Calltech
Comunicaciones Inteligentes

Call Processing Technologies, Calltech S.A.

CTMail

CTLog

Cumplimiento de Circular N° 052
con el Sistema de grabación CTLog ®

Cumplimiento de Circular N° 052 con el Sistema de grabación CTLog ®:

El sistema de grabación digital y monitoreo Web en línea CTLog ®, cumple los criterios de seguridad y calidad de la información exigidos por la norma 052.

Con la presente yo Carlos Augusto Villamizar Cadena como gerente general de Call Processing Technologies Calltech S.A., certifico que el producto CTLog ®, cumple los criterios de seguridad y calidad de la información exigidos por la norma 052 y continuación mostrare cada uno de los puntos de la Norma 052, que se pueden cumplir gracias al sistema de grabación digital y monitoreo Web en línea CTLog ®, con una descripción de los procesos que realizan cada uno de los módulos de nuestro producto y que lograran que su empresa cumpla esta normativa y de esta forma velar por la seguridad y la calidad de la información de sus clientes y usuarios.

*"**2. Definiciones y criterios de seguridad y calidad:***
Para el cumplimiento de los requerimientos mínimos de seguridad y calidad de la información que se maneja a través de canales y medios de distribución de productos y servicios para clientes y usuarios, las entidades deberán tener en cuenta las siguientes definiciones y criterios:
2.1. Criterios de Seguridad de la información:
***a) Confidencialidad:** Hace referencia a la protección de información cuya divulgación no está autorizada.*
***b) Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.*
***c) Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.*
2.2. Criterios de Calidad de la información:
***a) Efectividad:** La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.*
***b) Eficiencia:** El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.*
***c) Confiabilidad:** La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones."*[1]

Seguridad y calidad de la información:

"***3.1. Seguridad y Calidad***
En desarrollo de los criterios de seguridad y calidad, y considerando los canales de distribución utilizados, las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:
***3.1.1.** Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.*
***3.1.4.** Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad."*[2]

CTLog ® cuenta con los criterios de Seguridad de la información que se solicitan en la circular N° 052: Confidencialidad, integridad y disponibilidad, ya que es una herramienta robusta, confiable y rentable con tecnología Web, que garantiza la seguridad de la información, respaldada por Microsoft Windows Server 2003/2008 y los principales fabricantes de los componentes telefónicos como

[1] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 96
[2] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 97

Audicodes. Los criterios de confidencialidad, integridad y disponibilidad, son garantizados a través del módulo de firma digital de algoritmo RSA-DSA, con el cual se garantiza la seguridad, autenticidad e integridad de las grabaciones ya que no podrán modificarse o alterarse, y que mostrara alertas de vulnerabilidad en caso de realizarse un intento de violación a la integridad del sistema. Al igual para cumplir los criterios de calidad de la información: efectividad, eficiencia y confiabilidad, CTLog® cuenta con una plataforma distribuida de diseño modular y arquitectura abierta que evoluciona de acuerdo a sus necesidades. Cuenta con sus grabaciones de manera fácil, segura y con entrega oportuna, correcta y consistente, que permite resolver dificultades relacionadas en la comunicación con sus clientes y sus transacciones y detectar llamadas sospechosas o maliciosas para su análisis.

Nota: El sistema de grabación digital y monitoreo Web en línea CTLog ®, también cumple ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

"***3.1.8.*** *Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.*
3.1.18. *Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.*"[3]

Para cumplir los anteriores numerales 3.1.8. y 3.1.18., CTLog ®, cuenta con:
Módulo de Alarmas – CTLog ® Alarm: que identifica todas las alarmas necesarias para determinar el correcto funcionamiento de la plataforma. Con el que se podrán recibir alarmas visibles, audibles y vía e-mail del funcionamiento del sistema.
Módulo de Respaldo CTLog ® Backup: que respalda en DAT, DVD, Blu Ray de forma manual o automática las grabaciones y su información, de acuerdo a la configuración que usted determine y permite establecer criterios de respaldo de acuerdo a sus necesidades.
Módulo de Supervisión – CTLog® Telemanagement: envía alarmas visibles y audibles acerca del funcionamiento del sistema y permite visualizar el estado del canal de grabación, el medio de almacenamiento y su porcentaje de uso.

"***3.3. Documentación***
En materia de documentación las entidades deben cumplir, como mínimo, con los siguientes requerimientos:
3.3.1. *Dejar constancia de todas las operaciones que se realicen a través de los distintos canales de distribución de servicios para clientes y usuarios que contenga por lo menos lo siguiente: fecha, hora, código del equipo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión)número de la operación, cuenta(s), costo de la misma para el usuario."*

Para cumplir el numerales 3.3.1., CTLog ®, cuenta con:

[3] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 98

Módulo de Supervisión – CTLog® Telemanagement: el cual permite monitorear en tiempo real las conversaciones y pantallas, buscar y escuchar grabaciones históricas de manera sencilla y a través de diferentes criterios de búsqueda como: fecha, hora, campaña o sub-campaña utilizando: palabras literales, campos estándares o campos personalizados de las grabaciones.

Para cumplir el numerales 3.3.1., CTMail ®, cuenta con:
La Interfaz Web de Administración y Gestión OA&M, que contiene el módulo CTMail® SDK: el cual extiende las funcionalidades de su Sistema de Audio Respuesta (IVR) y audio texto desarrollando aplicaciones que interactúan, mediante XML y RPC, con CTMail®. Ideal para servicios de información que utilicen Bases de Datos, Sockets o WebServices.

*"**3.3.3.** Mantener a disposición de la SFC estadísticas anuales con corte a 31 de diciembre de cada año respecto de la prestación de servicios a través de cada uno de los canales de distribución, que contemplen: el número de operaciones realizadas y el nivel de disponibilidad del canal. Esta información deberá ser conservada por un término de tres (3) años."*[4]
*"**3.3.4.** Cuando a través de los distintos canales se pidan y se realicen donaciones, se deberá generar y entregar un soporte incluyendo el valor de la donación y el nombre del beneficiario.*
***3.3.5.** Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestarán sus servicios.*
Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información deberá ser conservada por lo menos por dos (2) años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.
***3.3.6.** Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deberán establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.*
***3.3.9.** Grabar las llamadas realizadas por los clientes a los centros de atención telefónica que conlleven a la consulta o actualización de su información.*
***3.3.10.** La información a que se refieren los numeral 3.3.1, 3.3.6 y 3.3.9 deberá ser conservada por lo menos por dos (2) años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.*
***3.4.5.** Establecer y publicar por los canales de distribución, en los que sea posible, las medidas de seguridad que deberá adoptar el cliente para el uso de los mismos."*[5]

Se logra cumplir los numerales 3.3.3., 3.3.4., 3.3.5., 3.3.6., 3.3.9. y 3.3.10. Gracias a los siguientes módulos:
Módulo de Administración - CTLog® Configurator: los administradores podrán configurar su plataforma de grabación de manera simple, rápida y efectiva vía web.

[4] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 98
[5] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 99

Administrar uno o varios servidores de grabación desde un único acceso a través de la web, así garantizar el espacio suficiente para el almacenamiento histórico de las grabaciones durante los tres años exigidos, junto con sus informes y estadísticas.
Con la posibilidad de asignar niveles de autorización y acceso a cada uno de los usuarios del sistema de acuerda a las instrucción que su empresa establezca para el manejo y conservación de esta información.
Permite gestionar campañas o grupo de sub-campañas de grabación para facilitar su búsqueda en los históricos.
Módulo de Supervisión – CTLog® Telemanagement: el cual permite monitorear en tiempo real las conversaciones y pantallas, buscar y escuchar grabaciones históricas de manera sencilla y a través de diferentes criterios de búsqueda como: campaña, sub-campaña, identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora, utilizando: palabras literales, campos estándares o campos personalizados de las grabaciones.

Con CTMail ® Operadora Automática, usted podrá publicar a través de su canal telefónico las medidas de seguridad que deben adoptar sus clientes y usuarios para el uso de sus diferentes canales mientras ellos se encuentran en la cola de espera, gracias a la configuración del AudioTexto: usted podrá reproducir información pregrabada a sus clientes. CTMail® permite, por ejemplo, crear líneas de información para usuarios del sistema, brindar instrucciones sobre un servicio, direcciones de oficinas o cómo completar un formulario.

*"**3.4.7.** Expedir un soporte, en papel o por medios electrónicos, al momento de la realización de cada transacción. Dicho soporte deberá contener al menos la siguiente información: fecha, hora (hora y minuto), código del equipo (para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles: el número desde el cual se hizo la conexión), número, costo de la operación para el cliente o usuario, tipo, entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan la operación. Se deberán ocultar los números de las cuentas con excepción de los últimos cuatro (4) caracteres, salvo cuando se trate de la cuenta que recibe una transferencia. Cuando no se pueda entregar el soporte, se deberá advertir previamente al cliente o usuario de esta situación. Para el caso de IVR se entenderá cumplido el requisito establecido en este numeral cuando se informe el número de la transacción. En relación con el costo de la operación y tratándose de cajeros automáticos la obligación solo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia."*[6]

Se cumplirá el numeral 3.4.7., con CTLog ®, mientras se realice la grabación de llamada en donde el cliente o usuario acepte la transacción y quien lo asesore suministre el número de transacción, para que así repose este archivo en los históricos.

*"**4.1.1.** Los sistemas informáticos empleados para la prestación de servicios en las oficinas deben contar con soporte por parte del fabricante o proveedor.*
***4.1.5.** La información que viaja entre las oficinas y los sitios centrales de las entidades deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los*

[6] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 99

Establecimientos de Crédito el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados."[7]

Para el cumplimiento de los numerales 4.1.1., y 4.1.5., Calltech S.A. cuenta con un servicio de soporte y mantenimiento preventivo para todas sus soluciones de Hardware y Software, que se adapta a las necesidades de los clientes y garantizará que no se interrumpa la operación. Personal calificado y especializado de Calltech S.A., lo atenderá de manera amable y oportuna diagnosticando los síntomas de falla, determinando los pasos de solución, aplicando la solución en el cliente y verificando el correcto funcionamiento.
Se cuenta con tres tipos de soporte dentro de los cuales se encuentra el Soporte Platinum que incluye: atención telefónica, actualizaciones de software a nuevas versiones, atención Email y Fax, atención con acceso remoto, acceso a portal de soporte Calltech S.A. y atención presencial en la Sede del cliente, este último permitirá que no se utilice información de sus clientes por terceros pues el soporte se realizara directamente en su empresa y bajo su supervisión.
Consulte más información sobre Tech Support y el modelo de soporte Calltech S.A. Aquí

Medios y canales de distribución de productos y servicios

*"**4.6. Sistemas de Audio Respuesta (IVR)***

Los sistemas de audio respuesta deberán cumplir, como mínimo, con los siguientes requerimientos:

***4.6.1.** Permitir al cliente confirmar la información suministrada en la realización de la transacción.*

***4.6.2.** Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público."*

*"**4.7.** Centro de Atención Telefónica (Call Center, Contact Center)*

Los centros de atención telefónica deberán cumplir, como mínimo, con los siguientes requerimientos:

***4.7.1.** Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.*

***4.7.2.** Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.*

***4.7.3.** Dotar a los equipos que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.*

***4.7.4.** Garantizar que los equipos destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.*

***4.7.5.** En los equipos usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el*

[7] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 100

intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos un (1) año o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto."[8]

Cumplimiento de 4.6.1. live vox….

Cumplimiento de 4.6.2. Operadora automática,
CTMail® Operadora Automática:
Operadora por Horario: Configure cada empresa con operadoras diurnas, nocturnas y para días festivos con menús y comportamientos diferentes.
Enrutamiento de llamadas: Permita a los usuarios contactar a una extensión o departamento de su empresa, así como brindarle opciones de dejar un mensaje, llamar a otra extensión o ser transferido a una operadora.
Call Screening: Solicite al llamante su nombre y compañía y permita al usuario contestarle, transferirlo a la operadora o a su buzón de voz.
Llamadas Perdidas (Missed Call Alert): Conozca quién llamó cuando no pudo contestar la llamada, CTMail® notifica cada llamada perdida en el buzón de voz mediante un correo electrónico.
Call Online Response - Respuesta a llamadas en línea: Envíe mensajes de texto convertidos en voz a quien lo está llamando en momentos que no pueda atenderlo. Por ejemplo: "los asesores se encuentran ocupados en estos momentos, en cuanto se desocupen le devolveremos la llamada".
CTMail® Lite Vox Sistema de Audio Respuesta: Incorpore su sistema de telefonía a otras fuentes de información.
El Módulo de Audio Respuesta (IVR por sus siglas en inglés). Lite VOX Incorpora funciones para acceso a Bases de Datos mediante OLE DB y ODBC.

Modelo de seguridad ctmail y ctlog logeo

Módulo de Administración - CTLog® Configurator: Asigne niveles de autorización y acceso a cada uno de los usuarios del sistema.

Cumplimiento de 4.7.3. CTLog y CTLog Plus

Para el cumplimiento de los numerales 4.7.3., Calltech S.A. cuenta con un servicio de soporte y mantenimiento preventivo con atención presencial en la Sede del cliente, este permitirá que no se utilice información de sus clientes por terceros pues el soporte se realizará directamente en su empresa y bajo su supervisión, ni tampoco el uso de dispositivos de almacenamiento no autorizados por la entidad y tampoco se utilizará otro tipo de conexión a red distinta a la usada para la prestación del servicio.

[8] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 101

Consulte más información sobre Tech Support y el modelo de soporte Calltech S.A. Aquí

Cumplimiento de 4.7.5. CTLog Plus, grabación de pantallas, chat y si se requiere redes sociales

*"**7. Análisis de Vulnerabilidades***
Las entidades deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos:
***7.1.** Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.*
***7.2.** Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC."*[9]

[9] CAPITULO DECIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN A TRAVÉS DE MEDIOS Y CANALES DE DISTRIBUCIÓN DE PRODUCTOS Y SERVICIOS, Página 103