| | | | |
|---|---|---|---|
| **FECHA DEL INFORME:** | 30/09/2019 | **PROCESO AUDITADO:** | Otorgamiento de crédito |
| **LIDER DEL PROCESO:** | Coordinador Grupo de Crédito | **AUDITADOS:** | Fredy Fontecha – Coordinador de Crédito VCC<br>Lucio Navarro – Líder MECI-Calidad VCC |
| **AUDITOR LÍDER:** | Adriana Aranguren | **EQUIPO AUDITOR:** | Adriana Aranguren |
| **LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:** | Sede Principal<br>VP crédito y cobranza.<br>Piso 6<br>24/09/2019 | **CRITERIOS DE AUDITORÍA:** | Norma Técnica ISO 27001:2013<br>Lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información, Política de Gobierno Digital y Política de Seguridad Digital.<br>Documentación del Sistema de Gestión de Seguridad de la Información. Planes de mejoramiento.<br>Normatividad aplicable. |

## 1. OBJETIVO

Evaluar el cumplimiento o la conformidad del Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información, de acuerdo con los requisitos de las normas técnicas vigentes aplicables, normativos y de la Entidad; en el proceso de Otorgamiento de crédito, identificando oportunidades de mejora.

## 2. ALCANCE

Se auditó la gestión general del proceso teniendo en cuenta las actividades realizadas del año 2018 hasta la fecha, con base en el ciclo PHVA y el cumplimiento de normas y lineamientos transversales del Sistema de Gestión de Seguridad de la Información, en lo aplicable al proceso.

## 3. FORTALEZAS

Se destaca la buena disposición para la atención de la auditoría por parte de los auditados y la disponibilidad de la información.

## 4. RESULTADOS

| CRITERIO DE AUDITORIA | NO CONFORMIDAD | OPORTUNIDAD DE MEJORA |
|---|---|---|
| Norma ISO 27001:2013<br>Anexo A<br>Dominio A.8 Gestión de activos<br>A.8.1. Responsabilidad sobre los activos<br><br>Modelo de Seguridad y Privacidad de la Información.<br>Fase: Planificación<br>Inventario de activos de | | Se recomienda revisar y ajustar el registro de activos de información, dado que se evidencia el “aplicativo C&CTEX” , clasificado como “sistema” dentro de un registro que solamente aplica para activos de información tipo dato (documentos en diferentes medios de soporte o bases de datos). En este caso, el registro se debería referir a la base de datos del aplicativo C&CTEX. Además, aparece como responsable |

| | | |
|---|---|---|
| Información.<br><br>Ley 1712 de 2014<br>Decreto 103 de 2015<br>Decreto 1081 de 2015 | | de generar la información la Dirección de Tecnología, cuando esa dependencia realmente cumple el rol de custodio. |

| | | |
|---|---|---|
| Norma ISO 27001:2013<br>6.1.2. Apreciación de los riesgos de seguridad de información<br><br>Modelo de Seguridad y Privacidad de la Información.<br>Fase: Planificación<br>Identificación, valoración y tratamiento de riesgo | | Se recomienda revisar la identificación de riesgos de seguridad de la información del proceso, de manera que se considere incluir el riesgo de falla de integridad de la información (asociado a manipulación de bases de datos de Core, dado que actualmente es operado por un tercero) y el de falla de disponibilidad de los sistemas de información, que tendría gran impacto sobre el proceso; en caso de materializarse. |

| | | |
|---|---|---|
| Norma ISO 27001:2013<br>Anexo A<br>A.12.4.2. Protección de la información de registro | Se presenta un incumplimiento de los requisitos de la Norma ISO 27001:2013, Anexo A, control A.12.4.2.Protección de la información de registro, por la pérdida de integridad de la información fuente para los comités de crédito de la Convocatoria II-2019, dadas las inconsistencias en la información registrada en los formularios del Core; lo cual se reportó como evento de riesgo y producto/servicio no conforme. Se deben tomar las acciones correctivas dentro del Sistema de Gestión de Seguridad de la Información, para evitar que se vuelva a presentar. | |

## 5. CONCLUSIONES

Se han logrado el objetivo y alcance de la auditoría y se puede concluir, con base en la muestra auditada, que el proceso presenta una “no conformidad” con respecto a los requisitos de la norma técnica ISO 27001:2013 y demás criterios aplicados. Ésta debe ser corregida y analizada para definir e implementar acciones correctivas, de acuerdo con el procedimiento de la entidad.

Así mismo, se detectaron en la auditoría dos oportunidades de mejora, las cuales se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro. El proceso no tenía planes de mejoramiento pendientes, por no conformidades de la anterior auditoría de seguridad de la información.

## 6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.