FECHA DEL INFORME:	30/08/2019	**PROCESO AUDITADO:**	Atención al cliente
LIDER DEL PROCESO:	Jefe de Oficina Comercial y de Mercadeo	**AUDITADOS:**	Marisol Castellanos – Profesional de Calidad - Oficina Comercial y de Mercadeo Claudia Stella Cortés – Coordinadora de Riesgos No Financieros
AUDITOR LÍDER:	Adriana Aranguren	**EQUIPO AUDITOR:**	Adriana Aranguren
LUGAR Y FECHA DE REALIZACIÓN DE AUDITORÍA:	Sede Principal Oficina Comercial y de Mercadeo. Piso 4. 22/08/2019	**CRITERIOS DE AUDITORÍA:**	Norma Técnica ISO 27001:2013 Lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información, Política de Gobierno Digital y Política de Seguridad Digital. Documentación del Sistema de Gestión de Seguridad de la Información. Planes de mejoramiento. 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 Atención al cliente y sus procedimientos, 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 las auditadas.

4. RESULTADOS

CRITERIO DE AUDITORIA	NO CONFORMIDAD	OPORTUNIDAD DE MEJORA
Norma ISO 27001:2013 Anexo A A.8 Gestión de activos A.8.2. Clasificación de la información Ley 1712 de 2014 Decreto 103 de 2015		Es importante revisar la clasificación de confidencialidad del activo “Exención de impuestos de clientes” a la luz de las normas de Transparencia y de Protección de Datos, ya que solamente contiene nombres y números de identificación (datos públicos). Debe estar incluido en la Tabla de Retención Documental de la OCM, de manera que se identifique específicamente como documento independiente, para la gestión de archivo. Se requiere revisar la manipulación de esta información porque se almacena en un

		archivador dentro de la Oficina Comercial y de Mercadeo, la funcionaria no se encontraba y estaba sin llave.
Norma ISO 27001:2013 Anexo A A.8 Gestión de activos A.8.2. Clasificación de la información Ley 1712 de 2014 Decreto 103 de 2015 Resolución 3564 de 2015		Debe revisarse y actualizarse el inventario de activos de información, dado que el activo llamado “Notificación de escalonamiento a proceso misional” aparece con medio de almacenamiento físico, pero según se informó en auditoria se consulta en Mercurio y no se imprime en la OCM. Sin embargo, en la TRD dice que está almacenado digitalmente en el CRM. Por otra parte, para el activo “Informes periódicos de la gestión por canales, servicios y puntos de atención”, se evidencia que la información contenida es pública (sólo incluye algunos informes que tienen nombres, número de documento y fecha de ingreso del personal de atención al cliente). La clasificación, en todo caso debería ser parcial y se debe justificar en el campo “fundamento jurídico de la excepción” en el índice de información clasificada y reservada. También debería incluirse este documento en la Tabla de retención documental de la OCM.
Norma ISO 27001:2013 6.1.2. Apreciación de los riesgos de seguridad de información 6.1.3. Tratamiento de los riesgos de seguridad de información		La causa del riesgo RSI3 - Falla de confidencialidad por inadecuado manejo de activos de información, redactada como CASI41-Incumplimiento en los lineamientos en la gestión de activos de información, corresponde a una debilidad de control general, que podría aplicar para cualquier proceso. Se recomienda especificar mejor dicha causa. El control planteado menciona el etiquetado, pero dadas las políticas y procedimientos establecidos en la entidad, el etiquetado no se aplica aún para los activos físicos.
Norma ISO 27001:2013 6.1.2. Apreciación de los riesgos de seguridad de información 6.1.3. Tratamiento de los riesgos de seguridad de información Anexo A A.15. Relación con proveedores		La redacción del control de selección de personal establecido frente al riesgo RSI4-Falla de confidencialidad por inadecuado manejo de proveedor en temas de seguridad digital, causa CASI30-Contratistas ejecutan acciones no autorizadas no es claro. Al parecer, se refiere a la selección que realiza el proveedor de servicio al cliente, la cual según se informó no incluye exigir al proveedor realizar estudios completos de seguridad previos al ingreso del personal; lo cual se debería tener en cuenta para la nueva contratación del proveedor.
		Se deberían tomar medidas más efectivas para la recolección de la autorización para el tratamiento de datos personales que exige la

Ley 1581 de 2012 Decreto 1377 de 2013 (compilado en el Decreto 1081 de 2015)		Ley 1581 de 2012, para los usuarios que se acercan a las oficinas de atención personalizada. El aviso de privacidad que se presenta en los puestos de atención solamente se informa la finalidad del ejercicio de las funciones de seguridad de la entidad y las personas; pero no se puede asumir que se trata de una autorización de tratamiento de datos para la solución de peticiones, quejas y reclamos; porque además en la política publicada para el tratamiento de datos no se incluye dicha finalidad. Se evidencia que existe un guión aplicable de manera verbal; sin embargo, se recomienda conservar evidencia de la autorización del usuario para el canal de atención personalizada, la cual debe incluir la información al ciudadano sobre sus derechos y autorización expresa para la recolección de datos sensibles y datos personales de niñas, niños y adolescentes. (En cumplimiento del Decreto 1377 de 2013, Artículos 5 y 6).
Norma ISO 27001:2013 8.1. Planificación y control operacional Anexo A A.15 Relación con proveedores A.15.1. Seguridad en la relación con proveedores		Es necesario continuar de manera permanente con la supervisión al cumplimiento de la normatividad, políticas y controles de seguridad de la información y de protección de datos personales en los diferentes canales y sedes de atención, por parte del personal del tercero que realiza la atención al cliente. Se deben exigir al proveedor acciones correctivas que permitan evitar que se vuelvan a presentar las no conformidades y realizar el respectivo seguimiento de su ejecución y efectividad. Se recomienda tener en cuenta en el nuevo modelo de servicio y con el proveedor que inicia contrato. Esto porque se evidenció uso de usuarios de otros trabajadores y autoguardado en el navegador para el acceso al sistema de información CRM en la oficina de la sede Aguas (Manuel Quiñones, accede al CRM con un usuario ajeno -YIbarra); en las visitas de la OCI a Barranquilla y Medellín se evidenciaron equipos desatendidos, en Bucaramanga y Barranquilla no se evidenciaron avisos de privacidad. En esta última sede se encontró copia de cédula de un usuario, documento desatendido.
Norma ISO 27001:2013 Anexo A A.13.2.2. Acuerdos de intercambio de información	No se tiene establecido un acuerdo de intercambio de información con el proveedor de atención al cliente, lo cual cobra gran importancia dado el carácter confidencial de la información que se	

	intercambia con el tercero. Esto incumple con el control A.13.2.2 Acuerdos de Intercambio de información, del Anexo A de la Norma ISO 27001:2013.	

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 seis oportunidades de mejora, las cuales se recomienda analizar, con el fin de definir e implementar acciones que permitan evitar no conformidades en el futuro.

Como parte del seguimiento del plan de mejoramiento proveniente de los resultados de la anterior auditoría interna de seguridad de la información, se cierran las 5 no conformidades, considerando que se han tomado acciones para eliminarlas; aunque se dejan observaciones y recomendaciones frente a algunas de ellas. Ver Formato de seguimiento F86 anexo.

6. OBJECIONES DEL AUDITADO NO RESUELTAS

No aplica.