Informe resultado de medición de del nivel de madurez de seguridad y privacidad de la información de Fiducoldex S.A.

Diciembre de 2025

FIDUCOLDEX
GRUPO BANCOLDEX

GRUPO BICENTENARIO

Tabla de contenido

1. Objetivo

El presente documento tiene como objetivo compartir los resultados de la medición del nivel de madurez de seguridad y privacidad de la información, de acuerdo con el cumplimiento a los requerimientos establecidos por la regulación nacional (decretos reglamentarios de MINTIC, Circulares Externas de la Superintendencia Financiera de Colombia, entre otros) y de nuestras políticas internas de seguridad de la información (Buenas prácticas ISO 27001:2013)

2. Alcance

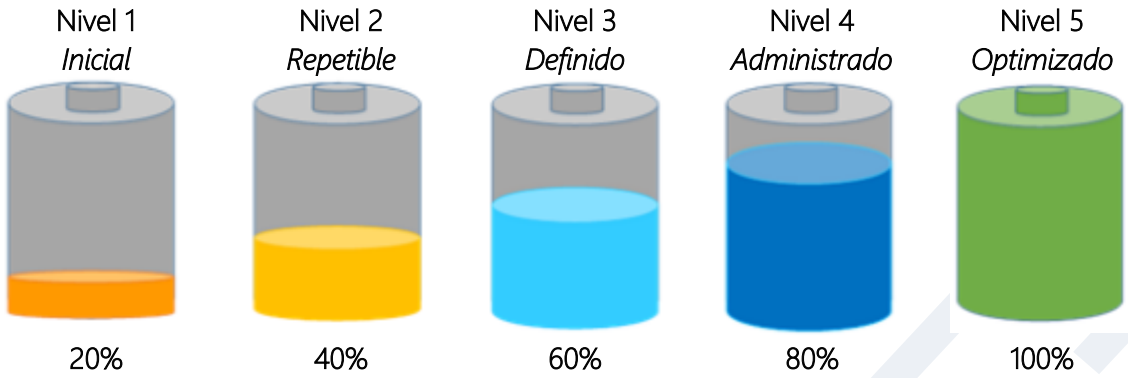
En el presente documento se muestra los resultados de la medición del modelo de madurez aplicada para el 100% de los controles (114) y dominios (14) de la norma ISO 27001:2013 ISO 27001:2013.

A.5 Políticas
A.6 Organización
A.7 Seguridad Recurso Humano
A.8 Gestión de Activos
A.9 Control de acceso
A.10 Criptografía
A.11 Seguridad física y del entorno
A.12 Seguridad de la Operaciones
A.13 Seguridad de las Comunicaciones
A.14 Adquisición, desarrollo y mantenimiento de sistemas
A.15 Relaciones con los proveedores
A.16 Gestión de Incidentes
A.17 Aspectos de Seguridad en la continuidad
A.18 Cumplimiento

3. Modelo de madurez

Este esquema permite identificar el nivel de madurez del SGSI en el que se encuentra la Fiduciaria, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado.

A continuación, se muestran los diferentes niveles que hacen parte del modelo de madurez:



Nivel 1 *Inicial*	Nivel 2 *Repetible*	Nivel 3 *Definido*	Nivel 4 *Administrado*	Nivel 5 *Optimizado*
En este nivel se encuentran las entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que le permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de esta, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.	En este nivel se encuentran las entidades, en las cuales existe procesos básicos de gestión de la seguridad de y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditoria al MSPI, recolectando información para establecer la efectividad de los controles.	En este nivel se encuentran las entidades, en donde existen un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

El esquema que muestra los niveles de madurez del SGSI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en la Fiduciaria.

4. Evaluación

Esta prueba está orientada a la evaluación del Sistema de seguridad y privacidad de la información basado en los requisitos de la norma ISO 27001:2013 anexo A (14 dominios, 35 objetivos de control y 114 controles):

A.5 Políticas (2 controles)
A.6 Organización (7 controles)
A.7 Seguridad Recurso Humano (6 controles)
A.8 Gestión de Activos (10 controles)

A.9 Control de acceso (14 controles)
A.10 Criptografía (2 controles)
A.11 Seguridad física y del entorno (15 controles)
A.12 Seguridad de la Operaciones (14 controles)
A.13 Seguridad de las Comunicaciones (7 controles)
A.14 Adquisición, desarrollo y mantenimiento de sistemas (13 controles)
A.15 Relaciones con los proveedores (2 controles)
A.16 Gestión de Incidentes (7 controles)
A.17 Aspectos de Seguridad en la continuidad (4 controles)
A.18 Cumplimiento (8 controles)

Par la evaluación de los 114 controles se mediante la Tabla de escala de valoración de controles ISO 27001:2013 ANEXO A, definida a continuación:

Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Falta total de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.

Descripción	Calificación	Criterio
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

5. Desarrollo

Evaluación de la madurez de los dominios:

A.5 Políticas (2 controles)

Se realizada evaluación de cada uno de los controles del dominio de Políticas, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	80 %

Control	Medición de cumplimiento	
Documento de la política de seguridad y privacidad de la Información	20 40 60	80 %
Revisión y evaluación	20 40 60	80 %

A.6 Organización

Se realizada evaluación de cada uno de los siete (7) controles del dominio de Organización, obteniendo una ponderación general de 76%, a continuación de describe cada uno de estos controles y su calificación:

RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN	20	76 %

Control	Medición de cumplimiento	
Roles y responsabilidades para la seguridad de la información	20 40 60 80	80 %
Separación de deberes / tareas	20 40 60 80	80 %

Contacto con las autoridades.	60 %
Contacto con grupos de interés especiales	80 %
Seguridad de la información en la gestión de proyectos	60 %
Política para dispositivos móviles	80 %
Teletrabajo	80 %

A.7 Seguridad Recurso Humano

Se realizada evaluación de cada uno de los seis (6) controles del dominio de Seguridad Recurso Humano, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

SEGURIDAD DE LOS RECURSOS HUMANOS	80 %

Control	Medición de cumplimiento
Selección e investigación de antecedentes	80 %
Términos y condiciones del empleo	80 %
Responsabilidades de la dirección	80 %
Toma de conciencia, educación y formación en la seguridad de la información	80 %
Proceso disciplinario	80 %
Terminación o cambio de responsabilidades de empleo	80 %

A.8 Gestión de Activos (10 controles)

Se realizada evaluación de cada uno de los 11 controles del dominio de Gestión de Activos, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

GESTIÓN DE ACTIVOS	80 %

Control	Medición de cumplimiento
Inventario de activos	80 %
Propiedad de los activos	80 %
Uso aceptable de los activos	80 %
Devolución de activos	80 %
Clasificación de la información	80 %
Etiquetado de la información	80 %
Manejo de activos	80 %
Gestión de medios removibles	80 %
Disposición de los medios	80 %
Transferencia de medios físicos	80 %

A.9 Control de acceso

Se realizada evaluación en conjunto a la Gerencia de Informática y Tecnología de cada uno de los 14 controles del dominio de control de acceso, obteniendo una ponderación general de 78%, a continuación de describe cada uno de estos controles y su calificación:

CONTROL DE ACCESO	78 %

Control	Medición de cumplimiento
Política de control de acceso	80 %
Acceso a redes y a servicios en red	80 %
Registro y cancelación del registro de usuarios	60 %

Suministro de acceso de usuarios		80 %
Gestión de derechos de acceso privilegiado		80 %
Gestión de información de autenticación secreta de usuarios		80 %
Revisión de los derechos de acceso de usuarios		80 %
Retiro o ajuste de los derechos de acceso		80 %
Uso de información de autenticación secreta		80 %
Restricción de acceso a la información		80 %
Procedimiento de ingreso seguro		80 %
Sistema de gestión de contraseñas		80 %
Uso de programas utilitarios privilegiados		60 %
Control de acceso a códigos fuente de programas	N/A	N/A

A.10 Criptografía

Se realizada evaluación en conjunto a la Gerencia de Informática y Tecnología de cada uno de los dos (2) controles del dominio de Criptografía, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

CRIPTOGRAFÍA		80 %

Control	Medición de cumplimiento	
Política sobre el uso de controles criptográficos		80 %
Gestión de llaves		80 %

A.11 Seguridad física y del entorno

Se realizada evaluación en conjunto a la Gerencia administrativa de cada uno de los 15 controles del dominio de Seguridad física y del entorno, obteniendo una ponderación general de 78%, a continuación de describe cada uno de estos controles y su calificación:

SEGURIDAD FÍSICA Y DEL ENTORNO	78 %

Control	Medición de cumplimiento
Perímetro de seguridad física	80 %
Controles físicos de entrada	80 %
Seguridad de oficinas, recintos e instalaciones	80 %
Protección contra amenazas externas y ambientales	80 %
Trabajo en áreas seguras	80 %
Áreas de despacho y carga	80 %
Ubicación y protección de los equipos	80 %
Servicios de suministro	80 %
Seguridad del cableado	60 %
Mantenimiento de equipos	60 %
Retiro de activos	80 %
Seguridad de equipos y activos fuera de las instalaciones	80 %
Disposición segura o reutilización de equipos	80 %
Equipos de usuario desatendidos	80 %
Política de escritorio y pantalla limpios	80 %

A.12 Seguridad de la Operaciones

Se realizada evaluación en conjunto a la Gerencia de Informática y Tecnología de cada uno de los 14 controles del dominio de Seguridad de la Operaciones, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

SEGURIDAD DE LAS OPERACIONES		80 %

Control	Medición de cumplimiento	
Procedimientos de operación documentados		80 %
Gestión de cambios		80 %
Gestión de capacidad		80 %
Separación de los ambientes de desarrollo, pruebas y operación		80 %
Controles contra códigos maliciosos		80 %
Respaldo de la información		80 %
Registro de eventos		80 %
Protección de la información de registro		80 %
Registros del administrador y del operador		80 %
Sincronización de relojes		80 %
Instalación de software en sistemas operativos		80 %
Gestión de las vulnerabilidades técnicas		80 %
Restricciones sobre la instalación de software		80 %
Controles sobre auditorías de sistemas de información		80 %

A.13 Seguridad de las Comunicaciones

Se realizada evaluación en conjunto a la Gerencia de Informática y Tecnología de cada uno de los 7 controles del dominio de Seguridad de las Comunicaciones, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

SEGURIDAD DE LAS COMUNICACIONES	80 %

Control	Medición de cumplimiento
Controles de redes	80 %
Seguridad de los servicios de red	80 %
Separación en las redes	80 %
Políticas y procedimientos de transferencia de información	80 %
Acuerdos sobre transferencia de información	80 %
Mensajería electrónica	80 %
Acuerdos de confidencialidad o de no divulgación	80 %

A.14 Adquisición, desarrollo y mantenimiento de sistemas

Se realizada evaluación en conjunto a la Gerencia de Informática y Tecnología de cada uno de los 13 controles del dominio de Adquisición, desarrollo y mantenimiento de sistemas, obteniendo una ponderación general de 73%, a continuación de describe cada uno de estos controles y su calificación:

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	73 %

Control	Medición de cumplimiento
Análisis y especificación de requisitos de seguridad de la información	80%
Seguridad de servicios de las aplicaciones en redes públicas	40%

Protección de transacciones de los servicios de las aplicaciones		40%
Política de desarrollo seguro		80%
Procedimientos de control de cambios en sistemas		80%
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		80%
Restricciones en los cambios a los paquetes de software		80%
Principios de construcción de sistemas seguros		80%
Ambiente de desarrollo seguro	N/A	N/A
Desarrollo contratado externamente		60%
Pruebas de seguridad de sistemas		80%
Prueba de aceptación de sistemas		80%
Protección de datos de prueba		80%

A.15 Relaciones con los proveedores

Se realizada evaluación de cada uno de los 2 objetivos de control del dominio de Relaciones con los proveedores, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

RELACIONES CON LOS PROVEEDORES		**80 %**
Control	**Medición de cumplimiento**	
Análisis y especificación de requisitos de seguridad de la información		80%
Seguridad de servicios de las aplicaciones en redes públicas		80%

A.16 Gestión de Incidentes

Se realizada evaluación de cada uno de los 7 controles del dominio de Gestión de Incidentes, obteniendo una ponderación general de 60%, a continuación de describe cada uno de estos controles y su calificación:

GESTIÓN DE INCIDENTES		**60 %**

Control	Medición de cumplimiento	
Responsabilidades y procedimientos	20 40 60	60%
Reporte de eventos de seguridad de la información	20 40 60	60%
Reporte de debilidades de seguridad de la información	20 40 60	60%
Evaluación de eventos de seguridad de la información y decisiones sobre ellos	20 40 60	60%
Respuesta a incidentes de seguridad de la información	20 40 60	60%
Aprendizaje obtenido de los incidentes de seguridad de la información	20 40 60	60%
Recolección de evidencia	20 40 60	60%

A.17 Aspectos de Seguridad en la continuidad

Se realizada evaluación de cada uno de los 4 controles del dominio de Aspectos de Seguridad en la continuidad, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

ASPECTOS DE SEGURIDAD EN LA CONTINUIDAD	20 40	80 %

Control	Medición de cumplimiento	
Planificación de la continuidad de la seguridad de la información	20 40	80%
Implementación de la continuidad de la seguridad de la información	20 40	80%
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	20 40	80%
Disponibilidad de instalaciones de procesamiento de información	20 40	80%

A.18 Cumplimiento

Se realizada evaluación de cada uno de los 8 controles del dominio de Cumplimiento, obteniendo una ponderación general de 80%, a continuación de describe cada uno de estos controles y su calificación:

CUMPLIMIENTO		80 %

Control	Medición de cumplimiento	
Identificación de la legislación aplicable y de los requisitos contractuales.		60%
Derechos de propiedad intelectual.		80%
Protección de registros.		60%
Protección de los datos y privacidad de la información relacionada con los datos personales.		80%
Reglamentación de controles criptográficos.		80%
Revisión independiente de la seguridad de la información		80%
Cumplimiento con las políticas y normas de seguridad.		80%
Revisión de cumplimiento técnico.		80%

6. Fortalezas

- ✓ La entidad ha realizado un proceso de actualización documental de los procesos y políticas relacionadas con el SGSI.
- ✓ La fiduciaria cuenta con un Plan de Continuidad de Negocio (CPDA y CAO) definido y probado, según los alcances establecidos inicialmente.
- ✓ La fiduciaria cuenta con copias de respaldo de la información con un esquema de respaldo definido que contempla respaldo en en cinta almacenadas fuera de la organización.
- ✓ La fiduciaria cuenta con Análisis de Vulnerabilidades y pruebas de Ethical Hacking que son ejecutadas por el proveedor externo con una periodicidad trimestral y anual respectivamente.
- ✓ La fiduciaria cuenta con Identificación y valoración de activos.
- ✓ La fiduciaria cuenta con controles biométricos de acceso a áreas restringidas (Mesa de Dinero).
- ✓ La fiduciaria cuenta con monitoreo permanente de la infraestructura tecnológica mediante un servicio "SOC" que se encuentra tercerizado, cuya protección para la entidad se refleja en un soporte y asistencia las 24 h. por 7 días a la semana.

7. Oportunidades de mejora

- Se debe realizar pruebas integrales del plan de continuidad de negocio, teniendo en cuenta los últimos BIA's y las necesidades propias del negocio.
- Realización y ejecución de los planes de mitigación de vulnerabilidades técnicas de manera más proactiva.
- Culminar el plan de trabajo para la autenticación integrada con Directorio Activo para las aplicaciones Core de negocio.
- Culminar la implementación en la segmentación de Redes
- Desarrollar e implementar la política de seguridad de la información en la gestión de proyectos
- Se debe implementar un plan de trabajo orientado al mantenimiento y pruebas periódicas de la planta eléctrica
- Se recomienda implementar protección para el cableado externo, cajas de conexión y paneles de conexión.
- Se recomienda mantener actualizada Hoja de vida de los servidores y crear el procedimiento de gestión de la capacidad
- Se debe actualizar la documentación existente de gestión de cambios y acorde con los cambios realizados en la Fiduciaria, incluir en esta, la ejecución de pruebas de seguridad de la información, ciberseguridad, continuidad del negocio.
- Se recomienda implementar protección contra fuga de datos (DLP)

Nota: Se informa que a partir del año 2026, la presente evaluación se realizará bajo la normativa ISO-27001/2022.