecimiento de Políticas de Acceso:

La ISO/IEC 27002:2022 proporciona directrices detalladas sobre el establecimiento de políticas de acceso que definen quién tiene acceso a qué recursos y en qué condiciones. Estas políticas son esenciales para cumplir con los requisitos de SOX en términos de controlar y limitar el acceso a la información financiera y otros activos críticos.

b. Implementación de Controles de Acceso:

La norma ofrece orientación sobre la implementación de controles de acceso técnicos y organizativos, como la autenticación multifactor, la gestión de contraseñas, la segregación de funciones y la revisión regular de privilegios. Estos controles ayudan a garantizar que solo las personas autorizadas tengan acceso a los datos financieros y que se minimice el riesgo de accesos no autorizados.

c. Gestión de Identidades y Accesos:

La ISO/IEC 27002:2022 aborda la importancia de establecer procesos para la gestión de identidades y accesos, incluyendo la creación, modificación y eliminación de cuentas de usuario de manera oportuna y precisa. Esto es esencial para cumplir con los requisitos de SOX en términos de mantener registros precisos y actualizados sobre quién tiene acceso a la información financiera.

d. Auditoría y monitorización de Accesos:

La norma también enfatiza la necesidad de realizar auditorías y monitorizar los accesos de usuarios de manera regular. Esto ayuda a detectar y mitigar cualquier actividad sospechosa o no autorizada, lo que es crucial para cumplir con los requisitos de SOX en términos de asegurar la integridad y confiabilidad de la información financiera.

En síntesis, la ISO/IEC 27002:2022 y sus controles proporcionan una guía valiosa para establecer y mantener un sólido sistema de gestión de acceso a la información, lo que es fundamental para el cumplimiento de los requisitos de la Ley Sarbanes-Oxley en cuanto a la protección de la información financiera y la prevención de fraudes.

4.3- Marco de Referencia COSO[5]

En 1992, el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) desarrolló el Marco COSO para evaluar los controles internos.

Este modelo ha sido adoptado como el marco generalmente aceptado para el control interno y es ampliamente reconocido como el estándar definitivo con el cual las organizaciones miden la efectividad de sus sistemas de control interno.

Está dedicado a brindar orientación a la gerencia ejecutiva y a las entidades gubernamentales en aspectos relevantes del gobierno corporativo, la ética empresarial, el control interno, la gestión de riesgos comerciales, el fraude y los informes financieros.

4.3.1- Componentes del Control Interno (COSO)

El marco COSO está integrado por 5 componentes:

1. Ambiente de control
2. Evaluación de riesgos
3. Actividades de control
4. Información y comunicación
5. Monitoreo

Que pueden ser operados a nivel de entidad, división, unidad operativa o función; con el objetivo de optimizar las operaciones, aumentar la precisión de los reportes y fomentar el cumplimiento de las leyes y reglamentos.

4.3.2- Explicación general de los Componentes COSO

4.3.2.1- Ambiente de Control

Establece el tono de una organización, e influye en la conciencia de control de los empleados. Los factores incluidos dentro del ambiente de control son:

a. Integridad, valores y competencia de los empleados, identidad
b. Filosofía de gestión y estilo operativo
c. Asignación de autoridad y responsabilidad
d. La atención y dirección brindada por la junta directiva

4.3.2.2- Gestión de Riesgos

Implica:

a. La consideración de los factores de riesgo
b. El reconocimiento de que toda organización enfrenta riesgos para su éxito
c. El reconocimiento de que las fuentes de riesgos son internas y externas
d. Identificación, análisis y acción para lograr los objetivos de la empresa

[5] COSO: Committee of Sponsoring Organizations of the Treadway Commission

4.3.2.3- Actividades de Control

Las actividades de control ocurren en toda la organización, en todos los niveles y en todas las funciones.

Las actividades de control son las políticas y los procedimientos que aseguran que se lleven a cabo las instrucciones de la gerencia, y la protección de los activos.

4.3.2.4- Información y Comunicación

La información se refiere al sistema de contabilidad, que registra, procesa, resume, informa sobre las transacciones de una organización, y mantiene la responsabilidad de los activos, pasivos y capital.

La comunicación ayuda al personal a comprender sus funciones y responsabilidades con respecto al control interno y sobre los informes financieros.

4.3.2.5- Monitoreo

Es el proceso que evalúa la calidad del desempeño del control interno a lo largo del tiempo.

Implica evaluar el diseño y la operación de los controles de manera oportuna.

Iniciar acciones correctivas cuando los controles específicos no funcionan correctamente.

4.4- Otras regulaciones

4.4.1- COBIT[6]

COBIT es un marco desarrollado por ISACA[7] que se centra en la gobernanza y gestión de tecnologías de la información. Puede ser útil para las empresas que buscan mejorar los controles relacionados con los sistemas de información.

4.4.2- ITIL[8]: Information Technology Infrastructure Library

ITIL es un conjunto de prácticas recomendadas para la gestión de servicios de tecnologías de la información. Puede ser relevante para fortalecer los controles de procesos y servicios de tecnología de la información.

4.4.3- NIST CSF[9]

Este marco proporciona orientación sobre cómo mejorar la ciberseguridad de una organización. Puede ser relevante para empresas que buscan fortalecer sus controles de seguridad de la información.

---

[6] COBIT: Control Objectives for Information and related Technology (Objetivos de Control para las Tecnologías de la Información y Relacionadas)

[7] ISACA *(Information Systems Audit and Control Association)*: Asociación de Auditoría y Control de Sistemas de Información

[8] ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información)

[9] NIST CSF: National Institute of Standards and Technology Cybersecurity Framework (Instituto Nacional de Estándares y Tecnología Marco de ciberseguridad)

5- Controles corporativos

En relación con la gestión de acceso a los sistemas de información, la organización identifica riesgos asociados con el acceso a sistemas y datos, por lo que se implementa tanto procesos manuales como automáticos con el objetivo de asegurar que el acceso a las funciones de los sistemas esté alineado con los roles de los usuarios y que se mantenga una adecuada segregación de funciones durante su ejecución.

5.1- Definición de riesgos

Con el objetivo de establecer un programa integral de control interno, se llevó a cabo una evaluación de los riesgos financieros y operativos en cada filial de la organización.

Esta evaluación permitió identificar las áreas clave donde se requería un mayor control, priorizando aquellos riesgos relacionados con la gestión de acceso lógico de usuarios en el área de la tecnología con enfoque de acceso no autorizado o inapropiado a información sensible o crítica.

En cuanto a protección de datos, se evaluó la protección de procesos contra intrusiones o acceso inadecuado a datos subyacentes, para prevenir, detectar y responder a amenazas a la seguridad de la información y gestionar adecuadamente las solicitudes de datos.

Área	**General**	**Acceso a programas y datos**				
Riesgos / **Controles**	R1	R2	R3	R4	R5	R6
	No se establece la gobernanza de los procesos de TI	Los deberes no están adecua-damente segrega-dos	Acceso no autorizado o inapropiado a sistemas y aplicaciones	Las cuentas de alto riesgo/privile-giados (por ejemplo, super usuario) evitan la autorización y la segregación de funciones impuestas por los sistemas	Se realizan cambios directos inadecuados en los registros de transacciones subyacentes o en los datos maestros	Los controles de contraseña débiles o las configuracio-nes de seguridad permiten eludir los derechos de acceso
Política y procedimien-to para la gestión de acceso de usuario	X					
Aprobación de nuevos usuarios y acceso al sistema		X	X		X	
Baja transaccional del acceso de los usuarios			X			
Revisión de bajas de usuarios al momento de su terminación			X			
Aprobación y revisión del			X		X	

Área	General	Acceso a programas y datos				
Riesgos / Controles	R1	R2	R3	R4	R5	R6
	No se establece la gobernanza de los procesos de TI	Los deberes no están adecua-damente segrega-dos	Acceso no autorizado o inapropiado a sistemas y aplicaciones	Las cuentas de alto riesgo/privile-giados (por ejemplo, super usuario) evitan la autorización y la segregación de funciones impuestas por los sistemas	Se realizan cambios directos inadecuados en los registros de transacciones subyacentes o en los datos maestros	Los controles de contraseña débiles o las configuracio-nes de seguridad permiten eludir los derechos de acceso
acceso de emergencia						
Revisión de actividades de usuarios con altos privilegios			X	X	X	
Definición de línea base de configuración de seguridad	X					
Revisión de la configuración de seguridad						X
Certificación periódica del acceso de los usuarios de tecnología de la información			X	X	X	
Certificación periódica del acceso de usuarios del negocio			X			

Tabla 1: Cruce de controles internos - riesgos identificados

5.2- Definición de controles

A continuación, se definen los controles específicos implementados para la gestión de acceso de usuarios. Se utilizará códigos para diferenciar los controles, se presenta la sigla CIA, bajo el concepto de Control de Identidad y Acceso.

Se detallan los controles específicos implementados para la gestión de acceso de usuarios:

5.2.1- Política y procedimiento para la gestión de acceso de usuario (CIA-1)

Objetivo del control	**Riesgo mitigado**
Se establecen e implementan políticas y procedimientos sobre los procesos de tecnología de la información.	R1
Descripción del control	
Existen políticas y procedimientos de control de acceso para otorgar (incluidos los de emergencia) y eliminar accesos a aplicaciones, bases de datos y sistemas operativos. Estas políticas y procedimientos se revisan anualmente para garantizar su idoneidad. La evidencia de la revisión se almacena en la herramienta tiquetes.	
Evidencia requerida	**Tipo de control**
1) Políticas y procedimientos de gestión de acceso de usuarios. 2) Revisión de políticas y procedimientos.	Preventivo
	Frecuencia
	Anual

5.2.2- Aprobación de nuevos usuarios y acceso al sistema (CIA-2)

Objetivo del control	**Riesgo mitigado**
Las solicitudes de acceso son revisadas y autorizadas adecuadamente por la gerencia.	R2, R3, R5
Descripción del control	
Todas las solicitudes de acceso de los usuarios que se producen a nivel de aplicación, base de datos y sistema operativo se documentan y aprueban en el sistema de emisión de tiquetes antes de ser otorgadas. El flujo de trabajo de aprobación está compuesto al menos por el gerente de línea y el dueño del sistema, de acuerdo con la política de control de acceso. La evidencia de la aprobación se almacena en el sistema de emisión de tiquetes.	
Evidencia requerida	**Tipo de control**
1) Políticas y procedimientos de gestión del acceso de los usuarios. 2) Tiquete de solicitud de usuario aprobado (incluidas las aprobaciones y evidencias de la disposición de acceso en la solicitud)	Preventivo **Frecuencia** Transaccional

5.2.3- Baja transaccional del acceso de los usuarios (CIA-3)

Objetivo del control	**Riesgo mitigado**
Los derechos de acceso de los usuarios de aplicaciones cancelados se eliminan oportunamente.	R3
Descripción del control	
Los accesos de usuarios a nivel de aplicación, base de datos y sistema operativo se dan de baja oportunamente, de acuerdo con la política de control de acceso, cuando un usuario (empleado o contratista) se retira de la compañía. Observación: Los accesos de usuarios podrán ser deshabilitados o eliminados, dependiendo de cada aplicación y capa.	
Evidencia requerida	**Tipo de control**
1) Política de control de acceso. 2) Última fecha de empleo. 3) Tiquete de solicitud de salida. 4) Evidencia de eliminación del usuario (incluida la fecha de desactivación o eliminación).	Preventivo **Frecuencia** Transaccional

5.2.4- Revisión de bajas de usuarios al momento de su término (CIA-4)

Objetivo del control	**Riesgo mitigado**
Los derechos de acceso de los usuarios de aplicaciones cancelados se eliminan oportunamente.	R3
Descripción del Control	
Mensualmente se realiza una revisión de los egresos (empleados y contratistas): - Recursos humanos u otras fuentes relevantes proporcionan una lista de personas retiradas de la organización. - La lista de usuarios que abandonaron se concilia con las listas de usuarios del sistema para garantizar que todas las cuentas de usuarios canceladas se hayan desactivado de manera oportuna, de acuerdo con los SLA[10]. - Las cuentas que fueron desactivadas después del SLA o las cuentas no desactivadas se investigan para determinar que no se produjo ningún acceso después de la fecha de terminación. Si el acceso se produjo después de la baja, se realiza una investigación detallada para verificar que no se realizaron cambios en el sistema ni en los datos que contiene. - Se crea una solicitud de servicio en el sistema de tiquetes para solicitar la desactivación de todas las cuentas no desactivadas. La evidencia de la revisión se almacena en la herramienta de tiquetes.	
Evidencia requerida	**Tipo de control**
1) Evidencia de revisión de egresos, incluyendo: a. Lista de egresos (empleados y contratistas). b. Lista de usuarios utilizada para comparar con la lista de egresos que figura en la letra (a). c. Análisis realizado. d. Acciones de seguimiento, cuando sea necesario.	Detectivo **Frecuencia** Mensual

[10] SLA: Acuerdo de nivel de servicio (Service Level Agreements). Describe métricas como tiempo de actividad, tiempo de entrega, tiempo de respuesta y tiempo de resolución.

5.2.5- Aprobación y revisión del acceso de emergencia (CIA-5.1)

Objetivo del control	**Riesgo mitigado**
Se monitorean las transacciones o actividades sensibles de usuarios con acceso de emergencia en las aplicaciones.	R3, R5
Descripción del control	
Los accesos de emergencia a aplicaciones, bases de datos y sistemas operativos están documentados y aprobados por los propietarios de los procesos de negocio en el sistema de tiquetes: - Los accesos se otorgan por un período de tiempo limitado y se eliminan en el momento oportuno. - Se revisa que las actividades realizadas con el acceso de emergencia sean apropiadas. La evidencia de la aprobación y la revisión de la actividad se almacenan en el sistema de emisión de tiquetes.	
Evidencia requerida	**Tipo de control**
1) Política y procedimiento de acceso de emergencia. 2) Solicitudes de acceso de emergencia con aprobación. 3) Evidencia del registro revisado.	Preventivo **Frecuencia** Transaccional

5.2.6- Revisión de actividades de usuarios con altos privilegios (CIA-5.2)

Objetivo del control	**Riesgo mitigado**
Se monitorean las transacciones o actividades sensibles de usuarios administrativos, super usuarios y los ID genéricos en las aplicaciones.	R3, R4, R5
Descripción del control	
Mensualmente, se revisa la idoneidad de la actividad crítica (incluidos los cambios en la configuración o los datos) realizada en los niveles de la base de datos o de la aplicación. Para los sistemas en los que no se puede monitorear la actividad crítica, se documenta un formulario de aceptación de riesgos (incluidos los controles de mitigación) y es aprobado por el dueño del sistema y el dueño del proceso de negocio. La evidencia de la revisión se almacena en la herramienta tiquetes.	
Evidencia requerida	**Tipo de control**
1) Inventario de actividad crítica que se puede realizar a nivel de base de datos o aplicación. 2) Evidencia de revisión de actividades críticas, incluyendo: a) Registro revisado. b) Acciones de seguimiento, cuando corresponda. 3) Formularios de aceptación de riesgos, si aplica.	Detectivo **Frecuencia** Mensual

5.2.7- Definición de línea base de configuración de seguridad (CIA-6.1)

Objetivo del control	**Riesgo mitigado**
Se definen las configuraciones de seguridad del sistema, incluidas las contraseñas.	R1
Descripción del control	
Los estándares de seguridad están documentados y establecidos para los sistemas operativos, bases de datos y aplicaciones y se revisan anualmente para determinar su idoneidad. Las líneas de base de seguridad se implementan en el momento de la puesta en funcionamiento del sistema. La evidencia de la revisión se almacena en la herramienta de tiquetes.	
Evidencia requerida	**Tipo de control**
1) Estándar de seguridad para cada sistema. 2) Revisión del estándar de seguridad.	Preventivo **Frecuencia** Anual

5.2.8- Revisión de la configuración de seguridad (CIA-6.2)

Objetivo del control	**Riesgo mitigado**
Se aplican las configuraciones de seguridad del sistema, incluidas las contraseñas.	R6
Descripción del control	
Anualmente, se realiza una revisión para garantizar que la línea base de seguridad esté implementada adecuadamente en los sistemas bajo alcance. Cuando la línea base de seguridad no se puede implementar plenamente debido a limitaciones técnicas y/u organizativas, se documenta un formulario de aceptación de riesgos (incluidos los controles de mitigación) y lo aprueban el dueño del sistema y el dueño del proceso de negocio. La evidencia de la revisión se almacena en la herramienta de tiquetes.	

Evidencia requerida	Tipo de control
1) Estándar de seguridad para cada sistema. 2) Evidencia de la revisión para garantizar que la configuración del sistema se implemente de acuerdo con los estándares de seguridad. 3) Formularios de aceptación de riesgos, si aplica.	Detectivo **Frecuencia** Anual

5.2.9- Certificación periódica del acceso de los usuarios de TI (CIA-7)

Objetivo del control	Riesgo mitigado
Los derechos de acceso a los sistemas se controlan periódicamente para comprobar su idoneidad.	R3, R4, R5
Descripción del Control	
Trimestralmente, se realiza una revisión de los usuarios privilegiados de TI en el sistema operativo, base de datos y niveles de aplicación: - Se extraen de los sistemas listas de usuarios y accesos privilegiados de TI. - El propietario del sistema valida la idoneidad de estos accesos de usuario. - Se realiza una verificación para garantizar que solo el equipo de operación tenga acceso para realizar los cambios en el entorno de producción (es decir, ningún desarrollador tenga acceso a la producción). - Se crea una solicitud de servicio en el sistema de tiquetes para solicitar la desactivación de todos los accesos no requeridos. La evidencia de la revisión y corrección se almacena en la herramienta de tiquetes.	
Evidencia requerida	**Tipo de control**
1) Definición de usuarios privilegiados de TI, por sistema y capa. 2) Evidencia de la revisión del usuario, que incluye: a. Listas de usuarios y accesos privilegiados. b. Evidencia de la revisión por parte de cada propietario designado. c. Acciones de seguimiento, cuando corresponda.	Detectivo **Frecuencia** Trimestral

5.2.10- Certificación periódica del acceso de usuarios del negocio (CIA-8)

Objetivo del control	Riesgo mitigado
Los derechos de acceso a los sistemas se controlan periódicamente para comprobar su idoneidad.	R3
Descripción del control	
Dos veces al año se realiza una revisión del acceso de los usuarios del negocio a nivel de aplicación: - Las listas de usuarios del negocio y derechos de acceso a nivel de aplicación se extraen del sistema. - Estos accesos de usuarios se envían a los propietarios del negocio, quienes garantizan que sean válidos y adecuados según la descripción de su puesto y sus necesidades laborales. - Se crea una solicitud de servicio en el sistema de tiquetes para solicitar la desactivación de todos los accesos no requeridos. La evidencia de la revisión y corrección se almacena en la herramienta de tiquetes.	
Evidencia requerida	**Tipo de control**
1) Evidencia de la revisión del usuario, que incluye: a. Listas de usuarios del negocio y derechos de acceso a nivel de aplicación. b. Evidencia de la revisión por parte de cada propietario designado. c. Acciones de seguimiento, cuando corresponda.	Detectivo **Frecuencia** Semestral

5.3- Implementación de controles

En esta sección se presenta un desglose detallado del proceso para la implementación y ejecución de los controles mencionados en el apartado anterior.

5.3.1- Política y procedimiento para la gestión de acceso de usuario (CIA-1)

1) Definir políticas y procedimientos para la gestión de acceso que cubra lo siguiente:
   a. Herramientas y sistemas de emisión de tiquetes utilizados para el proceso de asignación de acceso que contienen varias opciones y categorías para las siguientes opciones:

- sistemas de concesión de acceso (aplicación, base de datos, sistema operativo),
- niveles de acceso (acceso genérico, acceso privilegiado, acceso de administrador, modificación del acceso existente, cuentas de servicio),
- tipo de empleado (empleado de tiempo completo, empleado de tiempo parcial, contratista, tercerizado).

b. Grupo de personas/usuarios/designaciones que pueden solicitar la creación de acceso.
c. Matriz de aprobación (gerente de línea, dueño del sistema, dueño de procesos de negocio globales).
d. Acceso a responsabilidades y cronogramas de creación (SLA).
e. Comunicación de credenciales y política de contraseñas (por debajo).
f. Comprobaciones de separación de funciones que deben realizarse antes de crear/modificar el acceso.
g. Política de revocación de acceso que incluye lo siguiente:
   - cronogramas de revocación de acceso (SLA),
   - se recibirán autorizaciones para todos los sistemas a los que tuvo acceso el usuario en proceso de baja,
   - responsabilidades de revocación de acceso.
h. Describir las convenciones de nomenclatura de usuarios, incluidos las identidades genéricas y de servicio.
i. Incluir las actividades de seguimiento a realizar.
j. Definir qué tipos de roles se asignan en caso de emergencia a nivel de sistema operativo, base de datos y aplicación. Los tipos de acceso que normalmente se proporcionan en caso de emergencia son privilegios de tecnología de información o administrador. Si este acceso se puede brindar a nivel de negocio, lo cual no es habitual, pero por algún requerimiento específico la organización lo está considerando, la política debe definirlo.

2) Asegurar que la política sea revisada de manera periódica (por lo menos una vez al año).
3) Memorándum de la herramienta de flujo de trabajo/sistema de emisión de tiquetes que muestra una descripción de las medidas de seguridad tomadas sobre la herramienta de emisión de tiquetes/flujo de trabajo utilizada para respaldar el proceso. Este apéndice incluye acceso para mantener flujos de trabajo, funciones de administrador, seguimiento de auditoría que no se puede modificar ni alterar y acceso a la herramienta.
4) Asegurar de que la evidencia de la revisión esté documentada y colocada en la herramienta de tiquetes.

5.3.2- Aprobación de nuevos usuarios y acceso al sistema (CIA-2)

1) Definir, para cada uno de los sistemas en alcance, cómo se obtendrán los informes de creación de acceso de usuarios (incluidos filtros/consultas/informes). Si no es posible realizar informes, evaluar si se requiere un desarrollo.

2) Garantizar que los flujos de trabajo de acceso de usuarios se implementen en la herramienta de emisión de tiquetes, respaldada por la política del control CIA-1 y por la matriz de aprobación de acceso de usuarios.
3) Garantizar que los flujos de trabajo cuenten con la tarea de verificación de segregación de funciones (incluida la validación a nivel de grupo cuando corresponda) para las aplicaciones con riesgos de separación de funciones definidos.
4) Asegúrese que todos los niveles de aprobaciones son cumplidos antes de otorgar el acceso al menos por el equipo del negocio o por el equipo de tecnología de la información, por ejemplo, cuentas de servicio.
5) Asegúrese de que se realice la verificación de segregación de funciones antes de realizar las aprobaciones.
6) Asegúrese de que el acceso solo se proporcione después de que se hayan realizado todas las aprobaciones.
7) Asegúrese que todos los accesos proporcionados en los sistemas (roles, perfiles) estén de acuerdo con una solicitud aprobada y que no se hayan otorgado permisos adicionales.
8) Cuando corresponda, asegúrese de que toda la evidencia de respaldo fuera de la herramienta de emisión de tiquetes esté almacenada en el tiquete.

5.3.3- Baja transaccional del acceso de los usuarios (CIA-3)

1) Definir si la notificación de salidas se activará y enviará automáticamente al sistema de tiquetes (proceso automatizado), o si será enviada por el área de recursos humanos u otra área al equipo de tecnología de la información para crear los tiquetes manualmente (proceso manual). Cuando sea posible, opte por una notificación automatizada/integrada. Se debe tener en cuenta que las bajas podrían ser iniciadas por el área de recursos humanos (empleados), adquisiciones (contratistas) o los proveedores (proveedor de servicios).
2) Asegúrese de que las notificaciones incluyan a todo el personal de la organización, considerando empleados, tercerizados, contratistas, aprendices, proveedor de servicios) y defina quién será el propietario de la lista de tercerizados, contratistas y otro personal externo.
3) Implementar un mecanismo para identificar empleados en el sistema de recursos humanos y contratistas en usuarios en los sistemas relevantes (es decir, a través de correo electrónico o datos clave como número de identidad, usuario de identidad de empleado, correo electrónico).
4) Revisar todos los usuarios que no estén asignados a una persona existente y corregir cuando sea necesario.
5) Una vez que se recibe una notificación de egreso, para todos los que salen, incluidos terceros, el propietario del sistema de tecnología de información genera un tiquete de eliminación de acceso. El tiquete debe contener detalles de los sistemas y accesos que se eliminarán y la última fecha de trabajo, o debe haber varios tiquetes, uno para cada sistema.
    a. En caso de tener una identificación entre empleado y usuario de aplicación, los tiquetes pueden ser por aplicación.

b. Si no es posible demostrar la correlación entre el empleado y el usuario de la aplicación, se deben enviar tiquetes para todos los sistemas dentro del alcance.

6) Asegúrese de que el acceso esté deshabilitado/eliminado oportunamente, de acuerdo con el periodo de tiempo definido en la política de acceso de usuarios.
7) Asegúrese de que la evidencia de la eliminación esté documentada en el sistema de emisión de tiquetes, por ejemplo, basándose en un paso de aprobación del administrador del sistema.
8) Si no es posible visualizar la fecha en la que un usuario ha sido deshabilitado, asegúrese de obtener capturas de pantalla durante el proceso de deshabilitación y conservarlas en el sistema de emisión de tiquetes. No se deben realizar cambios de usuario adicionales después de la fecha de las capturas de pantalla.

5.3.4- Revisión de bajas de usuarios al momento de su término (CIA-4)

1) Implementar una revisión mensual para garantizar que se hayan eliminado todos los egresos en todas las aplicaciones incluidas en el alcance:
   i. Obtener el informe de egresos mensuales de todo el personal (empleados, contratistas, tercerizados, proveedores de servicios) del área de recursos humanos u otra área como adquisiciones, gerentes de contratos, con detalles de su última fecha de trabajo (a). Asegúrese de que el informe incluya detalles de cómo se generó.
   ii. Si no se puede obtener un listado de egresos de terceros, se deberá implementar una certificación mensual (CIA-7 y CIA-8).

   Para revisiones fuera de línea, en la pantalla, verificando para validar que los que los egresos se hayan eliminado, lo que requiere capturas de pantalla para cada cuenta de usuario y sistema:
   i. Obtener los usuarios completos con acceso a cualquier sistema del alcance (b). Debe incluir detalles de cómo se generan los informes.
   ii. Para cada aplicación dentro del alcance, realice una comparación entre (a) y (b) e identifique cualquier usuario que no haya sido eliminado dentro del cronograma esperado.

   Para revisiones en línea, en base a un reporte de usuarios del sistema, validar que el usuario haya sido eliminado:
   i. Realizar una búsqueda en los sistemas bajo alcance para confirmar si el usuario ha sido deshabilitado dentro del cronograma esperado. Si el sistema no muestra la fecha de inhabilitación, según definición del control CIA-3, deberá existir evidencia en el tiquete de baja de acceso. Si no hay pruebas, considere al usuario como "no eliminado" o identifique un método diferente para validar la eliminación.
2) Para aquellos usuarios que no fueron desactivados oportunamente, realice lo siguiente:
   i. Identificar el motivo por el cual no se ha eliminado el acceso.
   ii. Crear un tiquete de remoción de acceso para deshabilitar al usuario en el sistema dentro del alcance.

iii. Revisar la fecha del último inicio de sesión del usuario para confirmar si el usuario accedió al sistema después de la fecha de salida (c).
iv. Si los resultados de (c) muestran que el usuario inició sesión en el sistema después de la fecha de salida, realice un análisis de uso indebido verificando los registros y las transacciones financieras relevantes asociadas con el nivel de acceso, para garantizar que no se hayan realizado acciones no autorizadas. Esto se puede documentar en un archivo de texto describiendo los pasos realizados, los datos revisados y las conclusiones a las que se llegó.
v. Documentar este análisis y asegurarse de conservar evidencia de cómo se extrajo la información para realizar la investigación.
vi. Si existe un requisito comercial para permitir dicho acceso, identificar controles mitigantes y documentar el riesgo y el razonamiento en un registro de riesgos.

3) Asegúrese de que esta revisión esté documentada con todos los pasos realizados y aprobados por una persona adecuada.
4) Colocar la evidencia de los puntos de revisión y seguimiento en la herramienta de tiquetes.

5.3.5- Aprobación y revisión del acceso de emergencia (CIA-5.1)

Definición del proceso: El acceso de emergencia se proporciona cuando se espera o ha ocurrido una falla y se requiere un cambio para prevenir o corregir la situación. Puede que nunca suceda que se proporcione acceso de emergencia, pero es necesario planificar para tal caso y garantizar que existan controles, incluida la eliminación del acceso después del tiempo aprobado y la revisión de las actividades realizadas. Estas solicitudes de acceso deben evitarse en la medida de lo posible, incluso garantizando que el equipo de operación tenga los accesos necesarios para gestionar estas situaciones cuando ocurran.

1) Definir un documento de políticas y procedimientos para la gestión del acceso de emergencia que cubra lo siguiente, entre otros:
   a. Qué roles se otorgarán en caso de emergencia para cada sistema dentro del alcance, incluyendo aplicación, base de datos y sistema operativo.
   b. Matriz de aprobación de acceso de emergencia.
   c. Cómo se solicitará y aprobará el acceso, es decir, en qué categoría del sistema de emisión de tiquetes, para garantizar la integridad de la población.
   d. Durante cuánto tiempo se proporcionará el acceso y el mecanismo para garantizar que estos tiempos sean monitoreados, con el acceso eliminado de manera oportuna y las extensiones se aprueben en consecuencia.
   e. Garantizar que se puedan registrar las actividades críticas realizadas con los usuarios de acceso de emergencia.
   f. En caso de que no sea posible realizar registros, evalúe el uso de herramientas existentes o la implementación de nuevas herramientas para administrar el acceso con privilegios elevados con funcionalidad de registro.

g. Quién será el propietario de la revisión del registro para garantizar que las actividades realizadas por el usuario de emergencia estuvieran en línea con la solicitud aprobada.
h. Qué situaciones en las que el acceso de emergencia podría ser necesario, como ejemplos.
i. Qué pasos se llevarán a cabo para garantizar que el acceso de emergencia solo se conceda con un tiquete aprobado y el acceso permanezca restringido.

2) Implementar la categoría de tiquetes de emergencia y la matriz de aprobación de acceso de emergencia en el sistema de tiquetes.
3) Defina qué debe incluirse en el tiquete: sistemas de asignación de acceso (para qué aplicación, base de datos, sistema operativo), detalles del usuario (es decir, la persona que desea acceso de emergencia), período de tiempo para el acceso de emergencia, motivo por el cual se requiere el acceso, lista de actividades a realizar.
4) Asegúrese de que el acceso de emergencia sea revocado después del período de tiempo necesario y adjunte la documentación de respaldo en el tiquete.
5) Realizar la revisión del registro para garantizar que las actividades realizadas coincidan con la solicitud aprobada, documentar y cargarlo en el tiquete.
6) Asegúrese de que la evidencia de la revisión esté documentada y colocada en el tiquete de acceso de emergencia relacionado.

5.3.6- Revisión de actividades de usuarios con altos privilegios (CIA-5.2)

1) Documentar qué actividad se considera crítica para cada aplicación dentro del alcance y debe monitorearse y cómo se realiza el monitoreo (informes de origen, filtros, exclusiones, excepciones, repositorio).
2) Mensualmente, asegúrese de que la actividad crítica en los niveles de aplicación y base de datos se revise realizando los siguientes pasos:
   a. Extraer los registros de actividades críticas, cuando existan. Incluya documentación para garantizar que esté completa.
   b. Divida la lista según el sistema o el proceso de negocio y distribuya la lista al propietario correspondiente.
3) Cada propietario deberá validar el listado y obtener el registro de actividades realizadas y analizar si son adecuadas.
4) Cada revisor deberá identificar cualquier transacción que esté fuera del proceso ordinario y revisarla.
5) Cada propietario debe aprobar toda actividad apropiada.
6) En el caso de sistemas que no tengan capacidades de registro o seguimiento, identificar o actualizar los controles de mitigación, y documentar el riesgo y el argumento en un registro de riesgos.
7) Asegurar que haya una actualización al menos anual de las actividades que se están revisando para agregar/eliminar actividades que ya no se consideran críticas o que se han identificado nuevas.
8) Colocar la evidencia de los puntos de revisión y seguimiento en la herramienta de tiquetes.

Observación: La lista de usuarios privilegiados debe coincidir con la lista utilizada en el control CIA-7.

5.3.7- Definición de línea base de configuración de seguridad (CIA-6.1)

1) Definir los requisitos básicos del sistema, para cada sistema dentro del alcance, a nivel de aplicación, base de datos y sistema operativo, que contenga detalles de los parámetros mínimos de seguridad del sistema que deben habilitarse para garantizar el cumplimiento de los estándares de seguridad SOX. Como mínimo, asegúrese de que el documento incluya, al menos, lo siguiente:
   a. Parámetros mínimos de la contraseña: longitud mínima y complejidad, mayúsculas/minúsculas, números, caracteres especiales; antigüedad de la contraseña e historial de contraseñas.
   b. Bloqueo de cuenta después de n veces de intento de conexión fallida.
   c. Política de cifrado de contraseñas.
   d. Acceso restringido a las cuentas del sistema (es decir, configuración Su/Sudo/Admin).
      Observación: Esto debe documentarse para sistema operativo y base de datos. Para las aplicaciones, solo se aplican configuraciones de contraseña para SOX.
2) Defina cómo se compararán estos requisitos básicos con la información del sistema (extracción de configuración/herramientas/etc.), incluido el IPE[11] y evidencia adicional como capturas de pantalla de la configuración.
3) Programar una revisión anual de los parámetros de seguridad básicos y definir el propietario de la revisión.

5.3.8- Revisión de la configuración de seguridad (CIA-6.2)

1) Con base en el método de revisión definido, extraer la configuración de seguridad relevante de cada uno de los sistemas en alcance, a nivel de aplicación, base de datos y sistemas operativo. Asegúrese de documentar cómo se extrae la información (IPE), es decir, capturas de pantalla, reporte.
2) Compare la configuración del sistema con requisitos básicos de seguridad definida.
   En caso de identificar discrepancias:
   a. Crear una solicitud de cambio para modificar la configuración de seguridad para alinearla con la línea de base de seguridad.
   b. Si una configuración de seguridad no cumple, defina una acción correctiva y realice un seguimiento periódico.
   c. Si no se puede cumplir con la línea de base de seguridad debido a una limitación del sistema, documente una evaluación de riesgos para detallar cualquier riesgo generado por una configuración de seguridad no configurada correctamente e identifique controles de mitigación. Asegúrese de que esto sea aprobado por el dueño del negocio relevante para el sistema.

[11] IPE: información proveída/producida por la entidad (information provided/produced by the entity).

3) Documentar todos los análisis realizados en la herramienta de tiquetes.

5.3.9- Certificación periódica del acceso de los usuarios de TI (CIA-7)

1) Definir para cada aplicación dentro del alcance, qué usuarios se considerarán usuarios privilegiados de TI[12] y, por lo tanto, dentro del alcance de esta revisión (roles, responsabilidades, perfiles), incluyendo:
   a. A nivel de aplicación, solo los super usuarios que pueden cambiar/configurar el comportamiento de la aplicación. Estos roles están dedicados a los usuarios de TI y no deben confundirse con los roles privilegiados otorgados a los usuarios del negocio.
   b. A nivel de base de datos, usuarios (incluidos los usuarios del sistema) que pueden cambiar la estructura de la base de datos y los privilegios de usuario.
   c. A nivel de sistema operativo, usuarios que pueden instalar aplicaciones o parches, o modificar la configuración del sistema.

   Observación: Este control debe cubrir tanto a los usuarios nominales como a los genéricos (incluidos los del sistema o servicio). La documentación debe contener la definición del propietario (es decir, una persona identificada) para cada usuario genérico.
2) Definir quién será el responsable de revisar la validez del usuario en cada nivel (aplicación, base de datos, sistema operativo). Crear una matriz de revisión del propietario.
3) Definir el mecanismo para solicitar confirmación a los revisores (correo electrónico, tiquetes).
4) Definir cómo se extraerán las listas de usuarios para cada solicitud, incluida la evidencia para garantizar su integridad (IPE). Evaluar el desarrollo, si los informes no existen en la versión actual de los sistemas.
5) Obtenga la lista completa de identidades de usuarios de TI (a nivel de aplicación, sistema operativo y base de datos). Asegúrese de que los detalles para garantizar que estén completos estén documentados (IPE).
6) Divida la lista según la “Matriz de revisión del propietario” y distribuya la lista al propietario del sistema correspondiente. Asegúrese de que todos los usuarios hayan sido distribuidos.
7) Cada propietario del sistema de revisión debe validar la lista y evaluar lo siguiente:
   a. ¿La persona que tiene acceso a esta cuenta es adecuada?
   b. ¿Siguen siendo necesarias estas cuentas privilegiadas, es decir, todavía es un empleado/contratista, las responsabilidades laborales actuales aún requieren acceso?
   c. Los propietarios deben proporcionar confirmación y cerrar sesión en todos los accesos apropiados.
   d. Tiene esta persona un rol de desarrollador que no debería existir en el entorno de producción.
   e. Asegúrese de que los nombres de las descripciones de los puestos estén claramente definidos, no contengan títulos como "desarrollador", y que la

[12] TI: Tecnología de información

descripción de las funciones indique claramente quiénes pueden realizar cambios. Cuando se descubre que un desarrollador tiene acceso al ambiente de producción, asegúrese de que se investigue y se presente una solicitud para eliminar su acceso.

f. En caso de que exista un requisito de negocio o un límite técnico para permitir que los desarrolladores accedan o realicen cambios en la producción, documente este riesgo, identifique controles de mitigación y asigne propietario y detalles adicionales en una aceptación de riesgo.
g. En caso de que los proveedores tengan acceso para desarrollar y trasladar cambios a producción, se deben considerar los siguientes controles compensatorios, dependiendo del nivel de riesgo: El acceso de los proveedores se otorga bajo demanda (solo durante un tiempo limitado, es decir, las ventanas de mantenimiento) y luego es removido. Luego revise los registros para asegurarse de que solo se ejecutaron los cambios aprobados (revise que cierta configuración clave, tablas, no se modificaron a menos que sea necesario).

8) Asegúrese de que se hayan recibido todas las respuestas para completitud.
9) En caso de acceso innecesario:
   a. Levantar un tiquete para eliminar los accesos innecesarios, no relevantes y no autorizados.
   b. Seguimiento de la ejecución de tiquetes para asegurar que se eliminaran todos los accesos innecesarios.
   c. Seguir el procedimiento descrito en el punto 2 del control CIA-4 (usuarios que no fueron desactivados oportunamente).
10) Si existe un requisito de negocio para permitir que los usuarios comerciales tengan acceso con privilegio de TI, identifique controles de mitigación y documente el riesgo y argumentación en una aceptación de riesgo.
11) Colocar la evidencia de los puntos de revisión y seguimiento en la herramienta de tiquetes.

5.3.10- Certificación periódica de acceso de usuarios del negocio (CIA-8)

1) Con base en la definición realizada para el control CIA-7, asegurar que cualquier usuario y/o rol/responsabilidad/perfil de negocio no incluido en la revisión de TI esté cubierto.
   Observación: El 100% de los usuarios deben estar certificados, ya sea por el control CIA-7 o por el control CIA-8.
2) Definir con los equipos de negocio quiénes serán los responsables de revisar la validez del usuario para cada aplicación dentro del alcance. Crear una matriz de revisión del propietario del negocio.
3) Definir el mecanismo para solicitar confirmación a los revisores (correo electrónico, tiquetes).
4) Definir cómo se extraerán las listas de usuarios para cada solicitud, incluida la evidencia para garantizar su integridad (IPE). Evaluar el desarrollo si los informes no existen en la versión actual de los sistemas.
5) Obtenga la lista completa de identidad de usuario y su acceso (especialmente a nivel de aplicación). Asegúrese de que los detalles para garantizar que estén completos estén documentados (IPE).

6) Divida la lista según la matriz de revisión de propietario y distribuya la lista al propietario correspondiente. Asegúrese de que todos los usuarios se hayan distribuido para que estén completos.
7) Cada propietario de revisión debe validar la lista y evaluar lo siguiente:
   a. ¿El usuario sigue siendo un empleado/contratista activo de la compañía?
   b. ¿Es apropiada la función actual (es decir, puesto de trabajo) asignada a cada propietario o tienen acceso innecesario?

   Los propietarios de negocio deben proporcionar confirmación y aprobar todos los accesos apropiados.
8) Asegúrese de que se hayan recibido todas las respuestas para completitud.
9) En caso de acceso innecesario:
   a. Levantar un tiquete para eliminar el acceso no autorizado.
   b. Seguimiento de la ejecución de tiquetes para asegurar que se eliminaran todos los accesos innecesarios.
   c. Análisis de las actividades realizadas durante el periodo de validez del acceso.
10) Si existe un requisito de negocio para permitir que los usuarios de TI tengan acceso con privilegio de negocio, identifique controles de mitigación y documente el riesgo y el razonamiento en un registro de riesgos.
11) Colocar la evidencia de los puntos de revisión y seguimiento en la herramienta de tiquetes.

5.4- Flujograma de controles

5.4.1- Aprobación de nuevos usuarios y acceso al sistema (CIA-2)

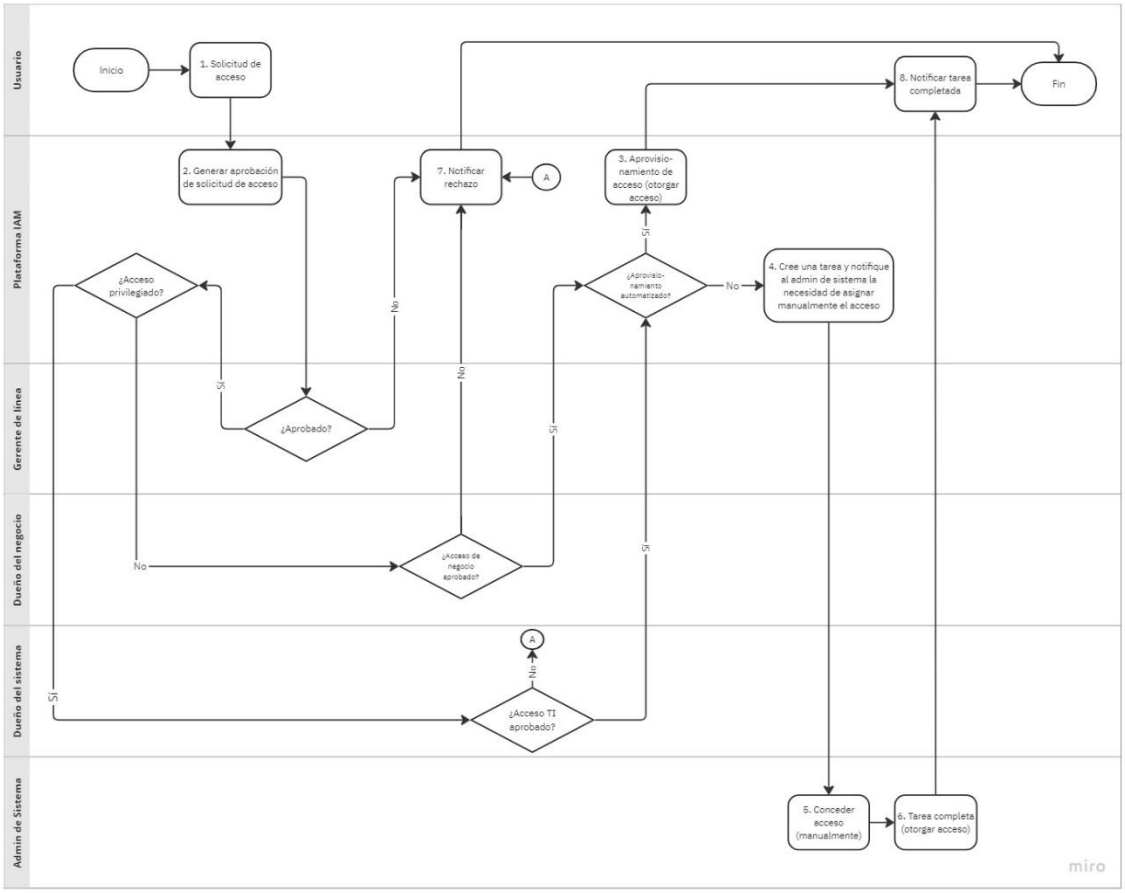


Ilustración 1 Flujograma CIA-2

5.4.2- Baja transaccional del acceso de los usuarios (CIA-3)

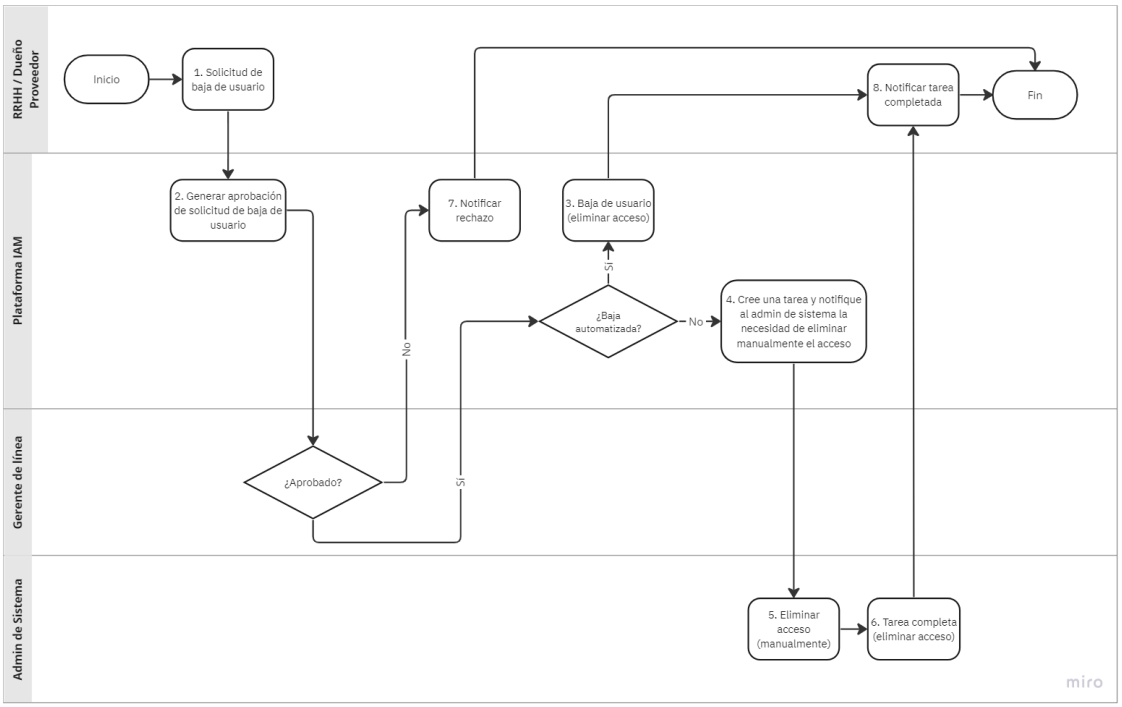


Ilustración 2: Flujograma CIA-3

5.4.3- Revisión de bajas de usuarios al momento de su término (CIA-4)

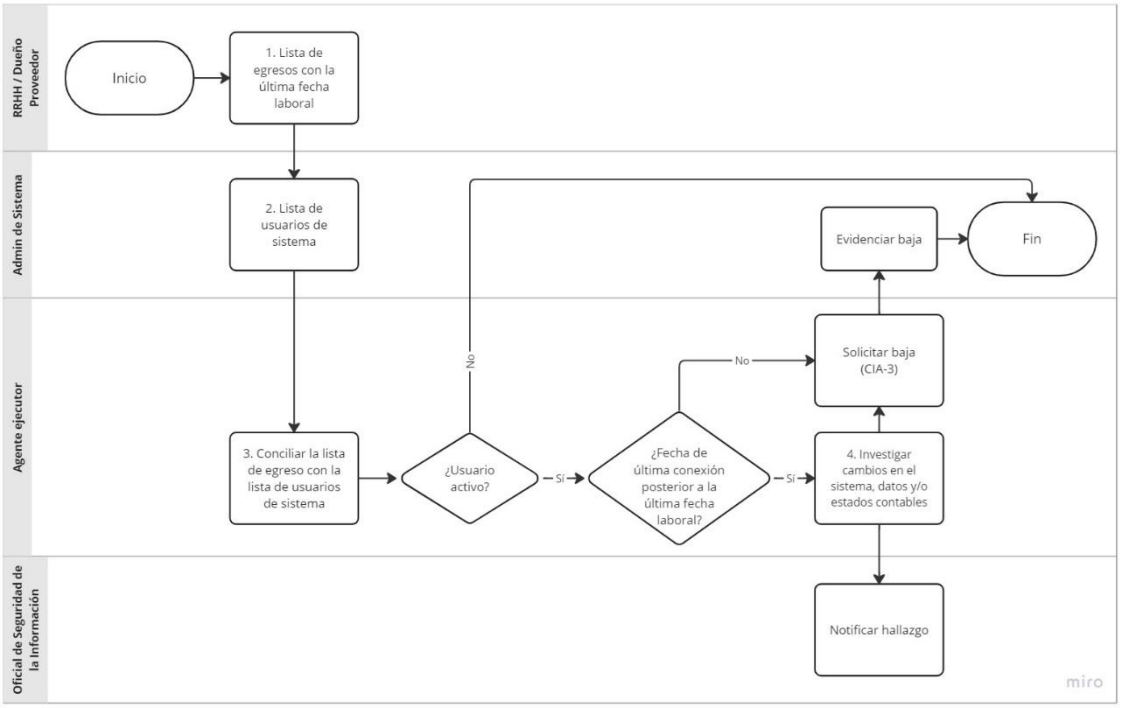


Ilustración 3: Flujograma CIA-4

5.4.4- Aprobación y revisión del acceso de emergencia (CIA-5.1)

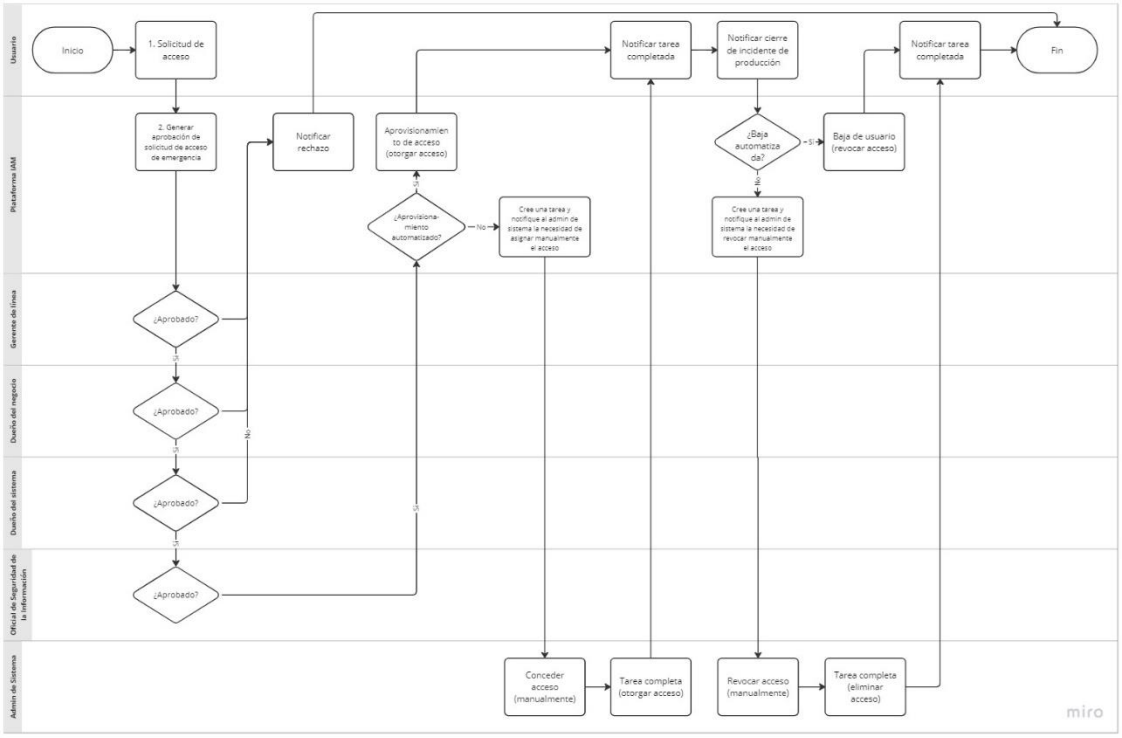


Ilustración 4: Flujograma CIA-5.1

5.4.5- Revisión de actividades de usuarios con altos privilegios (CIA-5.2)

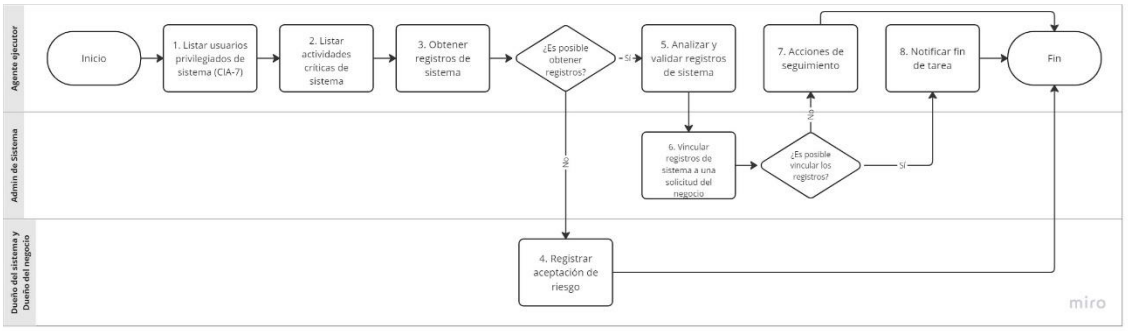


Ilustración 5: Flujograma CIA-5.2

5.4.6- Revisión de la configuración de seguridad (CIA-6.2)

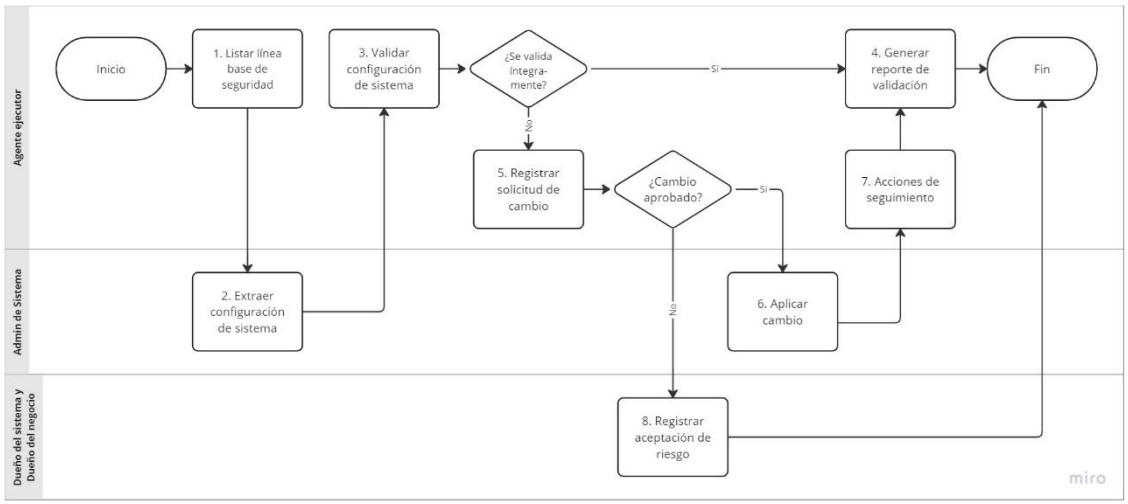


Ilustración 6: Flujograma CIA-6.2

5.4.7- Certificación periódica del acceso de los usuarios de TI (CIA-7)

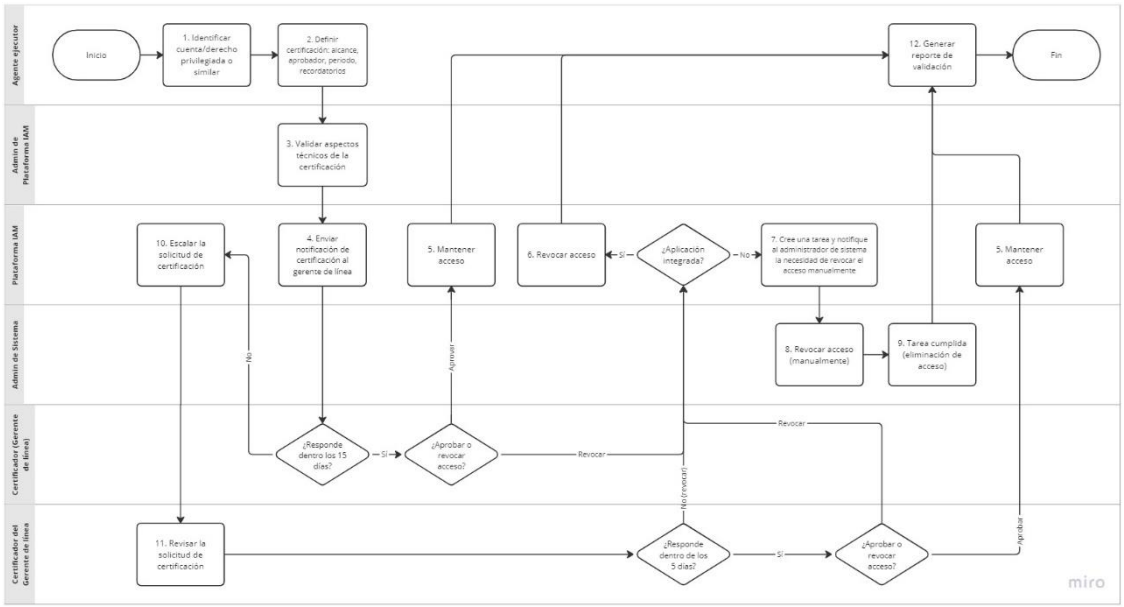


Ilustración 7: Flujograma CIA-7

5.4.8- Certificación periódica de acceso de usuarios del negocio (CIA-8)

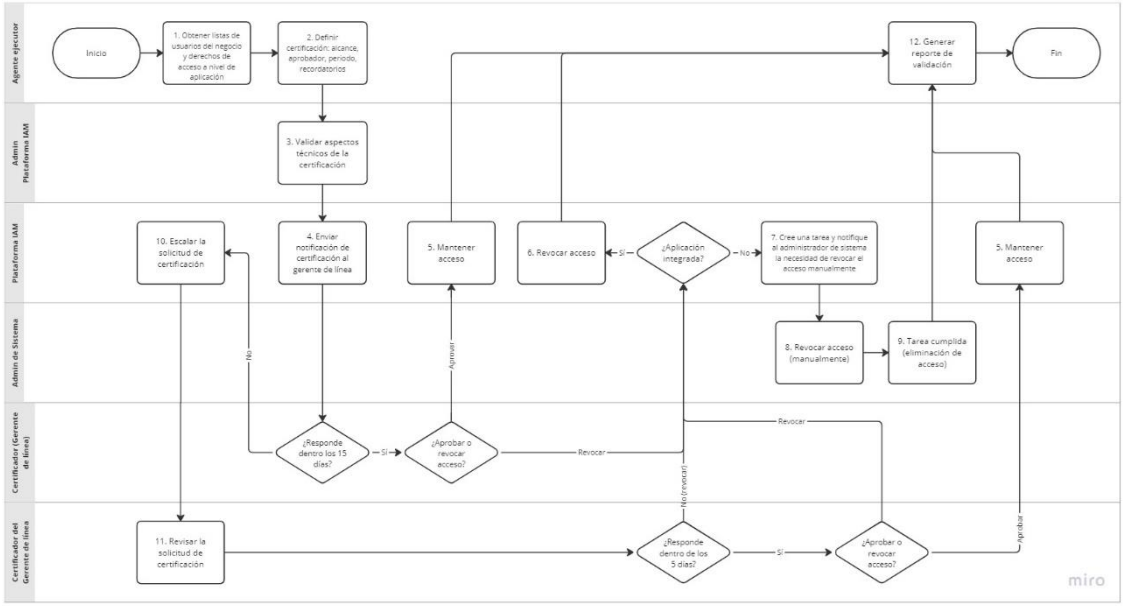


Ilustración 8: Flujograma CIA-8

5.5- Mapeo de controles CIA con la ISO/IEC 27002

La norma internacional ISO/IEC 27002 brinda orientación a una organización a establecer, implantar y mejorar un sistema de gestión de seguridad de la información.

La norma cita capacidades operativas que son esenciales para la implementación y el funcionamiento efectivos de controles. Estas capacidades proporcionan la base sobre la cual se construyen los controles y garantizan que se apliquen de manera consistente y eficaz en toda la organización.

Con base a la capacidad operativa en gestión de identidad y acceso, se procede a realizar un mapeo entre los controles de gestión de acceso implantados en la organización. Se agrega el control organizacional con referencia al control 5.1 de la ISO/IEC 27002 por ser la guía de definición de procesos.

Tipo de control	Control CIA / Control ISO/IEC	1	2	3	4	5.1	5.2	6.1	6.2	7	8
Organizacional	5.1. Políticas de seguridad de la información	✓						✓			
	5.3. Segregación de funciones		✓				✓			✓	
	5.15. Control de acceso		✓	✓	✓	✓			✓	✓	✓
	5.16. Gestión de identidad		✓	✓	✓	✓					
	5.17. Información de autenticación								✓		
	5.18. Derechos de acceso									✓	✓
Tecnológico	2. Derechos de acceso privilegiado		✓			✓				✓	
	3. Restricción de acceso a la información		✓			✓	✓			✓	
	4. Acceso al código fuente									✓	
	5. Autenticación segura								✓		

Tabla 2: Cruce entre controles ISO/IEC 27002 y controles internos

Luego de realizar la comparación de controles, es posible afirmar que se cuenta con los controles básicos para la gestión de identidad y accesos. Estos controles no son absolutos y siempre se debe tener en cuenta que deben ser complementadas con otros tipos de controles, como podría ser controles físicos, de procesos, y controles educativos y de concientización.

6- Resultados

Los controles orientados a la gestión de acceso de usuarios, como la segregación de funciones, la revisión de autorizaciones y la gestión de contraseñas, contribuyen al cumplimiento de la política de gestión de acceso. Estos mecanismos facilitan la identificación y prevención de riesgos específicos relacionados con el acceso no autorizado, el uso indebido de recursos y la manipulación de datos. La implementación de estos controles genera beneficios tangibles, como la reducción del fraude, la protección de la información confidencial y la mejora de la eficiencia operativa.

A continuación, se citan resultados, detecciones, como ventajas competitivas con base a los controles SOX implementados en la organización.

6.1- Política y procedimiento para la gestión de acceso de usuario (CIA-1)

a. Involucramiento de las partes interesadas.
b. Roles y responsabilidades definidos.
c. Proceso de gestión de cuentas de usuario optimizado.

6.2- Aprobación de nuevos usuarios y acceso al sistema (CIA-2)

a. Reducción en el número de accesos no autorizados a los sistemas y datos de la organización.
b. Se ha mejorado la seguridad de la información confidencial.

c. Reducción del tiempo necesario para aprobar una solicitud de acceso de 72 horas a 48 horas posterior a la implementación del proceso de revisión automatizado.

6.3- Baja transaccional del acceso de los usuarios (CIA-3)

a. Deshabilitación o eliminación de accesos innecesarios.
b. Restricción del acceso a los sistemas.
c. Reducción de los riesgos asociados a accesos no autorizados, como ser fuga de datos, reputación de marca, pérdida de datos.

6.4- Revisión de bajas de usuarios al momento de su término (CIA-4)

a. Hallazgo de errores en el proceso automatizado de bajas en el gestor de identidades.
b. Hallazgo en la capa de base de datos, esquemas asignados a usuarios nominales.
c. Adicionalmente, una vez por año, se realiza la limpieza de usuarios (*clean up*), disminuye el riesgo de contar con usuarios huérfanos.
d. Con los dueños de usuarios, se refuerza periódicamente la importancia de comunicar las bajas de personas tercerizadas y proveedores, pues en una oportunidad hubo un retraso de 60 días en la comunicación de bajas.

6.5- Aprobación y revisión del acceso de emergencia (CIA-5.1)

a. Se cuenta con el proceso definido para control y monitoreo de uso de accesos de emergencia, condicionando su uso a situaciones justificadas y revisando su pertinencia.

6.6- Revisión de actividades de usuarios con altos privilegios (CIA-5.2)

a. Hallazgo de errores de procesos automáticos en el sistema financiero con el seguimiento de actividades sensibles por usuarios privilegiados de TI.
b. Hallazgo de registros de actividades de proveedores que no han sido contemplados en la gestión de cambios.
c. Identificación de actividades críticas en los sistemas financieros, proceso que facilita la detección y prevención actividades sospechosas o maliciosas.

6.7- Definición de línea base de configuración de seguridad (CIA-6.1)

a. Se estableció configuraciones de seguridad estándar para los sistemas, reduciendo la superficie de exposición a amenazas.

6.8- Revisión de la configuración de seguridad (CIA-6.2)

a. En la primera ejecución del control, se promocionó las buenas prácticas para evitar vulnerabilidades y se logró optimizar la configuración de seguridad de los sistemas.
b. Gobernanza de configuración de seguridad a nivel aplicación, base de datos y sistema operativo.

c. En migraciones de plataformas, se ejecuta el control y se cuenta con la certeza que las configuraciones de seguridad están establecidas desde el inicio.

6.9- Certificación periódica del acceso de los usuarios de TI (CIA-7)

a. Identificación de usuarios que ya no necesitan acceso a ciertos recursos.
b. Identificación usuarios que tienen acceso a recursos que no deberían tener.
c. Identificación de accesos que no se están utilizando y que pueden ser eliminados.

6.10- Certificación periódica de acceso de usuarios del negocio (CIA-8)

a. Identificación de usuarios activos, pertenecientes a personas que ya cuentan con estado retirado en la organización.
b. Revisión y validación de la pertinencia de los accesos de usuarios del negocio, asegurando que se ajusten a sus roles y responsabilidades.

7- Auditoría

En la organización, se cuenta con tres tipos de auditorías. Estas trabajan juntas de manera complementaria para fortalecer el sistema de control interno de la organización y asegurar el cumplimiento de la Ley SOX. Primeramente, el equipo de control interno se encarga de la implementación y mantenimiento de los controles. La auditoría interna evalúa la eficacia del sistema y realiza recomendaciones para su mejora. La auditoría externa proporciona una opinión independiente sobre la confiabilidad de la información financiera.

Cada función utiliza diferentes metodologías y herramientas para llevar a cabo su trabajo. La auditoría interna y la auditoría externa deben ser independientes de la gerencia para garantizar su objetividad. Es fundamental una comunicación efectiva entre las tres funciones para asegurar la coordinación y el trabajo en equipo.

7.1- Auditoría Interna

7.1.1- Equipo de control interno

El equipo de control interno juega un papel fundamental en la implementación y el mantenimiento de los controles SOX. Sus funciones abarcan:

Pruebas de los controles: El equipo evalúa la eficacia de los controles existentes mediante pruebas y análisis específicos, verificando que estos operen de forma efectiva y cumplan con su propósito.

Diseño del control: Cuando se identifican riesgos o deficiencias en los controles existentes, el equipo se encarga de desarrollar e implementar nuevos controles para mitigar estos riesgos y fortalecer el sistema de control interno.

Asesoría y gobierno: El equipo brinda apoyo y orientación a la gerencia en materia de control interno, promoviendo una cultura de control dentro de la

empresa. Esto incluye ofrecer capacitación, desarrollar políticas y procedimientos, y realizar evaluaciones de riesgos.

Certificación SOX: Los informes y análisis del equipo sirven como base para la certificación anual de la gerencia sobre la efectividad del control interno. Esta certificación es un requisito fundamental para el cumplimiento de la Ley SOX.

Las actividades del equipo de control interno se orientan a lograr los siguientes objetivos:

Garantizar la existencia de un sistema de control interno adecuado y efectivo: El equipo se asegura de que la empresa cuente con un sistema de control interno robusto y bien diseñado, que pueda prevenir, detectar y corregir errores o irregularidades en la información financiera.

Proteger los activos de la empresa contra el fraude y el mal uso: El equipo implementa medidas para proteger los activos de la empresa contra el fraude, el robo y el uso indebido.

Asegurar el cumplimiento de las leyes y regulaciones aplicables: El equipo vela por que la empresa cumpla con todas las leyes y regulaciones aplicables a su actividad, incluyendo la Ley SOX.

Contribuir a la mejora continua de la organización: El equipo busca constantemente oportunidades para mejorar el sistema de control interno y la gestión de riesgos de la empresa.

7.1.2- Auditoría interna

La función de auditoría interna es fundamental para el éxito de la implementación de los controles SOX en la organización. Sus funciones abarcan:

Evaluación independiente: La auditoría interna realiza revisiones objetivas y sistemáticas de los procesos, actividades y riesgos de la empresa. Estas revisiones se basan en metodologías y herramientas de auditoría reconocidas, y permiten identificar las áreas donde los controles son adecuados y aquellos que requieren mejoras.

Identificación y reporte de deficiencias: La auditoría interna identifica las áreas donde los controles no son adecuados o no están funcionando correctamente. Estas deficiencias se reportan a la gerencia para que tome las medidas correctivas necesarias, asegurando así la mejora continua del sistema de control interno.

Recomendaciones de mejora: La auditoría interna no solo identifica las deficiencias, sino que también propone soluciones para fortalecer el sistema de control interno y mejorar la gestión de riesgos. Estas recomendaciones se basan en las mejores prácticas y en el conocimiento profundo de la empresa y sus operaciones.

Investigaciones: La auditoría interna también tiene la facultad de realizar investigaciones sobre posibles casos de fraude o irregularidades dentro de la empresa. Estas investigaciones se realizan con discreción y profesionalidad, y

buscan proteger los activos de la empresa y asegurar la transparencia en sus operaciones.

Las actividades de auditoría interna se orientan a lograr los siguientes objetivos:

Ayudar a la gerencia a mejorar la eficiencia y eficacia de las operaciones de la organización: La auditoría interna proporciona a la gerencia información valiosa sobre el estado del sistema de control interno, las áreas de mejora y las mejores prácticas para optimizar las operaciones de la empresa.

Promover una cultura de ética y responsabilidad dentro de la empresa: La auditoría interna contribuye a crear un ambiente donde los empleados se sientan responsables por sus acciones y donde se valore la ética y la transparencia.

Contribuir al cumplimiento de las leyes y regulaciones aplicables: La auditoría interna verifica que la empresa cumpla con todas las leyes y regulaciones aplicables a su actividad, incluyendo la Ley SOX.

7.2- Auditoría Externa

La auditoría externa es un componente fundamental del sistema de control interno, ya que proporciona una evaluación independiente y objetiva de la información financiera de la empresa. Sus funciones principales son:

Evaluación independiente: La auditoría externa examina los controles internos sobre la información financiera para determinar si están diseñados y operan de manera efectiva para prevenir, detectar y corregir errores o irregularidades en la información financiera. Esta evaluación se basa en las normas de auditoría generalmente aceptadas y en un profundo conocimiento de la compañía y su entorno.

Opinión sobre los estados financieros: La auditoría externa emite un informe que expresa su opinión sobre si los estados financieros de la empresa son confiables y presentan razonablemente la situación financiera y los resultados de sus operaciones. Esta opinión es fundamental para los usuarios de la información financiera, como los inversores, los acreedores y los reguladores.

Identificación y reporte de deficiencias: La auditoría externa también identifica las deficiencias significativas en los controles internos que puedan afectar la confiabilidad de la información financiera. Estas deficiencias se reportan a la gerencia y al directorio para que tomen las medidas correctivas necesarias.

Las actividades de la auditoría externa se orientan a lograr los siguientes objetivos:

Proporcionar a los usuarios de los estados financieros de la organización una seguridad razonable de que la información financiera es confiable: La opinión de la auditoría externa ayuda a los usuarios de la información financiera a tomar decisiones informadas sobre la empresa.

Contribuir a la transparencia y rendición de cuentas de la empresa: La auditoría externa es un mecanismo de transparencia que permite a las partes

interesadas tener una visión clara y precisa de la situación financiera de la empresa.

7.3- Evaluación y clasificación de las deficiencias

Las deficiencias de los controles serán evaluadas de acuerdo con su gravedad, donde individualmente o en combinaciones sean clasificadas como:

a) excepción, la falla detectada está dentro de un porcentaje de tolerancia razonable, o cuando se tratasen de aspectos de formalización;
b) deficiencia, cuando el diseño o la operación del control no permite prever o detectar a tiempo errores en los estados financieros;
c) deficiencia significativa, es menos grave que una debilidad material, pero lo suficientemente importante para merecer la atención de los responsables de la supervisión de los informes financieros de la organización; y
d) debilidad material, que permite la posibilidad razonable que un error material en la preparación y difusión de los estados financieros contenidos en el informe anual. [3]

8- Ejemplo práctico

Se opta por el control de revisión de bajas con frecuencia mensual para mostrar un ejemplo práctico de cómo se ejecuta un control en la organización.

8.1- Revisión de bajas de usuarios al momento de su término (CIA-4)

1) Mensualmente, desde el área de talento humano u otra área, se obtiene el reporte de personas con estado retirado, con el detalle del nombre, usuario, estado, fecha de retiro.

Nombre	Apellido	Codigo_usuario	Estado_Empleado	Fecha_Retiro
ROSA	CUEVA	ROSA.CUEVA	A	
GERALDINE	SALAZAR	GERALDINE.SALAZAR	R	3/5/2023
JUDITH	HERRERA	JUDITH.HERRERA	R	8/5/2023
Camila	Caballero	Camila.Caballero	R	19/5/2023
Tamara	Santos	Tamara.Santos	R	9/5/2023
Zahira	Vidal	Zahira.Vidal	A	

Ilustración 9: Reporte de nómina

2) Mensualmente, desde el sistema, se obtiene el reporte de usuarios con el detalle del nombre, usuario, estado, ultima conexión.

Nombre	Apellido	Codigo_usuario	Estado_Empleado	Ultima_conexion (crm)
ROSA	CUEVA	ROSA.CUEVA	A	12/5/2023 12:31
GERALDINE	SALAZAR	GERALDINE.SALAZAR	R	2/5/2023 17:07
JUDITH	HERRERA	JUDITH.HERRERA	R	6/5/2023 11:56
Camila	Caballero	Camila.Caballero	A	2/5/2023 16:15
Tamara	Santos	Tamara.Santos	R	31/5/2023 14:00
Zahira	Vidal	Zahira.Vidal	A	17/5/2023 14:35

Ilustración 10: Reporte de usuarios del sistema CRM

3) Se procede a realizar el cruce entre la lista de egreso y la lista de usuarios de sistema, se conoce sí coinciden el estado y si el usuario se conectó posterior a la fecha de retiro.

Nombre	Apellido	Codigo_usuario	Estado_Emp	Fecha_Retiro	CRM user	Ultima conexión	Desviación
GERALDINE	SALAZAR	GERALDINE.SALAZAR	R	3/5/2023	No analizar	2/5/2023 17:07	No Investigar
JUDITH	HERRERA	JUDITH.HERRERA	R	8/5/2023	No analizar	6/5/2023 11:56	No Investigar
Camila	Caballero	Camila.Caballero	R	19/5/2023	Analizar	2/5/2023 16:15	No Investigar
Tamara	Santos	Tamara.Santos	R	9/5/2023	No analizar	31/5/2023 14:00	Investigar

Ilustración 11: Cruce lista de nómina con lista de usuarios del sistema CRM

   a. El usuario Camila.Caballero con estado retirado en nómina, se encuentra activo en el sistema CRM[13], se procede a solicitar la baja por el proceso baja transaccional (CIA-3).
   b. El usuario Tamara.Santos con estado retirado en nómina, se conectó al sistema CRM posterior a su fecha de retiro, se procede a realizar una investigación de acciones realizadas.

4) Para concluir, la evidencia de la revisión, con los hallazgos y acciones realizadas, se almacena en la herramienta de tiquetes.

9- Control complementario de baja de usuarios

En el proceso de ejecución de bajas de cuentas de usuarios, en uno o varios sistemas un error puede representar un alto riesgo que puede derivar en pérdidas financieras, reputacional, operativo y competitivo, teniendo en cuenta que el control de gestión de accesos es un pilar en la seguridad de la información.

Es posible que el proceso automático de eliminación de usuarios desde la plataforma IAM[14] presente errores en la baja de identidades, por lo que se considera que el proceso de eliminación podría ser ineficiente. Demorar en la detección y resolverlo significa que existe un usuario activo en algún sitio que no debería ya estarlo, y esto representa un riesgo alto de seguridad para la organización.

Se ejecuta un control adicional que se encuentra basado en un modelo de análisis de datos que monitorea periódicamente la baja efectiva de accesos al concretarse el retiro de un colaborador.

El propósito refiere a que posterior a la solicitud de baja de usuario, se obtiene un reporte de los usuarios que permanecen activos en los sistemas, con una periodicidad diaria, esto ayuda a verificar que los accesos de los empleados han sido revocados correctamente, y tomar acción sobre los accesos no revocados.

[13] CRM *(Customer Relationship Management)*: Gestión de relaciones con el cliente
[14] IAM *(Identity and access management)*: Gestión de identidades y accesos

9.1- Flujograma del control complementario de baja de usuarios

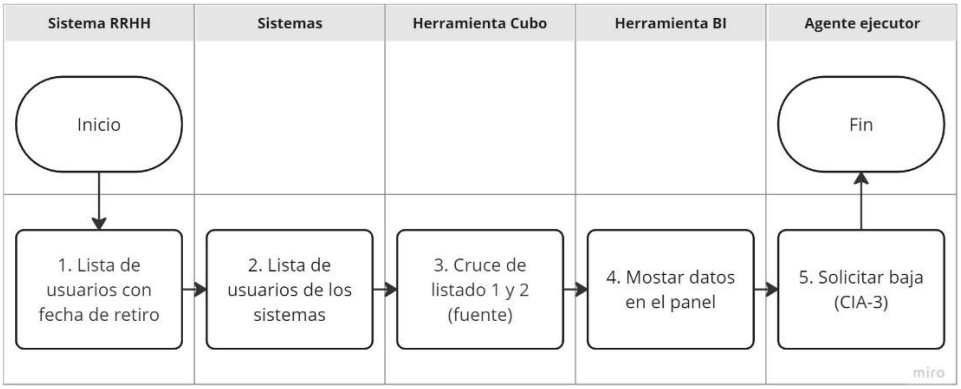
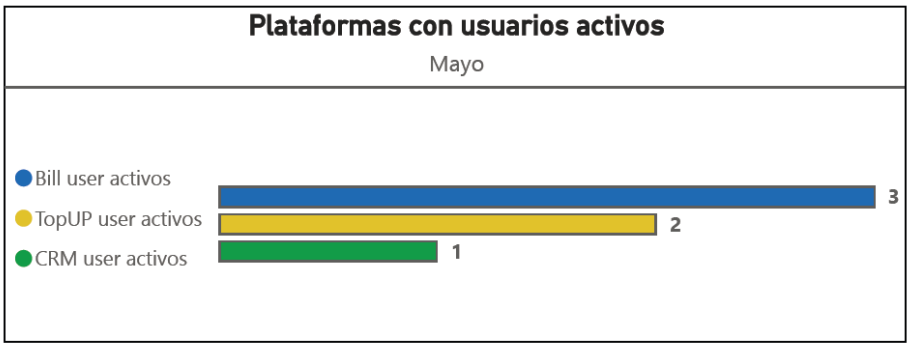


Ilustración 12: Flujograma control complementario CIA-4

9.2- Panel



Bill Sistema	Codigo_usuario	Fecha_Retiro	Suma de Días activos desde el retiro
Bill	HUGO.TAPIA	martes, 02 de mayo de 2023	30
Bill	Ivana.Herrero	viernes, 19 de mayo de 2023	13
Bill	Wendy.Vargas	lunes, 08 de mayo de 2023	24

TopUP Sistema	Codigo_usuario	Fecha_Retiro	Suma de Días activos desde el retiro
TopUP	JOSE.ALMEIDA	martes, 16 de mayo de 2023	16
TopUP	ALBERTO.CADENA	jueves, 11 de mayo de 2023	21

CRM Sistema	Codigo_usuario	Fecha_Retiro	Suma de Días actuvis desde el retiro
CRM	Camila.Caballero	viernes, 19 de mayo de 2023	13

Actualizado al 01/junio/2023

Ilustración 13: Panel y lista de plataformas con usuarios activos

10- Limitaciones, desafíos, superaciones

Desde el inicio de la implementación de los controles internos relacionados con la gestión de identidades y accesos se presentó y se siguen presentando diversas limitaciones, desafíos y superaciones. Abordar estos puntos es crucial para garantizar una implementación y mantenimiento exitoso de los controles.

A continuación, se detallan ciertas limitaciones más relevantes:

Los controles, en su mayoría, se ejecutan de forma manual, lo cual requiere una inversión significativa de tiempo por parte del ejecutor, siendo propenso a errores en el proceso de ejecución.

La disposición de recursos financieros y la inversión en tecnología fue mínima, esto impacta directamente al tiempo dedicado de los ejecutores de controles.

Cuando el aprovisionamiento no se encuentra automatizado, el proceso manual de alta de accesos es propenso a errores humanos. Tal cual también, se ve impactado en el proceso de baja de accesos.

Al implementar los procesos se obtuvo cierta resistencia debido a la percepción de que los procesos vuelven más burocráticos a las tareas rutinarias.

Seguidamente, se detallan algunos desafíos y superaciones más relevantes:

Implementar y mantener un sistema de control de acceso basado en roles es complejo con base a la cantidad de empleados que se cuenta en la organización (≥ 1000 empleados). Este sistema da permisos a los usuarios a solo lo necesario para sus funciones. Como punto complementario para futuro, considerar contar con herramientas de monitoreo y auditoría continua para identificar y corregir accesos inadecuados.

También, contar con un sistema de gestión de identidades y control de acceso colabora en disponer de forma automatizada flujos de trabajos para aprobación de solicitudes relacionadas con la identidad del usuario, además, de tener la integración de servicios para una fácil administración de cuentas de usuario. Es importante mencionar que desarrollar los conectores para la integración entre la herramienta IAM y los sistemas fue un gran esfuerzo e inversión presupuestaria por parte de la organización.

La automatización de controles puede ser técnicamente complicada, pero es necesaria para garantizar la consistencia y reducir los errores manuales. Es importante mencionar que un punto común de varios controles es contar con un listado de usuarios, es ideal identificar el proceso a utilizar para reducir el esfuerzo del ejecutor en este punto. Además, para monitoreo de acciones de usuarios privilegiados, el implementar soluciones de monitoreo continuo y análisis de comportamiento para detectar actividades de cambios, con alertas automáticas es un mejoramiento significativo pues se cuenta con ahorro de tiempo en análisis de registros.

La identificación y evaluación de riesgos asociados con el acceso a sistemas y datos es una tarea continua y permanente que requiere una comprensión profunda de las operaciones de la organización y las posibles amenazas que afectan, considerando las constantes nuevas tecnologías.

Para mantener los controles actualizados frente a nuevas amenazas y cambios regulatorios se debe contar con un ciclo de revisión y actualización continuo. Se debe tener en cuenta que los controles de acceso sean adaptables, escalables y sigan siendo efectivos.

Realizar habituales campañas de concienciación y formación para explicar los beneficios de la aplicación de controles. Involucrar a los empleados en el proceso de cambio para obtener su aceptación y apoyo.

11- Conclusiones

En el presente trabajo final de maestría se ha abordado en profundidad la temática de diseño e implementación de controles internos de seguridad de la información en el dominio de gestión de accesos con base a la Ley Sarbanes Oxley. A través del desarrollo del trabajo, se destaca la importancia de contar con una política de gestión de accesos el cual colabora en la gobernanza de los procesos que son aplicados a los controles internos en la organización, alineados a las regulaciones vigentes.

Se ha introducido al lector a estándares y marcos de seguridad, como marco regulatorio del proceso de implementación de los controles, que en forma general garantizan en la organización la exactitud y confiabilidad de la información financiera, gestionar las operaciones de manera eficiente y eficaz, y garantizar el cumplimiento de las leyes y regulaciones aplicables.

Principalmente se ha tomado el estándar internacional ISO/IEC 27002 como guía para construir los controles a implementar con base a riesgos identificados con enfoque de acceso no autorizado o inapropiado a información sensible o crítica. Los controles se resumen en definición de política y procedimientos para la gestión de acceso de usuarios, implementación del ciclo de vida de la cuenta de usuario, y monitoreo de acceso privilegiado.

La implementación de los controles de gestión de accesos de usuarios trajo consigo resultados de revisión y mejora en los procesos como, por ejemplo:

Establecimiento de un marco de gobernanza claro para la gestión de accesos, definiendo roles, responsabilidades y procesos.

Garantía que solo personal autorizado tenga acceso a los sistemas, reduciendo el riesgo de accesos no autorizados.

Al eliminar oportunamente los accesos de usuarios que ya no los necesitan, se mitiga el riesgo de accesos huérfanos. Con revisión periódica del proceso de baja se asegura la eliminación correcta, y se evita uso indebido de credenciales, accesos no autorizados a información confidencial, o incumplimiento normativo.

Con respecto a accesos de emergencia, se tiene establecido el control y el monitoreo de uso de estos accesos, limitando el uso a situaciones justificadas y revisando su pertinencia.

Se supervisa el uso de privilegios elevados para detectar y prevenir actividades inadecuadas, sospechosas o maliciosas.

Se establecen configuraciones de seguridad estándar para los sistemas, reduciendo la superficie de exposición a amenazas.

Se verifica periódicamente que la configuración de seguridad de los sistemas se mantenga alineada con los estándares definidos.

Se revisa y valida la pertinencia de los accesos de usuarios de TI y usuarios de negocio, asegurando que se ajusten a sus roles y responsabilidades.

Los controles desarrollados en este trabajo contribuyen a garantizar la seguridad, integridad y disponibilidad de la información, al tiempo que mitigan riesgos como accesos no autorizados, uso indebido de privilegios y configuraciones de seguridad deficientes. [4]

La auditoría se presenta como un ente verificador de la eficacia y confiabilidad de los controles implementados, realizando recomendaciones para su mejora si fuere el caso.

La auditoría interna para comprender y verificar la eficacia de los controles de los procesos realiza el recorrido de estos sin la necesidad de utilizar criterios de muestra mediante un análisis profundo, verifica que los controles implementados se alinean con los objetivos del proceso SOX y que su diseño es adecuado para mitigar los riesgos identificados; realiza una evaluación para asegurar que todos los riesgos potenciales asociados al proceso SOX han sido correctamente identificados y documentados; y a través de pruebas de conformidad sin muestra, se verifica que los controles implementados se ejecutan de manera efectiva y eficiente en una transacción específica.

La auditoría externa realiza las pruebas de eficacia operativa para evaluar la efectividad de los controles desarrollados por la organización, con base a los riesgos identificados. En este proceso, es utilizado la modalidad de prueba sustantiva, una técnica de auditoría que busca detectar y cuantificar errores que hayan podido ocurrir en el pasado pero que no fueron identificados o corregidos por las actividades de control implementadas. En las pruebas de control se selecciona una muestra representativa de transacciones o registros, esto permite obtener resultados confiables y representativos del funcionamiento general de los controles.

Adicionalmente, se han identificado desafíos y limitaciones que abren nuevas líneas de investigación para el futuro. Limitantes en cuanto automatización de controles, inversión mínima en tecnología, esto genera que en el futuro cuando se cuente con inversión se necesite y se dedique tiempo y esfuerzo para adecuar los controles ya implementados a la nueva modalidad con automatización. Otra limitante es que, en los controles propuestos, no se encuentra contemplado la promoción de cargo que se refiere al cambio de puesto y responsabilidades de la persona dentro de la organización.

Por otra parte, es posible considerar como futura línea de investigación el desarrollo de listas de comprobación para garantizar el cumplimiento de la Ley Sarbanes Oxley y reforzar los controles internos. Al mismo tiempo, se podría considerar complementar el presente trabajo con el análisis en la gestión de accesos en las promociones de cargos.

Se considera que el presente trabajo ofrece a una organización el aumento de nivel de seguridad, la minimización de riesgos, mayor madurez en la postura de seguridad para detectar, responder y solucionar amenazas, por medio de la gobernanza de políticas y procesos de seguridad definidos sobre los sistemas y colaboradores de la organización. Además, proporcionando información real y

relevante para organizaciones de cualquier rubro, profesionales de la seguridad de la información, e instituciones académicas.

Finalmente, es importante mencionar que, cuando una organización cuenta con una certificación en sus controles internos, al cliente se le ofrece garantías de protección de datos, integridad de la información, confidencialidad, y prevención de fraude, lo cual genera en el cliente seguridad, confianza, tranquilidad y empoderamiento sobre los servicios que este utiliza.

12- Glosario

Acceso privilegiado	Permiso para realizar actividades altamente privilegiadas.
Administrador de Sistema	Rol técnico responsable del mantenimiento, configuración y operación confiable de los sistemas.
Administrador del Sistema IAM	Responsable técnico quien establece los parámetros compartidos por el ejecutor de control para desencadenar el proceso de certificación.
Administradores de Contratos / Supervisor de Contratos	Cualquier persona que sea responsable del contratista/tercero relacionado con el proceso de gestión de acceso al ciclo de vida del usuario (incluida la certificación de acceso y el proceso de salida).
Agente ejecutor	Responsable de recopilar las cuentas privilegiadas o accesos de la aplicación en plataformas. Además, define el alcance, aprobador, período y recordatorios para cumplir con una certificación en función de los requisitos del calendario de pruebas.
Aplicación integrada	Aplicación descendente conectada a la Plataforma IAM para manejar el proceso del ciclo de vida.
Aprovisionamiento	Actividad que otorga acceso automáticamente.
Autenticación	El procedimiento realizado para verificar la identidad de un usuario o sistema al intentar acceder a un recurso tecnológico.
Autorización	Proceso mediante el cual, una vez autenticado, se designan ciertos privilegios a un usuario o sistema dentro del recurso tecnológico.
Certificador	Gerente de línea responsable de validar el acceso de sus subordinados directos, para verificar si es correcto y adecuado. Responsable directo del certificador.

Certificador del Gerente de línea	Gerente del certificador, quien será responsable de completar la certificación cuando el Gerente de línea inmediato no esté disponible para ello (escalamiento).
Contraseña	Una cadena de caracteres (letras, números y otros símbolos) que se utiliza para autenticar una identidad o verificar la autorización de acceso.
Cuenta de administrador	Una cuenta no nominativa y altamente privilegiada que puede existir en la infraestructura, sistema operativo, base de datos, o en la capa de aplicación, en una organización que es compartida por múltiples usuarios pero que solo debe usarse cuando sea estrictamente necesario.
Cuenta privilegiada	Un usuario nominativo que está autorizado para realizar funciones relevantes para la seguridad que los usuarios comunes no están autorizados a realizar.
Cuentas de usuario básicas	Son cuentas de usuario que no cuentan con altos privilegios en los sistemas y componentes de información.
Dueño del negocio	Es la persona que conoce el activo de información y su función dentro del proceso de negocio. En términos de seguridad, el dueño del negocio debe mantener y vigilar la administración de los accesos y perfiles otorgados a los activos de información.
Dueño del sistema	Es líder del equipo de tecnología y dueño técnico de la plataforma. El dueño del sistema es el rol responsable de aprobar el acceso privilegiado a las plataformas.
Egreso	Empleado, tercero o externo que sale de cualquier de la organización.
Empleado	Contratado directo de recursos humanos para unirse a la nómina de la organización.
Gerente de línea	Gerente directo de un usuario (empleado o tercero), principal responsable de aprobar o evaluar la idoneidad de un acceso.
Cuenta de usuario	Símbolo único o cadena de caracteres utilizado por un sistema de información para identificar a un usuario específico.
Identidad	Un registro en la herramienta IAM asociado a un empleado o tercero.

Ingreso	Empleado o tercero que se incorpora a la nómina de la organización.
Marco de seguridad de la información	Conjunto de documentos como ser políticas, estándares, procedimientos que define las prácticas de seguridad de la información implementadas y operadas en la compañía para lograr la confidencialidad, integridad y disponibilidad de la información.
Modificación	Empleado o tercero que presenta cambios en su rol, cargo o cualquier otra información relevante.
Perfiles	Los perfiles son las responsabilidades o funciones laborales asignadas a cada rol. Se debe garantizar que ningún rol tenga dos o más perfiles con responsabilidades de transacciones sensibles.
Plataforma IAM	Herramienta de gestión de acceso a identidades para la organización. Gestión de Identidades y Accesos (*Identity and Access Management*).
Privilegios mínimos	El principio de que una arquitectura de seguridad debe diseñarse de manera que a cada entidad se le otorguen los recursos mínimos del sistema y las autorizaciones que la entidad necesita para realizar su función.
Recursos humanos	Rol de la compañía que desencadena la solicitud inicial de actividades de creación, modificación y eliminación de personal (ingresos, traslados y bajas).
Roles	Una colección de permisos en el control de acceso basado en roles, generalmente asociados con un rol o puesto dentro de una organización.
Segregación de funciones	El principio de que ningún usuario debe tener suficientes privilegios para hacer un mal uso del sistema por sí solo.
Tarea	Una tarea creada y asignada por la herramienta IAM
Tercero	Persona o entidad externa que presta un servicio a la compañía.
Tercero o proveedor	Cualquier persona que no sea empleado de la organización y tenga acceso a activos de información o recursos tecnológicos, como ser contratista, proveedor.

Usuario	Todos los empleados, contratistas, consultores, empleados temporales, invitados y cualquier otro tercero que tenga acceso a los recursos de tecnología de la información de la compañía.
Usuario privilegiado	Un usuario que está autorizado (y, por tanto, de confianza) para realizar funciones relevantes para la seguridad que los usuarios normales no están autorizados a realizar.

13- Bibliografía

[1] M. S.A., «FORM 20-F,» 28 Febrero 2020. [En línea]. Available: https://www.millicom.com/2019annualreport/PDF/form-20f.pdf. [Último acceso: 02 Febrero 2024].

[2] Itaipu Binacional, «Asesoría de Compliance,» 07 05 2020. [En línea]. Available: https://www.itaipu.gov.py/es/pagina/asesoria-de-compliance. [Último acceso: 26 05 2024].

[3] B. Borsalli, «SoftExpert Blog,» Controles internos: cómo garantizar su eficacia, 19 09 2022. [En línea]. Available: https://blog.softexpert.com/es/controles-internos-como-garantizar-su-eficacia/. [Último acceso: 26 05 2024].

[4] Tigo Paraguay, «Ayuda Tigo Paraguay,» [En línea]. Available: https://ayuda.tigo.com.py/hc/es/articles/10166350238227-Millicom-comienza-a-cotizar-acciones-en-NASDAQ-en-los-Estados-Unidos-bajo-el-s%C3%ADmbolo-TIGO. [Último acceso: 25 11 2023].

[5] D. P. Duque Tirado y V. H. Duque Tirado, *Propuesta de metodología para preparar el cumplimiento de los requerimientos de la sección 404 de la Ley Sarbanes-Oxley, bajo un enfoque integral por procesos en un potencial emisor privado extranjero colombiano, para incrementar la probabilidad de éxito,* Medellín, 2022.

[6] Millicom, *SOX 101 - ESP 2022 - Introducción a SOX (Entrenamiento),* Miami, 2022.

[7] S. D. Luz, «Redes Zone - Para qué sirve el protocolo LDAP y cómo funciona,» 05 Septiembre 2023. [En línea]. Available: https://www.redeszone.net/tutoriales/servidores/que-es-ldap-funcionamiento/. [Último acceso: 08 Diciembre 2023].

[8] S. D. Luz, «Redes Zone - Descubre para qué sirve un servidor RADIUS y su funcionamiento,» 25 Abril 2023. [En línea]. Available:

https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/. [Último acceso: 08 Diciembre 2023].

[9] IBM, «IBM - ¿Qué es el inicio de sesión único?,» IBM, [En línea]. Available: https://www.ibm.com/es-es/topics/single-sign-on. [Último acceso: 09 Diciembre 2023].

[10] ManageEngine, «ManageEngine - ¿Qué es la gestión de acceso privilegiado?,» [En línea]. Available: https://www.manageengine.com/latam/privileged-access-management/que-es-la-gestion-de-acceso-privilegiado.html. [Último acceso: 09 Diciembre 2023].