PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

InfiValle

Instituto Financiero para el Desarrollo del Valle del Cauca

AAA Value & Risk Rating Sociedad Calificadora de Valores

sfc Superintendencia Financiera de Colombia

icontec ISO 9001

GOBERNACIÓN VALLE DEL CAUCA

CONTENIDO

I. Objetivo

Generar un plan de trabajo para cumplir con los requerimientos de la norma ISO 27001:2013 con base en las recomendaciones del análisis de brechas con el objetivo de priorizar las inversiones o mejoras en los procesos evaluados.

II. Alcance

En el análisis se contemplaron los siguientes aspectos:

- ✓ Inventario de los activos de información asociados a cada uno de los procesos de la entidad con el objetivo de determinar su nivel de criticidad.
- ✓ Análisis de riesgos de seguridad de la información asociada a los activos de información identificados en el literal anterior, determinando sus agentes o factores de amenaza, vulnerabilidad e impacto sobre los procesos de la entidad.
- ✓ Modelado de amenazas y vulnerabilidades en los activos de información de carácter tecnológico, por medio del uso de técnicas y herramientas de seguridad digital.
- ✓ Identificación y evaluación de los controles basados en buenas prácticas de seguridad y privacidad de la Información como la norma ISO/IEC 27001:2013 e ISO 27002, con el objetivo de determinar la brecha de controles que le permita a la entidad establecer un nivel de riesgo adecuado.

III. Procedimientos Aplicados

Los siguientes fueron los procedimientos que se llevaron a cabo:

Análisis de riesgos

- Entendimiento de los activos de información gestionados por cada uno de los procesos del Instituto y clasificación de los mismos de acuerdo con su criticidad. La criticidad es ponderada de acuerdo con los procesos que soporta.

- Identificación de las amenazas, vulnerabilidades (diseño, implementación u operación) y riesgos asociados a los activos identificados en el punto anterior.

- Identificación de los controles existentes en INFIVALLE para mitigar los riesgos identificados.

- Determinación de las brechas de control y emisión de las recomendaciones pertinentes de acuerdo al contexto de la organización.

OBSERVACIONES Y RECOMENDACIONES

No.	Observación	Riesgo	Recomendación	Implementación
1	**PROCEDIMIENTO GESTIÓN DE ACCESOS** Con respecto al procedimiento de Gestión de accesos se identificó que este no contempla novedades de personal relacionadas con: • Incapacidades • Vacaciones • Licencias Lo anterior ocasiona que las cuentas de estos funcionarios queden activas durante estos periodos.	a) Accesos no autorizados a las aplicaciones debido al uso de los usuarios asignados a personal ausente.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
2	**MAPAS DE SEGURIDAD APLICACIONES** a) Ausencia de mapas de seguridad para la administración de los accesos a las aplicaciones críticas	a) Acceso no autorizado a las aplicaciones debido a una asignación de permisos no acordes con	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	de la entidad. b) Ausencia de una revisión periódica de los usuarios con acceso a las aplicaciones.	las funciones asignadas a cada usuario. b) Asignación inadecuada de accesos la cual incurra en conflictos de segregación de funciones.		
3	**MONITOREO DE SUPERUSUARIOS PLATAFORMA Y APLICACIONES** No se cuenta con controles de monitoreo de las actividades ejecutados por los super usuarios en aplicaciones, base de datos y sistemas operativos.	Ejecución de acciones no autorizadas por inadecuada administración de super usuarios. Abuso de derechos y privilegios administrativos sobre plataformas tecnológicas.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
4	**LÍNEAS BASES DE CONFIGURACIÓN** Actualmente la entidad no cuenta con líneas bases de configuración seguras para servidores, estaciones de trabajo, dispositivos móviles, IoT, entre otros.	a. Acceso no autorizado a la administración de la plataforma b. Manipulación remota de plataformas	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
5	**INVENTARIO DE ACTIVOS TECNOLÓGICOS** Actualmente se cuenta con una solución que le permita a la entidad gestionar	Pérdida de visibilidad y control sobre los activos de información	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	centralizadamente un inventario de los activos tecnológicos, entre estos se destacan: Servidores, equipos clientes, Software base (Sistemas Operativos, Bases de datos, etc.), dispositivos de red, aplicaciones, etc.			
6	**GESTIÓN DE ACTUALIZACIONES PLATAFORMA** Actualmente no se dispone de un procedimiento para la gestión de actualizaciones en servidores y máquinas cliente.	Acceso no autorizado a la administración de la plataforma Manipulación remota de plataformas Mal funcionamiento en la plataforma.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
7	**PROCEDIMIENTO DE CAMBIOS DIRECTOS A DATOS** Se evidenció que la entidad no cuenta con un procedimiento para cambios directos a datos.	Modificación no autorizada de la información	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
8	**MONITOREO DE LOGS PLATAFORMA TECNOLÓGICA** Se evidenció la ausencia de un procedimiento para el monitoreo y revisión de los logs generados a nivel de la plataforma tecnológica de la entidad. Actualmente el instituto	Limitación en la asignación de responsabilidades y solución de eventos o incidentes	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	ha implementado una solución SIEM (Sistema de gestión eventos e información de seguridad) la cual debe ser ajustada para que recolecte información más precisa sobre los servicios tecnológicos.			
9	**PROTECCIÓN DE CORREO ELECTRÓNICO** Se evidenciaron las siguientes debilidades con respecto a los controles de seguridad del correo electrónico: • Factores de doble autenticación para limitar el acceso no autorizado. • No existen controles relacionados con la fuga de información confidencial o sensible.	Acceso no autorizado y fuga de información	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
10	**PRUEBAS PERIODICAS PLAN DE CONTINUIDAD** Se evidenció que la entidad cuenta con un plan contingencia y continuidad de negocio para el proceso de operación core. El plan de continuidad y contingencia de la entidad fue celebrado mediante acto administrativo el 20 de octubre de 2016.	Pérdida en la capacidad de continuidad ante un incidente o evento adverso	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	Actualmente el plan de continuidad no se encuentra debidamente actualizado, adicionalmente se deben considerar escenarios de riesgo enfocados en mitigar eventos adversos relacionados con la seguridad de la información. No se evidenciaron pruebas de continuidad de la seguridad de la información ante eventos adversos.			
11	**PLAN DE RECUPERACIÓN DE DESASTRES** Se evidenció que la entidad y el departamento de Gestión de las TIC's ha desarrollado un manual para la recuperación de la operación tecnológica ante un desastre o situación adversa. Por otra parte, pudo evidenciarse que dicho instructivo no se encuentra aprobado o no es conocido por otras áreas de interés de la entidad.	Pérdida en la capacidad de continuidad ante un incidente o evento adverso	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
12	**POLÍTICA DE RETENCIÓN DE DATOS** Se evidenció que actualmente La entidad no ha definido una política general para la retención de datos.	Perdidas económicas por Sanciones debido a incumplimientos legales	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
13	**PROGRAMA CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN - USUARIO FINAL** Se evidenció que la entidad no cuenta con un programa de concienciación de los usuarios finales con respecto a buenas prácticas en seguridad de la información.	Perdida de información por uso inadecuado de los recursos de TI debido a la ausencia de capacitación integral en seguridad de la información	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
14	**ESTANDAR DE DESARROLLO SEGURO DE SOFTWARE** Se evidenció que actualmente el instituto no considera estándares de desarrollo seguro tanto para soluciones inhouse o las desarrollados por terceros. Los requerimientos de seguridad son especificados de acuerdo a un estudio previo realizado por Gestión de las TIC's pero de manera ad-hoc.	Exposición insegura de los desarrollos internos o contratados a proveedores	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
15	**DEPENDENCIA PERSONAL CLAVE – GESTIÓN DOCUMENTAL** Se evidenció la existencia de personal crítico, los cuales ejecutan actividades neurálgicas del proceso, que, a su vez, en caso de ausencia, podrían impactar de	Indisponibilidad operativa para ejecutar actividades críticas.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	manera negativa la continuidad de algunos procesos de la entidad.			
16	**DATA LOSS PREVENTION "DLP"** Actualmente se cuenta con una solución o herramienta para evitar la fuga de información por los diferentes canales de comunicación utilizados por la entidad, pero no se encuentra implementada en la operación.	Perdidas económicas y/o reputacionales por fuga de información debido a la ausencia de controles que puedan restringir la transmisión o salida de información sensible y/o critica.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
17	**INDICADORES GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** Actualmente la entidad no ha definido indicadores claves de desempeño y/o riesgo que les permita medir el desempeño de los controles implementados, riesgos actuales y/o emergentes.	Ausencia de monitoreo de las políticas relacionadas con la seguridad de la información evitando tomar las acciones correctivas correspondientes	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
18	**GESTIÓN DE LA CRIPTOGRAFÍA** Aunque actualmente se encuentra definida una política para la gestión de la criptografía en la entidad, deben establecerse procedimientos para su	Fuga de información confidencial de los procesos o áreas críticas de la entidad	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	cumplimiento absoluto,			
19	**GESTIÓN DE LAS VULNERABILIDADES TECNOLÓGICAS** Aunque se realizan actividades para la detección de vulnerabilidades sobre los activos tecnológicos de la entidad, no se evidencian planes de acción orientados a mitigar las vulnerabilidades de seguridad tecnológicas.	Acceso no autorizado o sabotaje sobre la infraestructura tecnológica de la entidad.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
20	**SEGURIDAD DE LA INFORMACIÓN CON PROVEEDORES** No se evidenciaron mecanismos orientados a establecer la seguridad de la información con personal externo. Actualmente el personal externo contratado en el área de gestión de proyectos no cumple con los procedimientos o políticas de seguridad definidos por el instituto a cargo del área de gestión de TIC's	Fuga de información confidencial del Instituto.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
21	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	Pérdida de la confidencialidad, disponibilidad e integridad de la información de los	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	Aunque actualmente los incidentes de tipo operativo y funcional son reportados a la mesa de soporte por medio del software GLPI, no se ha implementado el procedimiento para la atención de incidentes de seguridad de la información el cual permita identificar, catalogar, contener, resolver y aprender de las situaciones adversas que puedan afectar la confidencialidad, disponibilidad e integridad de la información del instituto.	procesos afectados por un incidente.		
22	**SEGURIDAD FÍSICA Y CONTROL DEL ACCESO A LAS INSTALACIONES** Al realizar un recorrido por las instalaciones de la entidad, se observó que actualmente no se tiene implementado de forma homogénea un control de entrada y salida de equipos. Adicionalmente se observó que el personal visitante no se puede distinguir del funcionario ya que actualmente no se portan escarapelas para tal fin. No se dispone de controles detectivos (como alarmas) ni disuasivos (como cámaras) en las arenas	Robo de equipos y activos físicos, los cuales podrían ocasionar a su vez pérdidas de información o pérdidas de la operación.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	claves del instituto (segundo piso). Adicionalmente el perímetro de seguridad del instituto no se encuentra monitoreado por medio de sensores u otro mecanismo que permita mitigar el riesgo de infiltración física de amenazas.			
23	**ROLES Y RESPONSABLES DEL SGSI Y PDP** El instituto debe vincular talento humano que se encuentre en la capacidad de hacer frente a los requerimientos de ley como la 1581 de 2012 (Superintendencia de Industria y Comercio) y circulares como la 007 y 008 expedidas por la Superfinanciera. Actualmente la entidad no dispone de personal interno con competencias técnicas o especializadas para la atención de los requerimientos regulatorios enfocados en satisfacer las necesidades de ciberseguridad y privacidad de datos.	Incumplimientos regulatorios y sanciones al instituto por omisión de los requerimientos normativos.	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"
24	**ESTRATEGIA DE LA GESTIÓN TECNOLÓGICA** Revisar habilitadores transversales manual de	Incumplimientos regulatorios y sanciones al instituto por omisión de los requerimientos	"Información clasificada como pública reservada"	"Información clasificada como pública reservada"

No.	Observación	Riesgo	Recomendación	Implementación
	gobierno digital V5. Revisar Decreto 1008 del 14 de Junio de 2018 (Gobierno Digital)	normativos.		

El **Plan de Seguridad y Privacidad de la Información de Infivalle** contiene información clasificada como "pública reservada" conforme a la definición establecida en el artículo 6 de la Ley 1712 de 2014, información que podría poner en riesgo la seguridad de la misma, la tecnológica, de procesos y de las personas que laboran actualmente con el Instituto, por tanto, solo podrá ser conocido en su integridad por las partes interesadas competentes y/o autorizadas legalmente.

"Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley;"

CONTROL DE CAMBIOS

Versión	Acto Administrativo que lo Adopta o Actualiza	Fecha (Día/Mes/Año)	Descripción de la modificación y/o actualización	Validado por:
1	Resolución 022	31/01/2020	Creación del documento	Profesional Especializado TIC