CÓDIGO DE LA AUDITORÍA INTERNA: SIS-2021

DENOMINACIÓN DEL TRABAJO: Auditoría Interna con Base en Riesgos - Proceso ***"Sistemas".***

DESTINATARIOS:[1] Julio César González García, Director General del Banco Inmobiliario de Floridablanca - BIF y demás integrantes del Comité Institucional de Coordinación del Sistema de Control Interno.

EMITIDO POR: Héctor Fabio Rodríguez Devia, Profesional Especializado - Control Interno.

OBJETIVO DEL TRABAJO: Evaluar la solidez de los controles internos implementados para gestionar los riesgos asociados al Proceso ***"Sistemas"*** del Banco Inmobiliario de Floridablanca - BIF.

ALCANCE: El alcance establecido para la realización de este trabajo comprendió la evaluación de los controles internos propios del proceso auditado, relacionados con los siguientes tópicos:

- Política de operación Oficina Administrativa y Financiera de Sistemas de Información y TIC's.
- Plan de seguridad y privacidad de la información.
- Plan de tratamiento de riesgos de seguridad y privacidad de la información 2020 - 2023.
- Plan estratégico de tecnologías de la información (PETI) 2020 - 2023.
- Plan de Acción Institucional y Sistema de Administración de Riesgos.

Período auditado: 1-Ene-2020 al 28-Feb-2021

Limitaciones al Alcance: El proceso "Control Interno" del Banco Inmobiliario de Floridablanca - BIF, no cuenta con recurso humano calificado que ostente título de formación académica en el área de las Tecnologías de la Información y las Telecomunicaciones (Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Telecomunicaciones, etc.), razón por la cual, esta actividad fue ejecutada con las limitaciones propias derivadas de la carencia de las competencias técnicas específicas en tal área del conocimiento.

[1] Decreto 1083 de 2015 Artículo 2.2.21.4.7, Parágrafo 1° (modificado mediante el Artículo 1 del Decreto 338 de 2019) *"Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal el representante legal de la Entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva (…)"*

NORMATIVIDAD APLICABLE: Para la realización de este trabajo se consideraron como principales criterios, los siguientes:

- Decreto 1083 de 2015, Art. 2.2.22.3.8, numeral 6°.
- Decreto 1078 de 2015.
- Decreto 415 de 2016.
- Documentos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones:
  - G.ES.06 "Guía cómo estructurar el Plan Estratégico de Tecnologías de la Información - PETI" versión 2.0 (Julio de 2019).
  - Lineamientos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. Versión 1.2 (Octubre de 2019).
- Normatividad interna relacionada en el "Alcance" de este mismo documento.

RIESGOS SOBRE LOS CUALES SE FUNDAMENTÓ LA AUDITORÍA:

Identificados en el Mapa de Riesgos del Proceso Auditado:

- **R1:** Pérdida de información de la Entidad a beneficio de un tercero.

Identificados por el Auditor Interno:

- **R2:** Inconsistencias en la elaboración, implementación y/o cumplimiento de las políticas, planes de gestión o Plan de Acción Institucional.
- **R3:** Incidentes que comprometan la continuidad de la operación de la Entidad (ciberataques, interrupciones no planificadas, pérdidas de información, etc).

DECLARACIÓN: Esta auditoría fue realizada con base en el análisis de muestras aleatorias seleccionadas por el auditor a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

FORTALEZAS IDENTIFICADAS (ASPECTOS POSITIVOS): Como resultado de la evaluación practicada sobre el Proceso ***"Sistemas"*** del Banco Inmobiliario de Floridablanca - BIF y con fundamento en la información recibida durante la auditoría, se identificaron las siguientes fortalezas a resaltar:

1. Una vez analizado el Plan Estratégico de Tecnologías de la Información - PETI 2020 - 2023 de la Entidad, se pudo determinar que el mismo se ajusta a lo establecido en el documento G.ES.06 Guía para la Construcción del PETI (Versión 2.0), en lo relacionado con:

   - Esquema de seguimiento y control debidamente establecido.

   - Determinación de una estructura de medición fundamentada en indicadores.

   - Alineación de la estrategia de tecnologías de la información, describiendo cada uno de los objetivos y metas de TI.

   - Adopción, aprobación y publicación.

2. En relación con el Plan de Acción - Gobierno en Línea 2020, se verificó el cumplimiento de las siguientes actividades:

   - Acciones de capacitación (personalizada, correo o charlas grupales) impartidas a los funcionarios, en temas relacionados con Gobierno en Línea.

   - Convocatorias a la ciudadanía para participar en los espacios y procesos de rendición de cuentas.

3. Con base en la Política de Operación de la Oficina Administrativa y Financiera de Sistemas de Información, se observó el cumplimiento de los siguientes tópicos:

   - El Centro de Cómputo de la Entidad cuenta con: Extintor, Sistema de Aire acondicionado, cableado en conductos estructurados y protegidos, sin presencia de elementos combustibles.

   - La infraestructura tecnológica de la Entidad se encontraba conectada a los puntos de corriente regulada.

   - El acceso al Centro de Cómputo se encuentra restringido (sólo accede el personal autorizado).

OPORTUNIDADES DE MEJORAMIENTO (HALLAZGOS):

1. AUSENCIA DE FILTROS DE CONTENIDO Y NAVEGACIÓN WEB.

Al analizar la ejecución de los controles establecidos sobre el uso de Internet, se observó que la Entidad no ha implementado filtros de contenido y navegación en la red que restrinjan el acceso y consulta de páginas web indebidas (pornografía infantil, trata de personas o contrabando), infringiendo así lo determinado en el numeral 5.6 de la Política de Operación de la Oficina Administrativa y Financiera de Sistemas de Información y TIC's.

Causa probable: Limitaciones operacionales generadas con ocasión del Estado de Emergencia Económica, Social y Ecológica declarado con ocasión del Covid-19.

Riesgo (s) asociado (s): R2: Inconsistencias en la elaboración, implementación y/o cumplimiento de las políticas, planes de gestión o Plan de Acción Institucional. **R3:** Incidentes que comprometan la continuidad de la operación de la Entidad (ciberataques, interrupciones no planificadas, pérdidas de información.

Recomendación: Con el objetivo de gestionar los riesgos de seguridad de la información relacionados con el acceso a sitios web que pudieran representar amenazas para la Entidad, se recomienda:

- **Sensibilizar al recurso humano de la Entidad:** Diseñar y ejecutar estrategias de sensibilización que permitan al talento humano de la Entidad conocer las normas de seguridad de la Entidad, los riesgos derivados de la omisión de las prácticas seguras y las técnicas para reconocer y gestionar eventos y sitios sospechosos en la web.

- **Implementar filtros de contenido y navegación:** Adoptar y poner en operación los controles establecidos en la Política de Operación de la Oficina Administrativa y Financiera de Sistemas de Información y TIC's, relacionados con la implementación de medidas preventivas que impidan a los usuarios acceder a páginas web con contenido indebido o riesgoso, relacionadas (entre otros) con los siguientes tópicos: pornografía, trata de personas, contrabando, juegos (de azar o videojuegos), etc).

2. FALTA DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SERVICIOS TECNOLÓGICOS (SGSTI) CON BASE EN LA NORMA ISO 20000-1.

De acuerdo con la información obtenida durante el desarrollo de la auditoría, el Banco Inmobiliario de Floridablanca - BIF no ha iniciado un proceso formal para la implementación de su Sistema de Gestión de Servicios Tecnológicos (SGSTI) fundamentado en la Norma ISO 20000-1, razón por la cual, no fue posible cumplir la meta determinada en el numeral 9.3 del Plan Estratégico de Tecnologías de la Información PETI 2020 - 2023 de la Entidad (30% de implementación a 31-Dic-2020).

Causa probable:

- Limitaciones operacionales generadas con ocasión del Estado de Emergencia Económica, Social y Ecológica declarado con ocasión del Covid-19.

- Restricciones presupuestales relacionadas con los recursos asignados al proceso auditado.

Riesgo (s) asociado (s): R2: Inconsistencias en la elaboración, implementación y/o cumplimiento de las políticas, planes de gestión o Plan de Acción Institucional.

Recomendación: Corresponde al responsable del proceso auditado, exponer ante el Comité Institucional de Gestión y Desempeño los detalles pormenorizados del proyecto de implementación del Sistema de Gestión de Servicios Tecnológicos (SGSTI) fundamentado en la Norma ISO 20000-1 (horizonte de tiempo, hitos, alcance, recursos necesarios, etc.) esto con el fin de determinar la conveniencia o no de llevar a cabo este proceso.

En caso de que se dé vía libre a la implementación del SGSTI / Norma ISO 20000-1, se deben establecer etapas, entregables, metas parciales e indicadores que permitan monitorear de forma objetiva el grado de avance del proyecto.

Si por el contrario, la Entidad decide cancelar, postergar o reemplazar esta actividad, se debe gestionar la respectiva modificación del Plan Estratégico de Tecnologías de la Información PETI 2020 - 2023.

3. ACTIVIDADES DEL PLAN DE ACCIÓN - GOBIERNO EN LÍNEA 2020 (HOY GOBIERNO DIGITAL) SIN EJECUTAR (A 31-DIC-2020).

Al analizar la ejecución de seis (6) actividades incluidas en el Plan de Acción - Gobierno en Línea 2020 de la Entidad, no se obtuvo evidencia de la ejecución de cuatro (4) de estas:

ACTIVIDAD / ACCIÓN PLAN DE ACCIÓN GOBIERNO EN LÍNEA 2020	PLAZO MÁXIMO EJECUCIÓN
Promoción y divulgación de los avances de la implementación de la estrategia GEL en la Entidad. Ofrecer incentivos a los funcionarios que atiendan oportunamente a las capacitaciones ofrecidas, demuestren y apliquen lo aprendido.	Oct-2020
Seleccionar y aplicar una herramienta web que permita la validación automática sobre la accesibilidad a la página web institucional (Norma NTC 5854).	Oct-2020
Entrevistar a los líderes de cada proceso para identificar riesgos de TI.	Nov-2020
Gestionar que los formatos de los trámites que se realizan en el BIF puedan ser descargados por los Usuarios en el SUIT, así como un instructivo / demo, acerca de cómo diligenciar dichos formularios.	Nov-2020

Causa probable: Limitaciones operacionales generadas con ocasión del Estado de Emergencia Económica, Social y Ecológica declarado con ocasión del Covid-19.

Riesgo (s) asociado (s): R1: Pérdida de información de la Entidad a beneficio de un tercero. **R2:** Inconsistencias en la elaboración, implementación y/o cumplimiento de las políticas, planes de gestión o Plan de Acción Institucional.

Recomendación: Se recomienda al responsable del proceso auditado, gestionar una nueva versión del Plan de Acción - Gobierno en Línea (hoy Gobierno Digital) para ser implementado a partir de la vigencia 2021, en la cual se recojan aquellas actividades pendientes de ejecutar en la vigencia anterior, así como aquellas nuevas actividades de corto, mediano y largo plazo que permitan implementar a cabalidad la Política de Gobierno Digital (incluida en la 3ª dimensión del Modelo Integrado de Planeación y Gestión - MIPG).

Esta nueva versión del Plan de Acción (Gobierno Digital) debe ser estudiada y aprobada por el Comité Institucional de Gestión y Desempeño.

4. DEBILIDADES EN LA ESTRUCTURA DEL PETI 2020 - 2023.

Al comparar el Plan Estratégico de Tecnologías de la Información PETI 2020 - 2023 del Banco Inmobiliario de Floridablanca - BIF con respecto a los lineamientos determinados en el documento *G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI* (Versión 1.1) emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, se observaron las siguientes diferencias:

- En su numeral 6. "Análisis de la Situación Actual" el PETI 2020 - 2023 no contempla un Análisis Financiero mediante el cual se describan los costos actuales de operación y funcionamiento del área de TI, desglosando los costos de licenciamiento, costos de soporte y mantenimiento de los sistemas de información y los servicios tecnológicos, costos capacitación, entre otros (numeral 2.5.7 de la Guía).

- En su numeral 10. "Modelo de Planeación" el PETI 2020 - 2023 no contiene:

  - Lineamientos y/o principios que rigen el plan estratégico de TIC: En esta sección se deberían definir los lineamientos y principios que guían la definición del PETI como, por ejemplo: Los procesos se apoyarán con tecnología según su nivel de desarrollo y según la disponibilidad de herramientas tecnológicas.

  - Estructura de actividades estratégicas: Se deben relacionar las iniciativas estratégicas de TI, desagregando las mismas en subactividades, preferiblemente siguiendo la estructura del Plan de Acción Institucional y del Plan de Adquisiciones, constituyéndose así en la base para el seguimiento a la ejecución presupuestal (numerales 2.8.1 y 2.8.2 de la Guía).

- Aunque el PETI 2020 - 2023 contiene la sección 11. *"Plan de Comunicación"*, el contenido de la misma se limita a identificar la necesidad de realizar un plan de comunicaciones, sin que se describan las actividades de comunicación y sensibilización que se desarrollarán para apropiar el PETI en la Entidad (numeral 2.9 de la Guía).

- **Causa probable:** Desconocimiento de los lineamientos normativos y/o procedimentales aplicables a la estructura del Plan Estratégico de Tecnologías de la Información PETI.

- **Riesgo (s) asociado (s): R2:** Inconsistencias en la elaboración, implementación y/o cumplimiento de las políticas, planes de gestión o Plan de Acción Institucional.

- **Recomendación:** Se recomienda al responsable del proceso auditado, gestionar una nueva versión del Plan Estratégico de Tecnologías de la Información PETI de la Entidad, asegurándose que la misma se ajuste a los lineamientos determinados en el documento G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI (Versión 1.1) el emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones y demás criterios aplicables.

  Esta nueva versión del PETI debe ser estudiada y aprobada por el Comité Institucional de Gestión y Desempeño.

5. INCUMPLIMIENTO DEL CRONOGRAMA ESTABLECIDO EN EL CATÁLOGO DE SERVICIOS TIC y el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Entidad no ha llevado a cabo el proceso de elaboración, estudio, aprobación y socialización de la Política de Seguridad del Talento Humano y la Política de Gestión de Proveedores, situación que incumple el cronograma de actividades del Modelo de Seguridad y Privacidad de la Información, determinado en el numeral 10 del Plan de Seguridad y Privacidad de la Información de la Entidad, así como en el Catálogo de Servicios TIC.

Causa probable: Limitaciones operacionales generadas con ocasión del Estado de Emergencia Económica, Social y Ecológica declarado con ocasión del Covid-19.

Riesgo (s) asociado (s): R2: Inconsistencias en la elaboración, implementación y/o cumplimiento de las políticas, planes de gestión o Plan de Acción Institucional.

Recomendación: Se recomienda al responsable del proceso auditado, gestionar el cumplimiento del cronograma de actividades del Modelo de Seguridad y Privacidad de la Información (determinado en el numeral 10 del Plan de Seguridad y Privacidad de la Información de la Entidad), brindando especial prioridad a las actividades vencidas que debieron ejecutarse durante la vigencia anterior (Política de Seguridad del Talento Humano y Política de Gestión de Proveedores).

RESUMEN DE OPORTUNIDADES DE MEJORAMIENTO (HALLAZGOS):

N°	TÍTULO DEL HALLAZGO
1	Ausencia de filtros de contenido y navegación web.
2	Falta de implementación del Sistema de Gestión de Servicios Tecnológicos (SGSTI) con base en la Norma ISO 20000-1.
3	Actividades del Plan de Acción - Gobierno en Línea 2020 (hoy Gobierno Digital) sin ejecutar (a 31-Dic-2020).
4	Debilidades en la estructura del PETI 2020 - 2023.
5	Incumplimiento del cronograma establecido en el Catálogo de Servicios TIC y el Plan de Seguridad y Privacidad de la Información.

Notas:

- La naturaleza de la labor de auditoría interna se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.

- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por el personal perteneciente al proceso o actividad auditada. Nuestro alcance no pretende corroborar la precisión de la información y su origen.

- Es necesario precisar que las “Recomendaciones” propuestas en ningún caso son de obligatoria ejecución por parte de la Entidad, más se incentiva su consideración para los planes de mejoramiento a que haya lugar. La respuesta ante las situaciones observadas es discrecional de la Administración del Banco Inmobiliario de Floridablanca - BIF.

--

Floridablanca, 26 de marzo de 2021.

HÉCTOR FABIO RODRÍGUEZ DEVIA
Profesional Especializado - Control Interno