1. **AUDITORIA CIRCULAR 052**

El servicio de Auditoria de la seguridad Circular 052 identifica los controles sobre los cuales no se tiene cumplimiento al momento de la realización de la auditoría. Se busca en este proceso identificar de manera concisa y veraz si se está cumpliendo con el modelo de seguridad alineado directamente con los controles establecidos por la circular 052. Una vez realizado este estudio, es decir, la identificación de los controles sin soporte, se debe generar entonces un reporte de cumplimiento para que se tomen las medidas correctivas adecuadas de acuerdo a un plan de acción definido y aprobado por las directivas. La evaluación del cumplimiento de la circular 052 se puede cuantificar para dar una medida de la cercanía o lejanía con relación al 100% de los controles exigidos por la norma y con esta información realizar un *benchmarking* con relación a este sector productivo o comercial donde está radicada la compañía.

Referencia: Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

ACTIVIDADES RELACIONADAS CON LA AUDITORIA CIRCULAR 052

a. Conocimiento de la estructura y procesos del negocio
b. Conocimiento de la infraestructura de IT
c. Plan de la auditoría circular 052
    i. Obtención de datos.
    ii. Lista de personas a entrevistar.
    iii. Enfoque del trabajo
    iv. Obtención de políticas y normas
    v. Verificar los controles existentes.
d. Entrevistas (participan los dueños de los activos relacionados)

e. Revisión de documentos
f. Visitas a sitios físicos (Se requiere acompañamiento)
g. Revisión de informes
h. Elaboración del informe final auditoría circular 052
    i. Objetivo de la auditoría 052
    ii. Alcance de la auditoría 052
    iii. Hallazgos importantes
    iv. Recomendaciones
    v. Conclusiones

ITEMS A REVISAR AUDITORIA CIRCULAR O52

(Por definir según alcance específico[1])

2. Definiciones y criterios de seguridad y calidad
2.1. Criterios de Seguridad de la información
2.2. Criterios de Calidad de la información
3. Obligaciones Generales
3.1. Seguridad y Calidad
3.3. Documentación
3.4. Divulgación de Información
4. Obligaciones Adicionales por Tipo de Canal
4.1. Oficinas
4.2. Cajeros Automáticos (ATM)
4.3. Receptores de Cheques
4.4. Receptores de Dinero en Efectivo
4.5. POS (incluye PIN Pad)
4.6. Sistemas de Audio Respuesta (IVR)
4.7. Centro de Atención Telefónica (Call Center, Contact Center)

[1] Este alcance debe ser revisado de acuerdo con el cliente, lo mismo aplica para el valor total del proyecto una vez definido el alcance definitivo.

4.8. Sistemas de Acceso Remoto para Clientes
4.9. Internet
4.10. Prestación de Servicios a través de Nuevos Canales
5. Reglas sobre Actualización de Software
6. Obligaciones Específicas por Tipo de Medio – Tarjetas débito y crédito
7. Análisis de Vulnerabilidades

ANEXO: IMPLANTACION DE LA CIRCULAR 052

La implementación de la circular 052 se hará en tres etapas, la primera de las cuales inicia el 1º de julio del 2008 y la última finaliza el 1º de enero de 2010, conforme se señala a continuación:

La primera etapa de la implementación de la circular 052 rige a partir del 1º de julio del 2008 y en esa fecha las entidades deberán tener implementados, probados y en producción todos los procesos, mecanismos y sistemas de los cuales trata el Capítulo Décimo Segundo, Título I de la Circular Externa 007 de 1996 (Circular Básica Jurídica) anexa a la presente Circular, con excepción de los requerimientos indicados para la segunda y tercera fase. A partir del 1º de julio del 2008 y siempre que las entidades expidan o renueven tarjetas débito o crédito, estarán obligadas a dar cumplimiento a lo dispuesto en el numeral 6.9 del citado capítulo.

En la segunda etapa de la implantación de la circular 052 las entidades deberán atender lo señalado en los numerales 3.1.2, 3.1.3, 3.1.6, 3.1.9, 3.1.13, 3.1.16, 3.2.3, 3.3.1, 3.4.2, 3.4.7, 4.1.5, 4.2.2, 4.3 y 6.6 del capítulo en mención y contarán como plazo máximo para su implementación el 1º de enero del 2009.

En la tercera fase de la implantación de la circular 052 las entidades deberán dar cumplimiento a lo dispuesto en los numerales 3.1.10, 3.1.20, 4.1.3, 4.2.1, 4.5.2,

4.5.3, y 6.11 de dicha norma y el plazo máximo para la entrada en operación de estos requerimientos será el 1º de enero del 2010[2].

[2] Para mayor información consultar la circular 052.