
Departamento de Informática

PROYECTO FIN DE CARRERA

# AUDITORÍA Y CONTROL DE UNA PLATAFORMA DE CONTACT CENTER

Autor: Alberto Madera Chamorro

Tutor: Miguel Ángel Ramos González

Leganés, octubre de 2015

Título: Auditoría y Control de una Plataforma de Contact Center
Autor: Alberto Madera Chamorro
Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

# Agradecimientos

Agradezco a Miguel Ángel Ramos, mi coordinador, por la paciencia que ha tenido para desarrollar este proyecto.

A todos los profesores que durante la carrera me han enseñado los conocimientos y aquellos que siempre han dado pie a que continuaramos un paso más con los conceptos que adquirimos.

A todas las personas que me he encontrado en mi aventura profesional que de una forma u otra estimulaban el día a día.

Y por último a todas y cada una de esas personas que me recordaron una y otra vez que acabara la carrera. Sois tantas que sería difícil agradecéroslo una a una.

# Índice general

# 1. Introducción y objetivos

## 1.1 Introducción

La experiencia laboral que he acumulado a lo largo de estos años siempre ha estado ligada a los llamados “Contact Center” y gracias a la cual he aprendido a trabajar y entender como se realizaba un trabajo diario en este tipo de servicios. Seguramente por intentar comprender mejor mi entorno de trabajo, decidí profundizar mis conocimientos realizando este Proyecto Fin de Carrera.

La primera fase del proyecto fue establecer un marco en el que aplicar las buenas prácticas en el que se eligió una plataforma de Contact Center. Seguidamente se consideraron una serie de normas y estándares a través de los cuales se desarrollará y finalmente se trasladó todo a una propuesta para que se diese la aprobación.

## 1.2 Objetivos

El objetivo fundamental del proyecto es el de identificar los pasos a dar y puntos de control a establecer para estandarizar la revisión de este tipo de entornos realacionados con los Contact Center, tanto de los procesos humanos como de la tecnología asociada a la prestación de este tipo de servicios. En base a ese objetivo principal, se proponen los siguientes objetivos parciales:

El objetivo es reunir una serie de buenas prácticas para la gestión de una plataforma de Contact Center a través de varios estándares, normas, modelos o marcos descritos a lo largo del mismo.

- Desarrollar un prototipo para automatizar la recogida y tratamiento de la información en forma de tres cuestionarios que arrojarán una serie de resultados.
- Dar a conocer una serie de buenas prácticas a nivel de calidad, eficiencia, seguridad y legislación, para que puedan ser usadas en toda plataforma de Contact Center para la mejora de los procesos realizados diariamente.

- El objetivo marcado en este proyecto es el de intentar reunir una serie de buenas prácticas para un Contact Center. Se identificarán los Procesos, Objetivos, Métricas e Indicadores de este tipo de entidades a partir de normas de acreditación del sector, en este caso nos basaremos en COPC 2000, ya que suele ser una certificación muy común en este tipo de entidades, para la calidad y el servicio a través de sus métricas o KPIs más comunes que puedan existir para este tipo de centros, para los procesos que se desarrollen en ellos.

# 1.3 Fases del desarrollo

La primera fase del proyecto fue documentarse teóricamente sobre todo lo relacionado con los Contact Center para plasmar una visión genérica e inicial. A continuación, por parte de los coordinadores se recomendó una serie de lecturas de varios estándares, normas y metodologías que se usaban en la vida real con este tipo de entornos. Una vez que ya se tenía una base de conceptos se estableció un índice preliminar y el objetivo central del proyecto. La siguiente fase fue la de desarrollo, en ella se realizó una batería de preguntas por cada uno de los tres puntos a tratar en el Proyecto (Seguridad, Calidad y Legislación), se buscó una aplicación o plataforma para tratar de agruparlos, llegando a la conclusión que los cuestionarios gratuitos que ofrece Google serían la opción más recomendable. Una vez realizado, se pasó a completar la memoria, la cual tras unas pequeñas variaciones de estilo quedó finalmente conformada.

# 1.4 Medios empleados

Para la realización de este Proyecto Fin de Carrera han sido utilizados los ordenadores de la Universidad Carlos III de Madrid de sus aulas informáticas así como un ordenador personal para las horas fuera de la universidad.

# 1.5 Estructura de la memoria

La estructura se divide en 12 apartados que se explicarán brevemente a continuación:

- **Introducción y objetivo:** Este primer capítulo trata de explicar el propósito por el cual se eligió este tema para desarrollar un Proyecto Fin de Carrera y el objetivo que se quiere conseguir una vez realizado. Además incluye un breve comentario de las fases seguidas para su elaboración y los medios empleados para la misma.

- **¿Qué es un Contact Center?:** En esta parte se desgrana lo que es en detalle un Contact Center desde su definición hasta los tipos que puede haber pasando por los elementos que lo componen.

- **Seguridad en un Contact Center:** Apoyados en los estándares ISO 27001 e ISO 27002, se busca dar una visión de como tiene que ser la seguridad en estos entornos a nivel tanto físico, lógico o legislativo.

- **Calidad en un Contact Center:** Aquí entran en escena varias normas, estándares o metodologías como COPC PSIC, ISO 9001, Cobit, ITIL, CMMI y el Círculo de Deming, que son usadas o se usan en enornos reales de Contact Center para su cumplimiento o certificación. En este caso se usan como ejemplos o modelos de referencia para mostrar pautas de buena calidad relacionadas con un Contact Center.

- **Legislación en un Contact Center:** No podemos dejar de lado los problemas que se pueden derivar de un servicio realizado en una plataforma de Contact Center, por lo que se tiene que cumplir con la legislación, en este caso, española y europea. Para ello se explica la Ley Orgánica de Protección de Datos (LOPD), el Marco Europeo en materia de Protección de Datos, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) y por último la Ley de defensa de consumidores, donde se detalla los deberes y obligaciones de todas las partes que puedan estar involucradas en este tipo de entornos.

- **Auditoría y Control de una plataforma de Contact Center:** En este apartado se encuentra la parte central de la realización del proyecto. En ella se exponen los objetivos y problemas que pueden acontecer a este tipo de entornos. Se listan las métricas que se deben utilizar para medir este tipo de entornos y se muestran tres cuestionarios con preguntas para su realización para posteriormente explicar sus resultados que hemos querido sacar en claro. Un último punto da una visión global de la Auditoría Informática.

- **Conclusiones:** Se realizará una síntesis de lo que puede aportar el trabajo realizado.

- **Posibles proyectos o líneas de investigación:** En este punto se propondrán varias alternativas para continuar la línea iniciada por este Proyecto y que no se hayan podido realizar.

- **Memoria económica:** Aquí se detallará la planificación de las tareas seguidas a lo largo del desarrollo del proyecto, plasmado en un diagrama de Gantt, así como el presupuesto del mismo con el coste total en euros que ha costado llevarlo a cabo.

- **Glosario:** Todos los términos o definiciones que no se hayan explicado a lo largo de la memoria estarán en este apartado.

- **Referencias:** Toda la bibliografía o webgrafía que se haya utilizado para documentarse será listada en este punto.

- **Anexos:** Aquí se encontrarán reproducidos parte del estándar ISO 27002 y COPC 2000.

# 2. ¿Qué es un Contact Center?

## 2.1 Definición

**Imagen de una plataforma de Contact Center. Fuente: http://tribunacontactcenter.com/**

Los Contact Centers o Centros de Contacto en castellano (en adelante CC) se pueden definir como un conjunto de recursos que permiten la prestación de servicios a través de cualquier canal de comunicación como por ejemplo teléfono, correo electrónico, fax, correo postal, chat, etc… A un lado del canal estará un agente que pertenecerá a una entidad que brinda un servicio y en el otro el usuario final, que puede tener relación con el servicio por el cual se realiza la transacción o no. Cuando se habla de cliente se suele estar referenciando a un representante del servicio.

Nacieron históricamente como Call Centers o Centros de Llamadas, ya que su tarea principal era la de atender las llamadas que se recibían o se emitían, pero a lo largo de los años han ido evolucionando, en gran parte por las nuevas tecnologías, hasta convertirse

en algo más que un centro donde la parte principal era la llamada, pasando ahora a denominarse transacción o interacción.

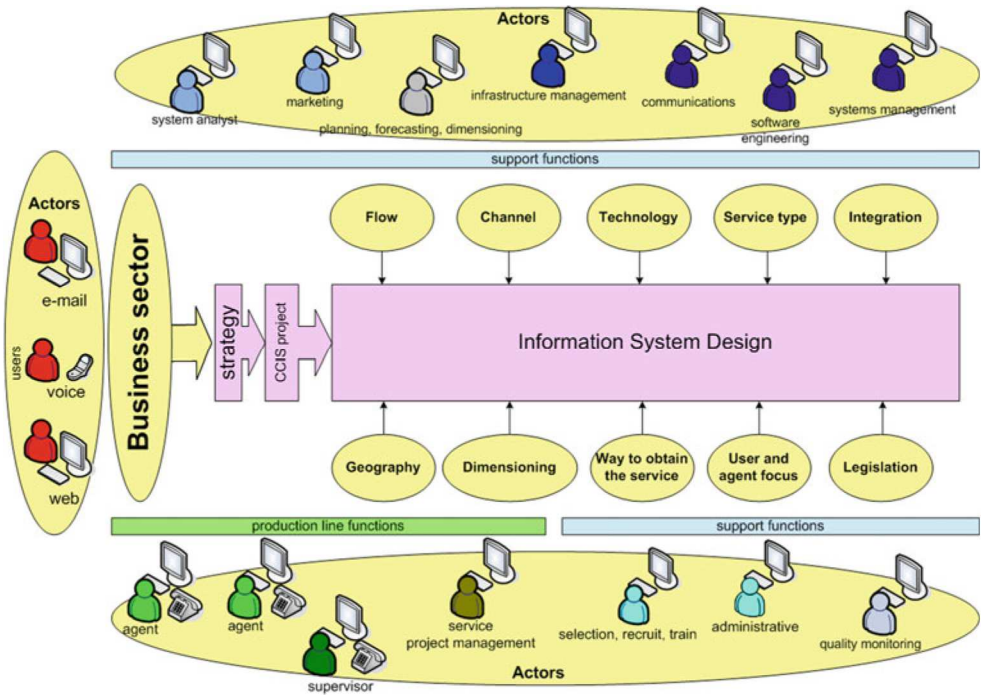
El objetivo primordial de todo Contact Center se basa en un equilibrio entre todas las partes que lo sustentan para garantizar su continuidad y supervivencia como entidad, basada en una mezcla entre la eficiencia del servicio, el beneficio económico y la satisfacción tanto del cliente como del usuario final. Dichos objetivos se pueden llevar a cabo mediante acciones como la resolución en primer contacto de transacciones, la evaluación del servicio mediante métricas, el dotar al personal de una carga de trabajo óptima, sin llegar a sobrecargarlo, o con el cumpliendo con la legislación aplicada para evitar denuncias o multas posteriores.

Sin embargo el resultado no siempre es el esperado y en múltiples ocasiones el usuario final no recibe la atención esperada, que va desde tiempos de espera eternos, múltiples contactos hasta la resolución del problema o transacciones no resueltas adecuadamente por parte de unos agentes que son conscientes de una inestabilidad laboral casi diaria.

El control y la auditoría del servicio se han convertido en dos aspectos claves para el negocio. Las estadísticas en tiempo real y el seguimiento diario es una práctica habitual en la mayoría de las entidades que a través de métricas pueden calcular desde el volumen de transacciones que puede tener un servicio, hasta el rendimiento de un agente en su jornada laboral.

Los profesores Rui Rijo, João Varajão, Ramiro Gonçalves realizaron un estudio en el que concluían que en un CC se pueden identificar varios factores: flujo, canales, tecnología, servicio tipo, la integración, la geografía, el dimensionamiento, manera de obtener el enfoque de servicio, el usuario y el agente, la legislación, dominio del negocio y actores relevantes. En el siguiente punto se reproducirá parcialmente su trabajo con algunas aportaciones adicionales que quedaron fuera del mismo.

## 2.2 Factores de un Contact Center




**Grafíco de los factores. Fuente: Contact center: information systems design**

## 2.2.1 Flujo

Debe existir con el fin de proporcionar el mejor servicio para los usuarios, pueden clasificarse en entrada, salida y mixtos. Se utilizan los términos de entrada y salida para considerar el flujo, pero lo que realmente importa es la interacción completa entre el usuario y la organización. En los entornos de entrada de transacciones, el agente, por lo general, debe tener más experiencia y contar con herramientas que le permitan tener más información porque puede que no sepa de antemano el motivo real de la interacción. En los flujos de salida, la especialización de un agente será clave a la hora de brindar un servicio correcto, ya que su conocimiento y manejo serán clave.

## 2.2.2 Canal

**Canales que pueden usarse. Fuente: http://www.contivio.com/**

Pueden clasificarse como autoservicio (self-service) o asistido. Canales asistidos, tales como el teléfono, el fax, el correo electrónico y el chat, requieren de agentes para procesar la interacción. Canales de autoservicio como IVR, Web y otros, no necesitan la intervención del agente. Se necesita un canal apropiado para las transacciones analizando si estas pueden ser automáticas o no para ajustarlas mejor a los objetivos, haciendo la elección con cuidado. Las llamadas telefónicas siguen siendo la mayoría de las interacciones, seguidas por el correo electrónico pero el chat, por ejemplo, es un canal en auge. Se debe considerar el servicio que se proporcione en el perfil de los clientes y la comercialización de imagen que la organización quiere. Si la interacción se realiza en una transacción, podemos usar los canales automáticos como el autoservicio. Estos canales suelen ser más baratos, sin embargo, debemos garantizar que el usuario es capaz de utilizarlos o de otra manera, podemos perder al cliente.

## 2.2.3 Tecnología

Debemos adecuar la arquitectura de la tecnología. La tecnología más utilizada en la gestión de la interacción suele ser el IVR, el ACD, el chat, el SMS y el correo electrónico. Las herramientas de monitoreo de la calidad permiten controlar y realizar ajustes en las operaciones. El uso de herramientas de inteligencia empresarial, CRM y operaciones de negocio de apoyo ayuda a la previsión de la estimación del volumen, del personal o del número de agentes necesarios para cubrir correctamente un servicio a través de una buena planificación. Las herramientas de informes se utilizan para dar retroalimentación a la alta dirección sobre la productividad y el logro de los objetivos de negocio. La arquitectura de la red es centralizada por medio de líneas dedicadas.

A continuación se explican varias de las herramientas de las que disponen los CC en su día a día.

### 2.2.3.1 ANI (Automatic Number Identification)

Identifica el número desde el cual se inicia la comunicación telefónica por parte del usuario final. Puede servir para reconocer a la persona llamante.


**Gráfico en el que interviene el ANI. Fuente: http://blogs.icemd.com/**

## 2.2.3.2 DNIS (Dialed Number Identification Service)

Identifica el número desde el cual se inicia la comunicación telefónica por parte del usuario final, que junto a otros sistemas como el IVR, puede ser gestionado de forma diferente dependiendo del número que se trate.

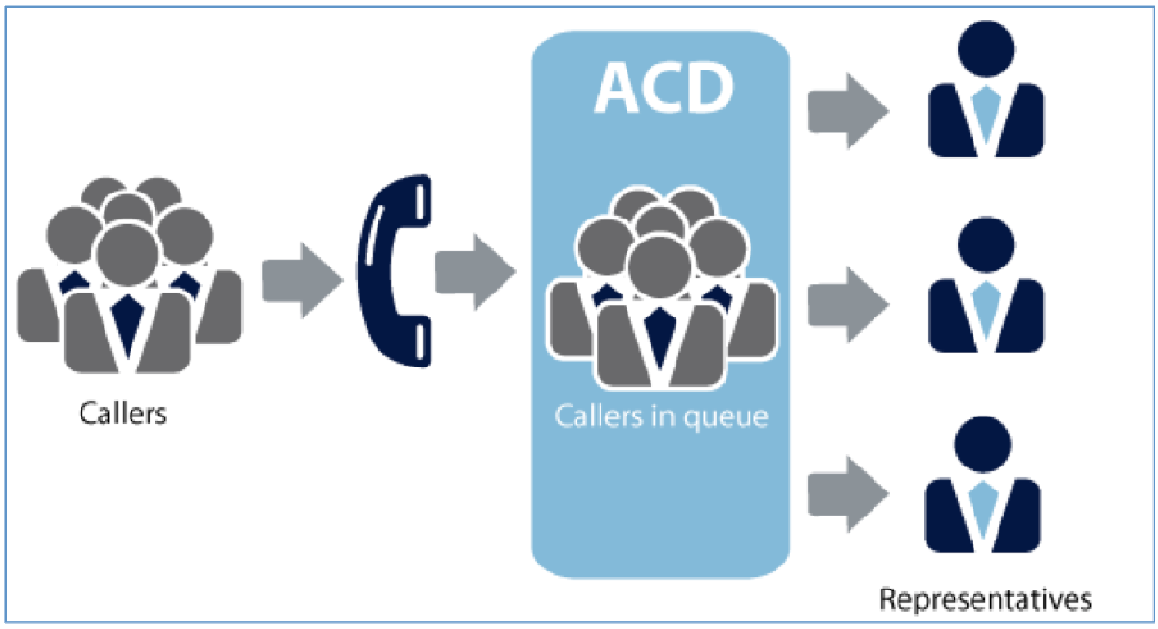
La diferencia con el ANI, es la localización en el esquema. Si tenemos en cuenta la imagen anterior, el DNIS, estaría situado después del ACD.

## 2.2.3.3 DNR (Dynamic Network Routing)

A través de diversos algoritmos, las llamadas son enrutadas dinámicamente con el fin de que éstas vayan a través de los caminos más cortos a la hora de transmitirse desde el usuario final hasta el destinatario.

## 2.2.3.4 ACD (Automatic Call Distribution)

Recibe, encola, rutea y asigna las llamadas entrantes que se puedan recibir telefónicamente hacia los diferentes agentes que puedan estar disponibles en ese momento.




**Esquema del ACD en una llamada. Fuente: blog.talkdesk.com/what-is-an-acd**

## 2.2.3.5 CTI (Computer/Telephone Integration)

Se corresponde a la integración de teléfono y equipo informático como un mismo sistema. El ordenador usa los datos provenientes de la llamada para obtener información o datos relevantes de la misma. Su propósito es el de aumentar la productividad del agente evitando requerir cualquier tipo de dato al usuario final del cual ya se disponga.

## 2.2.3.6 Dialer (Marcador)

Programa y marca llamadas telefónicas salientes para conectar a los agentes o un sistema de locución con un usuario final.

## 2.2.3.7 Marcación predictiva

Posee una lista de números, los cuales va marcando secuencialmente hasta que se sobrepasa un número máximo de intentos o se conecta con el usuario final satisfactoriamente. Inmediatamente después el éxito en la conexión se pasa la comunicación al agente para su gestión. Se ha regulado el uso de estos marcadores para evitar molestias a los usuarios finales.

## 2.2.3.8 Marcación primaria

También conocida como marcación previa, en ella el agente conoce información previa de antemano y debe de marcar manualmente o pulsar algún botón antes de que se inicie la llamada.

## 2.2.3.9 IVR (Interactive Voice Response)

Son una serie de autómatas informáticos especializados que permiten a los usuarios un servicio automático, mientras tratan de comunicar sus necesidades. Los usuarios que interactúan con el IVR utilizan el teclado del teléfono o, con la tecnología de reconocimiento de voz, comandos de voz para proporcionar información. En respuesta, el IVR utiliza voz sintetizada para reporta información. También pueden ser utilizados para enrutar las llamadas, el llamado enrutamiento basado en habilidades.

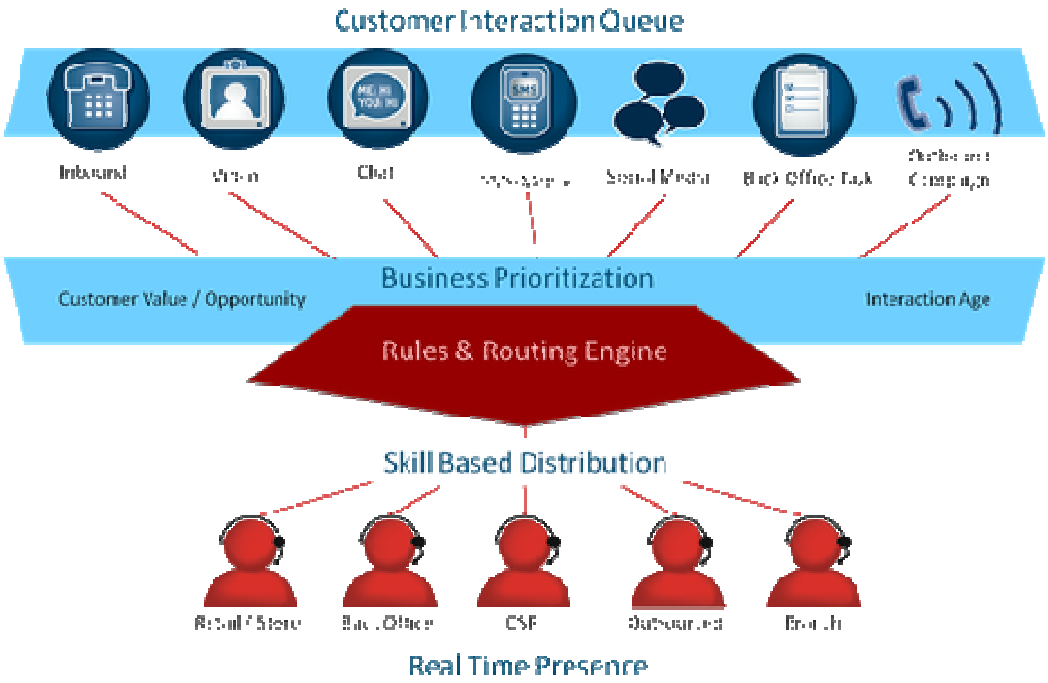

**Como funciona un IVR. Fuente: http://www.voip-sip-sdk.com/**

## 2.2.3.10 Enrutamiento basado en habilidades

Basado en un algoritmo, enruta la transacción hacia un agente que posea una mayor habilidad a la hora de gestionarla eficazmente.

## 2.2.3.11 Cola universal

Funciona como un embudo para todos los canales de comunicación (teléfono, correo electrónico, redes sociales…) y aplicando después las reglas de negocio como el ruteo, el encolado o la recolección de datos, con el fin de guiar la transacción al puesto justo para su correcta gestión.




**Esquema de la cola universal. Fuente: http://cdn.business2community.com/**

## 2.2.3.12 Colas FIFO

First In, First Out (Primero en Llegar, Primero en Salir). Las transacciones se gestionan tal y como llegan asignándose al agente con mayor disponibilidad, es decir, el cual lleve más tiempo lleve sin gestionar una transacción.

## 2.2.3.13 Tecnología de reconocimiento de voz

Normalmente va ligada al IVR, el cual que a través del reconocimiento de la voz humana, guía al usuario hacia un agente o aplicación específica para sus necesidades como alternativa al sistema de marcado de tonos.

## 2.2.3.14 Cola de prioridades

Se trata de un servicio que afecta a los agentes para la asignación de una transacción, entre las colas de llamadas y entre transacciones para una misma cola.

## 2.2.3.15 Gestión de la red

Es un software que distribuye las llamadas entre la plataforma basado en las reglas de enrutamiento establecidas por la organización. Suele utilizarse junto al CTI para incrementar la eficiciencia de este sistema en entornos multi sitio.

## 2.2.3.16 Servicio electrónico

Estos servicios se pueden encontrar accesibles tanto para los usuarios finales como para los agentes con el fin de contactar, solucionar o ayudar según se requiera en la gestión solicitada.

- Sistema de Gestión de Respuesta de Correo Electrónico (ERMS).
- Preguntas Frecuentemente Contestadas (FAQ).
- Web self-service o de ayudas.
- Chat.
- Colaboración (completar un formularios común).
- Cola Universal.
- Software de Gestión de campañas de Correo Electrónico salientes (CMS) (emiten correos electrónicos y permiten su recepción y procesamiento de respuestas).
- Software de Representante virtual o Bot.
- Gestor del conocimiento.
- Aplicaciones software.
- Intranet.
- Asistentes virtuales.
- Acceso a videollamada (Skype).

## 2.2.3.17 Sistema de reportes

Se pueden realizar a nivel de Agente, Cola o IVR por ejemplo. Normalmente se realizan en tiempo real para poder actuar en el caso de que los niveles estimados no sean los estimados.

## 2.2.3.18 Grabación

Aplicaciones que registran toda la interacción producida entre las dos partes ya sea en formato audio si se ha realizado telefónicamente o video y audio si se ha realizado por ejemplo tras conectarse remotamente con el usuario final. Se recomienda grabar el 100% de las transacciones y mantener una copia de las mismas.

## 2.2.3.19 Gestión de la calidad

Son una serie de aplicaciones que fueron introducidas en los Contact Center con el fin de mejorar la calidad del servicio como medir el grado en el que se adhieren los

agentes a las políticas del departamento y los procedimientos. Busca mejorar las métricas relacionadas con el servicio brindado.

### 2.2.3.20 WFM (Workforce Management)

Está relacionado con la gestión de los RR.HH. (mano de obra). Busca mejorar la productividad de los agentes y reducir la tasa de abandono de los mismos, junto con la satisfacción del usuario final y el cliente, entre otras finalidades. Puede usar herramientas como E-Learning, E-Coaching, Sondeos/Encuestas, Gestor de rendimiento o Análisis de voz, para detectar, corregir o mejorar los niveles de cada agente.

En base a los resultados se realizará una retroalimentación con el fin de corregir aquellos aspectos donde el agente no esté dentro de los niveles establecidos, con el objetivo de mejorarlos, adaptando la tecnología adecuada para ello.

Se puede realizar la formación de los agentes a nivel proactivo como planes estratégicos de la organización o reactivo con el fin de mejorar la consecución de los objetivos.

### 2.2.3.21 Pronóstico y Planificación

Se realizan con visión de futuro para la gestión del personal con vistas a la planificación venidera. Para ello también se pueden basar en la gestión de recursos en tiempo real que dictaminará si la planificación es adecuada o no, necesitando un apoyo o liberando a personal al no ser necesario para cumplir con lo pronosticado y planificado en su momento. Su objetivo es el garantizar el cumplimiento de las operativas, evitar cuellos de botella y establecer el tiempo estimado de cada tarea.

### 2.2.3.22 Coaching

A través de la monitorización de los agentes se puede establecer este método de formación de los agentes para aquellos que no alcancen los niveles esperados.

## 2.2.4 Servicios tipo

Se deben identificar inequívocamente los servicios que se van a proporcionar a los usuarios finales y si estos pueden ser facilitados internamente o se podrían subcontratar. El servicio de atención al cliente, sobre todo refiriéndose a la información acerca de la facturación y aprovisionamiento, es uno de los más importantes tipos de servicios de entrada. En las interacciones salientes, el cobro de deudas, llamadas de bienvenida (usuarios nuevos), la reducción del pérdida de clientes (churn), las ventas salientes, es decir, llamadas en frio, venta cruzada (cross selling) y oportunidad de venta (up-selling) y consultas (para la satisfacción del cliente, estudios de mercado y encuestas) son las

principales categorías. Cada caso es único, sin embargo, hay un paquete de servicios, donde la mayoría de las situaciones entran en él. Varios tipos de servicios son similares independientemente del área. El soporte técnico puede ser interno a los usuarios de una organización (help-desk) o externo a otras organizaciones o usuarios finales. Se deben buscar las mejores prácticas para cada tipo de servicio.

## 2.2.5 Dominio de negocio

La principal clave para decidir la creación de un centro de contacto es el número de clientes o usuarios finales. Las organizaciones con un gran número de usuarios finales se organizan horizontalmente, es decir, hay personas concretas (agentes) para interactuar con ellos. Los centros de contacto tienden a buscar la especialización de sus agentes, sin embargo en muchos casos buscan en ellos que sean multidisciplinares.

## 2.2.6 Integración

El objetivo de la integración es poner la información a disposición de los agentes y otros actores. La necesidad de los servicios de obtener/dar/generar información/acciones desde/hacia/en los sistemas existentes. Se debe escoger la mejor estrategia de integración para evaluar la complejidad de ésta. La mayoría de las veces los CC no empiezan de cero. La evaluación de la complejidad de la integración debe tener en cuenta, entre otras cosas: el número, la diversidad y el nivel de integración de los sistemas existentes; detalles tecnológicos de cada sistema (sistemas propios, estándar, código abierto, otros); el rendimiento de los sistemas; complejidad de la interfaz; decisión sobre la integración síncrona o asíncrona; número de transacciones de mantenimiento. En la mayoría de los casos servicios de entrada requieren un alto nivel de integración.

## 2.2.7 Geografía

Hoy en día la cuestión de la geografía no es un problema, desde el punto de vista de los sistemas de información. Las cuestiones geográficas están relacionadas con la madurez del mercado regional, la legislación y las formas culturales de interactuar y pensar. Cuando se instala algún centro fuera del país de origen del servicio (outshoring), normalmente basándose en la reducción de los costes, se debe tener en cuenta la capacitación de los agentes para hablar y pensar como una persona del mismo país para el cual se realiza el servicio.

Muchas entidades españolas han decidido externalizar parte de sus servicios en América Latina ya que el uso del castellano en la mayoría de sus países como Argentina, Colombia o Chile, sumado a la diferencia salarial que pueda haber con los empleados o la

menor tasa de rotación en la plantilla hacen que a la entidad pueda retribuirle un mayor beneficio.

## 2.2.8 Dimensionamiento

Se necesita saber un número aproximado de agentes y supervisores y deberán ser organizados para gestionar el servicio, esto se realiza a través de la previsión, la dotación de personal y la programación. Para el dimensionamiento de salida se requiere la definición de la meta volumen, la previsión de la duración media de la interacción y una meta para el porcentaje de contactos con éxito. Este objetivo es parámetro muy importante para establecer el número de agentes. Cuanto más alto el porcentaje de éxito requerido, mayor es el número de horas de operación requeridas. El dimensionamiento de entrada es más difícil de hacer y se necesitan datos históricos para predecir las necesidades, requiriendo la estimación de volumen esperado (número de las interacciones esperadas), duraciones esperadas de interacción, distribución esperada por día/mes/año, y el nivel de servicio destino.

## 2.2.9 Manera de obtener el servicio

Una organización tiene cuatro formas principales para la creación de un Contact Center: totalmente propia; primera línea externalizada, segunda línea propia; primera línea externalizada, la segunda línea subcontratada internalizada (la organización es propietaria de los sistemas y la infraestructura, pero la mano de obra viene de un tercero) y por último totalmente subcontratado. La curva de aprendizaje de la actividad de los centros de contacto es largo, de esta manera la decisión entre una operación en la empresa o externalizar es muy importante.

## 2.2.10 Actores relevantes

El personal humano se puede agrupar en Agentes, Coordinadores, Supervisores, Gerentes, personal de RRHH, personal de IT, personal de Seguridad, etc… Los agentes operan en la primera línea. Los supervisores tienen un gran impacto en la productividad del agente. Las organizaciones deben contar con un equipo para reclutar, contratar, capacitar y evaluar a los agentes y los supervisores. Se debe manejar la infraestructura y los sistemas de información para una mejor planificación, previsión, dimensionamiento y control de la calidad. En el caso de que los procesos y procedimientos no funcionen correctamente deben ser reorganizados.

Por ello a los agentes se les estimularán a la hora de desempeñar su trabajo bien sea con conocimientos u objetivos como los siguientes:

- Habilidades: orientación al servicio, capacidad de comunicación, empatía, excelencia, escucha activa.

- Competencias: procedimientos, dominio de herramientas, conocimiento del producto.

- Motivación: Rankings internos, Comisiones, Pluses, Incentivos, Premios.

- Formación cultural (Offshore).

### 2.2.11 Enfoque de usuario y agente

La creación de un Contact Center se basa en la creación de una fortaleza entre usuario final y entidad del servicio. En ella, el agente es la cara de la organización para el usuario final. La relación agente-usuario final es lo que hace la diferencia entre el éxito y el fracaso. Los sistemas deben ser compatibles con la relación entre los agentes y los usuarios. Al final, los agentes toman decisiones en base a una forma de hacer las cosas, según los procedimientos establecidos.

### 2.2.12 Legislación

La legislación varía dependiendo del país. En España, por ejemplo, los CC se atienen a varias leyes como la LOPD, LSSI, LGT u otros códigos deontológicos como el de Telemarketing o las conocidas como Listas Robinson.

## 2.3 Tipos de Contact Centers

Podemos realizar una distinción de los Contact Center de muchas maneras, eligiendo entre ellas varias de las más representativas en el mundo empresarial en el que están establecidos.

### 2.3.1 Según su estructura

#### 2.3.1.1 Internos

La organización del usuario final asume la responsabilidad de la adquisición de los bienes, la tecnología, las telecomunicaciones y los recursos de personal. Sin embargo, incluso en este modelo, los consultores pueden ser utilizados para asistirlo con varias implementaciones y todos o parte de la tecnología se pueden hospedar en el exterior.

### 2.3.1.2 Externos

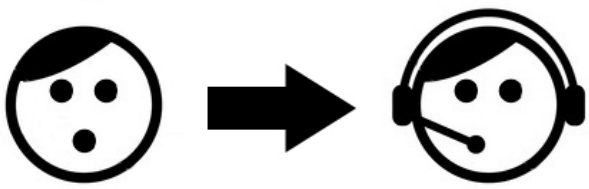
Algunas o todas las infraestructuras del CC, la tecnología o el personal se subcontrata a una tercera parte. La externalización tiene muchos modelos y puede hacer frente a toda la operación, o simplemente a la tecnología, el personal, o una combinación de ambos. En algunas situaciones, las empresas eligen utilizar su propia infraestructura de la tecnología, pero el personal de la empresa es externalizado, o, en el caso contrario, pueden utilizar la infraestructura de la empresa de externalización y su propio personal. En otras situaciones, la externalización será funcionar como un centro de copias de seguridad y recibe llamadas y correos electrónicos sólo cuando el sitio principal de la empresa supera un umbral de volumen predefinido. Otro escenario que tendrá la externalización será realizar sólo una o dos funciones de una empresa.

### 2.3.1.3 Compradores de Servicios a Terceros

Algunas o todas las aplicaciones se alquilan a un vendedor que generalmente maneja todos los aspectos de la aplicación. Pueden darse varios casos para todas las otras opciones para la construcción del CC, por lo que la gestión exacta de esta disposición varía. En algunas situaciones, la aplicación se encuentra alojada y gestionada desde el sitio de la empresa de alojamiento, y en otros, el servidor puede ser colocado en el sitio de la empresa principal, pero todavía es administrada y operada por la empresa de alojamiento. La diferencia clave entre el alojamiento y la externalización es que en el modelo ASP, la empresa de alojamiento posee y gestiona la aplicación.

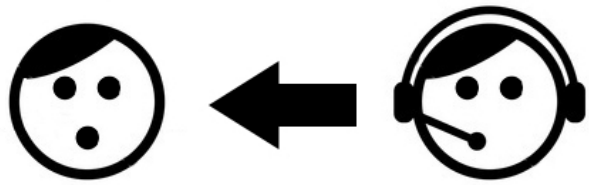
## 2.3.2 Según el flujo

### 2.3.2.1 Recepción (Inbound)



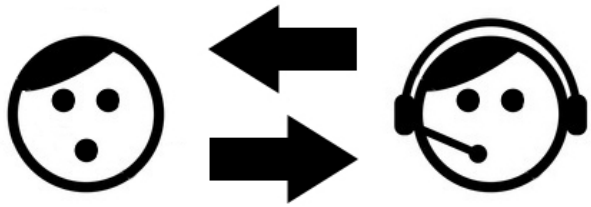
Las interacciones recepcionadas se inician por fuera del CC, siendo los usuarios los que solicitan algún servicio al centro.

### 2.3.2.2 Emisión (Outbound)



Las interacciones emitidas son las que inician desde dentro de un centro.

### 2.3.2.3 Recepción y Emisión (Inbound & Outbound)



La interacción con el Contact Center puede recibirse y enviarse de igual manera no ajustadas a un solo flujo.

## 2.3.3 Según el contacto

### 2.3.3.1 Front Office

Es el grupo de agentes/departamento que atiende al usuario final cuando éste inicia una transacción con el Contac Center. Puede haber varios niveles según su grado de conocimiento, permisos, etc…

### 2.3.3.2 Back Office

Es el grupo de agentes/departamento que gestiona la resolución de las transacciones del usuario final cuando no ha podido solucionarse en el primer contacto. Pueden o no contactar con el cliente.

### 2.3.3.3 Self Service (Autogestión)

No se genera contacto con ninguna persona física, sino que a través de una tecnología implementada por la entidad, el usuario final puede resolver la transacción por la cual hubiese contactado.

## 2.3.4 Según el tipo de negocio

La norma COPC PSIC, de la cual hablaremos más en profundidad más adelante en este documento, establece la siguiente clasificación.

### 2.3.4.1 Operaciones de Contacto con el Cliente Entrantes y Salientes

A estas operaciones se las conoce usualmente por “Call Centers”, sin embargo, la mayoría de estas operaciones de contacto con clientes interactúan con los usuarios finales vía teléfono, medios electrónicos (por ejemplo: correo electrónico, Internet, mensajes de texto), o los tradicionales correo o fax. Los servicios ofrecidos generalmente incluyen Atención al Cliente, Soporte Técnico, Reservas, Servicios de Operador, Ventas y otros.

### 2.3.4.2 Operaciones de Tercerización de Procesos de Negocios (BPO)

Estas operaciones se componen de una variedad de funciones de servicio incluyendo el alta y la activación de nuevas cuentas, gestión de registros, procesamiento de reclamaciones, reembolsos/canjes y otras funciones similares.

### 2.3.4.3 Centros de Procesamiento de Transacciones

Estas operaciones típicamente procesan transacciones no electrónicas como cartas y Fax.

### 2.3.4.4 Centros de Distribución

Estas operaciones realizan actividades de almacenamiento, montajes ligeros, y actividades de selección, empaquetado y envío. Usualmente esto se realiza como resultado de transacciones provenientes de una o más operaciones de contacto con clientes.

### 2.3.4.5 Procesamiento de Remesas

Estas operaciones procesan pagos del usuario final (por ejemplo: pagos hechos con tarjeta de crédito).

### 2.3.4.6 Operaciones de Servicio de Campo

Estas incluyen operaciones de envío de técnicos de servicio a usuarios finales para reparar o reemplazar productos cubiertos por garantía, contratos de servicio, o sobre una base de tiempo y materiales.

### 2.3.4.7 Procesamiento de Devoluciones

Estas operaciones reciben y procesan materiales devueltos (computadoras, productos electrónicos, indumentaria, etc.).

### 2.3.4.8 Servicios de Cobranzas/Recuperación

Estas operaciones contactan con usuarios finales comerciales y/o consumidores, para recuperar fondos adeudados.

### 2.3.4.9 Medios sociales

Realizan operaciones de edición, publicación e intercambio de información a través de redes sociales, blogs, microblogs, etc… A favor se tiene la velocidad de respuesta y en contra la privacidad, por ejemplo.

# 3. Seguridad en un Contact Center

## 3.1 ISO/IEC 27001

La información que se puede tener en una plataforma de un Contact Center es vital para el propio negocio, desde faxes o cartas en formato físico como ficheros almacenados en un ordenador o en un servidor. Por lo que se necesitará implementar una serie de controles y dotar de una seguridad a la plataforma para proteger y evitar cualquier tipo de manipulación no permitida, robo o pérdida que impidan o amenacen la continuidad del negocio.

Para tratar el aspecto de la seguridad de este tipo de centros vamos a utilizar como referencia el estándar ISO/IEC 27001 en su versión de 2013. El objetivo se define como una norma Internacional que se ha preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información.

En septiembre de 2014 se publicó la versión 2013 tanto de ISO 27001 como de 27002. Las novedades con respecto a la versión de 2005 son algunos cambios en los literales o los más relevantes como la reducción de los controles, que pasan de 133 a 114 y el aumento de las cláusulas que pasan de 11 a 14, siendo estas las siguientes:

- **Información de las políticas de seguridad** (1)

  Se mantiene, solo cambiando los nombres de los literales.

- **Organización de la seguridad de la información** (2)

  La información de seguridad de roles y responsabilidades se fusiona con la unión de dos, a) Asignación de responsabilidades de seguridad de la información y b) Roles y responsabilidades, de Gestión de activos.

  La Segregación de deberes también se incorpora a esta sección procedente de la Gestión de Comunicaciones y Operaciones.

  Se eliminan la sección de los Grupos o personas externas por Dispositivos móviles y teletrabajo, que estaban en Control de acceso.

- **Seguridad de Recursos Humanos** (3)

Se mantiene, solo cambia el orden en la norma y que afectará a otras secciones de la norma.

- **Gestión de Activos** (3)

  Pasa de 2 a 3, incorporando la Gestión de Medios, que estaba en el apartado de Gestiones de las Comunicaciones y Operaciones.

- **Control de Acceso** (4)

  Pasa de 7 a 4, fusionándose entre ellas y como anteriormente hemos comentado, pasando Dispositivos móviles y teletrabajo a la Organización de la seguridad de la información.

- **Criptografía** (1)

  Se desvincula de Adquisición, Desarrollo y mantenimiento de los sistemas de información para formar su propia sección.

- **Seguridad Física y Ambiental** (2)

  Añade a la sección de Equipamiento, el Equipo de usuario desatendido y la Política de escritorio y pantalla limpios, que se encontraban en la sección de control de acceso.

- **Gestión de Operaciones** (7)

  Pasa de 10 a 7, desligándose del Monitoreo y revisión de los servicios de terceros y la Gestión de cambios de los servicios de terceros, que crean la sección Relaciones con el proveedor.

  Tanto los Controles de red y la Seguridad de los servicios de red, como las Políticas y procedimientos de cambio de información, Acuerdo de cambio y Mensajes electrónicos, y el Comercio electrónico, Información disponible públicamente y Transacciones online, pasan a la Seguridad de las comunicaciones.

  Como hemos comentado anteriormente, el apartado de Gestión de Medios pasa a la Gestión de activos.

  Incorpora los Controles de auditoría de la sección de información que estaba en la sección de Cumplimiento. También se hace lo propio con el Control técnico de vulnerabilidad que estaba en la sección de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

- **Seguridad en las comunicaciones** (2)

Se crea con las secciones provenientes de la Gestión de operaciones indicadas en el apartado anterior junto con los Acuerdos de confidencialidad de la Organización de la seguridad de la información.

- **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información** (3)

  Pasa de 6 a 3, eliminándose el Procesamiento correcto de las aplicaciones.

  La Criptografía forma su propia sección.

  El Control técnico de vulnerabilidad pasa como Gestión técnica de la vulnerabilidad de la sección de Gestión de Operaciones.

  Se crea el Testeo de los datos como una nueva sección.

- **Relaciones con el proveedor** (2)

  Es una nueva sección creada a partir de la incorporación de la Gestión de la entrega de servicios de terceros de la Gestión de Comunicación y del Tratamiento de la seguridad cuando se trata con terceros de la sección de la Organización de la seguridad de la información.

- **Gestión de Incidentes de Seguridad de la Información** (1)

  Pasa de 2 a 1, fusionándose ambas secciones en una llamada Gestión de la seguridad de información de incidencias y mejoras.

- **Seguridad de la Información en aspectos de la Gestión de la Continuidad Comercial** (2)

  Pasa de 1 a 2, simplificándose la Seguridad de la continuidad de la información y añadiendo la sección de Redundancias.

- **Cumplimiento** (2)

  Pasa de 3 a 2, ya que la parte de Controles de auditoría de la sección de información pasa a la Gestión de operaciones. Se crea Revisiones de seguridad de la información a partir de la sección que se encontraba en la otra versión.

## 3.2 ISO/IEC 27002

La norma se divide en 14 dominios, 35 objetivos de control y 114 controles. En este apartado se reproducirá parcialmente la norma internacional y en el anexo del final se enumerarán junto con una breve explicación de cada uno de los 114 controles recomendados.

La entidad deberá identificar unos requerimientos de seguridad que serán evaluados en base a su riesgo. Una vez identificados se deberán formalizar los pertinentes controles para intentar minimizar su impacto en el negocio.

Teniendo en cuenta al estándar ISO 27002, los controles esenciales tanto para un CC como para cualquier negocio, atendiendo al punto de vista legislativo, serían los siguientes:

- Protección de datos y privacidad de la información personal.
- Protección de los registros de la organización.
- Derechos de propiedad intelectual.

En otro aspecto, los controles considerados práctica común para la seguridad de la información incluirían a estos:

- El documento de la política de seguridad de la información.
- La asignación de responsabilidades de la seguridad de la información.
- El conocimiento, educación y entrenamiento en seguridad de la información.
- El procesamiento correcto en las aplicaciones.
- La gestión de la vulnerabilidad técnica.
- La gestión de la continuidad comercial.
- La gestión de los incidentes y mejoras de la seguridad de la información.

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de cualquier organización:

- Políticas, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales.
- Un enfoque y marco para implementar, mantener, monitorear y mejorar la seguridad de la información, que sea consistente con la cultura de la organización.
- Soporte visible y compromiso de todos los niveles de gestión.
- Un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo.
- Marketing efectivo de la seguridad de la información con todos los gerentes, empleados y otras partes para lograr conciencia sobre el tema.

- Distribución de directrices sobre la política y los estándares de seguridad de la información para todos los gerentes, empleados y otras partes involucradas.
- Provisión para el financiamiento de las actividades de gestión de la seguridad de la información.
- Proveer el conocimiento, entrenamiento y educación apropiados.
- Establecer un proceso de gestión de incidentes de seguridad de la información.
- Implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para la mejora.

Para contextualizar la norma, se estructura en seis apartados: Liderazgo, Planificación, Apoyo, Operación, Evaluación de la ejecución y Mejora.

Al final de este texto se encuentra el Anexo 1 con los dominios, categorías y controles establecidos en la norma. Se establecerán los objetivos de control para cada categoría y los controles para que se cumplan de acuerdo a lo descrito en la norma. Las preguntas registradas en el cuestionario que se ha redactado más adelante en este documento buscan abarcar todos los controles descritos en esta norma.

# 3.2.1 Liderazgo

## 3.2.1.1 Liderazgo y compromiso

La alta dirección debe demostrar su liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información a través de:

a) Garantizar la política de seguridad de la información y de los objetivos de seguridad de la información que estén establecidos y sean compatibles con la dirección estratégica de la organización.

b) Garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización.

c) Garantizar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

d) Comunicar la importancia de una gestión eficaz de la seguridad de la información y de adaptarse a los requisitos del sistema de gestión de seguridad de la información.

e) Garantizar que el sistema de gestión de seguridad de la información alcanza su resultado previsto.

f) Dirigir y apoyar a las personas a contribuir a la eficacia del sistema de gestión de seguridad de la información.

g) Promocionar la mejora continua.

h) Apoyar a otras funciones de gestión relevantes para demostrar su liderazgo, ya que se aplica a sus áreas de responsabilidad.

### 3.2.1.2 Política

La creación y difusión de un documento de política de seguridad no tiene otro fin que hacer saber al personal de la organización y proveedores afectados que el uso de los servicios y los activos (hardware, software, red…) que ofrece la misma para su cumplimiento. El desconocimiento del mismo no exonera de responsabilidad al usuario ante cualquier evento que ocurra en materia de la seguridad de la información.

La alta dirección debe establecer una política de seguridad de la información que:

a) Sea apropiada para el propósito de la organización.

b) Incluya los objetivos de seguridad de la información (ver 3.2.2.2) o proporcione el marco para establecer los objetivos de seguridad de la información.

c) Incluya un compromiso para satisfacer los requisitos aplicables en materia de seguridad de la información.

d) Incluya un compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información deberá:

e) Estar disponible como información documentada.

f) Ser comunicada dentro de la organización.

g) Estar a disposición de las partes interesadas, según corresponda.

### 3.2.1.3 Roles de organización, responsabilidades y autoridades

La alta dirección debe asegurarse de que las responsabilidades y autoridades para las funciones relevantes para la seguridad de información son asignadas y comunicadas.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Garantizar que el sistema de gestión de seguridad de la información se ajusta a los requisitos de esta Norma Internacional.

b) Informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

La alta dirección también puede asignar las responsabilidades y autoridades para informar sobre el desempeño de la información del sistema de gestión de la seguridad dentro de la organización.

# 3.2.2 Planificación

## 3.2.2.1 Acciones para abordar los riesgos y oportunidades

### 3.2.2.1.1 Consideraciones generales

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones y los requisitos mencionados en materia de segurida de la información y determinar los riesgos y oportunidades que deben dirigirse a:

a) Asegurar que el sistema de gestión de seguridad de la información puede lograr los resultados previstos.

b) Prevenir o reducir los efectos no deseados.

c) Lograr la mejora continua.

La organización debe planificar:

d) Acciones para hacer frente a estos riesgos y oportunidades.

e) Como: 1- integrar y poner en práctica las acciones en sus procesos del sistema de gestión de seguridad de la información y 2- evaluar la eficacia de estas acciones.

### 3.2.2.1.2 Evaluación de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que:

a) Establezcan y mantengan los criterios de riesgo de seguridad de la información que incluyan: 1) Los criterios de aceptación del riesgo y 2) Los criterios para la realización de las evaluaciones de riesgos de seguridad de la información.

b) Se asegure de que las evaluaciones de riesgos de seguridad de la información, repetidas, producen resultados consistentes, válidos y comparables.

c) Identifique los riesgos de seguridad de la información: 1) Aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información en el ámbito de aplicación del sistema de gestión de seguridad de la información y 2) Identificar a los propietarios de los riesgos.

d) Analice los riesgos de seguridad de la información: 1- Evalúe las posibles consecuencias que resultarían si los riesgos identificados en esta parte llegaran a materializarse; 2- Evalúe la probabilidad realista de la ocurrencia de los riesgos identificados en esta parte y 3- Determine los niveles de riesgo.

e) Evalúe los riesgos de seguridad de la información: 1- Compare los resultados del análisis de riesgos a los criterios de riesgo establecidos en el punto 3.2.2.1.2 a) y 2- Priorice el análisis de riesgos antes que el tratamiento de riesgos.

La organización conservará información documentada sobre el proceso de evaluación de riesgos de seguridad de información.

### 3.2.2.1.3 Tratamiento de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) Seleccionar las opciones de tratamiento de riesgos de seguridad de la información adecuados y teniendo en cuenta los resultados de la evaluación de riesgos.

b) Determinar todos los controles que sean necesarios para poner en práctica la opción de tratamiento de riesgos de seguridad de la información elegida.

Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.

c) Comparar los controles determinados en 3.2.2.1.3 b) con los del Anexo A de esta norma y compruebe que no hay controles necesarios que se han omitido.

El Anexo contiene una lista completa de los objetivos de control y controles. Los usuarios de esta norma se dirigen a Anexo A para asegurarse de que no hay controles necesarios que se pasan por alto.

Los objetivos de control están implícitamente incluidos en los controles seleccionados. Los objetivos de control y controles que se enumeran en el Anexo A no son exhaustivos y puedan ser necesarios como objetivos de control y controles adicionales.

d) Producir una Declaración de Aplicabilidad que contenga los controles necesarios (véase 3.2.2.1.3 b) y c)) y la justificación de las inclusiones, si están aplicando o no, y la justificación de las exclusiones de controles del Anexo A.

e) Formular un plan de tratamiento de riesgos de seguridad de la información.

f) Obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos de seguridad de la información residuales propietarios de los riesgos.

La organización deberá conservar la información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

La evaluación de riesgos de seguridad de información y el proceso de tratamiento en esta norma internacional se alinea con los principios y directrices genéricas previstas en la norma ISO 31000.

### 3.2.2.2 Los objetivos de seguridad de información y la planificación para alcanzarlos

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deberán:

a) Ser coherentes con la política de seguridad de la información.

b) Ser medibles (si es posible).

c) Tener en cuenta los requisitos de seguridad de la información aplicables, así como los resultados de la evaluación y tratamiento de riesgos.

d) Ser comunicados.

e) Ser actualizados según corresponda.

La organización conservará información documentada sobre los objetivos de seguridad de la información.

Cuando se planifica cómo alcanzar los objetivos de seguridad de la información, la organización debe determinar:

f) ¿Qué se hará?

g) ¿Qué recursos serán necesarios?

h) ¿Quién será responsable?

i) ¿Cuándo se completará?

j) ¿Cómo se evaluarán los resultados?

## 3.2.3 Apoyo

### 3.2.3.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

### 3.2.3.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de las personas que hacen el trabajo bajo su control que afecte al rendimiento de seguridad de la información.

b) Asegurarse de que estas personas son competentes en base a una educación adecuada, formación o experiencia.

c) Cuando fuese aplicable, tomar las acciones para adquirir la competencia necesaria y evaluar la eficacia de las medidas adoptadas.

d) Retener la información documentada apropiada como evidencia de la competencia.

Las acciones aplicables pueden incluir, por ejemplo: la oferta de formación, la enseñanza o la reasignación de los empleados actuales o la contratación de personas competentes.

### 3.2.3.3 Conocimiento

Las personas que realizan un trabajo bajo el control de la organización deben tener en cuenta:

a) La política de seguridad de la información.

b) Su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información.

c) Las consecuencias de que no se cumpla con los requisitos del sistema de gestión de seguridad de la información.

### 3.2.3.4 Comunicación

La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para el sistema de gestión de seguridad de la información que incluyendo:

a) Cómo comunicarse.

b) Cuándo comunicarse.

c) Con qué comunicarse.

d) Quién deberá comunicar.

e) Los procesos por los cuales la comunicación se efectuará.

## 3.2.3.5 Información documentada

### 3.2.3.5.1 General

El sistema de gestión de seguridad de la información de la organización debe incluir:

a) La información documentada requerida por esta Norma Internacional.

b) La información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.

El alcance de la información documentada para un sistema de gestión de seguridad de la información puede diferir de una organización a otra debido a:

1) El tamaño de la organización y de su tipo de actividades, procesos, productos y servicios.

2) La complejidad de los procesos y sus interacciones.

3) La competencia de las personas.

### 3.2.3.5.2 Creación y actualización

Al crear y actualizar la información documentada de la organización debe asegurarse apropiadamente:

a) La identificación y descripción (por ejemplo, un título, fecha, autor o el número de referencia).

b) Tipo (por ejemplo, idiomas, versión del software, gráficos) y del formato (por ejemplo, papel, electrónico).

c) La revisión y aprobación por la idoneidad y adecuación.

### 3.2.3.5.3 Control de información documentada

La información documentada requerida por el sistema de gestión de seguridad de la información y por esta Norma Internacional debe ser controlada para asegurar:

a) Que sea apropiada y esté disponible para su uso, donde y cuando sea necesario.

b) Que esté protegida de forma adecuada (por ejemplo, de pérdida de confidencialidad, uso inadecuado o la pérdida de integridad).

Para el control de la información documentada, la organización debe responder a las siguientes actividades, según corresponda:

c) La distribución, acceso, recuperación y uso.

d) El almacenamiento y conservación, incluyendo la preservación de la legibilidad.

e) El control de cambios (por ejemplo el control de versiones).

f) La retención y disposición.

La información documentada de origen externo, que la organización determina que son necesarios para la planificación y operación del sistema de gestión de seguridad de la información, se debe identificar apropiadamente y controlarse.

El acceso implica una decisión sobre el permiso para ver la información documentada solamente, o el permiso y la autoridad para ver y cambiar la información documentada, etc…

# 3.2.4 Operación

## 3.2.4.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para conocer los requisitos de la seguridad de la información y para poner en práctica las acciones determinadas en el punto 3.2.2.1. La organización debe implementar también planes para lograr los objetivos de seguridad de la información determinados en el apartado 3.2.2.2.

La organización debe mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo previsto.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados, tomando medidas para mitigar los posibles efectos adversos, según sea necesario.

La organización debe asegurarse de que los procesos externalizados están determinados y controlados.

## 3.2.4.2 Evaluación de riesgos de seguridad de la información

La organización debe llevar a cabo unas evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan modificaciones importantes o se producen, teniendo en cuenta los criterios establecidos en el punto 3.2.1.2 a).

La organización conservará la información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

### 3.2.4.3 Información de tratamiento de riesgos de seguridad

La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.

La organización conservará la información documentada de los resultados del tratamiento de los riesgos de seguridad de información.

## 3.2.5 Evaluación del desempeño

### 3.2.5.1 Monitorización, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.

La organización debe determinar:

a) Lo que necesita ser monitoreado y medido, incluyendo los procesos de seguridad de la información y los controles.

b) Los métodos de monitorización, medición, análisis y evaluación, si fuesen aplicables, para garantizar la validez de los resultados.

Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

c) Cuando se llevarán a cabo el seguimiento y medición.

d) Quien monitorizará y medirá.

e) Cuando se analizarán y evaluarán los resultados de monitorización y medición.

f) Quien analizará y evaluará estos resultados.

La organización conservará la información documentada apropiada como prueba de los resultados del monitoreo y medición.

### 3.2.5.2 La auditoría interna

La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

a) Cumple: 1- que las propias necesidades de la organización para su sistema de gestión de seguridad de la información y 2- los requisitos de esta Norma Internacional.

b) Está implementada y mantenida de manera eficaz.

La organización debe:

c) Planificar, establecer, implementar y mantener programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y reportes. Los programas de auditoría deberán tener en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores.

d) Definir los criterios de auditoría y el objetivo de cada una.

e) Seleccionar auditores y realizar auditorías que garanticen la objetividad e imparcialidad del proceso de auditoría.

f) Asegurarse de que los resultados de las auditorías se reportan a la gerencia pertinente.

g) Conservar la información documentada como prueba de los programas de auditoría y los resultados de las mismas.

### 3.2.5.3 Revisión de la dirección

La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia.

La revisión de la dirección debe tener en consideración:

a) El estado de las acciones de las revisiones de la dirección previas.

b) Los cambios en los problemas externos e internos que son relevantes para la gestión del sistema de seguridad de la información.

c) La retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:

    1) Las no conformidades y acciones correctivas.

    2) Monitorización y medición de los resultados.

    3) Resultados de las auditorías.

    4) El cumplimiento de los objetivos de seguridad de la información.

d) La retroalimentación de las partes interesadas.

e) Los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos.

f) Las oportunidades de mejora continua.

Las salidas de la revisión de la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y de cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.

La organización conservará información documentada como evidencia de los resultados de las revisiones de la dirección.

# 3.2.6 Mejora

## 3.2.6.1 No conformidad y acciones correctivas

Cuando se produce una no conformidad, la organización deberá:

a) Reaccionar a la no conformidad, y según sea el caso:

    1) Tomar medidas para controlarlo y corregirlo.

    2) Hacer frente a las consecuencias.

b) Evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o se produzcan en otros lugares, a través de:

    1) La revisión de la no conformidad.

    2) Determinar las causas de la no conformidad.

    3) Determinar si existen incumplimientos similares o si podrían producirse.

c) Implementar cualquier acción necesaria.

d) Revisar la eficacia de las medidas correctivas adoptadas.

e) Realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.

Las acciones correctivas deben ser apropiadas a efectos de las no conformidades encontradas.

La organización conservará información documentada como evidencia de:

f) La naturaleza de las no conformidades y de cualquier acción tomada posteriormente.

g) Los resultados de cualquier acción correctiva.

### 3.2.6.2 Mejora continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de seguridad de la información.

# 4. Calidad en un Contact Center

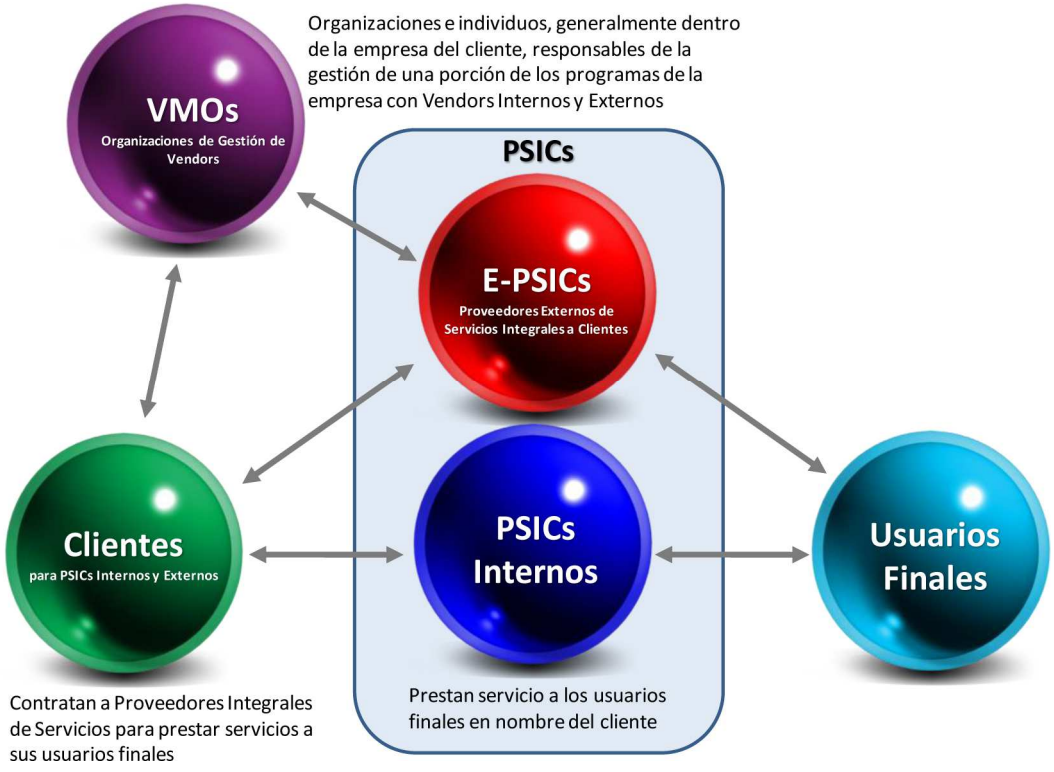
*No se puede controlar lo que no puedes medir.* Tom De Marco

*Lo que no se puede medir, no se puede gestionar.* Lord Kelvin

## 4.1 COPC PSIC

Para explicar los procesos y sus respectivas métricas usaremos los recogidos en la norma COPC (**C**ustomer **O**perations **P**erformance **C**enter) PSIC, reproducida parcialmente en este apartado. Esta norma comprende un conjunto de prácticas de gestión, métricas, mediciones clave y capacitación para operaciones de servicio centradas en el cliente.

El objetivo final marcado en ella es a través de la eficiencia maximizar el servicio, la calidad y los ingresos, junto con la satisfacción del cliente y la rentabilidad, minimizando los costes.




**Esquema establecido por la norma COPC. Imagen: COPC PSIC**

Desde el punto de vista del **PSIC** (Organización a la cual pertenece el Contact Center), suele estar en medio del Cliente y el Usuario Final, sirviendo de nexo entre ambos.

Otra perspectiva sería desde el lado del **Cliente**, el cual puede requerir los servicios de un Contact Center externo o que el Contact Center se encuentre dentro de la organización internamente.

De igual manera se puede ver desde el otro lado como **Usuario Final**, recibiendo este último el servicio o bien desde el propio PSIC interno del Cliente o de uno externo.

Por últimos los **VMO**s pueden ser contratados directamente por el PSIC o en su defecto por el Cliente quien tiene la potestad de otorgar permisos al PSIC para el uso de ellos.

En el Anexo 2, situado al final de este documento, se listan y explican los procesos y métricas sobre las que está basado el cuestionario sobre calidad que se ha realizado más adelante.

## 4.1.1 Objetivos y uso

Cuando hablamos de servicio nos referimos al tiempo que se tarda en realizar cualquier acción que implique al PSIC o en nuestro caso al PSIC, siempre desde el punto de vista del cliente.

La calidad será el grado de medición de la gestión de cualquier transacción que se atienda correctamente, siempre buscando la resolución en primer contacto, con el fin de evitar que se dupliquen las interacciones con la plataforma, generando una pérdida de calidad y aumentando los costes.

Los ingresos afectarán a operaciones de contacto en las que se involucre a centros de cobranzas y ventas.

La cuantificación que se busca con la aplicación de esta norma se puede distinguir en varias categorías, como el ahorro y las ganancias, diferenciando los siguientes:

## 4.1.2 Ahorros

**a) Mejoras en la calidad:**

i. **Aumento del FCR** (First Contact Resolution): al resolver las transacciones en un primer contacto se elimina la generación de transacciones posteriores que incumban la misma tipología, lo que reducirá el requerimiento de agentes u otros operadores para el servicio.

ii. **Costes de la mala calidad**: son los costes generados para compensar a un usuario final que ha recibido una mala información u operación que le afecte directamente. Las compensaciones pueden ser aumentos de suscripciones, vales, productos gratuitos, compensaciones económicas directas, entregas urgentes o eliminación de costes de tramitación.

**b) Mejoras en eficiencia:**

i. **Tiempo medio operativo** (Average Handle Time, AHT): Se refiere al tiempo en el que un operador resuelve la transacción que le acomete. Su reducción puede ser un factor que afecte al dimensionamiento de la plantilla o el ahorro en la misma. Se mantendrán unos umbrales de cumplimiento y la dirección de la empresa deberá hacer todo lo posible para que cualquier operador se mantenga dentro de ellos con el fin de mejorar la capacidad del desarrollo de los procesos.

ii. **Ocupación**: Este factor está relacionado con el tiempo en el que un agente no está siendo productivo. El objetivo es la minimización de este tiempo ya que repercute directamente en el servicio. Gestionar más carga de trabajo con el mismo número de personas o reducir el número de agentes para la misma carga de trabajo influirán en este factor.

iii. **Utilización**: Se deberá minimizar la cantidad de tiempo de trabajo en el cual los agentes no están disponibles para gestionar cualquier transacción, reducirá el número de agentes necesarios.

iv. **Coste por transacción**: Cuando se midan los detalles mencionados anteriormente para la eficiencia, esto repercutirá en una disminución en el coste por transacción.

**c) Mejoras en el servicio:**

i. **Reducción de pendientes**: Mejorando la velocidad de respuesta en transacciones retrasadas, evita la generación de pendientes de transacciones adicionales posteriores.

ii. **Reducción de pagos de multas al cliente**: cumpliendo con los niveles de servicio que se acordaron con el cliente, se reducirán o eliminarán las posibles multas por incumplimientos de los compromisos contractuales.

**d) Reducción en el volumen de transacciones:**

Se puede alcanzar mediante:

i. Un aumento del FCR.

ii. Reducción de pendientes.

iii. Identificación y resolución de causas de contacto.

iv. Métodos alternativos para que los usuarios finales resuelvan sus problemas, por ejemplo: servicio en Internet o Applets.

v. Automatización de los contactos (opciones de auto servicio en el IVR).

e) **Mejoras en el compromiso del personal**:

Se pueden medir en:

**i. Rotación**

Este factor es bastante frecuente en los PSIC por lo que normalmente el personal no suele tener una estancia demasiado prolongada en su puesto de trabajo. Para estimar el coste de la rotación se incluirán:

- **Costes de salario durante la formación:** Los costes del salario pagado a los agentes durante la formación antes de la contratación, incluyen salario más beneficios y costes adicionales de incidentes, pero no incluyen costes fijos tales como estaciones de trabajo, etc.

- **Costes directos de reclutamiento:** A una agencia o costes internos específicamente destinados a reclutamiento, excluyendo costes fijos.

- **Costes de horas extras:** Para cubrir a quienes se hayan ido hasta que los nuevos reclutados entren en operación.

- **Productividad reducida de nuevos contratados:** Los nuevos contratados tienen peores tiempos de manejo que el personal existente. En un típico programa de servicio al Cliente, de duración de llamada media, se observa que a un nuevo contratado puede llevarle hasta siete semanas desde el fin de su formación para alcanzar la eficiencia de los agentes existentes.

- **Costes directos de formación:** Materiales, contratación de equipamiento adicional, costes directamente atribuibles, excluyendo los costes fijos.

- **Para los PSIC externos a los que se paga por Empleado a Tiempo Completo (ETC):** Se deberá también tomar en cuenta un impacto en los ingresos al calcular los costes de la rotación.

- **Costes Fijos:** Es discutible si los costes de gastos indirectos como los de departamentos de reclutamiento y formación, las instalaciones de formación, etc.…, deberían o no incluirse en el coste por partida. La norma no incluye normalmente estos costes en el cálculo de ahorros, dado que generalmente la reducción de la rotación no tiene un gran impacto en estos departamentos, debido a que la reducción de los costes se dará en cada paso más que por individuo que parte. Si se los fuera a incluir en estos costes, es mejor pronosticar la rotación anual y distribuir los costes fijos

sobre el número total de partidas estimadas en un año para obtener el costo total por partida.

**ii. Ausentismo**

Con el fin de evitar problemas en el servicio se deberá tener en cuenta la capacidad del volumen de trabajo para dimensionar la plantilla ya que el ausentismo, debido a la rotación del personal, puede darse diariamente. Puede ser repentino como una falta injustificada o enfermedad o programado como una formación, vacaciones, días libres, maternidad, etc. El cálculo del impacto del ausentismo incluirá:

- **Costes salariales directos:** de personal adicional reclutado para cubrir la ausencia.
- **Horas extra:** pagadas a los agentes existentes.

**f) Ganancias Directas en Resultados:**

Una mejora en el desempeño del servicio, la calidad y la eficiencia repercutirán en las ganancias. Se podrán medir de la siguiente forma:

- Si la operación de contacto con clientes realiza ventas o cobranzas, se puede medir en el valor en $/€ del desempeño que ha mejorado.
- Si la operación de contacto con clientes realiza captación de clientes, esto deberá convertirse a una cifra de ingresos mediante la utilización de un factor de conversión y un valor de ventas promedio.
- Para procesos de retención, los ahorros se calculan como el gasto anual esperado del usuario final retenido (a menudo el ahorro es sólo considerado como tal si el cliente sigue manteniendo el servicio después de los 90 días).
- La mejora en cobranzas se calcula como la mejora real en cobranzas, calculada como una cifra anual.

**g) Beneficios Intangibles:**

- Lealtad/Incremento de la satisfacción y Churn o Pérdida de clientes/Disminución de la insatisfacción.
- Satisfacción del cliente.
- Identificación de otras áreas problemáticas en la Organización.

# 4.1.3 Visión general de la norma


**Esquema establecido por la norma COPC. Fuente: COPC PSIC**

La norma se divide en tres grupos: Conductores, Facilitadores y Objetivo. El primero de ellos descrito en la sección Liderazgo y Planeamiento busca la conducción de la gestión del desempeño focalizada en el Cliente, personificada en las características y actividades de liderazgo. El segundo está compuesto de los Procesos y los Recursos Humanos, representando a los facilitadores de la organización que definen a una fuerza de trabajo formada y motivada, que utiliza procesos bien diseñados y maneja esos mismos con la información apropiada. Por último estarían los Resultados, una composición balanceada de satisfacción del cliente y del usuario final, del desempeño de productos y servicios y productividad.

Dentro de ellas se encuentran los 30 items formalizados en la norma, que se explicarán brevemente su función u obligación para que su cumplimiento.

## 4.1.3.1 Liderazgo y Planeamiento

Focaliza en cómo el PSIC ejerce liderazgo apropiado y en cómo esto permite que el PSIC alcance sus objetivos

### 4.1.3.1.1 Declaración de la Dirección

Debe tener una declaración de dirección global documentada (visión, misión o propósito) que clarifique su compromiso hacia clientes y usuarios finales.

#### 4.1.3.1.2 Desarrollo de Planes de Negocio

Debe tener y usar un enfoque documentado para desarrollar planes de negocios anuales.

#### 4.1.3.1.3 Definición de Objetivos

Debe tener un enfoque para definir objetivos para todas las métricas listadas en el Anexo 2 que asegure alto desempeño y mejora sostenida, donde la mejora sostenida conduciría a resultados en satisfacción del usuario final o financieros.

#### 4.1.3.1.4 Revisión de los Resultados del Negocio

Debe tener y usar un enfoque documentado para revisar el desempeño de planes de negocios y objetivos.

#### 4.1.3.1.5 Revisión Interna de la Norma COPC

Debe llevar a cabo una revisión abarcativa del uso e implementación de la Norma COPC PSIC (sistema de gestión de desempeño) al menos anualmente, y debe tomar acciones para corregir deficiencias y desvíos identificados en esta revisión.

### 4.1.3.2 Procesos

Focaliza en los Procesos Clave Relacionados con el Cliente (PCRCs) y Procesos Clave de Apoyo (PCAs) que los PSICs usan para desarrollar y entregar sus productos y servicios.

#### 4.1.3.2.1 Gestión de Cambios

Debe tener un enfoque de gestión de cambios estructurado para controlar los cambios que se realizan en la provisión de servicios al cliente.

#### 4.1.3.2.2 Procesos, Procedimientos y Metodologías

Debe asegurar que sus PCRCs están definidos y operan efectivamente para lograr objetivos consistentemente.

#### 4.1.3.2.3 Acciones Correctivas y Mejora Sostenida

Debe utilizar un enfoque estructurado para identificar y resolver las causas raíz del bajo desempeño para aquellas métricas que no alcanzan consistentemente los requisitos y objetivos.

#### 4.1.3.2.4 Monitoreo de Transacciones

Debe contar con un enfoque para el monitoreo de transacciones diseñado para alcanzar los requisitos y objetivos del PSIC, del cliente y del usuario final. Este enfoque debe focalizar en dos niveles: a nivel de proceso y a nivel de agente. Haciendo especial énfasis en:

1. Precisión del error crítico para el usuario final: Satisfacción/Insatisfacción del usuario final.

2. Precisión del error crítico para el negocio: El cliente sobre el Contact Center, que costes le repercute.

3. Precisión del error crítico de cumplimiento: en base a las regulaciones.

4. Precisión del error no crítico: profesionalismo.

#### 4.1.3.2.5 Pronóstico, Planificación y Programación del Personal

Debe pronosticar y programar los requisitos de planificación del personal de tal manera que pueda cumplir con las demandas de volumen de transacciones.

#### 4.1.3.2.6 Cumplimiento

Debe asegurar el cumplimiento de requisitos regulatorios y proteger la información y los datos sensibles y propietarios del Usuario Final.

#### 4.1.3.2.7 Tecnología

Debe tener enfoques para la implementación y gestión de soluciones tecnológicas a fin de proveer altos niveles de servicio tanto a usuarios finales como a usuarios internos.

#### 4.1.3.2.8 Gestión de Proveedores Clave

Debe gestionar el desempeño de sus proveedores clave, por ejemplo los que desarrollan PCRCs o PCAs.

#### 4.1.3.2.9 Gestión de Cambios

Debe establecer un plan documentado que clarifique el enfoque del PSIC frente a la provisión de servicio durante interrupciones menores (de hasta 6 horas) y la recuperación luego de interrupciones de larga duración.

#### 4.1.3.2.10 Gestión de Cambios

Debe reportar en todas las métricas requeridas.

### 4.1.3.3 Recursos Humanos

Requiere de una fuerza de trabajo apropiadamente formada, instruida y motivada para que los PSICs tengan enfoques de gestión de recursos humanos que permitan a todo el personal brindar productos y servicios de calidad en forma efectiva y eficiente.

#### 4.1.3.3.1 Definición del Puesto de Trabajo

Debe poseer, por escrito, claras definiciones de las habilidades mínimas y conocimientos requeridos para cada Puesto Clave Relacionado con el Cliente.

#### 4.1.3.3.2 Reclutamiento y Contrataciones

Debe reclutar personal que tenga altas probabilidades de desempeñarse exitosamente en los Puestos Clave Relacionados con el Cliente.

#### 4.1.3.3.3 Formación y Desarrollo

Debe proveer la formación y desarrollo requeridos para todo el personal que se desempeña en Puestos Clave Relacionados con el Cliente para adquirir y mantener las habilidades y los conocimientos requeridos para sus posiciones.

#### 4.1.3.3.4 Verificación de Habilidades y Conocimientos

Debe verificar que todo el personal (incluyendo personal indefinido y personal temporario) que se desempeña en Puestos Clave Relacionados con el Cliente, posee todas las habilidades y conocimientos requeridos para el puesto.

#### 4.1.3.3.5 Gestión de Desempeño del Personal

Debe apoyar la Declaración de la Dirección del PSIC y los objetivos de resultados del negocio.

#### 4.1.3.3.6 Gestión del Feedback del Personal

Debe utilizar un enfoque estructurado para solicitar feedback a su personal de manera proactiva, para luego evaluarlo y tomar las acciones apropiadas que surjan a partir del feedback obtenido por parte de los Agentes y Supervisores.

#### 4.1.3.3.7 Rotación y Ausentismo del Personal

Debe medir y gestionar la rotación del personal para los Agentes y Supervisores y el ausentismo para el personal que se desempeña en Puestos de Representantes de Atención al Cliente.

### 4.1.3.4 Resultados

Su función es la de ayudar a alcanzar altos niveles de satisfacción de clientes y usuarios finales, desempeño de productos y servicios y eficiencia e incrementar estos niveles de manera sostenida.

#### 4.1.3.4.1 Satisfacción e Insatisfacción del Usuario Final

Debe medir y gestionar la satisfacción e insatisfacción del usuario final de forma global y con cada uno de los atributos que la forman. Se recomienda el uso de cuestionarios tras la interacción.

#### 4.1.3.4.2 Satisfacción e Insatisfacción del Cliente

Debe medir y gestionar la satisfacción e insatisfacción del cliente haciendo valer las encuestas, quejas y devoluciones obtenidas por la organización.

#### 4.1.3.4.3 Desempeño del Servicio

Debe medir el desempeño del servicio y los ingresos de cada Proceso Clave Relacionado con el Cliente. El objetivo de hacerlo es tanto alcanzar altos niveles de resultados como mejorar el desempeño en los casos en los que los niveles alcanzados se encuentran por debajo de los objetivos.

#### 4.1.3.4.4 Desempeño de la Calidad

Debe medir y gestionar el desempeño de la calidad de cada Proceso Clave Relacionado con el Cliente. El objetivo de hacerlo es tanto alcanzar altos niveles de desempeño como mejorar el desempeño en los casos en los que los niveles alcanzados se encuentran por debajo de los objetivos.

#### 4.1.3.4.5 Desempeño de las Ventas

Debe medir y gestionar los resultados de ventas para cada Proceso Clave Relacionado con el Cliente. El objetivo de esto es alcanzar altos niveles de resultados y mejorar los resultados donde los niveles alcanzados estén por debajo de los objetivos.

#### 4.1.3.4.6 Desempeño de los Costes y Eficiencia

Debe medir y gestionar la eficiencia al nivel de sus procesos para Procesos Clave Relacionados con el Cliente y gestionar los ahorros al nivel de la entidad o del programa.

#### 4.1.3.4.7 Desempeño de los Procesos Claves de Apoyo

Debe medir y gestionar el desempeño del servicio y la calidad de cada Proceso Clave de Apoyo. El Objetivo de esto es alcanzar altos niveles de desempeño y mejorar el desempeño donde los niveles alcanzados estén por debajo de los objetivos.

#### 4.1.3.4.8 Alcanzando Resultados

Debe alcanzar los objetivos de nivel de desempeño y mostrar una tendencia sostenida de mejora en la mayoría de sus métricas de Servicio, Calidad, Ventas, Costos y Eficiencia, y Satisfacción del Cliente y del Usuario Final.

# 4.2 ISO 9001

Es una norma que determina los requisitos de un sistema de gestión de la calidad que cualquier organización pueda establecer internamente.

Está distribuida en ocho capítulos, siendo los más importantes los cinco últimos (Sistema de Gestión de la Calidad, Responsabilidad de la dirección, Gestión de recursos, Realización del producto/servicio y Medición, análisis y mejora)

- **Sistema de Gestión de la Calidad**: contiene los requisitos generales y aquellos pertenencientes a la gestión de la documentación.
- **Responsabilidad de la dirección**: contiene los requisitos relacionados con la dirección, como la definición de la política de calidad, planificación, o la responsabilidad, autoridad y comunicación.
- **Gestión de recursos**: establece los requisitos de los tres grupos en los que se divide: RRHH, la infraestructura y el ambiente de trabajo.
- **Realización del producto/servicio**: delimita todos los requisitos desde la planificación del producto/servicio hasta la entrega del mismo.
- **Medición, análisis y mejora**: aquí aparecen los requisitos para los procesos que recopilarán la información necesaria para ser posteriormente analizada y tomar las decisiones acordes con los resultados.

Esta norma es muy similar a la metodología del Círculo de Deming, de la cual hablaremos más adelante. Ambas buscan la satisfacción final del cliente por medio de una mejora continua basada en los requisitos.

# 4.3 Otros Marcos, Modelos, Metodologías y Buenas Prácticas

## 4.3.1 Cobit

Cobit en su versión 5.0 de define como un proveedor de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Teniendo muy en cuenta el papel fundamental de la información en todos los procesos que le atañen.

Esta versión sigue basándose en Cobit 4.1 pero con varios cambios. En esta versión más actual se ha integrado tanto Val IT 2.0 como Risk IT a su marco.

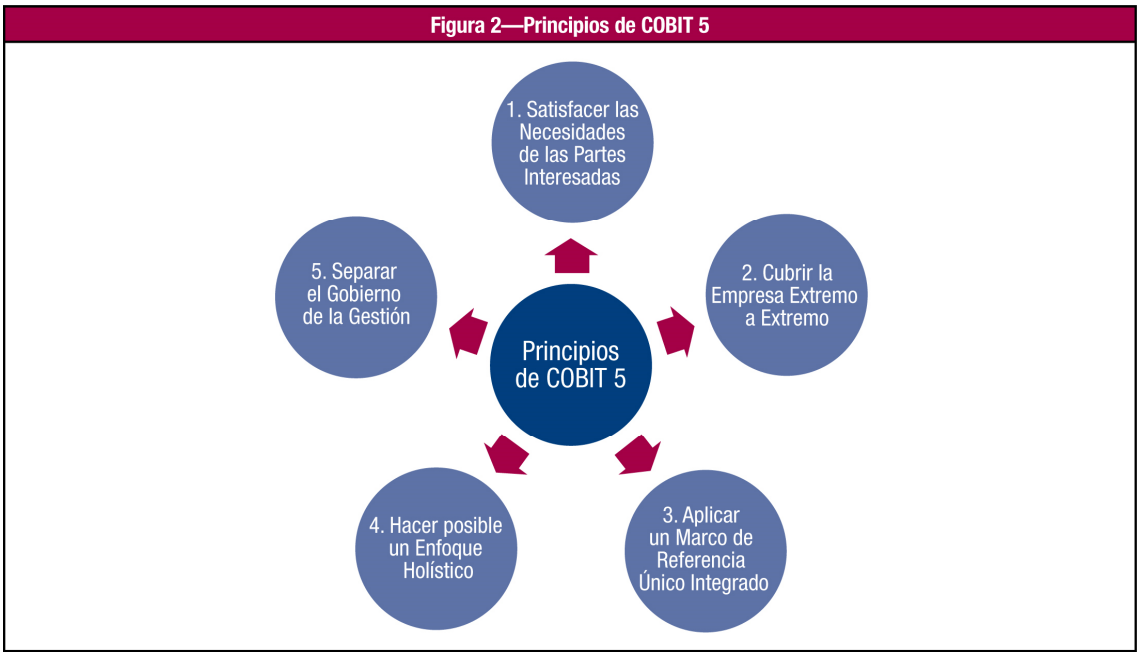
El marco trata de integrar a las dos partes involucradas:

- El **gobierno**, el cual busca que los objetivos de la empresa se logren a través de una evaluación de las necesidades y estableciendo una dirección mediante prioridades y toma de decisiones. Para ello supervisará el desempeño, el cumplimiento y el progreso de dichos objetivos. Se lo conoce como el ciclo EDM.

- Y la **gestión** o **administración**, la cual planea, construye, ejecuta y monitorea actividades de acuerdo a lo fijado por el gobierno de acuerdo con dichos objetivos. Se lo conoce como el ciclo PBRM.

Se alinea con otros marcos de referencia como puede ser ISO/IEC 9001, ISO/IEC 27000 o ITIL de los cuales hemos hablado previamente o posteriormente.

Se nueva estructura se basa en 5 principios claves representada a través de la siguiente tipología:




**Principios de Cobit 5. Fuente:ISACA**

En un breve resumen se explica a que corresponde cada uno de los principios pero más adelante se desarrollarán como está establecido en el marco.

**• Principio 1. Satisfacer las necesidades de las partes interesadas.**

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

COBIT 5 provee todos los procesos necesarios y otros habilitadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

**• Principio 2: Cubrir la empresa de extremo a extremo**

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

– Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.

– Considera que los habilitadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

**• Principio 3: Aplicar un marco de referencia único e integrado**

Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

**• Principio 4: Hacer posible un enfoque holístico**

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de habilitadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los habilitadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de habilitadores:

– Principios, Políticas y Marcos de Trabajo

– Procesos

– Estructuras Organizativas

– Cultura, Ética y Comportamiento

– Información

– Servicios, Infraestructuras y Aplicaciones

– Personas, Habilidades y Competencias

**• Principio 5: Separar el Gobierno de la Gestión**

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

– Gobierno:

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas

equilibradas y acordadas, estableciendo la dirección a través de la priorización y la toma de decisiones y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

– Gestión:

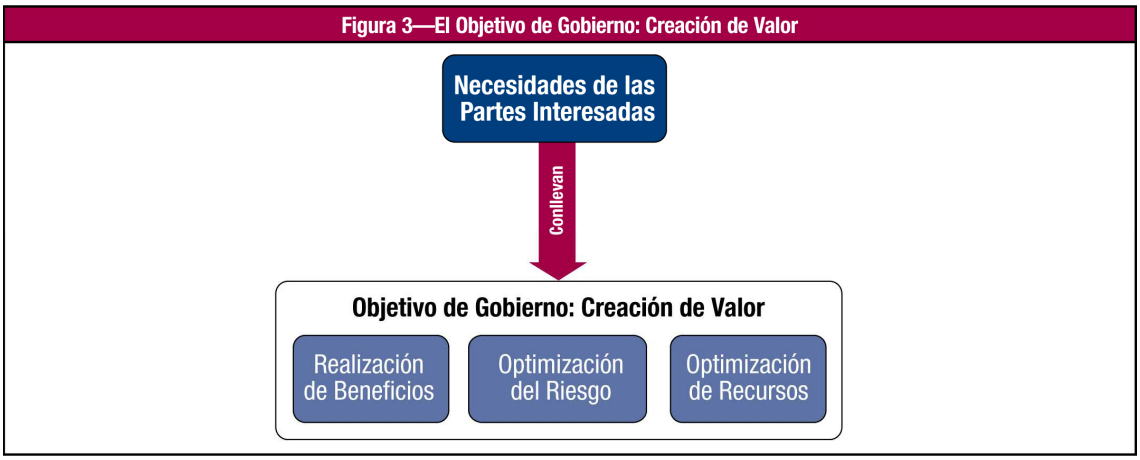
La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

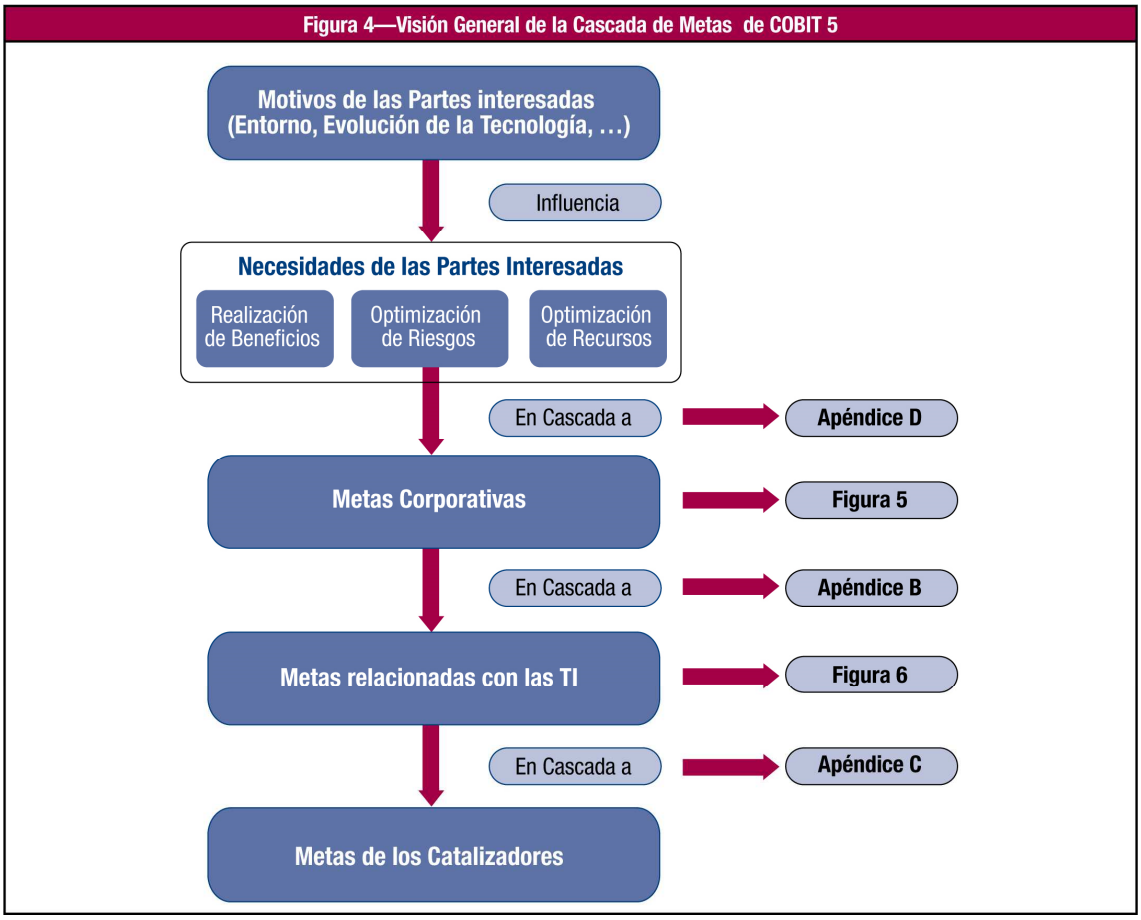
## Principio 1: Satisfacer las necesidades de las Partes Interesadas

El objetivo del Gobierno es la creación de valor, por ello las necesidades de las partes interesadas conllevan la realización de beneficios y la optimización del riesgo y de los recursos. La creación de valor por parte del Gobierno puede entrar en conflictos entre las diferentes partes interesadas en las que influyen dichos beneficios, riesgo y recursos.




**Objetivo de Gobierno: Creación del valor. Fuente:ISACA**

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas habilitadoras específicas, útiles y a medida.




**Cascada de metas de Cobit 5. Fuente:ISACA**

### Paso 1. Los motivos de las Partes Interesadas influyen en las necesidades de las Partes Interesadas

Las necesidades de las partes interesadas están influenciadas por diferentes motivos, por ejemplo, cambios de estrategia, un negocio y entorno regulatorio cambiantes y las nuevas tecnologías.

### Paso 2. Las necesidades de las Partes Interesadas desencadenan Metas Empresariales

Las necesidades de las partes interesadas pueden estar relacionadas con un conjunto de metas empresariales genéricas.

Estas metas corporativas han sido desarrolladas utilizando las dimensiones del Cuadro de Mando Integral (CMI. En inglés: Balanced Scorecard, BSC) y representan una lista de objetivos comúnmente usados que una empresa puede definir por sí misma. Aunque esta lista no es exhaustiva, la mayoría metas corporativas específicas de la empresa pueden relacionarse fácilmente con uno o más de los objetivos genéricos de la empresa.

Define 17 metas corporativas u objetivos agrupadas según su encaje en el CMI con una relación primaria o secundaria con respecto a los beneficios, riesgos y recursos.

| Figura 5—Metas Corporativas de COBIT 5 | | | | |
|---|---|---|---|---|
| | | Relación con los Objetivos de Gobierno | | |
| Dimensión del CMI | Meta Corporativa | Realización de Beneficios | Optimización de Riesgos | Optimización de Recursos |
| Financiera | 1. Valor para las partes interesadas de las Inversiones de Negocio | P | | S |
| | 2. Cartera de productos y servicios competitivos | P | P | S |
| | 3. Riesgos de negocio gestionados (salvaguarda de activos) | | P | S |
| | 4. Cumplimiento de leyes y regulaciones externas | | P | |
| | 5. Transparencia financiera | P | S | S |
| Cliente | 6. Cultura de servicio orientada al cliente | P | | S |
| | 7. Continuidad y disponibilidad del servicio de negocio | | P | |
| | 8. Respuestas ágiles a un entorno de negocio cambiante | P | | S |
| | 9. Toma estratégica de Decisiones basada en Información | P | P | P |
| | 10. Optimización de costes de entrega del servicio | P | | P |
| Interna | 11. Optimización de la funcionalidad de los procesos de negocio | P | | P |
| | 12. Optimización de los costes de los procesos de negocio | P | | P |
| | 13. Programas gestionados de cambio en el negocio | P | P | S |
| | 14. Productividad operacional y de los empleados | P | | P |
| | 15. Cumplimiento con las políticas internas | | P | |
| Aprendizaje y Crecimiento | 16. Personas preparadas y motivadas | S | P | P |
| | 17. Cultura de innovación de producto y negocio | P | | |

**Metas Corporativas. Fuente:ISACA**

Las preguntas entre el Gobierno y la Gestión (partes interesadas) tienen una relación con las metas corporativas.

**Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión**

| NECESIDADES DE LAS PARTES INTERESADAS | Valor para los Interesados de las Inversiones de Negocio<br>1. | Cartera de productos y servicios competitivos<br>2. | Riesgos de negocio gestionados (salvaguarda de activos)<br>3. | Cumplimiento de leyes y regulaciones externas<br>4. | Transparencia financiera<br>5. | Cultura de servicio orientada al cliente<br>6. | Continuidad y disponibilidad del servicio de negocio<br>7. | Respuestas ágiles a un entorno de negocio cambiante<br>8. | Toma estratégica de Decisiones basada en Información<br>9. | Optimización de los costes de los procesos de negocio<br>10. | Optimización de la funcionalidad de los procesos de negocio<br>11. | Programas gestionados de cambio en el negocio<br>12. | Productividad operacional y de los empleados<br>13. | Cumplimiento con las políticas internas<br>14. | Cumplimiento con políticas internas<br>15. | Personas preparadas y motivadas<br>16. | Cultura de innovación de producto y negocio<br>17. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ¿Cómo se consigue valor mediante el uso de TI? ¿ Está el usuario final satisfecho con la calidad del servicio de TI? | ■ | ■ | | | | ■ | ■ | | | | | | ■ | | | ■ | ■ |
| ¿Cómo se gestiona el rendimiento de TI? | | ■ | | | ■ | | | | ■ | ■ | ■ | ■ | | ■ | | | |
| ¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas? | ■ | ■ | | | | | | ■ | | | | | ■ | | | ■ | ■ |
| ¿Cómo puedo construir y estructurar mejor mi departamento de TI? | | | | | | | | ■ | | ■ | ■ | ■ | | ■ | ■ | ■ | |
| ¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos? | | | ■ | ■ | | | | | | ■ | | | | | | | |
| ¿Cuáles son los requisitos (de control) para la información? | | | | ■ | | | | | ■ | | | | | | ■ | | |
| ¿He contemplado todo los riesgos relacionados con TI? | | | ■ | | | | ■ | | ■ | | | | | | ■ | | |
| ¿Estoy ejecutando una operación de TI eficiente y robusta? | | | | | ■ | | ■ | | | | | | | | | | |
| ¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes? | | | | | | | | | | ■ | | ■ | | ■ | | | |

**Mapeo de las Metas Corporativas y las preguntas del Gobierno y la gestión. Fuente:ISACA**

**Figura 24—Mapeo entre las Metas Corporativas de COBIT 5 y las Preguntas del Gobierno y la Gestión *(cont.)***

| NECESIDADES DE LAS PARTES INTERESADAS | 1. Valor para los Interesados de las Inversiones de Negocio | 2. Cartera de productos y servicios competitivos | 3. Riesgos de negocio gestionados (salvaguarda de activos) | 4. Cumplimiento de leyes y regulaciones externas | 5. Transparencia financiera | 6. Cultura de servicio orientada al cliente | 7. Continuidad y disponibilidad del servicio de negocio | 8. Respuestas ágiles a un entorno de negocio cambiante | 9. Toma estratégica de Decisiones basada en Información | 10. Optimización de los costes de los procesos de negocio | 11. Optimización de la funcionalidad de los procesos de negocio | 12. Programas gestionados de cambio en el negocio | 13. Productividad operacional y de los empleados | 14. Cumplimiento con las políticas internas | 15. Cumplimiento con políticas internas | 16. Personas preparadas y motivadas | 17. Cultura de innovación de producto y negocio |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento? | | | | | | | | | | ■ | | ■ | | ■ | | | |
| ¿Cómo consigo confianza sobre TI? | | | | ■ | | | | | | | | | | | ■ | | |
| ¿Está bien securizada la información que se está procesando? | | | | ■ | | | ■ | | | | | | | | ■ | | |
| ¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de IT más flexible? | ■ | | | | | | | ■ | | | | | | | | ■ | ■ |
| ¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué permanece la TI en el camino de ejecutar la estrategia de negocio | ■ | ■ | ■ | | | | | ■ | | | ■ | ■ | ■ | | | | |
| ¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible? | ■ | ■ | | | | | ■ | | | | | | | | | | |
| ¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio? | ■ | ■ | | | | | | | | | ■ | ■ | | | | | |
| ¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI? | | | | | ■ | | | | | ■ | | ■ | | ■ | | | |
| ¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio? | | ■ | ■ | | | | | | | | | ■ | | | | | |
| ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos? | | ■ | | | ■ | | | | | ■ | | ■ | | | | | |
| ¿Cuánto se tarda en la toma de decisiones importantes de TI? | ■ | ■ | | | ■ | | | ■ | | | | | | | | | |
| ¿Son transparentes el esfuerzo y las inversiones totales en TI? | | ■ | | ■ | ■ | | | | | | | | | | ■ | | |
| ¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables? | | | | ■ | | | | | | | | | | | ■ | | |

**Mapeo de las Metas Corporativas y las preguntas del Gobierno y la gestión. Fuente:ISACA**

## Paso 3. Cascada de Metas de Empresa a Metas Relacionadas con las TI

El logro de metas empresariales requiere un número de resultados relacionados con las TI (en el caso que nos aplica), que están representados por las metas relacionadas con

la TI. Se entiende como relacionados con las TI a la información y tecnologías relacionadas, y las metas relacionadas con las TI se estructuran en dimensiones del CMI.

Define 17 metas u objetivos de información y tecnologías, agrupadas según su encaje en el CMI.

| Figura 6—Metas relacionadas con las TI | | |
|---|---|---|
| **Dimensión del CMI TI** | **Meta de Información y Tecnología Relacionada** | |
| Financiera | 01 | Alineamiento de TI y estrategia de negocio |
| | 02 | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas |
| | 03 | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI |
| | 04 | Riesgos de negocio relacionados con las TI gestionados |
| | 05 | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI |
| | 06 | Transparencia de los costes, beneficios y riesgos de las TI |
| Cliente | 07 | Entrega de servicios de TI de acuerdo a los requisitos del negocio |
| | 08 | Uso adecuado de aplicaciones, información y soluciones tecnológicas |
| Interna | 09 | Agilidad de las TI |
| | 10 | Seguridad de la información, infraestructura de procesamiento y aplicaciones |
| | 11 | Optimización de activos, recursos y capacidades de las TI |
| | 12 | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio |
| | 13 | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. |
| | 14 | Disponibilidad de información útil y fiable para la toma de decisiones |
| | 15 | Cumplimiento de las políticas internas por parte de las TI |
| Aprendizaje y Crecimiento | 16 | Personal del negocio y de las TI competente y motivado |
| | 17 | Conocimiento, experiencia e iniciativas para la innovación de negocio |

**Metas realacionadas con las TI. Fuente:ISACA**

También existe una relación donde cada meta corporativa es soportada por varias metas relacionadas con TI de forma primaria o secundaria.

**Figura 22—Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI**

| | | | Meta corporativa | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Valor para las partes interesadas de las Inversiones de Negocio | Cartera de productos y servicios competitivos | Riesgos de negocio gestionados (salvaguarda de activo) | Cumplimiento de leyes y regulaciones externas | Transparencia financiera | Cultura de servicio orientada al cliente | Continuidad y disponibilidad del servicio de negocio | Respuestas ágiles a un entorno de negocio cambiante | Toma estratégica de Decisiones basadas en información | Optimización de costes de entrega del servicio | Optimización de la funcionalidad de los procesos de negocio | Optimización de los costes de los procesos de negocio | Programas gestionados de cambio en el negocio | Productividad operacional y de los empleados | Cumplimiento con las políticas internas | Personas preparadas y motivadas | Cultura de innovación del producto y del negocio |
| | | | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. | 9. | 10. | 11. | 12. | 13. | 14. | 15. | 16. | 17. |
| | | Meta relacionada con las TI | Financiera | | | | | Cliente | | | | | Interna | | | | | Aprendizaje y Crecimiento | |
| Financiera | 01 | Alineamiento de TI y la estrategia de negocio | P | P | S | | | P | S | P | P | S | P | S | P | | | S | S |
| | 02 | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | | | S | P | | | | | | | | | | | P | | |
| | 03 | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | P | S | S | | | | | S | S | | S | | P | | | S | S |
| | 04 | Riesgos de negocio relacionados con las TI gestionados | | | P | S | | | P | S | | P | | | S | | S | S | |
| | 05 | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | P | P | | | | S | | S | | S | S | P | | S | | | S |
| | 06 | Transparencia de los costes, beneficios y riesgos de las TI | S | | S | | P | | | | S | P | | P | | | | | |
| Cliente | 07 | Entrega de servicios de TI de acuerdo a los requisitos del negocio | P | P | S | S | | P | S | P | S | | P | S | S | | | S | S |
| | 08 | Uso adecuado de aplicaciones, información y soluciones tecnológicas | S | S | S | | | S | S | | S | S | P | S | | P | | S | S |
| Interna | 09 | Agilidad de las TI | S | P | S | | | S | | P | | | P | | S | S | | S | P |
| | 10 | Seguridad de la información, infraestructuras de procesamiento y aplicaciones | | | P | P | | | P | | | | | | | | P | | |
| | 11 | Optimización de activos, recursos y capacidades de las TI | P | S | | | | | | S | | P | S | P | S | S | | | S |
| | 12 | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | S | P | S | | | S | | S | | S | P | S | S | S | | | S |
| | 13 | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad | P | S | S | | | S | | | | S | | S | P | | | | |
| | 14 | Disponibilidad de información útil y relevante para la toma de decisiones | S | S | S | S | | | P | | P | | S | | | | | | |
| | 15 | Cumplimiento de TI con las políticas internas | | | S | S | | | | | | | | | | | P | | |
| Aprendizaje y Crecimiento | 16 | Personal del negocio y de las TI competente y motivado | S | S | P | | | S | | S | | | | | | P | | P | S |
| | 17 | Conocimiento, experiencia e iniciativas para la innovación de negocio | S | P | | | | S | | P | S | | S | | S | | | S | P |

**Mapeo de las Metas Corporativas y las Metas Relacionadas. Fuente:ISACA**

## Paso 4. Cascada de Metas Relacionadas con las TI Hacia Metas Habilitadoras

Alcanzar metas relacionadas con las TI requiere la aplicación satisfactoria y el uso de varios habilitadores. Los habilitadores incluyen procesos, estructuras organizativas e información, y para cada habilitador puede definirse un conjunto de metas relevantes en apoyo de las metas relacionadas con la TI. Los procesos son uno de los habilitadores.

La relación entre metas relacionadas con las TI y los procesos relevantes de COBIT 5, los cuales contienen metas de los procesos relacionados.

**Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos**

| | | | Meta relacionada con las TI | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Alineamiento de TI y la estrategia de negocio | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | Riesgos de negocio relacionados con las TI gestionados | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | Transparencia de los costes, beneficios y riesgos de las TI | Entrega de servicios de TI de acuerdo a los requisitos del negocio | Uso adecuado de aplicaciones, información y soluciones tecnológicas | Agilidad de las TI | Seguridad de la información, infraestructura de procesamiento y aplicaciones | Optimización de activos, recursos y capacidades de las TI | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. | Disponibilidad de información útil y relevante para la toma de decisiones | Cumplimiento de las políticas internas por parte de las TI | Personal del negocio y de las TI competente y motivado | Conocimiento, experiencia e iniciativas para la innovación de negocio |
| | | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Procesos de COBIT 5 | | | Financiera | | | | | | Cliente | | Interna | | | | | | | Apren-dizaje y Creci-miento | |
| Evaluar, Orientar y Supervisar | EDM01 | Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno | P | S | P | S | S | S | P | | S | S | S | S | S | S | S | S | S |
| | EDM02 | Asegurar la Entrega de Beneficios | P | | S | | P | P | P | S | | | S | S | S | S | | S | P |
| | EDM03 | Asegurar la Optimización del Riesgo | S | S | S | P | | P | S | S | | P | | | S | S | P | S | S |
| | EDM04 | Asegurar la Optimización de los Recursos | S | | S | S | S | S | S | S | P | | P | | S | | | P | S |
| | EDM05 | Asegurar la Transparencia hacia las partes interesadas | S | S | P | | | P | P | | | | | | S | S | S | | S |
| Alinear, Planificar y Organizar | APO01 | Gestionar el Marco de Gestión de TI | P | P | S | S | | | S | | P | S | P | S | S | S | P | P | P |
| | APO02 | Gestionar la Estrategia | P | | S | S | S | | P | S | S | | S | S | S | S | S | S | P |
| | APO03 | Gestionar la Arquitectura Empresarial | P | | S | S | S | S | S | S | P | S | P | S | | S | | | S |
| | APO04 | Gestionar la Innovación | S | | | S | P | | | P | P | | P | S | | S | | | P |
| | APO05 | Gestionar el portafolio | P | | S | S | P | S | S | S | S | | S | | P | | | | S |
| | APO06 | Gestionar el Presupuesto y los Costes | S | | S | S | P | P | S | S | | | S | | S | | | | |
| | APO07 | Gestionar los Recursos Humanos | P | S | S | S | | | S | | S | S | P | | P | | S | P | P |
| | APO08 | Gestionar las Relaciones | P | | S | S | S | S | P | S | | | S | P | S | | S | S | P |
| | APO09 | Gestionar los Acuerdos de Servicio | S | | | S | S | S | P | S | S | S | S | | S | P | S | | |
| | APO10 | Gestionar los Proveedores | | S | | P | S | S | P | S | P | S | S | | S | S | S | | S |
| | APO11 | Gestionar la Calidad | S | S | | S | P | | P | S | S | | S | | P | S | S | S | S |
| | APO12 | Gestionar el Riesgo | | P | | P | | P | S | S | S | P | | | P | S | S | S | S |
| | APO13 | Gestionar la Seguridad | | P | | P | | P | S | S | | P | | | | P | | | |

**Mapeo de las Metas Relacionadas con las TI. Fuente:ISACA**

**Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos *(cont.)***

| | | | Meta relacionada con las TI | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Alineamiento de TI y la estrategia de negocio | Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas | Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI | Riesgos de negocio relacionados con las TI gestionados | Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI | Transparencia de los costes, beneficios y riesgos de las TI | Entrega de servicios de TI de acuerdo a los requisitos del negocio | Uso adecuado de aplicaciones, información y soluciones tecnológicas | Agilidad de las TI | Seguridad de la información, infraestructura de procesamiento y aplicaciones | Optimización de activos, recursos y capacidades de las TI | Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio | Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. | Disponibilidad de información útil y relevante para la toma de decisiones | Cumplimiento de las políticas internas por parte de las TI | Personal del negocio y de las TI competente y motivado | Conocimiento, experiencia e iniciativas para la innovación de negocio |
| | | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **Procesos de COBIT 5** | | | **Financiera** | | | | | | **Cliente** | | **Interna** | | | | | | | **Aprendizaje y Crecimiento** | |
| Construcción, Adquisición e Implementación | BAI01 | Gestionar los Programas y Proyectos | P | | S | P | P | S | S | S | | | S | | P | | | S | S |
| | BAI02 | Gestionar la Definición de Requisitos | P | S | S | S | S | | P | S | S | S | S | P | S | S | | | S |
| | BAI03 | Gestionar la Identificación y la Construcción de Soluciones | S | | | S | S | | P | S | | | S | S | S | S | | | S |
| | BAI04 | Gestionar la Disponibilidad y la Capacidad | | | | S | S | | P | S | S | | P | | S | P | | | S |
| | BAI05 | Gestionar la introducción de Cambios Organizativos | S | | S | | S | | S | P | S | | S | S | P | | | | P |
| | BAI06 | Gestionar los Cambios | | | S | P | S | | P | S | S | P | S | S | S | S | S | | S |
| | BAI07 | Gestionar la Aceptación del Cambio y de la Transición | | | | S | S | | S | P | S | | | P | S | S | S | | S |
| | BAI08 | Gestionar el Conocimiento | S | | | | S | | S | S | P | S | S | | | S | | S | P |
| | BAI09 | Gestionar los Activos | | S | | S | | P | S | | S | S | P | | | S | S | | |
| | BAI10 | Gestionar la Configuración | | P | | S | | S | | S | S | S | P | | | P | S | | |
| Entregar, dar Servicio y Soporte | DSS01 | Gestionar las Operaciones | | S | | P | S | | P | S | S | S | P | | | S | S | S | S |
| | DSS02 | Gestionar las Peticiones y los Incidentes del Servicio | | | | P | | | P | S | | S | | | | S | S | | S |
| | DSS03 | Gestionar los Problemas | | S | | P | S | | P | S | S | | P | S | | P | S | | S |
| | DSS04 | Gestionar la Continuidad | S | S | | P | S | | P | S | S | S | S | S | | P | S | S | S |
| | DSS05 | Gestionar los Servicios de Seguridad | S | P | | P | | | S | S | | P | S | S | | S | S | | |
| | DSS06 | Gestionar los Controles de los Procesos del Negocio | | S | | P | | | P | S | | S | S | S | | S | S | S | S |
| Supervisión, Evaluación y Verificación | MEA01 | Supervisar, Evaluar y Valorar Rendimiento y Conformidad | S | S | S | P | S | S | P | S | S | S | P | | S | S | P | S | S |
| | MEA02 | Supervisar, Evaluar y Valorar el Sistema de Control Interno | | P | | P | | S | S | S | | S | | | | S | P | | S |
| | MEA03 | Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos | | P | | P | S | | S | | | S | | | | | S | | S |

**Mapeo de las Metas Relacionadas con las TI. Fuente:ISACA**

## Principio 2: Cubrir la empresa extremo a extremo

Cobit:

• Integra el gobierno de la empresa TI en el gobierno corporativo.

• Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

Además del objetivo de gobierno, los otros elementos principales del enfoque de gobierno incluyen habilitadores, alcance y roles, actividades y relaciones.

- **Habilitadores de Gobierno**

Los habilitadores de gobierno son los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que o hacia los que las acciones son dirigidas y los objetivos pueden ser alcanzados. Los habilitadores también incluyen los recursos corporativos – por ejemplo, capacidades de servicios (infraestructura TI, aplicaciones, etc.), personas e información. Una falta de recursos o habilitadores puede afectar a la capacidad de la empresa de crear valor.

- **Alcance de Gobierno**

El gobierno puede ser aplicado a toda la empresa, a una entidad, a un activo tangible o intangible, etc. Es decir, es posible definir diferentes vistas de la empresa a la que se aplica el gobierno, y es esencial definir bien este alcance del sistema de gobierno. El alcance de COBIT 5 es la empresa – pero en esencia, COBIT 5 puede tratar con cualquiera de las diferentes vistas.

- **Roles, Actividades y Relaciones**

Un último elemento son los roles, actividades y relaciones de gobierno. Definen quién está involucrado en el gobierno, como se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno. En COBIT 5, se hace una clara diferenciación entre las actividades de gobierno y de gestión en los dominios de gobierno y gestión, así como en la interconexión entre ellos y los actores implicados.

## Principio 3: Aplicar un marco de referencia único e integrado

Cobit es un marco único e integrado por estos motivos:

• Se alinea con otros estándares y marcos de referencia relevantes y  por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno.

• Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no técnico y tecnológicamente agnóstico.

• Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente.

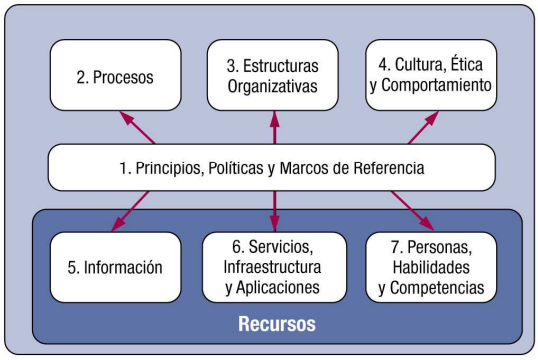
• Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA.

## Principio 4: Hacer posible un enfoque holístico

Los habilitadores son factores que, individual y colectivamente, influyen sobre si algo funcionará – en este caso, el gobierno y la gestión de la empresa TI. Los habilitadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes habilitadores deberían conseguir.

El marco de referencia COBIT 5 describe siete categorías de habilitadores:

Figura 12—Catalizadores Corporativos COBIT 5




**Catalizadores Corporativos. Fuente:ISACA**

**1- Principios, políticas y marcos de referencia.**

Son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.

A partir de este habilitador el resto están interconectados entre sí, es decir, se benefician de los resultados de otros habilitadores y proporcionan una salida para beneficio del resto.

**2- Procesos.**

Describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

**3- Estructuras organizativas.**

Son las entidades de toma de decisiones clave en una organización.

**4- Cultura, ética y comportamiento.**

Estos factores de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.

**5- Información.**

Impregna a toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.

**6- Servicios, infraestructuras y aplicaciones.**

Incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

**7- Personas, habilidades y competencias.**

Están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

Estas tres últimas están integradas conjuntamente como habilitadores de recursos. Son también recursos corporativos que también necesitan ser gestionados y gobernados. Por ejemplo, la información necesita ser gestionada como un recurso. Alguna información, tal como informes de gestión y de inteligencia de negocio son importantes habilitadores para el gobierno y la gestión de la empresa.

Todos los habilitadores tienen un conjunto de dimensiones comunes. Son las siguientes cuatro:

**• Grupos de interés**

Cada habilitador tiene grupos de interés (partes que juegan un rol activo y/o tienen un interés en el habilitadores). Por ejemplo, los procesos tienen diferentes Metas que realizan actividades y/o tienen un interés en los resultados del proceso; las estructuras organizativas tienen grupos de interés, que son parte de las estructuras. Los grupos de interés pueden ser internos o externos a la empresa, cada uno de ellos con sus propias necesidades e intereses, algunas veces contrarios entre sí. Las necesidades de los grupos de interés se traducen en metas corporativas, que a su vez se traducen en objetivos de TI para la empresa.

**• Metas**

Cada habilitador tiene varias metas, y los habilitadores proporcionan valor por la consecución de dichas metas. Las metas pueden ser definidas en términos de:

- Resultados esperados del habilitador.
- Aplicación u operación del habilitador en sí mismo.

Las metas del habilitador son el paso final en la cascada de metas de COBIT 5. Las metas pueden ser divididas a su vez en diferentes categorías:

a) **Calidad intrínseca**: Medida en que los habilitadores trabajan de manera precisa, objetiva y proporcionan resultados precisos, objetivos y de confianza.

b) **Calidad contextual**: Medida en que los habilitadores y sus resultados son aptos para el propósito dado el contexto en el que operan. Por ejemplo, los resultados deben ser relevantes, completos, actuales, apropiados, consistentes, comprensibles y fáciles de usar.

c) **Accesibilidad y seguridad**: Medida en que los habilitadores y sus resultados son accesibles y seguros, tales como:

• Los habilitadores están disponibles cuando, y si, se necesitan.

• Los resultados son asegurados, es decir, el acceso está restringido a aquellos autorizados y que lo necesitan.

**• Ciclo de vida**

Cada habilitador tiene un ciclo de vida, desde el comienzo pasando por su vida útil / operativa hasta su eliminación. Esto aplica a información, estructuras, procesos, políticas, etc. Las fases del ciclo de vida consisten en:

- Planificar (incluye el desarrollo y selección de conceptos)
- Diseñar
- Construir / adquirir / crear / implementar
- Utilizar / operar
- Evaluar / monitorizar
- Actualizar / eliminar

**• Buenas prácticas**

Para cada uno de los habilitadores, se pueden definir buenas prácticas. Las buenas prácticas soportan la consecución de los objetivos del habilitador. Las buenas prácticas proporcionan ejemplos y sugerencias sobre cómo implementar de la mejor manera el habilitador y qué productos o entradas y salidas son necesarias.

En la gestión del rendimiento de los habilitadores, se tienen que formular las siguientes preguntas y posteriormente ser respondidas regularmente (basándose en métricas):

- Indicadores de retraso (en que medida se alcanzan las metas):

• ¿Se atienden las necesidades de las partes interesadas?

• ¿Se alcanzan las metas del habilitador?

- Indicadores de avance (funcionamiento actual del habilitador):

• ¿Se gestiona el ciclo de vida del habilitador?

• ¿Se aplican buenas prácticas?

## Principio 5: Separar el gobierno de la gestión

La distinción entre gobierno y gestión es:

**• Gobierno**

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

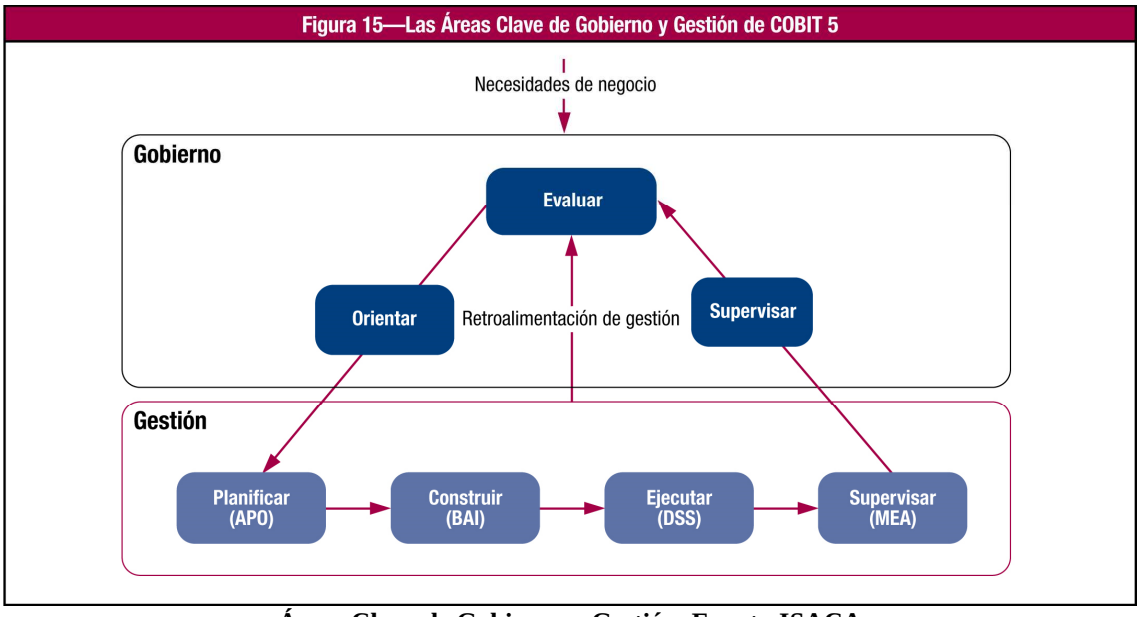
En la mayoría de las empresas, el gobierno es responsabilidad del consejo de administración bajo la dirección de su **presidente**.

**• Gestión**

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo la dirección del **CEO**.

Figura 15—Las Áreas Clave de Gobierno y Gestión de COBIT 5




**Áreas Clave de Gobierno y Gestión. Fuente:ISACA**

Las interacciones entre gobierno y gestión se pueden definir para cada tipo de habilitador de la siguiente manera:

- **Procesos**

Se distingue entre los procesos de gobierno y de gestión, incluyendo conjuntos específicos de prácticas y actividades para cada uno.

- **Información**

El modelo de procesos describe las entradas y salidas de los distintos procesos basados en prácticas a otros procesos, incluyendo la información intercambiada entre los procesos de gobierno y gestión. La información empleada en evaluar, orientar y supervisar la TI empresarial es intercambiada entre gobierno y gestión tal y como se describe en las entradas y salidas del modelo de procesos.

- **Estructuras organizativas**

En cada empresa, se definen varias estructuras organizativas. En función de su composición y ámbito de decisiones, las estructuras pueden ubicarse en el área de gobierno o en el de gestión. Dado que el gobierno trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno. Por ejemplo, decidir sobre la cartera de inversiones y establecer el umbral de riesgo y las decisiones y operaciones que las implementan.

- **Principios, políticas y marcos**

Los principios, políticas y marcos son los vehículos mediante los cuales las decisiones de gobierno son sancionadas en la empresa y por esa razón son una interacción entre las decisiones de gobierno (establecer orientaciones) y gestión (ejecutar las decisiones).

- **Cultura, ética y comportamientos**

El comportamiento también es un habilitador clave del buen gobierno y la gestión empresarial. Se establece al más alto nivel (liderando mediante el ejemplo) y es, por tanto, una interacción importante entre el gobierno y la gestión.

- **Personas, habilidades y competencias**

Las actividades de gobierno y de gestión requieren conjuntos de habilidades distintas, pero una habilidad esencial para miembros tanto del órgano de gobierno como de gestión es entender tanto las propias actividades como cuáles son sus diferencias.

- **Servicios, infraestructura y aplicaciones**

Se requieren servicios, soportados por las aplicaciones e infraestructura, para proporcionar la información adecuada al órgano de gobierno y soportar las actividades de gobierno a la hora de evaluar, establecer la orientación y supervisar.

El modelo de referencia de procesos divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

• **Gobierno**

Contiene cinco procesos de gobierno. Dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).

• **Gestión**

Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM) y proporciona cobertura extremo a extremo de las TI.

- Alinear, Planificar y Organizar (Align, Plan and Organise, APO)
- Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)
- Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

En total son 37 procesos de gobierno y gestión


**Modelo de Referencia de Procesos. Fuente:ISACA**

Hay nuevos y modificados procesos, en particular los siguientes:

APO03, APO04, APO05, APO06, APO08, APO13, BAI05, BAI08, BAI09, DSS05 y DSS06.

## Guía de Implantación

Se debe realizar de arriba hacia abajo, involucrando a todas las partes implicadas.

Contexto empresarial, factores:

• Ética y cultura

• Leyes aplicables, regulaciones y políticas

• Misión, visión y valores

• Políticas y prácticas de gobierno

• Plan de negocio y perspectivas estratégicas

• Modelo operativo y nivel de madurez

• Estilo de gestión

• Umbral de riesgo

• Capacidades y recursos disponibles

• Prácticas de la industria

Algunos factores críticos de éxito para una implementación con éxito son:

• Que la alta dirección proporcione la orientación y directrices para la iniciativa, así como un decidido compromiso y apoyo.

• Todas las partes deben apoyar los procesos de gobierno y gestión, para entender el negocio y las metas de TI.

• Asegurar la comunicación efectiva y la habilitación de los cambios necesarios.

• Personalizar COBIT y otras buenas prácticas y estándares empleados para ajustarlos al entorno único de la empresa.

• Enfocarse en resultados inmediatos (quick wins) y priorizar las mejoras más beneficiosas que sean más sencillas de implementar.

La implementación del ciclo de vida proporciona a las empresas una manera para solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones. Se dividirá en las siete fases del ciclo de vida.

El caso de negocio es una valiosa herramienta disponible para la dirección que dirige la creación de valor de negocio. Como mínimo, el caso de negocio debería incluir lo siguiente:

• Los objetivos de beneficio de negocio, su alineación con la estrategia de negocio y los propietarios asociados del beneficio (quién dentro del negocio será responsable de asegurarlos). Esto podría basarse en puntos débiles o desencadenantes de eventos.

• Los cambios de negocio requeridos para crear el valor previsto. Esto podría basarse en comprobaciones y análisis de deficiencias de capacidad y deberían indicar claramente qué está dentro del ámbito y qué está fuera de él.

• Las inversiones precisas para realizar los cambios de gobierno y gestión de TI corporativa (basado en estimaciones de proyectos necesarios).

• Los costes ordinarios de TI y de negocio.

• Los beneficios esperados de operar en el nuevo modo.

• El riesgo inherente en los puntos anteriores, incluyendo cualquier restricción o dependencia (basado en los desafíos y factores de éxito).

• Roles, responsabilidades y obligaciones relativas a la iniciativa.

• Cómo la inversión y la creación de valor serán supervisadas a través del ciclo de vida económico y cómo se usarán las métricas (basado en metas y métricas).

La **fase 1** comienza con el reconocimiento y aceptación de la necesidad de una iniciativa de implementación o mejora.

Identifica los puntos débiles actuales y desencadena y crea el ánimo de cambio a un nivel de dirección ejecutiva.

La **fase 2** se concentra en definir el alcance de la iniciativa de implementación o mejora empleando el mapeo de COBIT de metas empresariales con metas de TI a los procesos de TI asociados, y considerando cómo los escenarios de riesgos podrían destacar los procesos clave en los que focalizarse. Los diagnósticos de alto nivel también pueden ser útiles para delimitar y entender áreas de alta prioridad en las que hacer foco. Se lleva a cabo una evaluación del estado actual y se identifican los problemas y deficiencias mediante la ejecución de un proceso de revisión de capacidad. Se deberían estructurar iniciativas de gran escala como múltiples iteraciones del ciclo de vida – para cada iniciativa de implementación que exceda de seis meses, existe un riesgo de perder el impulso, el foco y la involucración de las partes interesadas.

Durante la **fase 3**, se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos (quick wins) y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser

aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

La **fase 4** planifica soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados.

Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

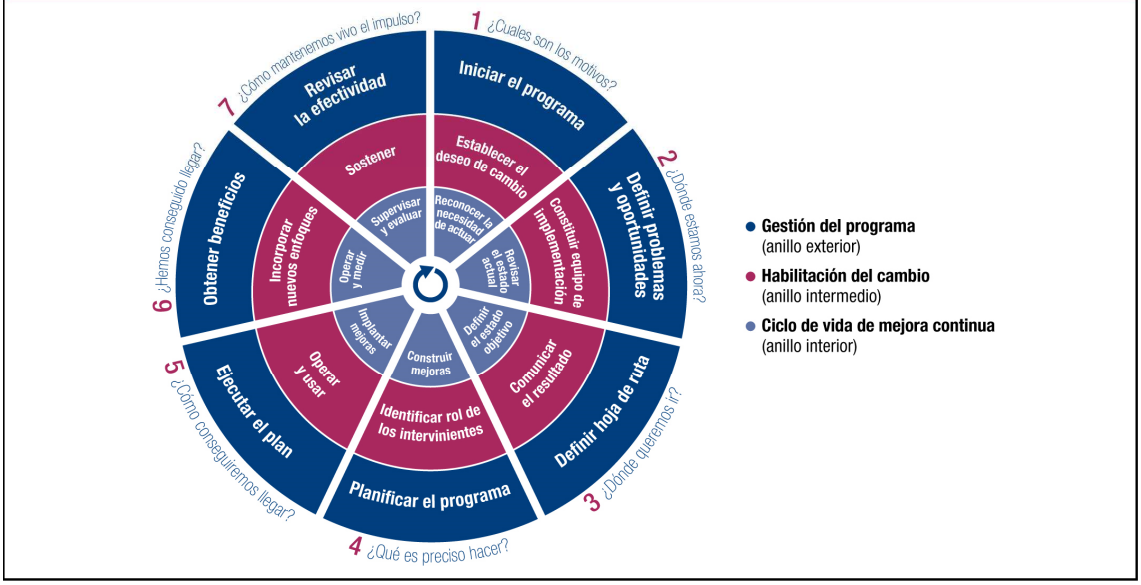
Las soluciones propuestas son implementadas en prácticas día a día en la **fase 5**. Se pueden definir las mediciones y establecer la supervisión empleando las metas y métricas de COBIT para asegurar que se consigue y mantiene la alineación con el negocio y que el rendimiento puede ser medido. El éxito requiere el compromiso y la decidida apuesta de la alta dirección así como la propiedad por las partes afectadas a nivel TI y de negocio.

La **fase 6** se focaliza en la operación sostenible de los nuevos o mejorados habilitadores y de la supervisión de la consecución de los beneficios esperados.

Durante la **fase 7**, se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua.

A lo largo del tiempo, el ciclo de vida debería seguirse de modo iterativo, al tiempo que se construye un modelo sostenible de gobierno y gestión de TI corporativa.

**Figura 17—Las Siete Fases de la Implementación del Ciclo de Vida**




**Siete fases del Ciclo de Vida. Fuente:ISACA**

## El modelo de capacidad de los procesos de COBIT 5

Existen seis niveles de capacidad que se pueden alcanzar por un proceso, incluida la designación de “proceso incompleto” si las prácticas definidas en el proceso no alcanzan la finalidad prevista:

**• 0 Proceso incompleto**

El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

**• 1 Proceso ejecutado** (un atributo)

El proceso implementado alcanza su propósito.

**• 2 Proceso gestionado** (dos atributos)

El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

**• 3 Proceso establecido** (dos atributos)

El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

**• 4 Proceso predecible** (dos atributos)

El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

**• 5 Proceso optimizado** (dos atributos)

El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo.

Esta guía de buenas prácticas concede beneficios a varios niveles.

- Con respecto al negocio

- Alinear los servicios de TI a las necesidades del negocio.

- Asegura que los servicios de TI se encuentren alineados para satisfacer las necesidades del negocio.

- Reducir costes y generar negocio.

- Tomar decisiones con base a indicadores de negocio y de TI.

- Entregar servicios a un coste efectivo.

- Aumentar el perfil y competitividad de las organizaciones de TI.

- Con respecto al cliente:

- Aumentar la satisfacción del cliente

- Visión clara de la capacidad del departamento de TI

- Promover la adopción integral de buenas prácticas para la entrega de servicios que cubran las necesidades del negocio y los requerimientos del cliente.

- Con respecto al departamento de TI

- Entender las mejores prácticas, sus objetivos, beneficios y posibles problemas con la Gestión de Servicios de TI.

- Proporcionar la habilidad para medir la calidad de los servicios proporcionados por los departamentos de TI.

- Cambia la visión de los departamentos de TI centrados en la tecnología, a enfocarse a los servicios y a las buenas prácticas o procesos.

- Con respecto a la calidad

- Proporcionar una adecuación a la gestión de la calidad.

- Maximizar la calidad y eficiencia del servicio.

- Reducir los riesgos asociados al servicio de TI.

- Minimizar el tiempo de ciclos de cambios y mejora de resultados con base a métricas.

- Proporcionar control, mayor eficiencia y oportunidades de mejora.

# 4.3.2 ITIL

ITIL es la abreviatura de Information Technology Infrastructure Library, una serie de buenas prácticas creadas en 1980 para la gestión de servicios, que se han ido adaptando a lo largo de los años, siendo la versión más reciente la V3 del año 2011.

Están recopilados en cinco libros que abarcan el ciclo de vida del servicio: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio. El contenido de dichos libros se ve complementado con publicaciones adicicionales.

**La gestión de servicios se puede explicar en cuatro puntos:**

- Entender los servicios que se proveen.
- Asegurar que esos servicios realmente facilitan los resultados que sus clientes quieren alcanzar.
- Comprender el valor de los servicios a sus clientes.
- Endender y gestionar todos los gastos y riesgos asociados a cada servicio.


**Ciclo de vida de ITIL. Fuente: http://www.tecnofor.es/**

El diagrama muestra como funciona el ciclo de vida, iniciándose con un cambio en los requisitos de la entidad. Dichos requisitos se identifican y acuerdan dentro de la **Estrategia del Servicio**, pasándose posteriormente al **Diseño del Servicio**, fase en la cual se produce todo lo necesario para la realización del servicio, llegando a la **Transición del Servicio**. En dicha fase se evalúa, verifica y valida todo lo anterior y una vez aceptado se pasaría a la **Operación del Servicio**. La **Mejora Continua del Servicio** implica que si en algún momento se identifican oportunidades para mejorar las oportunidades o fallos en cualquiera de las etapas anteriores se deberían modificar.

1. **Estrategia del Servicio**

Su propósito radica en la búsqueda de un servicio que satisfaga al cliente a través de estudios de mercado y las diferentes posibilidades que pueda ofrecer el mismo. Se divide en tres procesos: Gestión Financiera, Gestión del Portafolio y Gestión de la demanda.

2. **Diseño del Servicio**

Identificados los servicios donde realizar la intervención, esta fase se encarga de analizar todo el montante que pueda suponer antes de ponerlo en práctica. Hay ocho procesos en esta fase: Gestión del Catálogo de Servicios, Gestión de Niveles de Servicios, Gestión de la Disponibilidad, Gestión de la Capacidad, Gestión de la Continuidad de los Servicios de TI, Gestión de Proveedores, Gestión de la Seguridad de Información, Coordinación del Diseño*.

3. **Transición del Servicio**

Antes de ponerlo en funcionamiento se evaluará, verificará y validará todo lo anterior en un escenario de prueba pero siempre cerca del nivel real esperado. Se distribuye en siete procesos: Gestión de la Configuración y Activos, Gestión del Cambio, Gestión del Conocimiento, Planificación y Soporte a la Transición, Gestión del Lanzamiento y Despliegue, Gestión Validación y Pruebas y Evaluación del cambio.

4. **Operación del Servicio**

En esta fase se monitoriza todo lo acontecido al servicio para garantizar que se está cumpliendo lo acordado en apartados anteriores a través de los siguientes cinco procesos: Gestión de Incidentes, Gestión de Problemas, Cumplimiento de Solicitudes, Gestión de Eventos, Gestión de Accesos.

5. **Mejora Continua del Servicio**

La última fase, en la cual se mide todo lo relacionado con el servicio para arrojar unos resultados referentes a los mismos que se puedan medir, estudiar y evaluar con el fin de corregir posibles problemas ocasionados o mejoras que en su momento no se tuvieron en cuenta durante el ciclo de vida del servicio.

# 4.3.3 CMMI

La Integración del Modelo de Capacidad y Madurez o CMMI, viene de las siglas inglesas Capability Maturity Model Integration. Según su definición se trata de un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software.  La versión más actual es la 1.3 liberada en el año 2010.

## 4.3.4 Círculo de Deming

Es una metodología que se basa en la mejora continua de la calidad mediante cuatro pasos: **Planear, Hacer, Verificar** y **Actuar**.


**Círculo de Deming. Fuente: mgifil.files.wordpress.com**

- **Planear**: se establecen los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización.
- **Hacer**: implementar los procesos.
- **Verificar**: realizar un seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.
- **Actuar**: tomar acciones para mejorar continuamente el desempeño de los procesos.

# 5. Legislación en un Contact Center

La protección de datos es un derecho reconocido tanto en la Constitución Española como en la Unión Europea, cuya protección se lleva a cabo en nuestro país a través de la Ley Orgánica de Protección de Datos. Actualmente consta en vigor la Ley Orgánica 15/1999 que adapta la legislación española al marco europeo, a través de la directiva 95/46/CE.

## 5.1 LOPD

El RLOPD 1720/2007 aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de carácter personal (RLOPD), la cual ampara a los ciudadanos españoles y que según el propio escrito tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal, por lo que las empresas, en este caso los CC, tienen que tener especial cuidado en no vulnerar estos derechos a la hora de tratar con los datos de carácter personal, es decir, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, que usan en sus transacciones.

El objetivo de la ley involucra tanto al tratamiento automatizado como al no automatizado de los datos en soportes físicos, que a posteriori se usen en sectores públicos o privados. El ámbito territorial de aplicación para el tratamiento de datos, es decir, cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias, se regirá en territorio español, exceptuando los supuestos en los que el responsable del tratamiento no esté establecido en territorio español, en los cuales se regirá por otras normas europeas o mundiales en base a lo dictado por la ley.

Los apartados sucesivos harán referencia a dicha ley total o parcialmente en las partes a desarrollar.

### 5.1.1 Principios de protección y calidad de los datos

Atendiendo al **artículo 8** sobre los **principios de protección y de calidad**, los datos que se van a utilizar durante la actividad de cualquier CC:

1- Deberán ser tratados de forma leal y lícita y se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2- Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3- No podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4- Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5- Serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

6- Serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

   No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

7- Serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

En los casos en los cuales los datos sean utilizados con fines estadísticos, históricos o científicos el punto tres del apartado anterior no se recogería como “incompatible” si los datos se usan para otras finalidades diferentes con las que fueron recogidos en su momento. En el caso del apartado seis, sobre la cancelación de dichos datos, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

La subcontratación (outsourcing) es algo bastante común en el ámbito de los CC, por lo que respecta al al cumplimiento de la ley con el **tratamiento y la cesión de datos** que supone su revelación a una persona distinta del interesado, deben de cumplirse en base a lo dictaminado por el **artículo 10**.

1- Únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello, entendiendo por consentimiento como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

2- No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

   a. Lo autorice una norma con rango de ley o una norma de derecho comunitario.

   b. Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3- Podrán tratarse sin necesidad del consentimiento del interesado cuando:

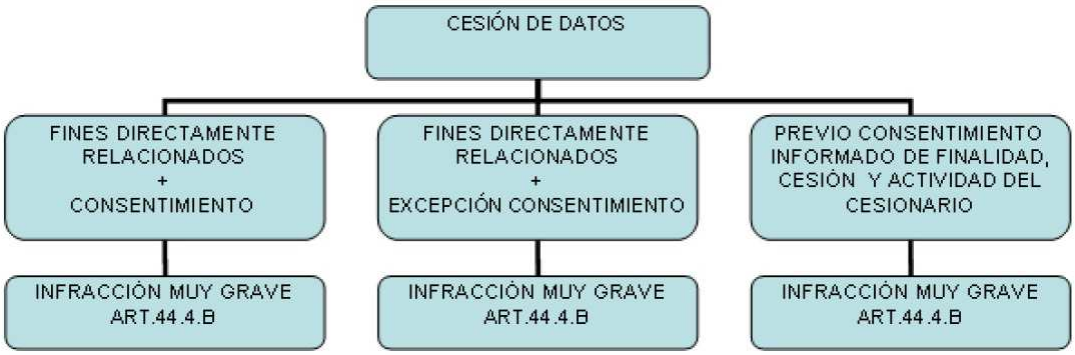
   a. Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

   b. Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

4- Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

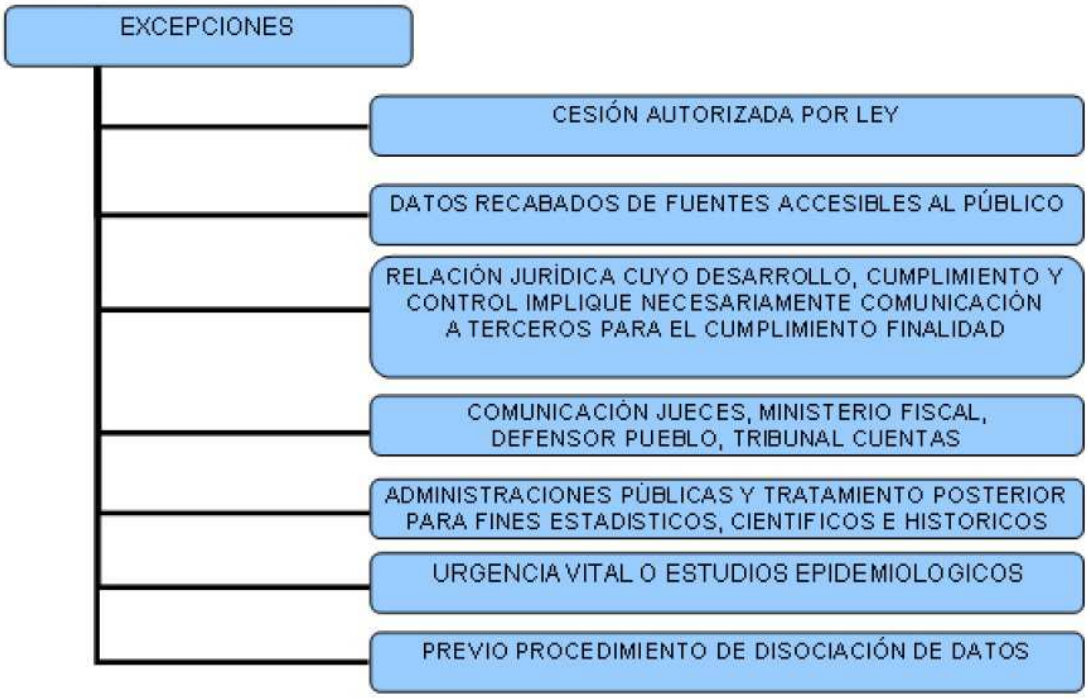
La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

En el siguiente esquema se representan las diferentes opciones en el uso de la cesión de datos y las infracciones relacionadas con su incumplimiento:




**La cesión de datos. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**

Las **excepciones** indicadas anteriormente se pueden ver en este esquema:




**Excepciones. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**

A la hora de recabar toda la información de los **datos del afectado**, este deberá dar su **consentimiento** y se deberá informar según en base a lo dictaminado por el **artículo 12**.

1- El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

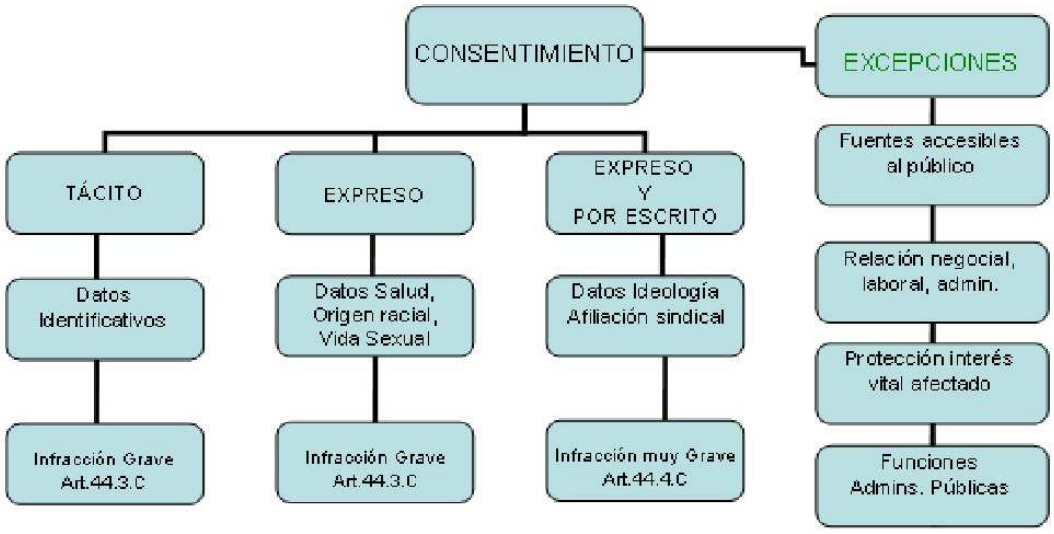
2- Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario, la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos (podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados). En caso contrario, el consentimiento será nulo.

3- Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

La **revocación del consentimiento** podrá ser ejercida por el afectado en base al **artículo 17** a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento.

En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

En el siguiente gráfico se identifican los tipos de consentimientos, así como las infracciones por su incumplimiento y los supuestos que quedan excluidos, explicadas anteriormente.




**El consentimiento. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**

### 5.1.2 Encargado/Responsable del tratamiento

Según el **artículo 20**, la **relación entre el responsable y el encargado del tratamiento** deberá cumplir los siguientes puntos:

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Como hemos hablando anteriormente, la **subcontratación** (u outsourcing) es algo muy utilizado en los ambientes de los CC por lo que deberán regirse en base **al artículo 21** de la ley:

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

   a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

   Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

   b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

   c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

   En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el **artículo 20.3** de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Las pautas que debe cumplir el encargado del tratamiento para la **conservación de los datos** quedan reflejadas en el **artículo 23**.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

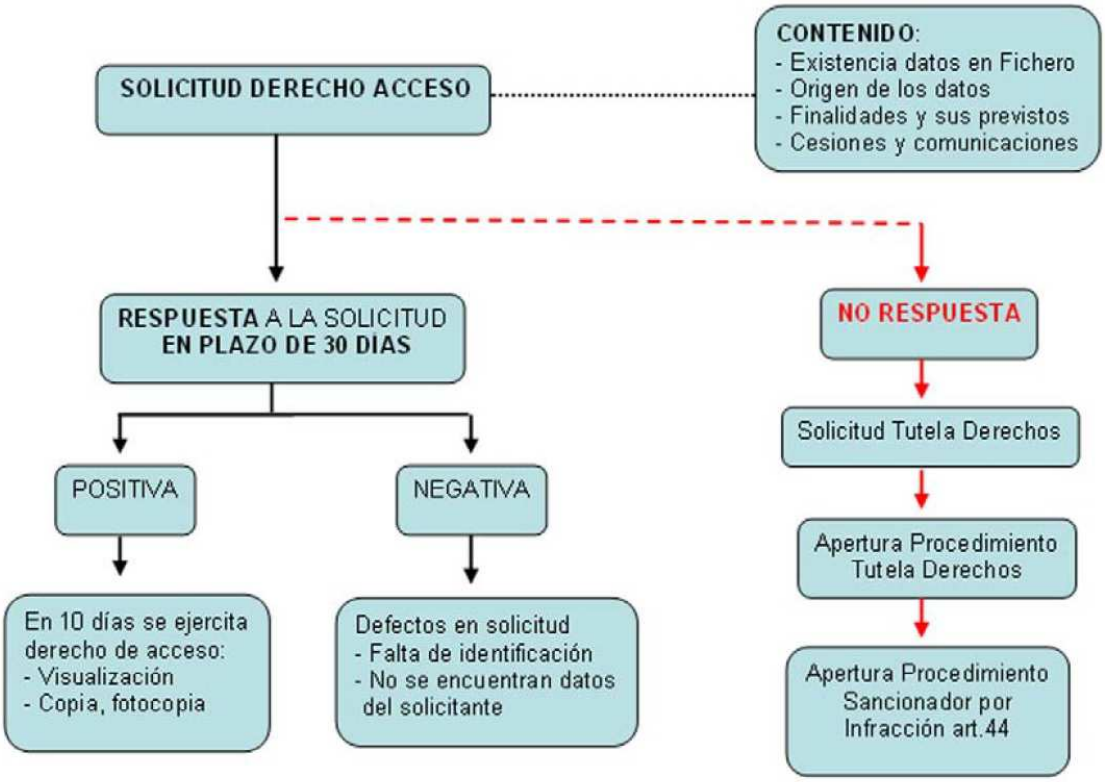
No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

### 5.1.3 Derechos de acceso, rectificación, cancelación y oposición

Se desarrollan desde el **artículo 23 al 36**, son los llamados **derechos ARCO**: **acceso** (artículos del **27 al 30**), **rectificación**, **cancelación** (artículos del **31 al 33**) y **oposición** (artículos **34 al 36**).

- **Derecho de acceso**: es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. En el siguiente esquema se representa como ejercer el derecho al mismo.

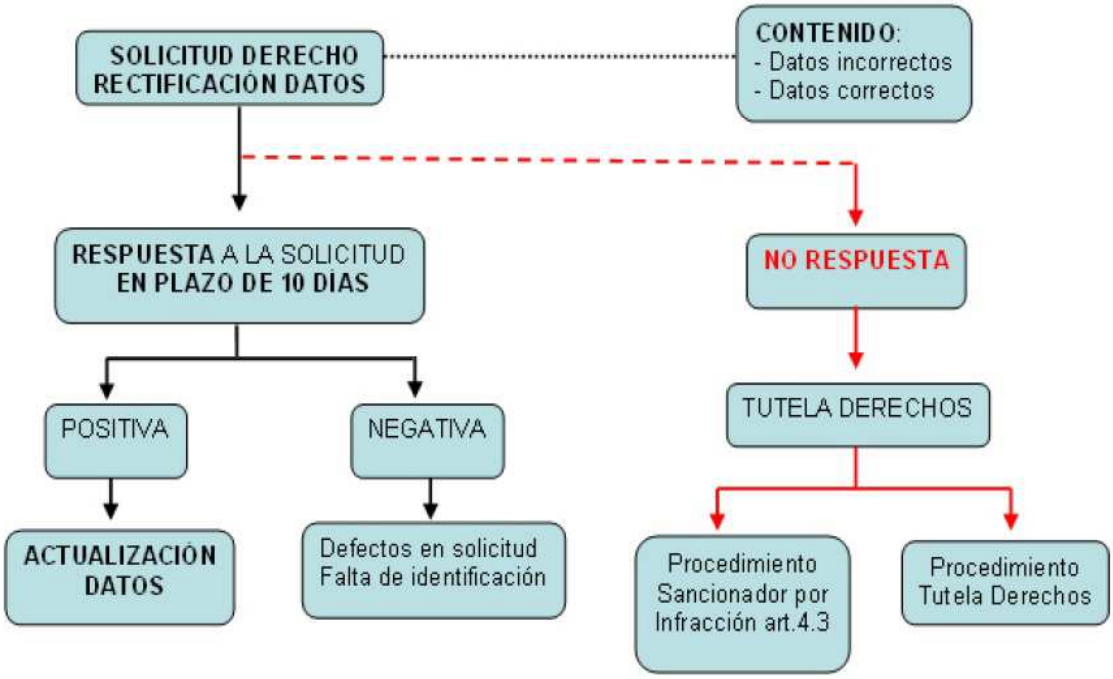



**Solicitud de acceso. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**

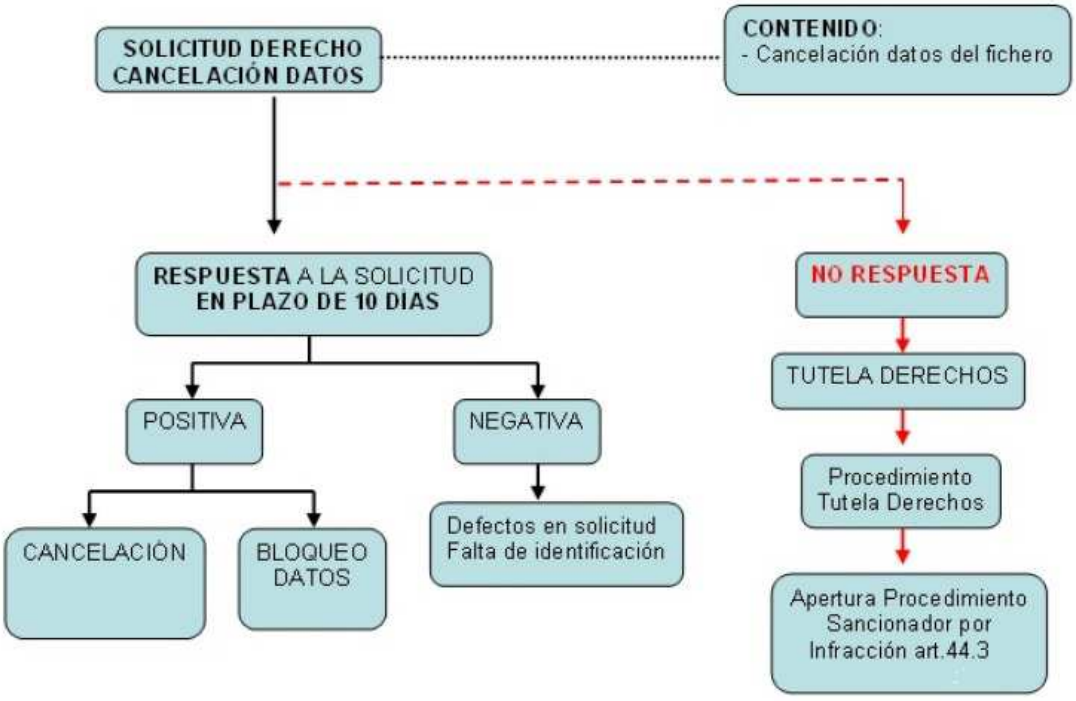
- **Derecho de rectificación y cancelación**: son los derechos del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. A través de estos derechos el afectado podrá o bien rectificar los datos que no se correspondan o cancelar aquellos que ya no quiera que estén bajo tratamiento.

Se entenderá por **cancelación** al procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo

de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos. En el siguiente esquema se representa como ejercer el derecho a los mismos.




**Solicitud de rectificación. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**




**Solicitud de cancelación. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**

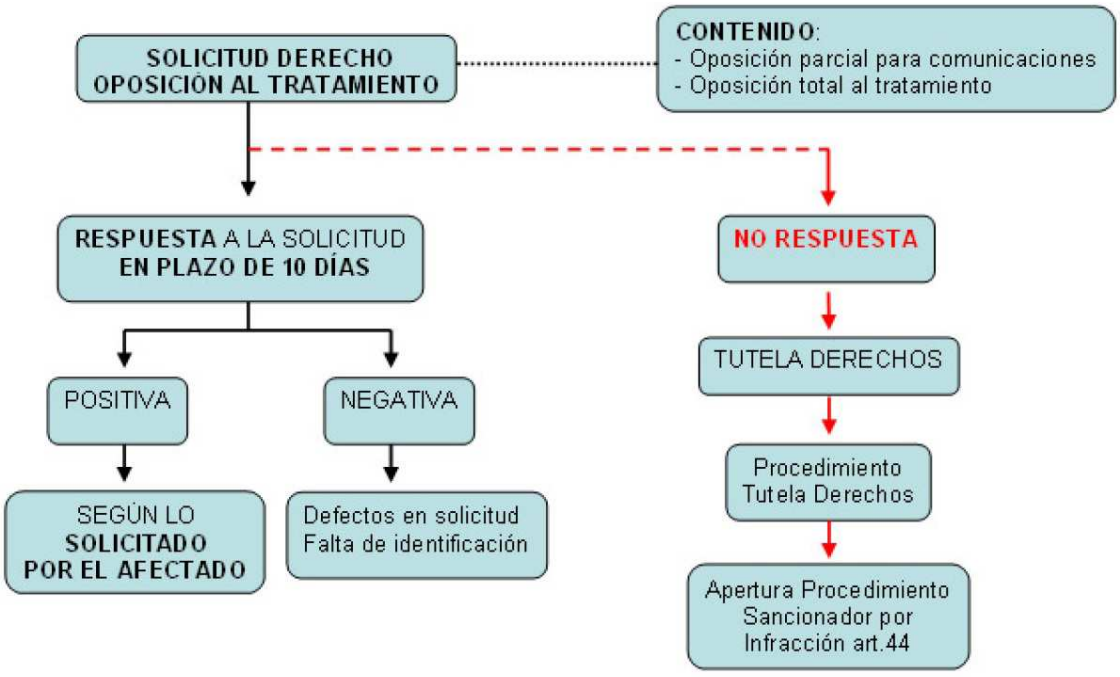
- **Derecho de oposición**: es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

    a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

    b) Cuando se trate de ficheros que tengan por finalidad la realización de **actividades de publicidad y prospección comercial**, en los términos previstos en el **artículo 51** de este reglamento, cualquiera que sea la empresa responsable de su creación.

    c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

En el siguiente esquema se representa como ejercer el derecho al mismo.




**Solicitud de oposición. Fuente: Curso de adaptación a la LOPD. Formación sin barreras**

Poseen las siguientes características:

- Son **derechos personalísimos**, es decir, solo pueden ser ejercidos por el titular de los datos, por su representante legal (en caso de ser menor o de incapacidad) o por un representante voluntario expresamente designado para el ejercicio del derecho que se trate. En caso de no ser el titular de los datos o no acredite

debidamente que actúa en su representación, el responsable del derecho denegará el ejercicio de estos derechos.

- Son derechos **independientes**, de tal forma que no se corresponden en el caso de que uno sea requisito previo de otro.
- Las **obligaciones** del responsable del fichero son facilitar el ejercicio de estos derechos, dar al afectado una respuesta en los plazos legales establecidos.
- El **procedimiento** a seguir se llevará a cabo utilizando medios gratuitos y sencillos que el responsable del fichero tiene la obligación de facilitar al afectado o bien en los términos que establece el artículo 25.
- La **Agencia Española de Protección de Datos** (AEPD) servirá de regulador en el caso de que el responsable del fichero no atienda al ejercicio de los derechos expresados por el afectado dentro de los plazos establecidos.

La mayoría de los CC no suelen gestionar este tipo de ejercicios ya que normalmente, o bien al ser subcontrataciones dependen del cliente o bien se hacen manualmente por departamentos ajenos a estos centros.

### 5.1.4 Disposiciones aplicables a determinados ficheros de titularidad privada

Se entenderán por este tipo a los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

**A) Ficheros de información sobre solvencia patrimonial y crédito**

Están redactados en los **artículos del 37 al 4**4 y tratan sobre la morosidad del afectado, recogiendo datos sobre deudas vencidas y no pagadas. Se debe informar de su inclusión en dichos fichero al afectado y solo podrán ser consultados por terceros cuando se pretenda enjuiciar la solvencia económica de dicho afectado.

Normalmente son usados en centros de cobros donde una entidad exige los pagos pendientes de uno de sus clientes o a la hora de contratar cualquier producto o servicio para medir el grado de solvencia que puede tener una persona.

**B) Tratamientos para actividades de publicidad y prospección comercial**

Se rigen por los **artículos** comprendidos entre el **45 y el 51**, incluyendo ambos. Se comprende por afectados de este tratamiento a quienes se dediquen a la recopilación

de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros.

Su utilización solo podrá ser usada en casos en los que figuren en alguna de las fuentes accesibles al público y siempre y cuando el cliente no haya manifestado su negativa u oposición al uso de ellos, o bien si han sido facilitados por el propio afectado con su consentimiento para las finalidades comerciales determinadas, explícitas y legítimas. Se podrán ejercer cualquiera de los derechos ARCO que hemos hablado previamente para el tratamiento en este tipo de ficheros.

En los ámbito de los CC, es bastante frecuente el uso de estos ficheros con el de captar clientes o para dar a conocer nuevos productos a través de cualquier canal. Aquí entraría también en juego las llamadas “Listas Robinson”, las cuales una persona o entidad puede incluirse en ellas para no ser objeto de estos ficheros a la hora de no ser objetivo de cualquier campaña de publicidad o marketing telefónico, por ejemplo.

### 5.1.5 Obligaciones previas al tratamiento de los datos

**A) Creación, modificación o supresión de ficheros de titularidad pública**

Se entenderá por fichero de titularidad pública a los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

Esto incumbe a las Administraciones públicas que funcionan como responsable del fichero. Los CC a no ser que sea uno propio y público no estarían regulados bajo los artículos relacionados con esta parte.

**B) Notificación e inscripción de los ficheros de titularidad pública o privada**

La notificación deberá ser realizada a la Agencia Española de Protección de Datos, por el órgano competente de la Administración responsable del fichero para su inscripción, en el caso de ser un fichero de titularidad pública, o en caso privado, por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La inscripción será realizada por el elemento regulador de esta ley, la AEPD, una vez que se haya dictado su resolución.

Como en el apartado anterior, estos trámites afectan al responsable del fichero los cuales deberán realizar dicha notificación e inscripción de acuerdo a lo dictaminado con

la ley. Las plataformas de CC que no se encuentren en este supuesto harán caso omiso y el resto deberán realizarlo en base a lo estipulado.

### 5.1.6 Transferencias internacionales de datos

La globalización también lleva afectando a los Contact Centers desde hace décadas, por lo que cada vez más, muchas empresas deciden exteriorizar sus servicios (offshoring), transportándolos a otros países extranjeros, con el fin de reducir costes o aumentar beneficios, es decir, de hacer más competitiva a la empresa. Con lo que respecta a España, la zona de Latinoamérica está siendo uno de los destinos más recurridos a la hora de externalizar servicios, gracias en parte al uso del castellano en estos países.

Para la cumplimiento y realización de los servicios, los datos deben de transportarse fueras de las fronteras españolas, pero la LOPD regula este tipo de transferencias internacionales a través de los **artículos** comprendidos entre **66 y el 70**, establecidos en el Real Decreto 1720.

Se conocerá por transferencia internacional al tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

La **autorización y notificación de las transferencias de datos internacionales** quedan relejadas en el **artículo 66** del Real Decreto por el cual dicta que será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador, la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una **transferencia de datos de carácter personal a un país tercero**, aporte las garantías a las que se refiere el **artículo 70** del presente reglamento.

**- La autorización no será necesaria:**

a) Cuando el Estado en el que se encontrase el importador, es decir, la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero, ofrezca un nivel adecuado de protección.

   Según la AEPD se consideran países con nivel de protección adecuado al que presta la Ley Orgánica 15/1999, los Estados Miembros de la Unión Europea, Islandia, Liechtenstein, Noruega y los Estados que la Comisión Europea ha declarado que garantizan un nivel de protección adecuado: Suiza, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva

Zelanda, las entidades estadounidenses adheridas a los principios de «Puerto Seguro», Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos y los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos de América.

b) Cuando la transferencia se encuentre en uno de los siguientes supuestos:

1) La transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

2) La transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

3) La transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.

4) Se refiera a transferencias dinerarias conforme a su legislación específica.

5) El afectado haya dado su consentimiento inequívoco a la transferencia prevista.

6) La transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

7) La transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

8) La transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

9) La transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

10) La transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

c) En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

**- La autorización será necesaria:**

1) Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección (véase la lista del apartado anterior), será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

2) La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

3) En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, en algún tipo de situaciones.

4) También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

## 5.1.7 Códigos tipo

Están recogidos **entre los artículos 71 y 78** y tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Códigos como el “Código Deontológico de la Empresa de Telemarketing” o “Código regulador del servicio de listas Robinson” creados por Agencia Española de Marketing (AEMT-FECEMD) sirven para marcar unas pautas acordes para el cumplimiento de la ley.

#### 5.1.7.1 Código deontológico de la empresa de Telemarketing

Se crea para definir las reglas ético/profesionales que las empresas de Telemarketing y por extensión, en una plataforma de Contact Center, se deben preservar. Trata sobre los siguientes puntos:

- **Ley y autorregulación aplicable:**

  Las empresas de Telemarketing deberán asegurarse de que toda emisión de llamadas cumpla con la legislación y con las prácticas de autorregulación aplicables en el país de origen de la llamada, excepto en los casos específicos citados en estos principios. Con respecto a la recepción, las llamadas deberán cumplir con la legislación nacional y con las prácticas de autorregulación aplicables en el país donde es atendida la llamada.

- **Cualificación de los teleoperadores:**

  Las llamadas serán realizadas por personal cualificado, personal que ha superado un proceso de selección, ha sido especialmente formado y preparado por la empresa. Estas llamadas podrán ser realizadas en los locales de las empresas de Telemarketing o de la empresa cliente, bajo la supervisión y control de supervisores y coordinadores.

- **Llamadas "predictivas" inteligentes:**

  Si un teleoperador no está disponible para atender la llamada generada por el marcador, el equipo deberá anular la llamada y liberar la línea en un tiempo máximo de un segundo.

- **Protección de Datos:**

  Cuando los datos son recogidos por las empresas de Telemarketing, el consumidor debe ser informado de cualquier fin que no sea el que inicialmente tenía previsto la campaña sobre el uso de alguno de sus datos. La información obtenida en el curso de una acción de Telemarketing, encargada por un cliente, así como las Bases de Datos

suministradas por el mismo, son propiedad exclusiva del cliente. La empresa de Telemarketing adquiere el compromiso de no hacer uso de esa información, a no ser que se disponga de una autorización escrita y expresa del cliente para ello.

- **Servicios de Preferencia Telefónica (Lista de oposición):**

Las empresas de Marketing deben disponer de un sistema de documentación donde cualquier particular puede registrar que no desea recibir llamadas con fines comerciales.

- **Confidencialidad:**

La grabación y escucha de las llamadas sólo deberá llevarse a cabo para formación o control de calidad. Las verificaciones y grabaciones del contenido de la llamada no deben ser utilizadas con otros fines.

- **Tarifas con coste adicional:**

Cuando se promueva un número de teléfono de tarifas con coste adicional, el anunciante deberá dejar claro que el número es de tarifa superior, debiendo indicar además el coste por minuto.

- **Números que no figuran en los listines:**

No se debe hacer una prospección con propósitos de Marketing con números que no figuran en el listín, exceptuando los casos donde el número haya sido suministrado por el interesado a la organización o a terceros, o cuando el número sea escogido aleatoriamente para investigación de mercado.

- **Llamadas automáticas:**

Las llamadas no solicitadas por los abonados con fines comerciales que se efectúen mediante sistemas de llamada automática, a través de servicios de telecomunicaciones, sin intervención humana (aparatos de llamada automática) o facsímil (fax), sólo podrán realizarse a aquellos abonados que hayan dado su consentimiento previo.

- **Asesoramiento:**

Las empresas de Telemarketing asesorarán a los clientes según su mejor entender basándose en sus conocimientos profesionales y experiencias y rehusarán efectuar campañas que incorporen publicidad engañosa, fraudulenta o deshonesta.

- **Conformidad:**

La Asociación de Empresas de Telemarketing, es responsable de la rigurosa aplicación de sus principios autorreguladores. Si estos no se siguen, AEMT-FECEMD, a través de su Comisión Etica, aplicará las medidas cautelares que crea oportunas.

La **AEMT** (**A**sociación **E**spañola de **E**mpresas de **T**elemarketing) lleva a cabo la supervisión del cumplimiento de las normas éticas, aprobadas por todas las empresas asociadas, así como el cumplimiento de los principios profesionales entre miembros y terceros.

Se ha creado este código ético por el cual todas las empresas asociadas actúan bajo las reglas antes referidas.

En base al anterior código deontológico, las principales compañías de telecomunicaciones que operan en España (Telefónica, Orange, Vodafone, Ono y Yoigo) firmaron el 25 de noviembre de 2010 otro para autorregular sus operaciones de televenta de cara a sus clientes, con las siguientes buenas prácticas:

- Una vez que el consumidor atienda la llamada de televenta, al menos en un 98% de los casos se garantizará que conteste un teleoperador antes de los tres segundos.

- Cuando un consumidor conteste la llamada y manifieste no tener interés por la propuesta, la operadora no volverá a llamar al cliente hasta después de tres meses a partir de esa llamada.

- Las operadoras de telecomunicaciones contarán con procedimientos que garanticen que no se contactará con los consumidores incluidos en listas en las que se explicita expresamente el deseo de no recibir este tipo de llamadas o publicidad.

- No se utilizarán medios engañosos, fraudulentos ni, en general, desleales para la competencia, para obtener del consumidor datos y/o contestaciones que pudieran interpretarse como una aceptación al cambio de operadora ni para obtener del consumidor cualquier otro comportamiento económico.

- Se limita a tres el número de intentos mensuales sobre líneas no contactadas. Se entenderá por “intento” la serie de llamadas efectuadas a un consumidor de forma consecutiva en un breve espacio de tiempo con el fin de establecer un contacto.

- Limitación de las franjas horarias de ejecución de llamadas a horarios no intrusivos para los consumidores, considerándose como tales de lunes a viernes de 9 a 22 horas, sábados de 9 a 14 horas, evitándose las llamadas los domingos y festivos.

- Identificar de forma clara e inequívoca la operadora que efectúe la llamada o en cuyo nombre se efectúe la llamada, evitando manifestaciones que puedan llevar a confusión o engaño a este respecto.

- Identificar el número desde el que se genere el contacto con el consumidor, de forma que el mismo aparezca en la pantalla del terminal.

- Se facilitará toda la información que precise el consumidor para tomar una decisión informada, incluyendo todos los cargos derivados de la contratación del servicio o producto ofertado.

- Todas las operadoras se abstendrán de utilizar manifestaciones falsas, engañosas, denigratorias o, en general desleales para la competencia, para referirse a los productos y servicios de otras operadoras.

- Las Compañías dispondrán de mecanismos de verificación y control interno de estas medidas.

- Las operadoras acuerdan que se reunirán con periodicidad semestral con el fin de compartir el resultado de la aplicación del presente Código.

- También se acuerda favorecer la adhesión al presente Código de otras operadoras de telecomunicaciones que manifiesten su voluntad de cumplir con las medidas previstas en el mismo.

## 5.1.7.2 Listas Robinson

Tiene por objeto permitir a los consumidores eliminar su nombre y dirección de los listados de publicidad con el fin de reducir al mínimo la cantidad de publicidad que reciben en sus hogares en la forma de mailing dirigido personalmente a ellos. Los consumidores que deseen recibir menos publicidad en sus hogares, podrán solicitar el Servicio de Listas Robinson, y formar parte de manera gratuita de la Lista Robinson. Aquellas personas que por el contrario, estén interesadas en recibir más envíos publicitarios, y en particular, sobre algún tema determinado, también podrán solicitar el Servicio de Listas Robinson, y formar parte de manera gratuita, de la Lista de Preferencia.

Estas listas serán proporcionadas a las empresas miembros, quienes garantizarán que dichos nombres y direcciones dejan de figurar, o en su caso se incluyen, en los listados de consumidores que utilizan con fines de Marketing Directo. El Servicio de Listas Robinson será gestionado por la Federación de Comercio Electrónico y Marketing Directo (FECEMD), quién supervisará el correcto cumplimiento de las normas por parte de sus miembros.

### 5.1.7.2.1 Normas Generales

1. La condición de miembro del SLR presupone la aceptación y cumplimiento del presente Código Regulador.

2. Las Listas Robinson son propiedad de FECEMD, y no podrán ser usadas por los miembros adheridos al servicio, para una finalidad distinta que no sea la supresión o exclusión de sus nombres y direcciones en sus listas de consumidores.

3. No estará permitido transferir dichos registros para otros fines que los arriba indicados.

4. El uso de las Listas Robinson no se considera apropiado para envíos publicitarios de partidos políticos.

5. Estas normas cubrirán el uso de los ficheros utilizados por los miembros adheridos al sistema: Empresas de Venta por Correo, Propietarios y titulares de listados, Agentes de listados, Listas Brokers, Servicios Informáticos de proceso de datos, Manipuladores, Agencias de Publicidad Directa, Consultores, etc. Estas categorías no son necesariamente exclusivas, y estas reglas deben ser respetadas por todos los miembros tanto en su letra como en su espíritu.

### 5.1.7.2.2 Normas de uso

El sistema de supresión de nombres de un fichero consistirá en retener el nombre y dirección y aplicar un signo de supresión a dichos datos.

1. No será obligatoria para una compañía la supresión de los datos de una persona que se inscriba en la Lista Robinson, cuando esta persona sea cliente de la misma, salvo si en las obligaciones legales o contractuales de la compañía con el cliente se prevé lo contrario.

2. Todo miembro deberá adoptar e interpretar de la forma más restrictiva posible la categoría de productos o servicios en la cual se ha registrado el sujeto dentro del marco de la Lista de Preferencia.

3. Las empresas de Venta por Correo deben garantizar:

• La correcta actualización de todos sus ficheros con los nuevos registros de la Lista Robinson, antes de que sean usados en sus mailing promocionales.

• La cancelación en sus listas de aquellos nombres y direcciones de las personas que lo soliciten directamente a la empresa, siempre y cuando la persona le suministre la información necesaria para que pueda llevarse a cabo su petición. Cuando no sea suficiente la información dada por la persona, la empresa deberá advertirle de los datos suplementarios que necesita para llevar a cabo su petición.

• Que en caso de recibir peticiones muy exaltadas y generalizadas contra la publicidad directa, las empresas aconsejarán a la persona la necesidad de dirigirse a FECEMD para apuntarse al Servicio de Listas Robinson.

4. Los Propietarios y Agentes Titulares de Listados deben garantizar:

• Que los listados que puedan ofrecer, ya sea directamente a empresas de Venta por Correo, o a través de Lists Brokers, hayan sido actualizados con los nuevos registros de la Lista Robinson.

• La cancelación, en sus propias listas o en aquellas que van a ofrecer, de los nombres y direcciones de aquellas personas inscritas en la lista Robinson o aquellas que, de manera individual, se dirijan a ellas y soliciten su deseo de no estar incluidas en listas para promociones publicitarias.

5. List Brokers, Servicios Informáticos y Manipuladores.

Los Lists Brokers, Servicios Informáticos y Manipuladores adheridos al servicio deben garantizar que no usarán listas de consumidores que no hayan sido o vayan a ser actualizadas con los nuevos registros de la Lista Robinson, así como aconsejar a sus clientes su adhesión como miembros al Servicio de Listas Robinson.

6. Agencias de Publicidad y Consultorías.

Las Agencias de Publicidad y Consultorías adheridas al servicio, deberán aconsejar a sus clientes su adhesión como miembro al Servicio de Listas Robinson, o en su caso, hacer sólo uso de listas de consumidores que hayan sido o sean actualizadas con los nuevos registros de la Lista Robinson.

### 5.1.7.2.3 Incumplimiento de las normas

1. Cualquier infracción al cumplimiento de las normas del presente Código, será remitida, debidamente motivada, al Comité de Protección del Tratamiento Automatizado de los Datos de carácter personal de FECEMD.

2. Las competencias y funcionamiento de este Comité, están reguladas por el art. 8 del Código Ético de Protección de Datos Personales del sector del Marketing Directo de FECEMD.

3. Si el Comité decide realizar una acción disciplinaria, informará de ello a la empresa, y le dará la oportunidad de justificarse de manera escrita u oral.

4. Si el Comité considera que el incumplimiento de las normas ha sido no intencionado y dicho miembro se compromete a que no volverá a ocurrir, no se adoptarán acciones mayores.

5. Si por el contrario, el Comité considera que sí ha existido una grave violación de las normas, podrá recomendar una acción disciplinaria, o en caso de incumplimiento grave, la suspensión como miembro adherido al Servicio.

6. El aviso o la sanción del Comité serán notificados a la empresa miembro y/o a la persona afectada, por medio del Secretario del citado Comité. El Comité se reserva el derecho de dar publicidad externa a la sanción, así como de emprender acciones legales por haberse visto afectada la credibilidad de la profesión.

### 5.1.7.2.4 Utilización del sello de Garantía del Servicio de Listas Robinson

La aceptación de las reglas del Código Regulador autoriza a las empresas miembros adheridas a utilizar el sello del SLR. La utilización del sello es facultativa. Es obvio, sin embargo, que cada cual se aprovechará de la publicidad hecha por los otros miembros adheridos, por lo que afecta al interés de todos el promover la difusión de este sello.

1. **Modalidades de Utilización**. Dado su objeto esencial que es el constituir una marca distintiva colectiva, el sello no podrá ser dispuesto ni, en todo caso, utilizado en documentos de venta o en la publicidad, de tal forma que pueda ser considerado:

   • Ya sea como una marca propia de la empresa usuaria.

   • Ya sea como una garantía (en especial, de origen o de calidad) de los productos o servicios ofrecidos a la venta. FECEMD se reserva el derecho, en todo momento, de apreciar y controlar las condiciones de utilización del sello y de tomar todas las disposiciones útiles en caso de utilización anómala. A este efecto, las empresas usuarias de la marca colectiva se comprometen:

   • A comunicar cualquier documento a la FECEMD en cuanto ésta lo solicite.

   • A aplicar sin demora y sin reserva las instrucciones de utilización que les sean comunicadas por la FECEMD. Queda prohibida, salvo autorización expresa y escrita de FECEMD cualquier reproducción del sello que se utilice fuera de los documentos comerciales o publicitarios.

2. **Retirada**. La pérdida de la condición de miembro del SLR conlleva ipso facto la supresión del derecho a utilizar el sello. El Comité de Protección de datos de FECEMD, puede igualmente pronunciar sanciones o decidir la retirada temporal o definitiva de la marca, cuando se haya hecho de ella un uso abusivo, ilícito, desleal o fraudulento.

En ningún caso la utilización de materiales que lleven el sello y que existan en la fecha de la retirada o expulsión de una empresa miembro, sería tolerada sin el acuerdo especial de FECEMD.

# 5.1.8 Medidas de seguridad en el tratamiento de datos de carácter personal

## 5.1.8.1 Medidas de seguridad aplicables a los ficheros y tratamientos automatizados

El encargado/responsable del tratamiento deberá/n implantar una serie de **medidas** en lo dispuesto a la ley para garantizar la **seguridad** de los datos a la hora de su tratamiento.

La mayoría de los CC suelen funcionar como encargados del tratamiento de otros ficheros de los cuales no son responsables, por lo que según el **artículo 82** de la ley, deberán adoptar las siguientes acciones:

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

   Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en el reglamento.

Se deberá limitar a todo el personal ajeno que no esté relacionado directamente con el tratamiento de datos el acceso a los soportes o recursos del sistema de información. También se podrá delegar en otras personas diferentes al responsable del fichero o tratamiento, pero deberán constar dichas personas en el documento de seguridad que acuerden las dos partes.

En caso de una **cesión a un tercero**, en aplicación **al artículo 88**, este documento, deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el

encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

El **acceso a los datos a través de redes de comunicación** se deberá hacer en base a un nivel de seguridad equivalente a los accesos en modo local según dicta el **artículo 85**.

El **teletrabajo** es algo común en las empresas que operan en CC por lo que se deberá cumplir con el **artículo 86** que marca un nivel de seguridad para el fichero tratado y de una autorización que deberá constar en el documento de seguridad.

Las medidas de seguridad se agruparán en tres niveles: básico, medio y alto.

#### 5.1.8.1.1 Medidas de seguridad de nivel básico

En disposición del **artículo 90** de la ley, se deberá crear un **registro de incidencias** que cumpla con lo siguiente:

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Los usuarios que realicen el **tratamiento de datos** deberán cumplir los siguientes puntos de acuerdo al **artículo 91**.

1. Tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

El **artículo 93**, trata de que a través de dichos usuarios el responsable del fichero o tratamiento deberá adoptar las **medidas que garanticen la correcta identificación y autenticación** de ellos y será de forma inequívoca y personalizada para todo aquel que intente acceder al sistema de información siendo verificado que está autorizado para ello.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Para mejorar la seguridad contra imprevistos, se deberán implementar programas proactivos y reactivos de copias y respaldos de recuperación con lo registrado en el **artículo 94** de la ley acordes a los siguientes puntos:

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

### 5.1.8.1.2 Medidas de seguridad de nivel medio

El **artículo 96** de la ley, obliga por necesidad a realizar un **proceso de auditoría** a los sistemas de las entidades implicadas de acuerdo a los siguientes apartados:

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

El **artículo 98 refuerza al 92** en el caso de que se intente reiteradamente el **acceso no autorizado** al sistema de información.

De igual manera se pondrá especial atención a lo dictaminado en el artículo 93 para el acceso a los lugares donde se encuentren los equipos físicos que den soporte a los sistemas de información, por parte del personal autorizado, recogido en el documento de seguridad.

Al tratarse muchas veces de datos críticos, sería conveniente que los CC aplicaran el **artículo 100** de la ley que añade a los **registros de incidencias** (tratados en el **artículo 90**), la capacidad de consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

### 5.1.8.1.3 Medidas de seguridad de nivel alto

Con respecto a las copias de respaldo y recuperación tratadas en el artículo 94, en este nivel y según lo establecido en el **artículo 102**, se deberá **conservar una copia de respaldo de los datos y de los procedimientos de recuperación** de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando

elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

El **artículo 95** completa el procedimiento de registro de **acceso a los sistemas** que contienen la información de los datos y se regirán por los siguientes puntos:

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

    a) Que el responsable del fichero o del tratamiento sea una persona física.

    b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Para un nivel de seguridad alto con respecto a las telecomunicaciones, el **artículo 104** dictamina que la **transmisión de datos** de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

## 5.1.8.2 Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Muchas plataformas de CC operan a través de correo ordinario o fax por lo que veremos a continuación las medidas de seguridad que se deben de tomar para este tipo de servicios.

### 5.1.8.2.1 Medidas de seguridad de nivel básico

Las obligaciones comunes con respecto a los ficheros y el tratamiento automatizado se les aplicarán también a los no automatizados de acuerdo con el artículo 105.

Según el **artículo 106**, el **archivo de los soportes o documentos** se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

También con respecto a los **dispositivos de almacenamiento** se seguirán las directrices enunciadas en el **artículo 107**. Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Se deberá hacer un **uso seguro de los soportes** de acuerdo con el **artículo 108**, el cual dice que mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

### 5.1.8.2.2 Medidas de seguridad de nivel medio

Deberá designarse un **responsable de seguridad** (al igual que en el artículo 95 del tratamiento automatizado) y se deberán realizar **servicios de auditoría** de igual manera según lo estipulado en los **artículos 109 y 110**.

### 5.1.8.2.3 Medidas de seguridad de nivel alto

Con respecto al **almacenamiento**, el **artículo 111** indica que:

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

El **artículo 112** indica el **procedimiento** a seguir para las **copias o reproducciones** de acuerdo a los siguientes puntos.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Los **accesos y traslados de la documentación** se realizaran en conveniencia a lo escrito en los **artículos 113 y 114**:

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

### 5.1.9 Procedimientos tramitados por la Agencia Española de Protección de Datos

La AEPD podrá iniciar cualquier procedimiento que atañe a la protección de los datos por medio de una reclamación, se podrán presentar vías de recurso para ellos y finalmente dictará una resolución.

#### 5.1.9.1 Infracciones y sanciones

Actualmente estás son las sanciones dispuestas por la AEPD:

| NIVEL | CUANTÍA | PRESCRIPCIÓN |
|---|---|---|
| LEVE (Art. 44.2) | DE 900 € A 40.000 € | 1 AÑO |
| GRAVE (Art. 44.3) | DE 40.001 € A 300.000 € | 2 AÑOS |
| MUY GRAVE(Art. 44.4) | DE 300.001 € A 600.000 € | 3 AÑOS |

## 5.2 Marco Europeo

Este reglamento, todavía no aprobado, pretende establecer un marco jurídico de regulación a nivel europeo para los estados miembro relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.

Prácticamente complementa a ley española, regulada como hemos comentado anteriormente, recogida en la LOPD pero con algunos aspectos añadidos o diferenciados como los siguientes:

- Crea la **figura del delegado de protección de datos**. (**Artículos 35, 36 y 37**).
- Añade la existencia de un **representante** que será el **responsable del tratamiento en un tercer país**, que garantice un nivel de protección. (**Artículo 25**)
- Mecanismos y procedimientos como las **consultas previas**. (**Artículo 34**)
- Notificación de **violación de la privacidad** y **certificaciones** orientadas a la **privacidad**. (**Artículos 31, 32 y 39**)
- Establecimiento a **derechos de olvido** y **portabilidad de datos**. (**Artículos 17 y 18**)
- **Excepciones a transferencias internacionales**. (**Artículo 44**)
- La creación de una **Comisión y Consejo Europeo de Protección de Datos** ante los cuales cada autoridad de control deberá elaborar y presentar un informe anual sobre sus actividades. (**Artículo 54**)
- Ámbito de aplicación de la norma.
    - En Europa el **consentimiento de menores para el tratamiento de datos**, será solo **relativo a la oferta de servicios de la sociedad de la información**, mientras que en España se aplicará a todos. (**Artículo 8**)

- Para **mayores de 13 años**, el **consentimiento** no será necesario la **autorización de padres o tutores**. En España esta edad se amplía a 14. (**Artículo 8**)

- **Sanciones dependientes de estados y autoridades de control**.

- También impondrá sus **propias sanciones** de acuerdo a las siguientes (**Artículos 78 y 79**):

| NIVEL | CUANTÍA |
|---|---|
| A | 0,5% FACTURACIÓN MUNDIAL O 250.000 € |
| B | 1% FACTURACIÓN MUNDIAL O 500.000 € |
| C | 2% FACTURACIÓN MUNDIAL O 1.000.000 € |

# 5.3 LSSI

La LSSI o **L**ey 34/2002, de 11 de julio, de **S**ervicios de la **S**ociedad de la **I**nformación y de Comercio Electrónico también es tenida en cuenta para los CC pero en menor medida que la LOPD, ya que no tienen tanta relación directa y se identifica más con el contacto a través de redes de telecomunicaciones, en especial Internet, y vía electrónica que se realiza dentro del territorio español (aunque incorpora parte de la Directiva 98/27/CE, del Parlamento Europeo. El régimen jurídico aplicable será el mismo que en la LOPD en referencia a la obtención de datos personales, información a los interesados y creación y mantenimiento del fichero de datos personales.

Se acoge, en la Ley, un concepto amplio de "servicios de la sociedad de la información", que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Nos centraremos en cuatro artículos de la ley.

- **Artículo 18. Códigos de conducta.**

A pesar de ser voluntarios, son recomendables su elaboración y aplicación por parte de las corporaciones, asociaciones u organizaciones comerciales. Las plataformas que envíen por vía electrónica comunicaciones comerciales no solicitadas por los destinatarios pueden verse afectadas.

- **Artículo 20. Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.**

Puede darse que en alguna campaña de un CC relacionada con ventas se envíen comunicaciones comerciales, ofertas promocionales o concursos, por lo que se deberán tener en cuenta los siguientes aspectos.

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

En el caso en el que tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra "publicidad" o la abreviatura "publi".

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo, comercio electrónico o publicidad.

4. En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo.

- **Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.**

Si el envío de comunicaciones comerciales se hiciese sin el consentimiento previo del destinatario o se hubiesen obtenido los datos de forma ilícitamente se estaría incurriendo en esta ley de acuerdo a los siguientes aspectos.

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que

previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

- **Artículo 22. Derechos de los destinatarios de servicios.**

De acuerdo a lo comentado en el artículo anterior y al igual que en la LOPD el destinatario de la información podrá ejercer sus derechos para evitar nuevamente que sus datos sean utilizados con estos fines comerciales.

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

## 5.4 Ley de defensa de consumidores y usuarios

También podemos mencionar la Ley de Defensa de Consumidores y Usuarios, la cual ha sufrido cambios para adaptarse a su directriz europea (2011/83/UE) con el fin de que los contratos realizados a través de Internet o teléfono garanticen una seguridad para el consumidor y/o usuario. Las novedades del anteproyecto son las siguientes:

- **Deber de información al usuario**: El empresario deberá ofrecer al consumidor información clara y comprensible y previa a la formalización del contrato. El consumidor deberá tener acceso a las condiciones aplicables al contrato que va a suscribir.

- **Aceptación del pago**: En los supuestos de comercio electrónico, el consumidor ha de ser informado hasta el último momento, de que la aceptación de la oferta implica una obligación de pago por su parte, lo cual, puede suponer que el empresario deba agregar en su página web, en el botón de "comprar", una expresión tal como "contrato el servicio y pago el mismo."

- **El comerciante deberá mostrar el precio final del producto o servicio contratado antes de que se concluya la transacción**, que deberá ser aceptado por el consumidor. En caso de que el cliente no reciba el precio final desde el principio, podrá recuperar la diferencia entre el coste inicial y el final.

- **Contratación telefónica**: En los contratos realizados fuera de los establecimientos del empresario, por ejemplo, los realizados vía telefónica (por ejemplo: servicios de luz, gas, Internet), el empresario deberá contar con la aceptación del consumidor por escrito, no siendo válida la mera aceptación verbal por teléfono. De tal modo que la oferta no será vinculante hasta que el consumidor haya firmado la oferta o enviado su acuerdo por escrito ya sea en papel, por fax, correo electrónico o por un mensaje de SMS. Las grabacaciones de dichos contratos deberán realizarse desde un teléfono gratuito que no deba suponer un coste adicional para el consumidor.

- **Plazo de devolución**: Se amplía el actual plazo de siete días hábiles a catorce días naturales. El empresario deberá disponer de la certeza de que el consumidor ha quedado informado de este punto, ya que en caso contrario, el plazo de catorce días podría quedar ampliado a 12 meses a contar desde la fecha de expiración del periodo inicial.

- **Llamadas comerciales**. En ningún caso se efectuaran antes de la 9h ni más tarde de las 21h, ni en festivos o fines de semana. Las llamadas se han de realizar mediante un teléfono identificable.

La nueva ley deberá incorporar un formulario de desistimiento, que se facilitará junto con la información previa al contrato. Estas medidas serán de obligado cumplimiento a partir del 13 de junio de 2014.

# 6. Auditoría y Control de una plataforma de Contact Center

## 6.1 Objetivos

A continuación se listan varios de los objetivos que se buscan alcanzar a través del control y la auditoría en una plataforma de Contact Center.

- **Mejora continua del servicio y generación de beneficios.**

La mejora continua del servicio es una pauta que prácticamente todas las normas, estándares o marcos que hemos mencionado a lo largo del documento, gracias a ello se conseguirá optimizar todos los recursos. La generación de beneficios siempre será positiva cuando sea acorde con los controles que se realicen para evitar que los fondos de la entidad se destinen a pagar posibles multas, sanciones o correcciones.

- **Eficiencia del trabajador.**

Se busca un modelo en el cual el agente está cargado pero no sobrecargado de trabajo. El objetivo siempre busca minimizar los tiempos en los que el agente no está ejerciendo un trabajo efectivo que reporte un beneficio para la entidad.

- **Uso de medidas para evaluar el servicio.**

A través de las métricas y los KPIs se obtendrán una serie de datos que se deberán analizar y comparar para tomar una serie de decisiones acordes con los objetivos marcados en su momento.

- **Búsqueda de la satisfacción del cliente y usuario final.**

Uno de los objetivos primordiales es la satisfacción de dos de las partes implicadas más importantes y que conforman los dos lados de la cadena. Una satisfacción positiva del cliente hará que éste tenga una mejor impresión del servicio brindado, aumentando su confianza y reduciendo los posibles costes económicos que pueda causar un mal desempeño. En el otro lado se encontraría el

usuario final, el cual a través de encuestas se puede valorar el nivel de satisfacción que puede tener con el servicio que se le brinda. Una buena satisfacción del usuario final repercutirá positivamente en el cliente, ya que muchos Contact Center externos son la “cara” del cliente.

**- Resolución de transacciones en primer contacto.**

La resolución en primer contacto es un objetivo principal con el fin de evitar réplicas de las transacciones por parte del usuario final. El ahorro en personal, costes y tiempo repercute positivamente en la entidad por lo que tanto los agentes a través de los procedimientos deben dejar totalmente cerrado el contacto por el cual el usuario final lo inició.

**- Cumplimiento de la legalidad y leyes vigentes.**

No se debe obviar el cumplimiento con la legislación actual que se rige, en este caso, en España. Se ha hablado anteriormente de las leyes y los códigos a los que se rigen los Contact Center que operan España, por lo que se deberá informar a todo el personal y en especial a los agentes de normas que deben cumplir en el desempeño de su trabajo diario con el fin de evitar multas o sanciones posteriores.

**- Mapear procesos. Localizar las transacciones más emitidas/recibidas.**

De todas las transacciones que se reciben a diario en un Contact Center se deberán seleccionar las más comunes para establecer un procedimiento estándar con el fin de agilizar este tipo de transacciones. De igual manera, todo el resto de transacciones deberán estar procedimentadas para que cada agente sepa en todo momento de que manera solucionarlo de la mejor forma posible. A lo largo del servicio se pueden encontrar dudas o novedades sin resolución que deberán ser reportadas a los superiores para o bien fornir a los procedimientos ya existentes o bien para crear nuevos que palien esas deficiencias existentes.

**- Eliminar transacciones innecesarias.**

En muchos casos los usuarios finales contactarán con el Contact Center para tratar de solucionar interacciones triviales. Para evitar este tipo de interacciones se deberán localizar dichas transacciones e implementar vías de respuesta adicionales como por ejemplo un self service o cualquier servicio web que libere de una mayor carga de trabajo a los agentes de la plataforma para que éstos puedan ser más eficientes en otros ámbitos donde se les requiera.

Para alcanzar estos objetivos se recomienda el uso de las siguientes medidas de mejora para la atención telefónica:

Están basadas parcialmente en un manual realizado por el Grupo Konecta.

**- Educación y amabilidad**:

- Sonrisa telefónica: percepción del tono agradable.
- Formulas de cortesía: trato de usted, frases educadas empezadas o acabadas con un “por favor” o “si es tan amable”, por ejemplo.
- Eschucha activa, empatía con el cliente: actuar poniéndose en el lugar del cliente.
- No interrumpir: tratar de que por ambas partes haya una comunicación fluida.

- **Voz**:

- Entonación correcta, sin musicalidad: mantener un tono conciliador siempre y con sensación positiva pensando en la resolución correcta por la cual se requiere la ayuda.
- Correcta articulación: pronunciar las palabras, sobre todo en el uso mnemotecnico de saludos y despedidas.
- Velocidad de elocución: adecuada a cada persona, debe comprender todo el mensaje que se transmite.
- Volumen: tratar de mantener un nivel medio, ni muy alto que pueda sonar desagradable o muy bajo apenas perceptible.

- **Tratamiento de la llamadas**:

- Sondeo correcto (recepción): realizar preguntas con el fin de conseguir la mayor información correcta y útil posible.
- Transmisión del mensaje (emisión): tratar de introducir a la otra parte en la conversación, transmitiéndole pequeños mensajes y reinforzando al final de los mismos la intención de que no hay ninguna duda con los mismos.
- Capacidad de dirección del mensaje: relajar al interlocutor si muestra síntomas de nerviosismo, mostrándole confianza a través de la empatía y aportando argumentos y alternativas.
- Reformulación de datos: confirmar los datos emitidos o recibidos, en el caso que queden grabados confimar que se ha realizado correctamente.
- Personalización del trato: trasladar al interlocutor comodidad para que éste sienta una distancia menor entre ambas partes y ayude a la explicación de la situación.
- Lenguaje claro y sencillo: Evitar muletillas y frases coloquiales.
- Corrección gramatical: no utilizar el argot.

- Uso de lenguaje propio o tecnicismo: evitarlo y solo en el segundo si es necesario, explicarlo al interlocutor.

- **Resolución y suficiente conocimiento**:

  - Evitar llamada posterior del cliente: ser precisos en la resolución en primer contacto.

  - Búsqueda activa de la solución ventajosa: obtener la satisfacción del cliente y evitar reclamaciones por si existen mejores opciones de resolución no planteadas.

  - Firmeza y seguridad en las soluciones: utilizar el tiempo de duración acorde al tipo de transacción, satisfacción y transmitiendo seguridad al interlocutor.

  - Conocimiento de productos y servicios: el propósito final es la resolución de la transacción a través de los conocimientos que el agente posee sobre producto, argumentario y procedimientos.

  - Evitar silencios prolongados: no quedarse callado y explicar en todo momento al interlocutor si se va a retirar del puesto dejándolo en silencio, retomándolo con la explicación del motivo de ausencia.

- **Adaptación a la situación**:

  - Se identifica con la situación planteada: uso de las habilidades emocionales junto con la empatía.

  - Venta de imagen: hacer valer siempre una buena imagen de la compañía al interlocutor. No culpar a los compañeros y homogenizar criterios para evitar la disparidad de los mismos.

  - Saber positivizar: tratar de dar siempre una postura positiva ante una situación precedente negativa que transmita el interlocutor.

  - Convicción y persuasión: conseguir que el interlocutor acepte la solución propuesta por el agente a través de una argumentación sólida y segura.

- **Acogida y despedida**:

  - Uso de mensaje estándar: recibir y despedir al interlocutor con un saludo estándar que en algunos aspectos de pie a que el cliente exprese su satisfacción o no de la atención.

  - Evitar el uso de la monotonía: aportar dinamismo, evitando sensaciones negativas en todo momento a la conversación.

- Sensación positiva al acabar la transacción: sintiendo que el tratamiento ha sido el mejor y con sensación positiva en la resolución.

## 6.2 Problemas

Durante el desarrollo del servicio se pueden encontrar varios problemas. Seleccionamos los más comunes que puedan ocurrir en un Contact Center y como solucionarlos.

**- Retrasos en el IVR hasta la resolución del problema.**

Normalmente la situación ideal es que un usuario final contactase con el centro y una vez finalizase la interacción se resolviese el problema que tuviese. Es frecuente el lavado de manos por parte de los agentes, es decir quitarse de en medio al usuario final al no saber solventar el problema que le atañe. Normalmente esto puede deberse a un mal funcionamiento del IVR que hace desesperante la transacción del cliente y pueda terminar con un agente erróneo.

**- Tiempos de espera eternos.**

Es una utopía creer que los tiempos de espera no puedan existir, pero por norma general los Contact Center son sitios donde la paciencia es algo que escasea en ambos lados de la transacción. El canal a través del que se contacta ya puede ser una barrera en el tiempo sea cual sea, teléfono, chat, redes sociales, etc… Los cuellos de botella que se forman en un servicio es algo con lo que cualquier plataforma está totalmente familiarizado, eso repercute en el usuario final quien debe esperar un tiempo para ser atendido, lo cual no incluye la garantía de que el agente que lo atienda por primera vez solucione su problema. El tiempo de espera también se ve incrementado por dos aparatos muy usados por los agentes: el botón de Mute y Hold que se pueden encontrar en sus dispositivos. El primero de ellos silencia el micrófono del cliente y el segundo hace sonar una locución, mientras el usuario final se mantiene a la espera. Muchas entidades penalizan a sus agentes por el uso de estos botones.

**- Múltiples contactos antes de que se resuelva la transacción.**

Como hemos hablado anteriormente, este problema sería el contrario de la resolución en primer contacto. Una transacción no cerrada correctamente genererará réplicas por cualquier otro canal. Se debe hacer especial énfasis en la comunicación que se le proporciona al usuario final para que este asimile la información con el fin de guiarlo a su resolución, indicarle correctamente la información que solicita o del producto o servicio que contrate.

- **Inestabilidad laboral.**

El clima de trabajo que se puede respirar en una plataforma de Contact Center puede ser muy variado. Normalmente los agentes que trabajan en la primera línea, es decir, aquella que atiende al cliente por primera vez, suelen estar sometidos a una presión mayor en muchos aspectos lo que se traduce en un estrés casi constante. La rotación del personal en esta línea es mucho mayor que en cualquier otra debido a factores psicológicos, médicos o económicos. Finalización de campañas por parte del cliente, los sueldos algo precarios o los problemas que sufran los usuarios finales pueden repercutir en la autoestima y la salud del agente, causando su cambio en el puesto de trabajo.

- **Medidas de satisfacción del cliente.**

Normalmente estas medidas de satisfacción son bajas o ninguna. Los incentivos que pueda recibir el personal se basan en rankings entre los propios agentes basados en objetivos marcados sobre los cuales la competencia puede ser en muchos momentos deslean. Pueden ser económicos o en muchos casos recompensados con tiempo.

## 6.3 Métricas y KPIs

Las siguientes métricas y KPIs que se listan están basadas en los estándares ISO 27001 y COPC PSIC, siendo muchas de ellas de uso cotidiano para el desempeño del servicio que se pueda brindar en un Contact Center.

- **SEGURIDAD**:
  - Tiempo medio de revisión de la política de privacidad
  - Personal capacitado (%)
  - Activos recuperados de antiguos clientes (%)
  - Activos existentes recogidos en el inventario (%)
  - Cuentas redundantes
  - Cuentas bloqueadas por máximo de intentos permitidos
  - Cuentas bloqueadas por accesos fallidos resueltos sin incidentes (%)
  - Violaciones del control de acceso
  - Desastres naturales

- Ataques externos
- Accidentes
- Días que se almacena una copia de seguridad
- Infraestructura crítica con monitoreo automático (%)
- Parches de vulnerabilidades instalados (%)
- Aplicaciones evaluadas
- Tiempo promedio para corregir vulnerabilidades
- Transacciones en las que se revela información confidencial (%)
- Transacciones con información enviada erróneamente a un remitente (%)
- Incidentes por tiempo cerrados en ese tiempo (%)
- Incidentes con información de terceros (%)
- Incidentes sin identificar responsables
- Tiempo promedio de resolución de incidentes
- Incidentes escalados
- Tiempo medio de resolución de los incidentes.
- Aplicaciones en producción con no cumplimientos o demoradas por estos (%)
- Aplicaciones críticas testeadas (%)
- Impactos al negocio de incidentes críticos
- Planes probados (%)
- Procesos críticos con planes aprobados y testeados (%)
- Cantidad de medidas preventivas como respuesta a amenazas de seguridad identificadas.

- **CALIDAD**:

Explicadas en el Anexo 2 al final de este documento.

- Tasa de Abandono
- Puntualidad (On time)
- Pendientes

- Tasa de autoservicio
- Tasa de Conexión con la parte Correcta (RPC)
- Listado de pendientes
- Puntualidad en el cierre
- Pendiente de casos
- Precisión crítica para el Usuario Final
- Precisión del Error Crítico para el Negocio
- Precisión del Error Crítico de Cumplimiento
- Resolución en el contacto
- Tasa de escalamientos
- Tasa de salida
- Precisión del ruteo
- Tasa de Éxito
- Ventas
- Éxito de completitud
- Tasa de cierre
- Utilización de agentes
- Tiempo Medio de Manejo (AHT)
- Ocupación (Nivel de Servicio)
- Coste por x
- Eficiencia
- Coste por unidad
- Tasa de RPC
- Tasa de ventas
- Tasa de completitud
- Volumen
- Disponibilidad/Acceso

- Transacciones bloqueadas

- Adhesión

- Pedido en espera

- Precisión de la Base de Conocimiento

- Calidad

- Precisión de Pronóstico de Volumen para Programación

- Precisión de Pronóstico de AHT para Programación

- Calidad de reclutamiento

- Calidad de la formación

- Precisión

- Precisión en el recuento cíclico de inventario

- Precisión externa

- Satisfacción global del Usuario Final

- Insatisfacción global del Usuario Final

- Satisfacción global del Cliente

- Puntualidad en la gestión de las quejas

- Rotación de agentes

- Rotación de jefes de equipo

- Ausentismo de agentes

## 6.4 Cuestionarios

A continuación se mostrarán los cuestionarios implementados como parte central de este proyecto. Tratan de abarcar tres partes importantes que se pueden encontrar en un servicio desempeñado por un Contact Center: Seguridad, Calidad y Legislación, puntos tratados en desarrollado anteriormente. Cada uno tiene 248, 186 y 25 preguntas respectivamente, agrupadas cada una de ellas en categorías.

Todas las preguntas se contestarán en una escala de 1 a 5, siendo 1 el menor valor y 5 el máximo, pudiendo añadir cualquier comentario. Las opciones abarcan desde “Sí/Se

cumple", "Parcialmente se cumple", "Parcialmente no se cumple", "No/No se cumple" y "NS/NC". En algunos casos las opciones que se muestran son numéricas, indicándose previamente.

Los cuestionarios han sido implementados gracias a la herramienta gratuita para la elaboración de formularios de Google y se encuentran disponibles en Internet para su acceso. El único requisito es registrarse con una cuenta de Google para su posterior realización. Estos son los enlaces para su uso:

- **Seguridad**:

  https://docs.google.com/forms/d/19mC5nRtNIuyQW6zFIC3dnuFkowCOvB8JTr4Zn2dM9PY

- **Calidad**:

  https://docs.google.com/forms/d/1Zp1VBh8ToVrcYQ3WKCFUN2lUbEJqJQdfP1penImmhVM

- **Legislación**:

  https://docs.google.com/forms/d/1zcf7OiBkwTInWDayqMcq2WNTYkK12R7soWyubQXrA_M

## 6.4.1 Cuestionario sobre la Seguridad de la Información

### 6.4.1.1 Información de las políticas de seguridad

**- Política de seguridad:**

1 - ¿La organización dispone de una política de seguridad?

2 - ¿El documento en el que se recoge la política de seguridad es público y se comunica a todos las partes implicadas en el negocio?

3 - ¿El documento incluye los objetivos, alcance e importancia de la política de seguridad?

4 - ¿El documento incorpora un marco con los objetivos de control y controles, la evaluación del riesgo y la gestión del mismo?

5 - ¿En el documento se explican las políticas, principios, estándares y requisitos de conformidad de la seguridad de tipo legislativo, regulador o restrictivo, en educación, entrenamiento y conocimiento, en la continuidad del negocio y las consecuencias de la violación de la política de seguridad?

6 - ¿Hay una/s persona/s responsable/s de la política de seguridad y su desarrollo, revisión y evaluación?

#### 6.4.1.2 Organización de la seguridad de la información

**- Gerencia:**

7 - ¿La gerencia formula, aprueba y revisa la política de seguridad?

8 - ¿La gerencia asigna los roles y responsabilidades de seguridad?

9 - ¿La gerencia coordina y revisa la implementación de la seguridad para toda la organización?

10 - ¿La gerencia proporciona los recursos necesarios para la seguridad de la información?

11 - ¿Las nuevas instalaciones son autorizadas por la gerencia?

**- Organización:**

12 - ¿Se promueve de manera efectiva la formación, el entrenamiento y el conocimiento de la seguridad de la información a través de la organización?

13 - ¿Se evalúa la información recibida en las monitorizaciones y se revisan los incidentes de seguridad?

14 - ¿Los niveles de autorización están definidos y documentados?

15 - ¿Se identifican las vulnerabilidades y se implementan controles para el uso de instalaciones para el procesamiento de la información privadas o personales?

16 - ¿La organización trata de mejorar su conocimiento sobre las buenas prácticas y está al día con la información sobre seguridad relevante?

17 - ¿Se definen los roles y responsabilidades de la seguridad de las personas en concordancia con la política de seguridad de la información de la organización?

18 - ¿Las tareas y áreas de responsabilidades que puedan entrar en conflicto están separadas para reducir cualquier problema relacionado con el acceso, modificación o uso de activos no autorizado?

19 - ¿La organización establece algún tipo de control con el uso de medios de computación y comunicación móviles (portátiles, tarjetas inteligentes, móviles, tablets, etc…) asegurando que no se comprometa información confidencial?

20 - ¿Está aprobado el teletrabajo fuera de las instalaciones de la organización?

21 - ¿Se asegura la seguridad física del teletrabajo en los lugares del desempeño en las mismas condiciones o similares que los de las instalaciones de la organización?

22 - ¿Cada activo o proceso de seguridad tiene designado una persona responsable?

23 - ¿La organización dispone de un contacto adecuado con la policía, los bomberos o el proveedor de ISP en caso de que se produzca cualquier problema de seguridad?

**- Acuerdos de protección:**

24 - ¿En los acuerdos de protección de la información se define la información a proteger?

25 - ¿En los acuerdos de protección de la información se especifica la duración de los mismos, incluyendo casos donde se mantenga indefinidamente la confidencialidad?

26 - ¿En los acuerdos de protección de la información se reflejan las acciones requeridas cuando finalicen dichos acuerdos?

27 - ¿En los acuerdos de protección de la información se establecen las responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada?

28 - ¿En los acuerdos de protección de la información queda detallada el propietario de la información, secreto comercial y propiedad intelectual de cara a la protección de la información confidencial?

29 - ¿En los acuerdos de protección de la información se establece si el uso de la información confidencial está permitido por el firmante?

30 - ¿En los acuerdos de protección de la información se especifican los procesos de notificación y reporte cuando se produzca una divulgación no autorizada o el incumplimiento del acuerdo de información confidencial?

31 - ¿En los acuerdos de protección de la información se detallan las condiciones para el retorno o destrucción de la información una vez acabado el acuerdo?

32 - ¿En los acuerdos de protección de la información se informa de las acciones a realizarse en caso del incumplimiento del contrato?

33 - ¿La organización comparte e intercambia información sobre tecnologías, productos, amenazas o vulnerabilidades sobre la seguridad de la información?

34 - ¿La organización lleva a cabo acuerdos de intercambio de información?

35 - ¿Se identifican los requisitos de protección de información sensible en los acuerdos de intercambio de información?

### 6.4.1.3 Seguridad de los Recursos Humanos

**- Antes de la contratación:**

36 - ¿Se investigan y verifican los antecedentes de cualquier nuevo candidato al puesto de trabajo, llevándose a cabo en conformidad con las leyes, regulaciones y ética y siendo proporcionales a los requisitos del negocio, la clasificación de la información para tener acceso y los riesgos percibidos?

**- Durante la contratación:**

37 - ¿La organización cuenta con una lista de todos los empleados que trabajan para ella o para el lugar en que realicen dicho trabajo?

38 - ¿Se expone a todos los empleados o contratistas en los acuerdos contractuales sus responsabilidades y de la organización en el ámbito de la seguridad de la información?

39 - ¿Todos los empleados o contratistas firman un contrato con los términos y condiciones acordes a la política de seguridad?

40 - ¿Todos los empleados o contratistas reciben la documentación necesaria para ejercer su trabajo una vez que se da el establecimiento del contrato laboral?

41 - ¿Los usuarios están capacitados correctamente en cuestiones de seguridad de la información antes de que se establezca un contrato laboral con la organización?

42 - ¿Los empleados o contratistas aplican seguridad a la información en base a las políticas y procedimientos establecidos por la organización?

43 - ¿Los empleados o contratistas están consensuados y se forman y actualizan continuamente en las políticas y procedimientos de seguridad de la información?

44 - ¿Existen en la organización medidas disciplinarias para aquellos empleados que violen la seguridad de la información?

45 - ¿Los empleados o contratistas que cambien sus responsabilidades o empleo dentro de la organización modificarán sus roles y responsabilidades?

46 - ¿Se siguen procedimientos que aseguren la transferencia segura y borrado posterior de información si un empleado o contratista compra un equipo a la organización o utiliza el suyo propio?

**- Tras la contratación:**

47 - ¿Todos los derechos de acceso tanto físicos como lógicos son retirados a los empleados o contratistas que finalicen su labor en la organización?

48 - ¿Todos los activos tanto físicos como lógicos son devueltos por los empleados o contratistas que finalicen su labor en la organización?

#### 6.4.1.4 Gestión de activos

**- Activos:**

49 - ¿Están identificados y definidos claramente todos los activos y procesos de seguridad de la organización?

50 - ¿Todos los activos recogidos en el inventario son propios de la organización?

51 - ¿La responsabilidad de los activos está claramente definida en todos los casos?

52 - ¿Existe y se aplica un procedimiento de etiquetado de activos en base a la clasificación adoptada por la organización?

53 - ¿Los activos están clasificados por nivel de exposición y vulneración?

54 - ¿Existen normas para el uso aceptable de la información y de los activos asociados a la información y con los servicios de procesamiento de la información y son identificadas, documentadas e implementadas?

55 - ¿La información está clasificada en función de los requisitos legales, valor, criticidad y sensibilidad a la divulgación no autorizada o modificación?

56 - ¿La información está clasificada como pública, privada y confidencial?

57 - ¿Existe y se aplica un procedimiento de manipulación de activos (procesamiento, almacenamiento, transmisión, desclasificación y destrucción) en base a la clasificación adoptada por la organización?

**- Hardware y Software:**

58 - ¿El hardware y el software son validados para asegurarse de que son compatibles con otros componentes del sistema?

59 - ¿Existe y se aplica un procedimiento para la gestión de soportes extraíbles en base a la clasificación adoptada por la organización?

60 - ¿Existe y se aplica un procedimiento para la eliminación de soportes cuando ya no son necesarios?

61 - ¿Se protegen los soportes contra el acceso no autorizado, mal uso o corrupción durante su transporte?

#### 6.4.1.5 Control de acceso

**- Política de acceso:**

62 - ¿Existe, se aplica y se revisa una política de control de acceso en base a los requisitos de seguridad del negocio y la información?

63 - ¿Los requisitos de control de acceso son periódicamente revisados?

64 - ¿Se establecen reglas con la premisa “generalmente todo está prohibido a no ser que esté expresamente permitido” en la organización?

65 - ¿Existe y se aplica un procedimiento de aprovisionamiento para la asignación o revocación de los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios?

66 - ¿Existe y se aplica un procedimiento de alta o baja en los registros de usuarios?

67 - ¿Se verifica que el nivel de acceso por parte de los usuarios es apropiado para su puesto en la organización?

68 - ¿La asignación y uso de derechos de acceso privilegiados está restringida y controlada a los usuarios que no estén autorizados?

69 - ¿Existe y se aplica un procedimiento de asignación y uso de derechos de acceso privilegiados?

70 - ¿Los privilegios se asignan sobre la base de “solo lo que necesita saber”?

71 - ¿Los propietarios de los activos revisan periódicamente los derechos de acceso de los usuarios?

72 - ¿El acceso a las funciones de información y sistemas de aplicación está restringido en base a la política de control de acceso de la organización?

73 - ¿Se emiten alarmas cuando se violan las políticas de seguridad del sistema?

74 - ¿Está restringido el acceso al código fuente de los programas?

75 - ¿La información confidencial o crítica del negocio tanto lógica como física está guardada bajo llave cuando no está siendo utilizada, especialmente cuando no hay nadie en la plataforma?

76 - ¿Se controlan los derechos de acceso de usuario (lectura, escritura, eliminación o ejecución)?

77 - ¿El acceso a la configuración del sistema operativo de los equipos o servidores solo está permito al usuario administrador?

**- Acceso a la red:**

78 - ¿Los usuarios solo disponen de acceso a la red y a los servicios de red para aquellos que han sido debidamente autorizados?

79 - ¿Se realizan verificaciones periódicas para eliminar identificadores de usuario o cuentas redundantes?

80 - ¿Se utilizan cuentas temporales de usuario para brindarse a los usuarios que las necesiten en momentos puntuales?

81 - ¿Los usuarios siguen las prácticas impulsadas por la organización en materia de autenticación para el uso de información?

82 - ¿El inicio de sesión a los sistemas y aplicaciones está controlado por un procedimiento seguro?

83 - ¿Se registran los intentos exitosos y fallidos a la hora de entrar en un sistema?

84 - ¿Cuándo es apropiado, se restringe el tiempo de conexión a los usuarios?

85 - ¿Se solicita la re autenticación cada cierto tiempo en los sistemas?

86 - ¿Se lleva un registro sobre los logs de aplicaciones sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde el cual está conectado… para ser revisados posteriormente si hiciese falta?

87 - ¿Los logs contienen información relativa a nombres de usuarios, nivel de privilegios, IP del terminal, fecha y hora de acceso o utilización, actividad desarrollada…?

**- Contraseñas y claves:**

88 - ¿El sistema de gestión de contraseñas es interactivo y garantiza la calidad de ellas?

89 - ¿Las contraseñas se mantienen confidenciales entre todos los usuarios de la organización?

90 - ¿Se almacenan las contraseñas en formato físico o lógico sin ninguna medida de seguridad o método aprobado por la organización?

91 - ¿Las claves se cambian a intervalos de tiempo regulares?

92 - ¿Las claves se cambian en base al número de accesos?

93 - ¿Se garantiza la no reutilización de claves usadas anteriormente?

94 - ¿Las claves secretas se cambian la primera vez que se registra el ingreso?

95 - ¿Se incluyen las contraseñas en procesos automatizados (macros o función clave)?

96 - ¿Se muestran las claves a la hora de introducirlas en el sistema?

97 - ¿Se comparten contraseñas individuales entre los usuarios de la organización?

98 - ¿Los usuarios usan la misma clave para propósitos comerciales que no comerciales?

**- Equipamiento, periféricos y documentación:**

99 - ¿Está prohibido el uso de fotocopiadoras u otras tecnologías de reproducción como cámaras o escáneres?

100 - ¿Los documentos impresos con información confidencial son inmediatamente sacados de la impresora?

101 - ¿Se ofrece una protección segura contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso si este traspasa los controles del sistema o aplicación?

102 - ¿Los auriculares son proporcionados por la propia empresa?

103 - ¿Los equipos se apagan al terminar la jornada laboral?

### 6.4.1.6 Criptografía

**- Métodos criptográficos:**

104 - ¿Existe y se aplica una política de seguridad de controles criptográficos que protejan la información?

105 - ¿Existe y se aplica una política sobre la generación, el uso, la protección y la duración de las claves criptográficas a través de todo su ciclo de vida?

106 - ¿Se garantiza la confidencialidad, integridad/autenticidad y no repudio con las técnicas criptográficas usadas en la seguridad de la información?

### 6.4.1.7 Seguridad física y ambiental

**- Seguridad física:**

107 - ¿Están definidos los perímetros de seguridad que protejan a las áreas que contengan información sensible o crítica para la organización?

108 - ¿Existe una barrera que impida acceder al lugar de trabajo a las personas no autorizadas?

109 - ¿Existe y se aplica la seguridad en todas las instalaciones, oficinas y despachos?

110 - ¿Los puntos de acceso para carga y descarga y otros puntos donde personas no autorizadas pueden acceder son controlados y aislados, siempre que se pueda?

111 - ¿Se inspecciona todo el material que entra en los puntos de carga y descarga antes de que se traslade al interior de la plataforma?

112 - ¿Las ventanas y puertas de la plataforma garantizan la seguridad de la información que puedan guardar en sus habitaciones?

113 - ¿La plataforma está dotada en todas sus áreas de sistemas de detección de intrusos y alarmas?

114 - ¿Los recorridos y salidas de evacuación, extintores, bocas de incendios o cuadros eléctricos están correctamente señalizados y no obstaculizados?

115 - ¿El Centro de Procesamiento de Datos (o CPD) y la sala de servidores están separados físicamente mediante una división reconocible y segura, recubierta de un material aislante o protegido contra el fuego?

116 - ¿El rack se encuentra en un sitio correctamente refrigerado?

117 - ¿Los puntos de ingreso y salida de correo y fax están correctamente protegidos?

**- Acceso físico:**

118 - ¿Se dispone de personal en la recepción del edificio para controlar el acceso físico?

119 - ¿Se dispone de cámaras de seguridad en toda la plataforma?

120 - ¿Se registra la entrada y salida de los visitantes autorizados que acceden a la plataforma?

121 - ¿Se requiere cualquier tipo de procedimiento (tarjeta magnética o de proximidad, sistema biométrico…) para acceder al interior del edificio?

122 - ¿Se requiere a los empleados o visitantes que muestren una identificación visible dentro de la plataforma?

123 - ¿Los equipos están situados y protegidos para reducir los riesgos de amenazas ambientales o de acceso no autorizado?

124 - ¿El acceso a áreas seguras está protegido mediante controles de entrada adecuados que garanticen la entrada solo al personal autorizado?

125 - ¿El acceso al Centro de Procesamiento de Datos (o CPD) y la sala de servidores está restringido?

**- Desastres naturales, ataques y accidentes:**

126 - ¿El lugar de trabajo está protegido contra desastres naturales (terremotos, inundaciones, tormentas eléctricas…)?

127 - ¿El mobiliario de la plataforma está calificado como anti terremotos?

128 - ¿Las tuberías de la plataforma están aisladas de la red de cableado eléctrico y de telecomunicaciones?

129 - ¿Hay establecido un perímetro dentro de la plataforma para fumadores?

130 - ¿Se vigila que los empleados no fumen dentro de la plataforma como en baños o escaleras?

131 - ¿Se realizan temporalmente simulacros de incendios?

132 - ¿La plataforma dispone de equipo contra incendios adecuado?

133 - ¿El lugar de trabajo está protegido contra ataques maliciosos?

134 - ¿El lugar de trabajo está protegido contra accidentes?

135 - ¿El equipo de reemplazo y los medios de respaldo se encuentran a una distancia segura en caso de que un desastre afecte al local principal?

136 - ¿Existen y se aplican procedimientos para trabajar en áreas seguras?

**- Energía y cableado:**

137 - ¿Los equipos están protegidos contra el fallo en el sistema de energía?

138 - ¿Existe un equipo de SAI en la plataforma por si ocurriese cualquier problema con la red eléctrica principal?

139 - ¿Los equipos están conectados a tomas de corriente que son alimentadas por el SAI?

140 - ¿Los ladrones o las regletas se controlan para que no estén saturados a riesgo de que se produzca un incendio?

141 - ¿El cableado de la energía y de las telecomunicaciones (de red) que transporta datos, están instalados físicamente uno del otro para evitar interferencias?

142 - ¿El cableado de la energía y de las telecomunicaciones (de red) que transporta datos o apoya a los servicios de información están bien protegidos contra la interceptación, interferencia o daños?

**- Acceso a los equipos:**

143 - ¿Los equipos son correctamente mantenidos para asegurar su continua disponibilidad e integridad?

144 - ¿Los equipos, la información y el software no son retirados del sitio sin una autorización previa?

145 - ¿Se toman los controles oportunos cuando un activo o equipo sale fuera de las instalaciones para garantizar su seguridad?

146 - ¿Se verifican los medios que tiene un equipo contenidos previamente a su eliminación o reutilización?

147 - ¿Los usuarios están suficientemente concienciados para asegurar el equipo cuando está desatendido?

148 - ¿Se cierran las sesiones activas cuando superan un determinado espacio de tiempo de inactividad fijado?

149 - ¿Se desconecta a los usuarios de los mainframes, servidores y ordenadores cuando se finaliza la sesión?

150 - ¿Está activada la opción del protector de pantalla cuando se pasa un límite de tiempo fijado por la organización?

151 - ¿La sesión puede reanudarse mediante el acceso de una clave secreta cuando no estén en uso y se encuentre bloqueada?

152 - ¿Se aplica una política de escritorio limpio en los puestos de los usuarios evitando que sobre él se encuentren papeles o soportes extraíbles, por ejemplo?

**- Seguridad en el lugar de trabajo:**

153 - ¿La temperatura ambiente de la plataforma está comprendida entre los 20 y 24 grados?

154 - ¿La plataforma cuenta con unas condiciones de ventilación suficientes para que no se eleven los niveles de monóxido de carbono?

155 - ¿La iluminación de la plataforma tiene un 50% mínimo de luz natural?

156 - ¿La iluminación artificial perpendicular al puesto de trabajo de un agente es menor de 400 LUX?

157 - ¿Está prohibido el consumo de bebidas en los puestos de trabajo del operario?

158 - ¿Los usuarios utilizan cascos y auriculares incorporados teniendo libertad en ambas manos?

159 - ¿Los empleados o contratistas trabajan con un estrés que puede ser perjudicial para su trabajo?

160 - ¿Los empleados o contratistas disponen de herramientas ergonómicas que les ayuden físicamente en su trabajo?

161 - ¿Los empleados o contratistas disponen de reposapiés para evitar cargar la parte de la espalda al adoptar una posición sentada en una silla?

162 - ¿Se proporciona a los agentes almohadillas para cascos y micrófono con el fin de prevenir contagios de enfermedades entre ellos?

163 - ¿Se limpian los equipos, terminales y puestos de trabajo con suficiente regularidad para prevenir posibles contagios o problemas de suciedad?

#### 6.4.1.8 Seguridad en las operaciones

**- Política de seguridad en las operaciones**

164 - ¿Los procedimientos realizados en la organización relativos a las operaciones con la información están correctamente documentados y puestos a disposición de cualquier usuario que los necesite?

165 - ¿Los cambios en la organización, procesos de negocio, servicios de procesamiento de la información y sistemas que afectan a la seguridad son controlados?

166 - ¿La capacidad que garantiza el funcionamiento de los sistemas es supervisada y ajustada a las proyecciones futuras para el uso correcto de sus recursos?

167 - ¿Se realizan controles de detección, prevención y recuperación como protección al código malicioso (malware) junto con el conocimiento del usuario?

168 - ¿Se prohíbe la instalación de software no autorizado?

169 - ¿Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad están sincronizados con un solo tiempo oficial de referencia?

170 - ¿Está controlada la instalación de software en los sistemas de operación por medio de cualquier procedimiento?

171 - ¿Existen y se aplican normas para la instalación de software por medio de los usuarios?

172 - ¿Existe y se aplican procedimientos para identificar posibles vulnerabilidades técnicas?

**- Pruebas:**

173 - ¿Los entornos de desarrollo y pruebas están separados de los operacionales?

174 - ¿Se utilizan perfiles diferentes para los sistemas operacionales y de pruebas?

175 - ¿Hay datos confidenciales en entornos de prueba?

176 - ¿Se prueban y evalúan los parches antes de instalarlos para comprobar su efectividad y que no provoquen efectos secundarios en los sistemas?

177 - ¿Las comprobaciones se realizan con acceso limitado de lectura al software y datos?

**- Back ups:**

178 - ¿Se realizan backs ups, diariamente, semanalmente y trimestralmente para los activos de mayor importancia o críticos?

179 - ¿Las copias de seguridad (back ups), software e imágenes del sistema son tomadas y probadas regularmente?

180 - ¿Los back ups se almacenan en un lugar lo suficientemente apartado del local principal por si ocurriese algún desastre natural en él?

181 - ¿Los back ups son almacenados en unas condiciones físicas y ambientales apropiados?

182 - ¿Los back ups son probados regularmente para probar que pueden ser utilizados cuando se de una emergencia sin ningún problema?

183 - ¿Los procedimientos de back up son automatizados?

**- Protección de registros y actividades:**

184 - ¿Los registros de eventos graban las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información que se produzcan, cuidándose y revisándose regularmente?

185 - ¿Están protegidos los registros de servicios y de la información contra la falsificación y el acceso no autorizado?

186 - ¿Las actividades del administrador y del gestor de las actividades del sistema son registradas y revisadas periódicamente?

187 - ¿Los registros y actividades de auditoría relacionados con los sistemas de información se realizan de tal manera que se minimicen las interrupciones en los procesos de negocio?

188 - ¿Los registros y actividades de auditoría relacionados con los sistemas de información se realizan de tal manera que en ningún momento se modifica la información contenida?

189 - ¿Se registran todos los accesos a la red por medio de archivos de registro o logs?

**Auditoría:**

190 - ¿Las personas que llevan a cabo las auditorías son independientes de las actividades auditadas?

**- Almacenamiento y documentación:**

191 - ¿La eliminación de papeles, medios y equipos se realiza por parte de la propia organización o se delega en otra totalmente ajena?

192 - ¿La eliminación de documentos confidenciales en papel se realiza a través de un destructor de papel o por una empresa externa que aporte un certificado?

193 - ¿Los usuarios solo almacenan la información en la ruta destinada por organización?

## 6.4.1.9 Seguridad en las comunicaciones

**- Política de seguridad en las comunicaciones:**

194 - ¿Existen y se aplican procedimientos para notificar al remitente cuando se realice un intercambio de información en la transmisión, despacho y recepción?

195 - ¿Se usan firmas electrónicas por cada una de las partes implicadas cuando se realice una transacción de información?

196 - ¿Existen acuerdos para la transferencia de información con organizaciones externas?

197 - ¿Los acuerdos de confidencialidad y de no divulgación que salvaguarden la información de la organización son identificados, revisados regularmente y documentados?

198 - ¿Está especificada inequívocamente la información que deberá protegerse en los acuerdos de confidencialidad y de no divulgación?

**- Seguridad en la red:**

199 - ¿Las redes son gestionadas y controladas correctamente para preservar la seguridad de la información?

200 - ¿Se establecen controles especiales para salvaguardar la confidencialidad en redes públicas o inalámbricas por las que puede circular información?

201 - ¿Los servicios de red proveídos por la propia empresa o subcontratados son identificados e incluidos los mecanismos de seguridad, niveles de servicio y requisitos de gestión en los acuerdos de servicio de red?

202 - ¿Están segregados en redes los grupos de servicio de la información, usuarios y sistemas de información?

203 - ¿Existe y se aplica una política de transferencia de información, con procedimientos o controles, que protejan el uso de la información a través de todos los tipos de servicios de comunicación?

204 - ¿Los procedimientos del intercambio de información los protegen de la intercepción, copiado, modificación, enrutamiento equivocado y destrucción?

205 - ¿Se usan técnicas de codificación para proteger la confidencialidad, integridad y autenticidad de la información?

206 - ¿Existe algún tipo de protección para los mensajes que se envíen a través del correo electrónico?

**- Cumplimiento legal:**

207 - ¿El personal revela información confidencial al receptor cuando realiza una llamada telefónica?

208 - ¿La información obtenida cumple con la Ley Orgánica de Protección de Datos vigente actualmente en nuestro país?

209 - ¿Se avisa acerca de las grabaciones de datos personales?

210 - ¿La organización cumple con la Ley de Defensa de Consumidores y Usuarios con los contratos realizados telefónicamente o a través de internet?

**- Seguridad en los sistemas:**

211 - ¿El personal registra algún dato demográfico relativo a él en cualquier software?

## 6.4.1.10 Adquisición, Desarrollo y Mantenimiento de los sistema de información

**- Transmisión de la información:**

212 - ¿La información que se transmita a través de redes públicas está protegida de la actividad fraudulenta, disputa de contrato, la modificación y la divulgación no autorizada?

213 - ¿Se previene la transmisión incompleta, mal enrutamiento, alteración del mensaje no autorizado, la divulgación no autorizada, la duplicación de mensajes no autorizada o la reproducción en las transacciones de aplicación de la información?

**- Ciclo de vida de los sistemas de información:**

214 - ¿Existe y se aplica una política para el desarrollo de software y sistemas dentro de la organización?

215 - ¿Son controlados por medio de procedimientos formales los cambios en los sistemas dentro del ciclo de vida de desarrollo?

216 - ¿Son revisadas y probadas las plataformas de operación cuando son cambiadas con el fin de que no haya un impacto negativo en las operaciones de negocio de la organización o de la seguridad?

217 - ¿Las modificaciones en los paquetes de software están limitadas a cambios necesarios o controlados?

218 - ¿Se utilizan los principios de ingeniería segura de sistemas para la implementación de cualquier sistema de información?

219 - ¿Se garantiza una seguridad adecuada para los entornos de desarrollo para sistemas de desarrollo y esfuerzos de integración?

220 - ¿Se supervisan y monitorizan las actividades de desarrollo del sistema que estén externalizadas?

221 - ¿Las pruebas de funcionalidad de seguridad se llevan a cabo durante la fase de desarrollo?

222 - ¿Se establecen programas de prueba de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones o nuevas versiones?

223 - ¿Los datos de prueba son seleccionados cuidadosamente, protegidos y controlados?

## 6.4.1.11 Relaciones con proveedores

**- Política de seguridad con proveedores:**

224 - ¿Existe y está documentada una política de seguridad de la información para el acceso a los activos de la organización?

225 - ¿Los requisitos de seguridad de la información son establecidos y acordados con cada proveedor que tenga cualquier contacto con la información de la organización?

226 - ¿Los acuerdos con proveedores incluyen requisitos para tratar los riesgos de la seguridad de la información?

227 - ¿Se supervisa, revisa y audita el servicio entregado por proveedores regularmente?

228 - ¿Los cambios en la provisión de servicios por parte de los proveedores se gestiona para no perjudicar a la organización en materia de información, sistemas, procesos y reevaluación de riesgos?

## 6.4.1.12 Gestión de incidentes de seguridad de la información

**- Política de gestión de incidentes:**

229 - ¿Los procedimientos y responsabilidades garantizan una respuesta rápida, eficaz y ordenada siempre que se detecte una incidencia de seguridad de la información?

230 - ¿Los eventos de seguridad de la información se reportan con la mayor celeridad posible?

231 - ¿Los eventos de seguridad de la información se reportan a través de canales seguros?

232 - ¿Los eventos de seguridad de la información se analizan para determinar si son clasificados como incidentes de seguridad?

233 - ¿Los incidentes de seguridad de la información son respondidos en base a los procedimientos documentados?

234 - ¿Se utilizan técnicas de aprendizaje basadas en el análisis y la resolución de incidentes para reducir la probabilidad de que se den nuevos incidentes futuros?

235 - ¿Los procedimientos de identificación, recolección, adquisición y conservación están definidos para garantizar la evidencia de cualquier incidente de seguridad?

## 6.4.1.13 Seguridad de la información en aspectos de la Gestión de la Continuidad Comercial

**- Política de la Continuidad Comercial en materia de seguridad de la información:**

236 - ¿Se utilizan medidas preventivas para minimizar el uso de Plan de Continuidad Comercial?

237 - ¿Están determinadas las necesidades de seguridad de la información y continuidad de la gestión de la seguridad de la información en caso de que se de una situación adversa?

238 - ¿Están establecidos, documentados, implementados y mantenidos los procesos, procedimientos y controles que garanticen un nivel de continuidad necesario en caso de que se de una situación adversa?

239 - ¿Los controles que verifican que los procedimientos de continuidad de la seguridad de la información son revisados cada cierto tiempo para garantizar su validez y eficacia?

240 - ¿Las instalaciones de procesamiento de información satisfacen los requisitos de disponibilidad tiene una redundancia suficiente?

## 6.4.1.14 Cumplimiento

**- Legislación:**

241 - ¿La organización cumple con los estatutos legislativos, reglamentarios y contractuales y están identificados de manera explícita, documentada y mantenida?

242 - ¿La organización cumple con los derechos de propiedad intelectual y el uso de productos software de propietarios?

243 - ¿Los registros están protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada en base a su legislación y reglamentación?

244 - ¿La privacidad y la protección de información de carácter personal están protegidos en base a su legislación y reglamentación?

245 - ¿Los controles criptográficos se utilizan en base a su legislación y reglamentación?

**- Revisiones de cumplimiento a la política de seguridad:**

246 - ¿Se revisa periódicamente y de forma independiente el enfoque de la organización para la gestión de la seguridad de la información y su aplicación?

247 - ¿Se comprueba periódicamente a través de la gerencia si los procedimientos de procesamiento y la información cumplen con la política de seguridad, normas y otros requisitos de seguridad?

248 - ¿Se comprueba periódicamente si los sistemas de información cumplen con la política de seguridad de la información y otros estándares?

## 6.4.2 Cuestionario sobre la Calidad de la Información

### 6.4.2.1 Servicio

**- Calidad en el servicio:**

1 - ¿Se busca que los agentes den una solución para la transacción basada en la "resolución en el primer contacto" para evitar una generación posterior para la misma transacción?

2 - ¿Se utilizan suscripciones, vales, productos gratuitos, compensaciones económicas directas, entregas urgentes o eliminación de costes de tramitación para compensar a los usuarios por un mal servicio?

3 - ¿Se identifican y tipifican las transacciones más comunes para realizar sobre ellas procedimientos que agilicen y simplifiquen su resolución?

4 - ¿Se brindan a los usuarios finales alternativas a la resolución de sus problemas para evitar que utilicen el medio para el cual realizaron la primera interacción para resolver su consulta?

**- Eficiencia en el servicio:**

5 - ¿Se focaliza en el umbral del cumplimiento del "tiempo medio de gestión" para cada agente que atiende una transacción?

6 - ¿La ocupación del agente, es decir, el tiempo en el cual no hace ningún trabajo productivo, tiende a ser minimizada?

7 - ¿Se buscar reducir la utilización de los agentes, es decir, el tiempo el tiempo en el que no están listos para manejar una transacción, lo que implicará una reducción del número de agentes?

8 - ¿Se busca reducir el coste por transacción o no es una medida relevante para la organización?

9 - ¿Los agentes del servicio de atención al cliente son eficaces con las oportunidades de ventas (up-selling) o venta cruzada (cross-selling)?

**- Mejoras en el servicio:**

10 - ¿Se incide en la resolución de las consultas en la primera transacción para evitar la generación de una transacción pendiente para su resolución?

11 - ¿Se transmite a los empleados que una mala gestión en su trabajo puede repercutir en penalizaciones para la organización por parte del cliente?

**- Personal**

12 - ¿Se estima el coste de la rotación del personal teniendo en cuenta los costes directos de formación, productividad reducida de los nuevos contratados, costes de horas extras…?

13 - ¿Se calcula el impacto del ausentismo incluyendo costes salariales directos y horas extra?

14 - ¿Los estándares usados para medir la ejecución del personal reflejan productividad, calidad, contribución a las ventas y el beneficio y la satisfacción del cliente?

**- Ganancias directas en resultados.**

15 - ¿Las operaciones de contacto que repercuten un beneficio económico como ventas o cobranzas, se miden en €/$ del desempeño que ha mejorado?

16 - ¿Las operaciones de contacto que tratan sobre la captación de clientes se convierten en una cifra de ingresos en las que están relacionados un factor de conversión y un valor de ventas promedio?

17 - ¿Las operaciones de contacto que requieren la retención se calculan como el gasto anual de un usuario final retenido?

18 - ¿La mejora en cobranzas se evalúa como una mejora real en ella con respecto al año anterior?

**- Beneficios intangibles:**

19 - ¿Se tiene en cuenta la lealtad de los clientes y el incremento de su satisfacción con la organización al igual que pérdida de clientes y decremento de su satisfacción?

20 - ¿Se mide la satisfacción del cliente a través de encuestas para valorar su nivel?

#### 6.4.2.2 Liderazgo y planteamiento

**- Declaración de la dirección**

21 - ¿Está comprometida con el usuario final y clientes?

22 - ¿Contiene uno o más aspectos relativos a la satisfacción del cliente, satisfacción del usuario final, servicio, calidad, ventas o costes?

23 - ¿Las ventas, marketing y departamento del servicio (de la plataforma) se ven regularmente para discutir programas y problemas dirigidos al cliente?

24 - ¿Apoya el uso de múltiples canales de comunicaciones, incluyendo teléfono, e-mail, chat, fax, correo y redes sociales?

**- Desarrollo de Planes de negocio**

25 - ¿La organización incluye en sus planes de negocio a las redes sociales como elemento con un impacto potencial en la satisfacción del usuario final, ingresos y costes?

26 - ¿La organización dispone de un proceso para la gestión de las redes sociales en el cual por medio de un criterio se determina que transacciones se responderán o enviarán al departamento apropiado?

27 - ¿La organización tiene un proceso formal para capturar y compartir el conocimiento del usuario final e información competitiva con ventas, marketing, desarrollo del producto, operaciones y alta dirección en el momento oportuno?

**- Definición de objetivos**

28 - ¿Para todas las métricas requeridas, los objetivos son identificados claramente y se tiene la información suficiente para distinguir las tendencias?

29 - ¿Todos los departamentos dirigidos al cliente comparten objetivos comunes y estándares por éxito?

30- ¿El gestor del CC participa activamente en el ajuste de objetivos corporativos?

31 - ¿Tiene el CC objetivos de ventas y beneficios?

**- Revisión de los Resultados de Negocio**

32 - ¿Se realiza mensualmente un análisis del desempeño en resultados comparándolo con los objetivos y planes de negocio para todas las métricas requeridas?

33 - ¿Se toman acciones si los resultados están por debajo del objetivo marcado?

#### 6.4.2.3 Procesos

**- Gestión del cambio**

34 - ¿Se identifican los procesos y las métricas asociadas a ellos cuando se realice cualquier tipo de cambios importantes en productos, servicios, programas, requisitos del cliente o de usuarios finales?

35 - ¿Se avisa por métodos formales tanto a los usuarios finales como al personal si se produce cualquier tipo de cambio y se proporciona la formación requerida para cada caso?

36 - ¿Cada proceso se audita completamente al menos anualmente?

37 - ¿Se utilizan acciones correctivas para procedimientos que no están alcanzando el nivel de resultados en tres cuartas partes (¾) de periodos de tiempo?

38 - ¿La organización demuestra que las acciones llevadas a cabo han mejorado en el desempeño de los procesos?

**- Monitorizaciones**

39 - ¿El monitoreo de transacciones se realiza a nivel de proceso y de agente?

40 - ¿Se monitorea el 100% de las transacciones del usuario final?

41 - ¿Se realizan monitorizaciones tanto en remoto como en paralelo?

42 - ¿Cuántas transacciones se evalúan para cada empleado mensualmente?

43 - ¿Las transacciones a ser evaluadas se eligen de forma aleatoria?

44 - ¿La metodología usada para seleccionar las muestras a ser monitorizadas es lo suficientemente confiable?

45 - ¿Se monitoriza toda la información recogida y ofrecida por parte de los agentes en una transacción?

46 - ¿Se establece una relación entre los errores críticos del usuario final y los resultados de satisfacción e insatisfacción del usuario final?

47 - ¿Los agentes aprueban las monitorizaciones si se cometen uno o más errores críticos de cualquier tipo?

48 - ¿El personal que realiza las monitorizaciones está correctamente formado?

49 - ¿Se calibra a los agentes para comprobar que sus conocimientos y se evalúan dichas puntuaciones cada cierto tiempo?

50 - ¿Hay una consistencia en los resultados de los agentes dependiendo de que la monitorización sea realizada por una u otra persona?

51 - ¿Al analizar los resultados del monitoreo se toman acciones a nivel de programa y a nivel de agente si los resultados no son satisfactorios?

52 - ¿Los agentes que se han incorporado más recientemente a la organización son monitorizados con mayor asiduidad que el resto?

53 - ¿Se reporta al agente un resultado tanto positivo como negativo de sus monitorizaciones?

54 - ¿En caso de que cualquier agente no apruebe una monitorización, se realiza coaching o se utilizan aplicaciones especiales de aprendizaje sobre ellos?

55 - ¿En caso de que cualquier agente no apruebe una monitorización, se aumentará el número de éstas?

56 - ¿Se toman acciones correctivas para los agentes que continuamente suspenden las monitorizaciones sin mejoría alguna?

**- Pronóstico**

57 - ¿Se conoce o realiza el pronóstico del volumen futuro para cada tipo de transacción?

58 - ¿La precisión del pronóstico de volumen se realiza con suficiente antelación temporal?

59 - ¿La precisión del pronóstico del TMO (Tiempo Medio Operativo) o TMM (Tiempo Medio de Manejo) se calcula diariamente?

60 - ¿Los pronósticos relacionados con el objetivo de nivel de servicio o duración de ciclo se realizan a intervalos de tiempo suficientes?

**- Requisitos de demanda**

61 - ¿Se calcula la cantidad de personal requerido con la suficiente antelación para que en caso de que se necesite se pueda reclutar e incorporar?

62 - ¿La organización usa un modelo cuantitativo para crear programaciones para el personal requerido?

**- Programación**

63 - ¿Se establecen programaciones cada 30 minutos que calculen posibles minimizaciones entre los requisitos de la demanda y la capacidad asignada para ella para intervalos de entornos en tiempo real?

64 - ¿Se establecen programaciones para el cumplimiento de duración de ciclo que calculen posibles minimizaciones entre los requisitos de la demanda y la capacidad asignada para ella para intervalos de entornos en transacciones diferidas?

**- Gestión en tiempo real**

65 - ¿Se tienen en cuenta a nivel de planificación y programación los posibles inconvenientes que se puedan producir por causas de ausentismo, formaciones o un volumen mayor del esperado?

66 - ¿Se toman medidas para equilibrar el pronóstico o la planificación si el desempeño diario difiere del estimado por las causas anteriormente mencionadas (ausentismo, formaciones…)?

67 - ¿Se toman medidas cuando se presentan condiciones anormales durante el servicio o fuera de él?

**- Asignación de transacciones**

68 - ¿Se utiliza un enfoque estructurado para la asignación de transacciones tanto para operaciones normales como para aquellas en condiciones anormales que puedan presentarse?

69 - ¿Se realizan revisiones periódicas para optimizar las políticas y procedimientos del desempeño?

70 - ¿Se revisan los desvíos a centros específicos, colas o agentes periódicamente de acuerdo al enfoque estructurado (e incluso al basado en habilidades)?

71 - ¿Se monitorean los entornos de cola compartida en centros que trabajen en tiempo real para la puntualidad y la ocupación y/o utilización?

72 - ¿Se toman acciones correctivas cuando no se cumplen los objetivos del desempeño?

**- Cumplimiento**

73 - ¿Se asegura el cumplimiento de los requisitos regulatorios nacionales, autonómicos o locales dependiendo del país?

74 - ¿Se protege la privacidad del usuario final?

75 - ¿Se considera un error crítico la violación del cumplimiento o de la política de privacidad?

**- Tecnología**

76 - ¿Se brindan soluciones tecnológicas al personal de Sistemas de Contacto con Clientes, Sistemas Automatizados de Fuerza de Ventas y/o Sistemas Automatizados de Marketing, Sistemas de Producción y Sistemas de Soporte?

77 - ¿Para cada tecnología se aprueba para que cada sistema dé un servicio al usuario final y/o personal de manera correcta y eficiente?

78 - ¿Se realizan revisiones periódicas de los sistemas con el fin de actualizarlos a versiones más recientes o para cerciorarse de que funcionan correctamente?

79 - ¿Se realizan encuestas de satisfacción sobre el sistema a los usuarios finales?

80 - ¿Se invita y motiva al usuario final para que realice las encuestas?

81 - ¿Se recoge un feedback del personal que trabaja con los sistemas en cuanto a usabilidad y funcionalidad de los mismos?

82 - ¿Se miden y gestionan todas las métricas requeridas por los sistemas?

83 - ¿La información recogida en los sistemas es solo usada por los agentes o por los propios sistemas para su tratamiento?

84 - ¿Los términos o instrucciones del sistema siguen una consistencia con las comunicaciones externas o a un lenguaje intuitivo?

85- ¿Los sistemas permiten a los usuarios corregir o borrar algún dato si a la hora de introducirlos no fuesen de forma correcta?

86 - ¿Los Sistemas de Producción (Sistema de marcación, Gestor de Conocimiento…) cuentan con un enfoque estructurado respecto a las caídas de servicio que puedan ocurrir?

87 - ¿Se introducen sanciones y recompensas para motivar a los agentes en el uso del Gestor de Conocimiento?

88 - ¿La información del Gestor de Conocimiento está actualizada y posee un procedimiento para que siempre lo esté?

89 - ¿Cada cuánto tiempo se revisa la información del Gestor de Conocimiento?

90 - ¿Los Sistemas de Soporte utilizan al máximo su capacidad para mejorar la satisfacción de las personas del entorno de la organización y la calidad, servicio y eficiencia?

91 - ¿Se utilizan las redes sociales proactiva/reactivamente para cualquier gestión con usuarios finales?

92 - ¿La organización invierte en aplicaciones, como las del análisis de voz o analíticas en tiempo real, que capturan, analizan y sintetizan los datos en conversaciones y comunicaciones de usuarios finales inestructurados?

93 - ¿El IVR (Interactive Voice Response, sistema de Respuesta de Voz Interactiva) es una herramienta intuitiva y fácil de usar para el usuario final?

94 - ¿Se involucra a los agentes en el diseño del sistema del IVR y las pruebas del mismo si es posible por parte de la organización?

95 - ¿Se invierte en la interfaz de usuario de voz, el diseño del diálogo, el personaje del sistema, y la voz del IVR?

96 - ¿Los diálogos del IVR son breves y sencillos y usan el lenguaje adecuado?

97 - ¿El número de opciones del menú/submenús del IVR es menor de cuatro?

**- Gestión de proveedores clave.**

98 - ¿La organización cuenta con un contrato, acuerdo de nivel de servicio o carta de sus requisitos para cada proveedor?

99 - ¿Se analiza temporalmente el desempeño de los proveedores?

100 - ¿Se da un feedback temporalmente del desempeño a los proveedores?

101 - ¿Se desarrollan planes de acciones correctivas para aquellos proveedores en los cuales el desempeño fuese deficiente?

**- Continuidad del negocio.**

102 - ¿La organización evalúa los riesgos potenciales que puedan amenazar la continuidad del negocio y desarrolla planes de contingencia por si ocurriesen?

103 - ¿La organización establece planes documentados para interrupciones menores (de hasta seis horas)?

104 - ¿La organización prueba anteriormente los planes documentados, bien sea mediante simulaciones o sucesos reales?

105 - ¿La organización establece planes documentados para interrupciones mayores, en las que se establezcan el mantenimiento o restauración del servicio, la aseguración de la integridad de los datos y la capacidad de minimizar el tiempo de inactividad?

106 - ¿El personal de recuperación tiene claro el objetivo de restauración correspondiente a comunicaciones, servidores y ordenadores y aplicaciones de software?

**- Reportes e integridad de los datos.**

107 - ¿Hay un personal dedicado exclusivamente al *reporting*?

108 - ¿Para las métricas requeridas se asegura que los datos son correctamente recolectados, íntegros, es decir, significativos, objetivos, precisos y representativos?

109 - ¿Los reportes están disponibles solo para el personal apropiado?

#### 6.4.2.4 Recursos Humanos

**- Definición del puesto de trabajo.**

110 - ¿Se establecen unas habilidades y conocimientos mínimos para los puestos con el fin de garantizar que el desempeño por parte del usuario es el requerido para ocupar el puesto?

111 - ¿Las habilidades y conocimientos básicos para el puesto requieren de su verificación?

112 - ¿Reciben cualquier tipo de compensación el personal que realiza cambios en sus horarios u horas extras?

**- Reclutamiento y Contratación**

113 - ¿El enfoque del reclutamiento tiene como objetivo la incorporación de personas que cumplan una serie de requisitos mínimos y que tengan una alta probabilidad de desempeñar su trabajo exitosamente?

114 - ¿Se mide y gestiona el reclutamiento y contratación por medio de cualquier métrica de calidad?

115 - ¿Se prueba a los agentes antes de la contratación?

**- Formación y Desarrollo**

116 - ¿Se forma al personal para que adquiera las habilidades y el conocimiento necesario para desarrollar su desempeño a menos que ya las posea?

117 - ¿Se define la metodología o el marco de formación (aula, entrenamiento en el puesto de trabajo, teleformación…)?

118 - ¿Se enumeran las habilidades y conocimientos para el uso de cualquier sistema o seguimiento de un procedimiento o proceso?

119 - ¿El personal de formación está identificado y formado?

120 - ¿Están definidos los resultados deseados y requeridos por parte del proceso de formación?

121 - ¿Se realizan formaciones adicionales si los requisitos de habilidades y conocimientos cambian?

122 - ¿Se mide y gestiona la formación por medio de cualquier métrica de calidad?

123 - ¿Se utiliza una formación estructurada para establecer un plan de carrera para el personal de la organización?

124 - ¿Se realizan formaciones para conseguir agentes universales que puedan ser más multidisciplinares en ciertos momentos?

125 - ¿Se fomenta la promoción interna basada en conocimientos dentro de la organización?

**- Verificación de Habilidades y Conocimientos**

126 - ¿El personal que pasa los umbrales mínimos de desempeño, es capaz de realizar el desempeño satisfactoriamente de su puesto?

127 - ¿Se utiliza cualquier tipo de documentación en la formación que pueda ser auditada?

128 - ¿Existen planes de acción para el personal que no demuestra una habilidad y conocimiento mínimo requerido?

129 - ¿El personal temporal o externo siguen las mismas verificaciones que el indefinido?

130 - ¿Se verifican temporalmente las habilidades y conocimientos del personal?

**- Gestión del desempeño del personal**

131 - ¿Se realizan revisiones temporales del personal con respecto al desempeño individual en los objetivos?

132 - ¿Las evaluaciones del personal se centran tanto en las habilidades y conocimientos como en las monitorizaciones realizadas?

133 - ¿Se tiene un reporte formal o *scorecard* que refleje todas las actividades del agente en un documento?

134 - ¿Se cambia al personal más capacitado a puestos o departamentos donde las habilidades requieran una mayor dificultad sin su consentimiento?

**- Gestión del feedback del personal**

135 - ¿Se solicita de forma proactiva un feedback al personal de la organización?

136 - ¿Se realizan encuestas de satisfacción temporalmente al personal de la organización?

137 - ¿Se invita y motiva al personal para que realice las encuestas?

138 - ¿Se toman medidas correctivas una vez analizados los estudios del feedback del personal?

139 - ¿Reciben los agentes semanal o mensualmente sus reportes de ejecución?

140 - ¿Los agentes tienen la oportunidad de evaluar a sus supervisores y gerentes (una evaluación de 360 grados)?

**- Rotación y ausentismo del personal**

141 - ¿Hay objetivos definidos con la rotación y ausentismo del personal en base a los requisitos del negocio y las condiciones laborales?

142 - ¿La medición de la rotación y el ausentismo se hace en función del tipo de empleado (agente, supervisor, gerente…) y a nivel de entidad y de programa?

143 - ¿Se reporta con una cifra porcentual y anualmente la rotación del personal?

144 - ¿Cuál es la tasa de abandono de agentes anual?

145 - ¿Se distingue entre desvinculaciones voluntarias e involuntarias?

146 - ¿Se distingue entre desvinculaciones voluntarias e involuntarias para contratos temporales?

147 - ¿Se mide y gestiona la rotación y el ausentismo por medio de cualquier métrica de calidad?

## 6.4.2.5 Resultados

**- Satisfacción e insatisfacción del usuario final**

148 - ¿La organización identifica, evalúa cuantitativamente y comprende la importancia de los atributos que repercuten en la satisfacción e insatisfacción del usuario final?

149 - ¿La organización cuantifica estos atributos a nivel de transacción individual y de programa?

150 - ¿Con qué periodicidad se mide y se analiza la satisfacción e insatisfacción del usuario final?
**En esta pregunta las opciones serán Diaria, Semanal, Mensual, Anual, NS/NC*

151 - ¿Los objetivos de satisfacción e insatisfacción del usuario final se establecen de tal forma que sean representativos y están apoyados en estudios para desempeños iguales o similares?

152 - ¿Cada cuanto tiempo se actualizan los objetivos de satisfacción e insatisfacción?
**En esta pregunta las opciones serán Diaria, Semanal, Mensual, Anual, NS/NC*

153 - ¿Las muestras de satisfacción e insatisfacción del usuario final son lo suficientemente representativas?

154 - ¿Las muestras incluyen todo tipo de transacciones, en una proporción que tenga una relación con los volúmenes que maneje la organización?

**- Satisfacción del cliente**

155 - ¿Se cuantifica a nivel de programa la satisfacción del cliente de forma global y por atributos específicos?

156 - ¿Con qué periodicidad se mide y se analiza la satisfacción e insatisfacción del cliente?
**En esta pregunta las opciones serán Diaria, Semanal, Mensual, Anual, NS/NC*

157 - ¿Se mide la satisfacción del cliente con aquellos actores que tengan influencia en la organización o interacción con ella?

**- Insatisfacción del cliente**

158 - ¿De qué forma está definida una queja por parte del cliente?

159 - ¿Las quejas se gestionan a nivel de programa, de distintos programas con el cliente y a nivel de organización para los diferentes clientes?

160 - ¿Las quejas del cliente se clasifican y registran por causa o síntoma?

161 - ¿Hay un proceso para la gestión de respuesta a las quejas del cliente?

162 - ¿Se sigue una métrica de “puntualidad de respuesta” o “puntualidad de resolución” para las quejas del cliente que se hayan recibido?

163 - ¿Se utiliza un enfoque basado en la acción correctiva y mejora sostenida para las quejas recibidas por el cliente?

**- Desempeño del servicio**

164 - ¿Está contemplado el muestreo a la hora de recabar la información de los datos del desempeño del servicio?

165 - ¿Se analiza mensualmente la información del desempeño del servicio?

166 - ¿Los objetivos establecidos para cada métrica de desempeño son consistentes con respecto a la declaración de la dirección y el plan anual de negocio de la entidad, sobre todo en tiempo real, velocidad de respuesta y tasa de abandono?

167 - ¿Los datos del servicio se mantienen y no son destruidos o borrados?

168 - ¿Se comparan los datos de desempeño en métricas con organizaciones similares cada dos años?

**- Desempeño de la calidad**

169 - ¿Los datos basados en calidad se analizan mensualmente?

170 - ¿Los objetivos establecidos para cada métrica de calidad son consistentes con respecto a la declaración de la dirección y el plan anual de negocio de la entidad?

171 - ¿Los datos de la calidad se mantienen y no son destruidos o borrados?

172 - ¿Se comparan los datos de calidad en métricas con organizaciones similares cada dos años?

**- Desempeño de las ventas**

173 - ¿Está contemplado el muestreo a la hora de recabar la información de los datos de ventas?

174 - ¿Se analiza mensualmente la información de las ventas?

175 - ¿Los datos de las ventas se mantienen y no son destruidos o borrados?

176 - ¿Los objetivos establecidos para cada métrica de ventas son consistentes con respecto a la declaración de la dirección y el plan anual de negocio de la entidad?

177 - ¿Están los agentes recompensados por los objetivos de ventas conseguidos, incluso si ellos han incrementado su tiempo medio de llamada?

**- Desempeño de los costes y eficiencia**

178 - ¿Está contemplado el muestreo a la hora de recabar la información de los datos de los costes y eficiencia?

179 - ¿Los datos de los costes y eficiencia se mantienen y no son destruidos o borrados?

180 - ¿La organización tiene en cuenta que un ahorro potencial puede derivar en ganancias en eficiencia?

181 - ¿Los objetivos establecidos para cada métrica de costes y eficiencia son consistentes con respecto a la declaración de la dirección y el plan anual de negocio de la entidad?

**- Desempeño de los procesos claves de apoyo**

182 - ¿Está contemplado el muestreo a la hora de recabar la información de los datos de los procesos claves de apoyo?

183 - ¿Se analiza mensualmente la información de los procesos claves de apoyo?

184 - ¿Los datos de los procesos claves de apoyo se mantienen y no son destruidos o borrados?

185 - ¿Los objetivos establecidos para cada métrica de ventas son consistentes con respecto a la declaración de la dirección y el plan anual de negocio de la entidad?

186 - ¿Se comparan los datos de los procesos claves de apoyo en métricas con organizaciones similares cada dos años?

### 6.4.3 Cuestionario sobre la Protección de la Información

**- Principios de protección y calidad de los datos.**

1 - ¿Se tratan de forma leal y lícita los datos recogidos?

2 - ¿Se recogen de forma fraudulenta, desleal e ilícita los datos usados posteriormente?

3 - ¿El uso de los datos cumple las finalidades determinadas, explicitas y legítimas para las que fue autorizado?

4 - ¿Se usan los datos para aquellas finalidades diferentes para las que han sido recogidos inicialmente?

5 - ¿Los datos son exactos y están puestos al día para que sean veraces?

6 - ¿Son cancelados una vez que su uso ha dejado de ser necesario o pertinentes para la finalidad con la que hubiesen sido recabados, a excepción de algún tipo de la relación u obligación jurídica o de la ejecución de un contrato o de aplicación de medidas contractuales solicitadas por el usuario?

7 - ¿Los interesados han prestado su consentimiento previamente al tratamiento o cesión de datos?

8 - ¿El tratamiento o recolección de datos está autorizado a través de una norma con la cual no se requiere el consentimiento del interesado?

9 - ¿Se informa al interesado para que conozca inequívocamente la finalidad en la que sus datos pueden ser usados en caso de ser cedidos autorizándose con su consentimiento?

10 - ¿La revocación del consentimiento puede ser ejercida por el interesado de un modo sencillo, gratuito y que implique un ingreso para el responsable del fichero o del tratamiento?

**- Derechos de acceso, rectificación, cancelación y oposición**

11 - ¿Se garantizan los derechos ARCO (acceso, rectificación, cancelación y oposición) a todos los interesados?

**- Códigos tipo**

12 - ¿La organización sigue algún tipo de código tipo en sus prácticas habituales como el “Código Deontológico de la Empresa de Telemarketing” o “Listas Robinson”?

**- Medidas de seguridad aplicables a los ficheros y tratamientos automatizados de datos de carácter personal**

**Nivel básico**

13 - ¿Se establecen mecanismos para que el acceso a ficheros o recursos se realice acorde a los derechos distintos a los autorizados por medio de roles o perfiles?

14 - ¿Los usuarios se identifican y autentican de forma inequívoca y personalizada a la hora de acceder a los sistemas, verificando que la autorización es correcta?

15 - ¿Se realizan copias semanales de respaldo al menos semanalmente?

16 - ¿Se dispone de procedimientos de recuperación que realicen una reconstrucción del estado en el que se encontraba antes de cualquier desastre?

**Nivel medio**

17 - ¿Se realizan auditorías internas o externas al menos cada dos años para verificar el cumplimiento de la ley y del reglamento que la desarrolló?

**Nivel alto**

18 - ¿Se guarda una copia de respaldo de los datos y los procedimientos en un lugar diferente de aquel en el que se encuentran los equipos informáticos que los tratan?

19 - ¿Se registra por cada intento de acceso como mínimo la identificación del usuario, fecha y hora en la que se realizó, fichero accedido, tipo de acceso y si estaba autorizado o no?

**- Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados de datos de carácter personal**

**Nivel básico**

20 - ¿Se garantiza la correcta conservación de los documentos, la localización y consulta de la información?

21 - ¿La documentación con datos de carácter personal que no se encuentre archivada en dispositivos de almacenamiento está correctamente custodiada por una persona al cargo?

**Nivel medio**

22 - ¿Se realizan auditorías internas o externas al menos cada dos años para verificar el cumplimiento de la ley y del reglamento que la desarrolló?

**Nivel alto**

23 - ¿Los armarios, archivadores u otros elementos en los que se almacenen los ficheros con datos de carácter personal estarán en localizaciones con una seguridad física acorde para limitar su acceso solo al personal responsable para ello?

24 - ¿La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad?

25 - ¿Se destruyen las copias o reproducciones de documentos desechadas con el fin de evitar su acceso o recuperación posterior no autorizada?

## 6.5 Resultados

Cada vez que se complete un cuestionario, sus resultados serán volcados automáticamente a una hoja de cálculo. A través de la formula que nos proporciona Excel CONTAR.SI, se contará la respuesta a cada pregunta del cuestionario en cuestión arrojando el porcentaje de cada una de las cinco respuestas posibles.

Se verificarán posteriormente aquellas preguntas cuyos porcentajes sean más elevados en base a los criterios establecidos. Por norma general la opción “Sí/Se cumple” deberá ser la opción más óptima, sin embargo, en casos en las que la opción “No/No se cumple” o “NS/NC” sean las que tengan un porcentaje más elevado, deberán tomarse medidas, bien correctoras o para establecer un procedimiento ante el desconicimiento que pueda tener el personal.

## 6.6 Auditoría Informática

La siguiente información está sacada del libro Auditoría Informática, un enfoque práctico.

### 6.6.1 Control Interno y Auditoría Informática

- Controles: directivos, preventivos, detectivos, correctivos, de recuperación.

- Áreas: seguridad, cumplimiento, calidad, verificar controles, operativa-gestión (eficiencia-eficacia), apoyo a auditoría de cuentas, investigación de delitos-fraudes, relación con recursos humanos, de reglamento.

- Fases:

Encargo->Planificación->Programa->Revisiones, Entrevistas, Pruebas->Informe

La definición de auditoría sería: actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

El auditor confía:

- En el control interno establecido por la organización para reducir el 1er riesgo.
- En sus pruebas de deatelle y en sus otros procedimientos para el segundo.

Se deberán controlar las versiones del software.

Grupos de funciones a realizar por el auditor:

a) Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas.

b) Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la dirección, requerimientos legales, protección de confidencialidad…

c) Revisar y juzgar el nivel de eficacia, utilibilidad, fiabilidad y seguridad de los equipos e información.

Los tipos de controles se pueden diferenciar en:

- Preventivos: para tratar de evitar el hecho.
- Detectivos: cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
- Correctivos: facilitan la vuelta a la normalidad cuando se han producido incidencias.
- Directivos: establecen las bases, como las políticas o la creación de comités relacionados o de funciones.
- De recuperación: facilitan la vuelta a la normalidad después de accidentes o contingencias.

### 6.6.2 Metodologías de Control Interno, Seguridad y Auditoría

El nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia del conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y de sus medios de proceso. Para ello entran en juego una serie de contramedidas como las siguientes:

- La normativa: debe definir de forma clara y precisa todo lo que debe existir y ser cumplido.
- La organización: la integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobadas por la dirección de la empresa.
- Las metodologías: son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.
- Los objetivos de control: se deben cumplir para el control de procesos.
- Los procedimientos de control: son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por tanto, deben de estar documentados y aprobados por la Dirección.
- La tecnología de seguridad: incluye a todos los elementos ya sean software o hardware que ayudan a controlar un riesgo informático.
- Las herramientas de control: son elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Análisis de riesgos:

Las dos principales metodologías de evaluación de sistemas son las de análisis de riesgos y las de auditoría informática. Las amenazas reales se presentan de forma compleja y son difíciles de predecir. Todos los riesgos que se presentan se pueden evitar, tranferir, reducir o asumir.

Tipos de metodologías:

- **Cuantitivas**: Diseñadas para producir una lista de riesgos que puedan comparse entre sí con facilidad para tener asignados unos valores numéricos.
- **Cualitativas**: Se basan en métodos estadísticos y lógica borrosa.

La Metodología de análisis de riesgos se basa en seis etapas: Cuestionario, Identificar riesgos, Calcular el impacto, Identificar las contramedidas y el coste, Simulaciones y Creación de informes.

Las partes del plan del auditor informático:

- **Funciones**: Debe existir una clara segregación de funciones con la Informática y de control interno informático, y este debe ser auditado también.
- **Procedimientos**: Para las distintas tareas de las auditorías.
- **Tipos de auditorías**: Que se realizan. Metodologías y cuestionarios de las mismas.
- **Sistema de evaluación**: Además de los distintos aspectos que evalúa.
- **Nivel de exposición**.
- **Lista de distribución de informes**.
- **Seguimiento de las acciones correctoras**.
- **Plan quienal**.
- **Plan de trabajo anual**.

Funciones de la Auditoría Informática y el Control Interno Informático:

- Auditoría Informática:
    - Tiene la función de vigilancia y evaluación mediante dictámenes, y todas sus metodologías van encaminadas a esta función.
    - Tiene sus propios objetivos distintos a los auditores de cuentas, por ejemplo, aunque necesarios para que estos puedan utilizar la información de sus sistemas para sus evaluaciones.
    - Operan según el plan del auditor.
    - Utilizan metodologías de evaluación del tipo cualitativo con la característica de las pruebas de auditoría.
    - Establecen planes quinqueniales como ciclos completos.
    - Sistemas de evaluación de repetición de la auditoría por nivel de exposición del área auditada y el resultado de la última de esta área.
    - La función de soporte informático que todos los auditores (opcionalmente) aunque dejando claro que no se debe pensar con esto que la auditoría informática consiste en esto solamente.

- Control Interno Informático:

  - Tiene funciones propias.
  - Funciones de control dual con otros departamentos.
  - Función normativa y del cumplimiento del marco jurídico.
  - Operan según procedimientos de control en los que se ven involucrados y que luego se desarrollarán.
  - Al igual que en la auditoría y de forma opcional pueden dar el soporte informático de control interno no informático.

## 6.6.3 El informe de Auditoría

- **Normas**: basadas en el Libro Verde de la Auditoría.

- **Evidencias**: deben ser relevantes, fiables, suficientes y adecuadas.

- **Irregularidades**: relacionadas con el Libro Verde de la Auditoría. Aunque deba prevalecer el secreto profesional del auditor, en el caso de detectar fraude durante el proceso de auditoría procede actuar en consecuencia, con la debida prudencia.

- **Documentación**: comúnmente se conoce en el argot como ‘papeles de trabajo’ la totalidad de los documentos, preparados o recibidos por el auditor de manera que, en conjunto, constituyen un compedio de la información utilizada y de las pruebas efectuadas en la ejecución de su trabajo.

- **Informe**: tiene que estar basado en la documentación o papeles de trabajo. Se deberá separar lo significativo de lo no significativo.

Los puntos esenciales de dicho informe serán: Identificación del Informe, Identificación del Cliente, Identificación de la entidad auditada, Objetivos de la Auditoría Informática, Normativa aplicada y excepciones, Alcance de la auditoría, Conclusiones (Favorable, Con salvedades, Desfavorable o Denegada, más el Resumen), Resultados, Informes previos, Fecha del informe, Identificación y firma del Auditor y Distribución del informe.

## 6.6.4 Organización del departamento de Auditoría Informática

- **Perfil**: Persona o personas que integren esta función deben contemplar en su formación básica una mezcla de conocimientos de auditoría y de informática general.

- **Funciones a desarrollar**: Verificar el control interno, Análisis de gestión de los sistemas de la información, Análisis de la integridad fiabilidad y certeza de la información, Verificación del nivel de continuidad de las operaciones…

### 6.6.5 El marco jurídico de la Auditoría Informática

Se ha hablado anteriormente en el apartado 5.1 LOPD, del marco jurídico pero también se debe tener en cuenta otros como la Ley de propiedad intelectual, BBDD y multimedia, los delitos informáticos, los contratos informáticos, el Intercambio Electrónico de Datos (EDI), la Transferencia electrónica de fondos, la Contratación electrónica y los Documentos electrónicos, todos ellos dentro de una jurisdicción que se debe conocer.

### 6.6.6 Deontología del auditor informático y códigos éticos

El auditor deberá prestar sus servicios acreditando varios principios: calidad, capacidad, cautela, comportamiento profesional, concentración en el trabajo, confianza, criterio propio, discreción, economía, formación continuada, fortalecimiento y respeto de la profesión, independencia, información suficiente, integridad moral, legalidad, libre competencia, no discriminación, no injerencia, precisión, publicidad adecuada, responsabilidad, secreto profesional, servicio público, veracidad.

Cualquier actitud que anteponga intereses personales del auditor a los del auditado deberá considerarse como no ética, ya que limitará necesariamente la aptitud del primero en prestar al segundo toda la ayuda puede y debe aportarle. Para garantizar que esto no ocurra el auditor deberá tener una independencia total del auditado.

Deberá ser totalmente consciente de su compartimiento en materia de conocimientos y fundamentos humanísticos sin ignorar ninguna de ellas.

Hay diferentes códigos deontológicos profesionales como el de la ISACF (Information Systems Audit and Control Foundation) o códigos de conducta como el de la British Computer Society.

### 6.6.7 La Auditoría de seguridad física y lógica

Anteriormente en el apartado 3. Seguridad en un Contact Center se ha hecho más enfásisis en esta parte.

Se debe obtener y mantener un nivel de seguridad física sobre los activos antes, durante y después del empleo, haciendo especial hincapié en el centro de procesamiento de datos e instalaciones, Equipos y comunicaciones, ordenadores personales y la seguridad física del personal.

Se debe verificar que cada usuario solo puede acceder a los recursos a los que le autorice el propietario. Desde el punto de vista de la auditoría es necesario revisar como se identifican y sobre todo como se autentican los usuarios.

# 7. Conclusiones

Con este proyecto se quiere dar un primer paso a la hora de acercar el entorno de las plataformas de Contact Center y como a través del control y la auditoría su forma de gestión internamente para algo que es realmente cotidiano y que muchas veces no entendemos el funcionamiento interno por el que se pueden regir este tipo de centros.

Durante la realización de este proyecto se ha tratado de implementar una batería de preguntas recogidas en los cuestionarios lo suficientemente amplia para tratar de abarcar de una mejor forma el proceso de auditoría y control relacionados con la seguridad, calidad y legislación.

Se ha decidido utilizar la herramienta de Google Formularios tras descartar a muchas de ellas como Quiz Creator, Surveymonkey, por ejemplo que en su versión de prueba no ofrecían grandes ventajas a los requisitos propuestos inicialmente. Además de ser una herramienta gratuita, su uso no depende de plataformas o navegadores, por lo que su uso no está prácticamente restringido a nadie.

He intentado plasmar con teoría y práctica todo lo que he aprendido durante tantos años en el mundo laboral que he trabajado, ya que muchas de recomendaciones o buenas prácticas, que al final es lo que trata de ser este proyecto, han sido nuevos descubrimientos para mi a medida que iba desarrollando dicho proyecto.

# 8. Posibles proyectos o líneas de investigación futuras

La idea de este proyecto estaba basada en un nivel muy básico. Para posibles proyectos futuros se podría tomar como un primer paso este proyecto y tratar de llevarlo a cabo en una fase de auditoría en una plataforma de Contact Center para ver si su funcionamiento es correcto o positivo a la hora de la elaboración del mismo.

Otra de las líneas a seguir sería el de la automatización de los cuestionarios. Implementar una aplicación que los recoja y sea mucho más sencillo e intuitivo de cara al usuario de dicho cuestionario. Procesados los datos, debería arrojar unos resultados más veraces que los expuestos en este proyecto, con informes que incluyan autoconclusiones y gráficos para su mejor interpretación.

# 9. Memoria económica

## 9.1 Planificación

La duración estimada del proyecto han sido unos trece meses como tal. Normalmente trataba de encontrar pequeños ratos al volver del trabajo para dedicarme al proyecto por lo que no ha habido una disposición total en la realización del mismo.

Una vez elegido el proyecto del tablón, comenzó la documentación teórica basada en gran parte por las recomendaciones del tutor de cuales podrían encajar mejor. También hubo otra parte más relacionada con los Contact Center que fue documentación propia basada en publicaciones o en la experiencia laboral adquirida.

Establecidas las bases se realizó un índice que se envió al coordinador del proyecto. Dado el visto bueno se empezó a desarrollar en base al mismo la memoria y estructura del proyecto. Se fueron incorporando todos los elementos recopilados en esa documentación teórica y se realizaron los cuestionarios que iban a ser la parte central del proyecto.

Cada cierto tiempo envíaba un correo electrónico al coordinador con la memoria para que éste diera el visto bueno y continuar, después de haber corregido las indicaciones que hacía a la misma. De igual manera los correos no siempre se intercambiaban para este tipo de actos, si no que el propio coordinador me informaba de leyes, normas o marcos que cambiaban o salían durante la realización del proyecto.

Una vez que estuvo todo implementado y redactado se le entregó la memoria definitiva y se puso fin a la memoria.

En el siguiente diagrama de GANTT se explican las fases del proyecto:

| | Nombre de tarea | Duración | Comienzo | Fin | Predecesoras | Nombres de los recursos |
|---|---|---|---|---|---|---|
| 1 | Inicio | 0 días | lun 01/09/14 | lun 01/09/14 | | |
| 2 | Documentación teoríca | 191 días | lun 01/09/14 | lun 25/05/15 | | Autor del PFC |
| 3 | Elaboración del índice | 4 días | jue 02/10/14 | mar 07/10/14 | | Autor del PFC;Ordenador |
| 4 | Revisión del índice | 2 días | mié 08/10/14 | jue 09/10/14 | 3 | Tutor del PFC |
| 5 | Elaboración de los cuestionarios | 35 días | dom 11/01/15 | jue 26/02/15 | | Autor del PFC |
| 6 | Revisión de la memoria 1 | 1 día | vie 27/02/15 | vie 27/02/15 | 5 | Tutor del PFC |
| 7 | Modificaciones sugeridas por el tutor 1 | 7 días | lun 02/03/15 | mar 10/03/15 | 6 | Autor del PFC;Ordenador |
| 8 | Revisión de la memoria 2 | 1 día | lun 24/08/15 | lun 24/08/15 | | Tutor del PFC |
| 9 | Modificaciones sugeridas por el tutor 2 | 8 días | mar 25/08/15 | jue 03/09/15 | 8 | Autor del PFC;Ordenador |
| 10 | Revisión de la memoria 3 | 1 día | mar 08/09/15 | mar 08/09/15 | | Tutor del PFC |
| 11 | Modificaciones sugeridas por el tutor 3 | 9 días | mié 09/09/15 | lun 21/09/15 | 10 | Autor del PFC;Ordenador |
| 12 | Desarrollo de la memoria | 252 días | vie 10/10/14 | lun 28/09/15 | 4 | Autor del PFC;Ordenador |
| 13 | Fin | 0 días | lun 28/09/15 | lun 28/09/15 | | |

**Tareas del diagrama de GANTT**

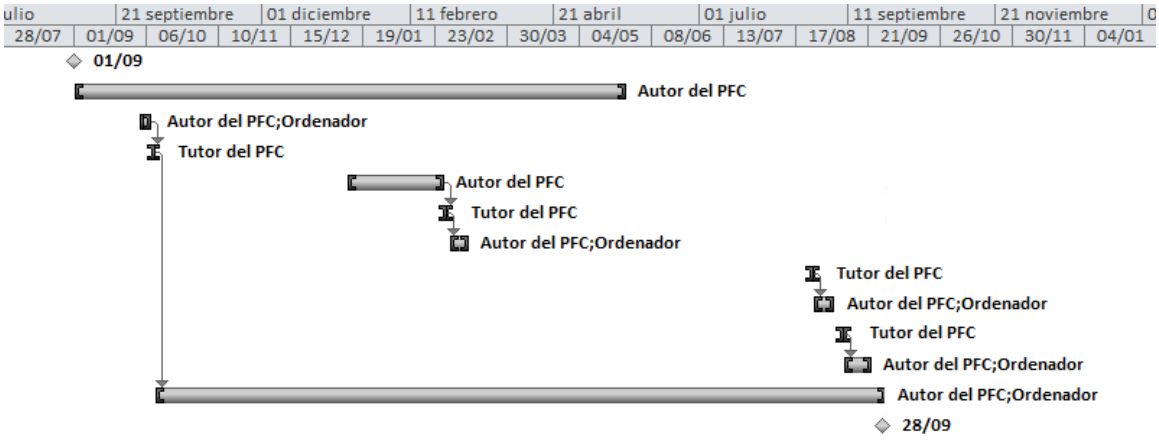



**Diagrama de GANTT**

# 9.2 Presupuesto

El coste del proyecto no ha sido elevado aunque se haya demorado en el tiempo más de un año. El proyecto en cuestión fue realizado por una sola persona, Alberto Madera Chamorro, trabajando algo menos de media jornada, estableciendo un coste en sueldo de unos 400 € mensuales multiplicados por los 13 meses de duración del proyecto resultan 5.200 €.

Compré un ordenador de segunda mano por 200 € para trabajar en casa lo que no podía realizar en las aulas informáticas de la universidad, donde realicé la mayora parte del trabajo.

Otros gastos fueron:

- Luz: la estimación del gasto de luz mensual podría ser de 10 €.
- Fotocopias: Mucha documentación preferí imprimirla, leerla y seleccionar las partes más importantes de los textos, estableciendo un coste estimado de unos 75 €.
- Licencias: Para Word, Excel y Project no hicieron falta, ya que fueron utilizadas las que estaban instaladas en los equipos de la universidad. La aplicación para realizar los cuestionarios es ofrecida libre y gratuitamente por Google.

El presupuesto total de este proyecto asciende a la cantidad de 6.928 €.

**UNIVERSIDAD CARLOS III DE MADRID**
**Escuela Politécnica Superior**

**PRESUPUESTO DE PROYECTO**

1.- Autor: Alberto Madera Chamorro

2.- Departamento: Informática

3.- Descripción del Proyecto:

- Titulo: **Auditoría y Control de una plataforma de Contact Center**
- Duración (meses): **13**
- Tasa de costes Indirectos: **20%**

4.- Presupuesto total del Proyecto (valores en Euros):

Euros

5.- Desglose presupuestario (costes directos)

**PERSONAL**

| Apellidos y nombre | N.I.F. (no rellenar - solo a titulo informativo) | Categoría | Dedicación (hombres mes) [a] | Coste hombre mes | Coste (Euro) | Firma de conformidad |
|---|---|---|---|---|---|---|
| Alberto Madera Chamorro | | Ingeniero | 13 | 400,00 | 5.200,00 | |
| | | | | | 0,00 | |
| | | | | | 0,00 | |
| | | | | | 0,00 | |
| | | | | | 0,00 | |
| | | **Hombres mes 13** | | **Total** | 5.200,00 | |

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

**EQUIPOS**

| Descripción | Coste (Euro) | % Uso dedicado proyecto | Dedicación (meses) | Periodo de depreciación | Coste imputable [d] |
|---|---|---|---|---|---|
| Ordenador Personal | 200,00 | 100 | 13 | 60 | 43,33 |
| | | | | **Total** | 43,33 |

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

**A** = nº de meses desde la fecha de facturación en que el equipo es utilizado
**B** = periodo de depreciación (60 meses)
**C** = coste del equipo (sin IVA)
**D** = % del uso que se dedica al proyecto (habitualmente 100%)

**SUBCONTRATACIÓN DE TAREAS**

| Descripción | Empresa | Coste imputable |
|---|---|---|
| | | |
| | **Total** | 0,00 |

**OTROS COSTES DIRECTOS DEL PROYECTO[e]**

| Descripción | Empresa | Costes imputable |
|---|---|---|
| Fotocopias | Copisteria universidad | 75,00 |
| Luz | Empresa eléctrica | 130,00 |
| Conexión a internet | Empresa telecomunicaciones | 325,00 |
| Licencias | Microsoft | 0,00 |
| | **Total** | 530,00 |

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

6.- Resumen de costes

| Presupuesto Costes Totales | **Presupuesto Costes Totales** |
|---|---|
| Personal | 5.200 |
| Amortización | 43 |
| Subcontratación de tareas | 0 |
| Costes de funcionamiento | 530 |
| Costes Indirectos | 1.155 |
| Total | 6.928 |

Leganés a 28 de Septiembre de 2015

El ingeniero proyectista

Fdo. Alberto Madera Chamorro

# 10. Glosario

**Accesos autorizados**: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

**Acuerdos de Nivel de Servicio (Service Level Agreements, SLA)**: Método aceptado para definir la calidad del servicio y los parámetros operacionales que los socios a los cuales se le externaliza un servicio deben entregar.

**Activo**: Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la Empresa. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

**Administración de RRHH**: Persona responsable de la previsión y planificación de los agentes para garantizar que el centro de contacto dispone del personal adecuado.

**Afectado**: Persona física titular de los datos que sean objeto del tratamiento.

**Agente**: Persona al más bajo nivel en el organigrama de la empresa y que ejecuta todos los procesos de la misma. Pueden dividirse en dos grupos: los de nivel II, con una experiencia mayor al año y de nivel I, con una inferior al año.

**Amenaza**: una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe.

**Autenticación**: procedimiento de comprobación de la identidad de un usuario.

**Cliente**: organizaciones que contratan a entidades externas para proveer de productos y servicios a sus usuarios finales a través de su Contact Center. También se puede referir a los grupos dentro de una empresa que obtienen servicios de Contact Center desde un grupo, división, departamento, o equipo dentro de la misma empresa.

**Cola universal**: software cuya función se asemeja a un embudo para todos los canales (teléfono, e-mail, chat…) que aplica en el negocio reglas de flujo de trabajo, enrutamiento, encolamiento y capacidad de recolección de datos igualmente para todas las transacciones de entrantes.

**Contraseña**: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

**Control de acceso**: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

**Copia de respaldo**: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

**Computer/Telephone Integration (CTI)**: La Integración Ordenador/Teléfono, es un "middleware" que integra más estrechamente los sistemas de información y el teléfono. Permite un enlace entre una llamada telefónica y el contexto asociado a esa llamada, incluidos los datos personales del usuario, servicio deseado y las operaciones realizadas durante la llamada. Se puede utilizar para mostrar automáticamente en pantalla los datos de la persona que contacta.

**Coordinador**: Persona responsable de los agentes que tiene por debajo suyo. Está colocado por debajo del Supervisor en el organigrama y se comporta como una segundo al mando en el CC. También llamado Agente nivel III.

**Cross-selling**: técnica de ventas que consiste en la "la venta cruzada" de artículos o productos, que pueden estar relacionados con la venta que se está negociando o basado en el conocimiento del cliente que tenemos.

**Cuadro de Mando Integral (Balanced Scorecard)**: Herramienta de la gestión estratégica del desempeño de una organización, basada en informes que se centran en los objetivos estratégicos y de rendimiento en todos los niveles (agentes, grupos y departamentos) creada inicialmente por Robert Kaplan y David Norton.

**Custom Relationship Manager (CRM)**: Gestión de la relación con el cliente.

**Director**: Persona que gestiona enteramente el entorno operacional de un Contact Center.

**Distribuidor automático de llamadas (Automatic Call Distributor, ACD)**: Sistema que distribuye las llamadas entrantes a un grupo determinado de terminales que utilizan los agentes.

**Documento**: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

**Encargado del tratamiento**: persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la

existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

**Enrutamiento basado en habilidades**: consiste en seleccionar al agente más adecuado para la transacción en función de sus capacidades, como idiomas o proveer un servicio mejor al usuario.

**Fichero**: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

**Fichero automatizado**: Ficheros informátizados.

**Ficheros de titularidad privada**: Ficheros de los que sean responsables las personas, empresas o entidades privadas.

**Ficheros de titularidad pública**: Ficheros de los que sean responsables los órganos constitucionales, el Estado o las instituciones autonómicas, las Administraciones públicas territoriales.

**Fichero no automatizado**: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

**Ficheros temporales**: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

**Formador**: Persona responsable de identificar las necesidades del agente y preparar y dar una formación para asegurarse que el agente da el mejor servicio.

**Gerente**: Persona responsable de las operaciones del día a día de un equipo, incluyendo la productividad, la calidad, la programación del agente, la adherencia, la gestión de la calidad, la satisfacción del cliente y la identificación de las necesidades de capacitación del agente.

**Gestor de red**: es un software normalmente usado para distribuir las llamadas entre la plataforma basado en reglas de ruteo establecidas por la entidad.

**Identificación**: procedimiento de reconocimiento de la identidad de un usuario.

**Impacto**: La evaluación del efecto del riesgo.

**Incidencia**: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

**Interactive Voice Response (IVR)**: serie de autómatas informáticos especializados que permite a los usuarios "autoservicio", mientras tratan de comunicar sus necesidades. Los usuarios que interactúan con el IVR utilizan el teclado del teléfono o, con la tecnología de

reconocimiento de voz, comandos de voz para proporcionar información. En respuesta, el IVR utiliza voz sintetizada para reportar información. También pueden ser utilizados para enrutar las llamadas, lo llamado enrutamiento basado en habilidades.

**Intercambio Electrónico de Datos (EDI)**: Sistema informático que permite las transacciones comerciales y administrativas directas a través del ordenador sin utilizar ningún trámite.

**Key Performance Indicator (KPI):** Indicador clave de desempeño.

**Marcador**: Sistema que automatiza la iniciación y marcación de llamadas salientes y las conecta a los agentes.

**Malware**: virus, gusanos de red, caballos de Troya y bombas lógicas.

**Motor de acción**: Sistema que automáticamente identifica y asigna acciones para optimizar una oportunidad o solucionar un problema. Detecta agentes que tienen parámetros de funcionamiento fuera de lo normal y asesora a los supervisores para asignar programas correctivos.

**Net Promoter Score (NPS)**: indicador que mide la lealtad de un cliente a una marca comercial. Según los resultados los clientes se pueden clasificar en promotores, pasivos y detractores.

**Organizaciones de Gestión de Proveedores (VMO)**: son unidades organizacionales de individuos, generalmente dentro de la empresa del Cliente, responsables de la gestión de al menos una porción de los programas de la empresa con los Contact Centers.

**Perfil de usuario**: accesos autorizados a un grupo de usuarios.

**Preguntas Frecuentemente Contestadas**: FAQ Frequently Asked Questions

**Procesos Clave de Apoyo (PCAs)**: son aquellos procesos necesarios para facili-tar que los PCRCs alcancen los objetivos de nivel de desempeño o los mantengan.

**Procesos Clave Relacionados con el Cliente (PCRCs)**: son aquellos procesos que son críticos para la posibilidad del Contact Center de brindar altos niveles de desempeño en los productos y servicios ofrecidos a usuarios finales.

**Proveedores de Servicios Integrales al Cliente (PSIC)**: Proveen servicios a usuarios finales en nombre de sus Clientes.

**Recurso**: cualquier parte componente de un sistema de información.

**Resolución en Primer Contacto (RPC)**: El porcentaje de transacciones procesadas con éxito durante el primer contacto efectuado por el usuario final y que no resultan en llamadas transferidas o repetidas con relación al mismo problema. También denominada “FCR”, por sus siglas en inglés “First Contact Resolution”.

**Responsable de calidad**: Persona responsable de la medición y la identificación de tendencias y formación de agentes para mejorar la calidad de la llamada.

**Responsable de seguridad**: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

**Responsable del fichero o del tratamiento**: a la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Ambos podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

**Riesgo**: La probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad.

**Sistema de Gestión de Respuesta de E-mail**: E-Mail Response Management System (ERMS). Aplicación que automatiza el manejo de correos electrónicos de los clientes. Gestiona el flujo de correo electrónico entrante y saliente de una organización y utiliza palabras clave para enrutar y encolar las transacciones.

**Sistema de información**: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

**Sistema de tratamiento**: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

**Soporte**: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

**Soporte Técnico**: Persona responsable de la supervisión de las aplicaciones, equipos, periféricos, software, etc… de la plataforma.

**Speech Recognition (Reconocimiento de voz)**: Tecnología normalmente conjunta al IVR que a través del reconocimiento de la voz humana, guía al usuario hacia un agente o aplicación específica para sus necesidades.

**Supervisor**: Persona responsable directa de la gestión de un equipo. Colocada en el organigrama de la empresa por debajo del Gerente y por encima del Coordinador.

**Tablero (Dashboard)**: Medidas personalizadas individuales, grupales, o del desempeño departamental, adaptadas a las necesidades de cada usuario. Paneles que permiten una organización tomar acciones para optimizar la experiencia del cliente, aumentando la eficacia de ventas y campañas de marketing y reducir los costes operativos.

**Tercero**: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

**Tiempo medio de manejo**: El tiempo total invertido dividido por el número transacciones, incluyendo tiempo de conversación (llamadas entrantes y salientes), tiempo no telefónico (e-mail, correspondencia), y todo tipo de trabajo posterior a la llamada. También se puede llamar "AHT" por sus siglas en inglés "Average Handle Time".

**Transacción**: Oportunidad de generar venta, beneficio, retención, lealtad o información a través de herramientas para asesorar a la otra parte.

**Transmisión de documentos**: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

**Usuario**: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

**Usuario final**: pueden ser consumidores, negocios, organizaciones, o los minoristas, distribuidores y especialistas que constituyen un canal de distribución. Pueden ser clientes de la propia organización o de una tercera.

**Up-selling**: técnica de ventas que consiste en ofrecer un producto de mayor valor al cliente que ya está buscando algo y que el vendedor le muestra otro producto, que quizás pueda convenirle más por ser más completo o directo a su necesidad.

**Vulnerabilidad**: La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático.

# 11. Referencias

## 11.1 Bibliografía


[AIUEP] Piattini Velthuis, Mario G. *Auditoría informática: un enfoque práctico.*

[TRTCC] Fluss, Donna. *The real-time Contact Center: strategies, tactics and technologies for building a profitable service and sales operation.*

[CCFD] Avaya Limited Edition.*Contact Centers For Dummies.*

[MAR] Miguel Ángel Ramos. *Apuntes asignatura Gestión y Calidad del Software.*

[MAR] Miguel Ángel Ramos. *Apuntes asignatura Auditoría Informática.*

[MMM] Grupo Konecta. *Manual de mejoras en Monitorización.*


## 11.2 Webgrafía


[BOE] SPAM telefónico, BOE jueves 31 de diciembre de 2009: <https://www.boe.es/boe/dias/2009/12/31/pdfs/BOE-A-2009-21162.pdf>

[BOE] Reforma de la Ley de Consumidores y Usuarios, BOE viernes 28 de marzo de 2014: < https://www.boe.es/boe/dias/2014/03/28/pdfs/BOE-A-2014-3329.pdf>

[CCI] Código deontológico de la empresa de Telemarketing: <http://www.contactcenterinstitute.es/Biblioteca/Codigo%20Deontologico%20de%20la%20Empresa%20de%20Telemarketing.pdf>

[CCI] Código regulador del servicio de Listas Robinson: <http://www.contactcenterinstitute.es/Biblioteca/Codigo%20Regulador%20Listas%20Robinson.pdf>

[CCISD] Contact center: information systems design. Rui Rijo, João Varajão y Ramiro Gonçalves.

< http://link.springer.com/article/10.1007%2Fs10845-010-0389-0#page-2>

[COBIT] Cobit 5.0: <http://www.isaca.org/cobit>

[COPC] Norma COPC PSIC < http://www.copc.com/>

[CURSO] ITIL – Gestión de servicios.

[FSB] Curso de adaptación a la Ley Orgánica de Protección de Datos. Formación sin barreras.

[ISACA] Métricas de seguridad <http://www.isaca.org/cobit>

[ISO] ISO 27001/2: <http://www.iso27001security.com/>

[LOPD] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal. (BOE)

[RD] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[SDP] Código de Televenta final, de 25 de noviembre de 2010: <http://saladeprensa.telefonica.es/documentos/nprensa/NP_codigo_Televenta_vfinal.pdf>

# A. Anexos

## Anexo 1 – Claúsulas, Categorías y Controles de ISO 27002

La disposición del estándar está contenida por las siguientes 14 cláusulas de control de seguridad en el siguiente anexo, que a su vez se dividirán en categorías (notificadas entre paréntesis):

- Información de las políticas de seguridad (1).
- Organización de la seguridad de la información (2).
- Seguridad de Recursos Humanos (3).
- Gestión de Activos (3).
- Control de Acceso (4).
- Criptografía (1)
- Seguridad Física y Ambiental (2).
- Seguridad en las Operaciones (7).
- Seguridad en las comunicaciones (2)
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información (3).
- Relaciones con proveedores (2)
- Gestión de Incidentes de Seguridad de la Información (1).
- Seguridad de la Información en aspectos de la Gestión de la Continuidad Comercial (2).
- Cumplimiento (2).

- **1 Información de las políticas de seguridad.**
  - **1.1 Dirección de Gestión de la Seguridad de la Información**
    Objetivo: Proporcionar y apoyar a la dirección gerencial para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

    - **1.1.1 Políticas para la seguridad de la información**
      Control: Se definirá un conjunto de políticas de seguridad de la información, aprobado por la administración, publicado y comunicado a los empleados y partes externas relevantes.
    - **1.1.2 Revisión de las políticas para la seguridad de la información.**
      Control: Las políticas de seguridad de la información, serán revisadas a intervalos planeados o si se producen cambios significativos para asegurar su continua conveniencia, adecuación y eficacia.

- **2. Organización de la seguridad de la información.**
  - **2.1 Organización interna.**
    Objetivo: Se deberá establecer un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.
    - **2.1.1 Responsabilidades y roles de la seguridad de la información.**
      Control: Todas las responsabilidades de la seguridad de la información deben estar definidas y asignadas.
    - **2.1.2 Segregación de tareas.**
      Control: Las tareas y áreas de responsabilidades que puedan entrar en conflicto deben estar separadas para reducir las oportunidades de modificación no autorizada o no intencionada o el mal uso de los activos de la organización.
    - **2.1.3 Contacto con las autoridades.**
      Control: Los contactos apropiados con las autoridades relevantes deben ser mantenidos.
    - **2.1.4 Contacto con grupos de interés especial.**
      Control: Los contactos apropiados con los grupos de interés u otros especialistas de debate de seguridad y asociaciones profesionales deben ser mantenidos.
    - **2.1.5 Seguridad de la información en la gestión de proyectos.**
      La seguridad de la información debe ser dirigida por la gestión de proyectos, independientemente del tipo de proyecto.
  - **2.2 Dispositivos para movilidad y teletrabajo.**
    Objetivo: Asegurar la seguridad del teletrabajo y uso de dispositivos móviles.
    - **2.2.1 Política de uso de dispositivos para movilidad.**
      Control: Una política y apoyo a las medidas serán adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.
    - **2.2.2 Teletrabajo.**
      Control: Una política y apoyo a las medidas serán implementados para proteger a la información accedida, procesada o almacenada en sitios de teletrabajo.
- **3. Seguridad de los recursos humanos.**
  - **3.1 Antes del trabajo.**
    Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados.
    - **3.1.1 Investigación de antecedentes (Screening).**
      Control: Se realizarán controles de verificación de antecedentes de todos los candidatos a puesto de trabajo, se llevarán a cabo en conformidad con las leyes, regulaciones y ética y serán proporcionales a los requisitos del negocio, la clasificación de la información para tener acceso y los riesgos percibidos.
    - **3.1.2 Términos y condiciones de contratación.**

Control: Los acuerdos contractuales con los empleados y los contratistas deberán exponer sus responsabilidades y de la organización para la seguridad de la información.

- **3.2 Durante el trabajo.**
  Objetivo: Asegurar que los usuarios empleados y contratistas conozcan y cumplan las responsabilidades de la seguridad de la información.
  - **3.2.1 Responsabilidades de gestión.**
    Control: La gestión requerirá a todos los empleados y contratistas aplicar seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
  - **3.2.2 Concienciación, educación y formación en la seguridad de la información.**
    Control: Todos los empleados de la organización y, en su caso, los contratistas deberán recibir una adecuada sensibilización y formación y actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para su función de trabajo.
  - **3.2.3 Proceso disciplinario.**
    Control: Habrá un proceso disciplinario formal y comunicado en lugar de tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.
- **3.3 Cese o cambio del puesto de trabajo.**
  Objetivo: Proteger los intereses de la organización como una parte del proceso de cambio o terminación del empleo.
  - **3.3.1 Responsabilidades del cese o cambio del puesto de trabajo.**
    Control: Las responsabilidades de la seguridad de la Información y deberes que siguen vigentes después de la terminación o el cambio del puesto de trabajo se definirán, comunicarán al trabajador o del contratista y se regularán.

- **4. Gestión de activos.**
  - **4.1 Responsabilidad sobre los activos.**
    Objetivo: Identificar los activos de la organización y definir la protección apropiada para su protección.
    - **4.1.1 Inventario de activos.**
      Control: Los activos relacionados con la información y con la instalación de procesamiento de la información deben ser identificados y un inventario de estos bienes será elaborado y mantenido.
    - **4.1.2 Propiedad de los activos.**
      Control: Los activos mantenidos en el inventario serán propios.
    - **4.1.3 Uso aceptable de los activos.**
      Control: Las normas para el uso aceptable de la información y de los activos asociados con la información y con los servicios de procesamiento de la información deben ser identificadas, documentadas e implementadas.
    - **4.1.4 Devolución de activos.**
      Control: Todos los empleados y usuarios del grupo externo deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.

- **4.2 Clasificación de la información.**
  Objetivo: Asegurar que la información reciba un nivel de protección apropiado de acuerdo a la importancia de la organización.
  - **4.2.1 Directrices de clasificación.**
    Control: La información se clasificará en función de los requisitos legales, valor, criticidad y sensibilidad a la divulgación no autorizada o
    modificación.
  - **4.2.2 Etiquetado de la información.**
    Control: Un conjunto apropiado de procedimientos para el etiquetado de información será elaborado y aplicado de acuerdo con el esquema de clasificación de la información adoptado por la organización.
  - **4.2.3 Manipulación de activos.**
    Control: Los procedimientos para el manejo de los activos deberán desarrollarse e implementarse de acuerdo con el esquema de clasificación de la información adoptado por la organización.
- **4.3 Manejo de los soportes de almacenamiento.**
  Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los soportes digitales (media).
  - **4.3.1 Gestión de soportes extraíbles.**
    Control: Los procedimientos serán implementados para la gestión de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización.
  - **4.3.2 Eliminación de soportes.**
    Control: Los soportes deberán ser desechados de forma segura cuando ya no sean necesarios, utilizando procedimientos formales.
  - **4.3.3 Transferencia física de soportes.**
    Control: Los soportes que contienen información deben estar protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte.

- **5. Control de acceso.**
  - **5.1 Requisitos de negocio para el control de acceso.**
    Objetivo: Limitar el acceso a la información y a los servicios de procesamiento de información.
    - **5.1.1 Política de control de acceso.**
      Control: Una política de control de acceso será establecida, documentada y revisada en base a los requisitos de seguridad del negocio y de la información.
    - **5.1.2 Control de acceso a las redes y servicios asociados.**
      Control: Los usuarios sólo deberán disponer de acceso a la red y a los servicios de red para los que han sido específicamente autorizados para su uso.
  - **5.2 Gestión de acceso de usuario.**
    Objetivo: Asegurar el acceso del usuario autorizado y prevenir el acceso no autorizado a los sistemas y servicios.
    - **5.2.1 Alta/baja del registro de usuarios.**
      Control: Un proceso de alta/baja de un usuario será implementado para permitir la asignación de derechos de acceso.

        - **5.2.2 Aprovisionamiento del acceso de usuarios.**
          Control: Un proceso de provisión de acceso de usuarios será implementado para asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.
        - **5.2.3 Gestión de los derechos de acceso privilegiados.**
          Control: La asignación y el uso de los derechos de acceso privilegiados será restringido y controlado.
        - **5.2.4 Gestión de la información confidencial de autenticación de usuarios.**
          Control: La asignación y el uso de los derechos de acceso privilegiados será controlada a través de un proceso de gestión formal.
        - **5.2.5 Revisión de los derechos de acceso de los usuarios.**
          Control: Los propietarios de activos revisarán los derechos de acceso de los usuarios en intervalos regulares.
        - **5.2.6 Retirada o adaptación de los derechos de acceso.**
          Control: Los derechos de acceso de todos los empleados y los usuarios externos a los servicios de procesamiento de la información y de la información serán eliminados después de la terminación de su empleo, contrato o acuerdo, o se ajustarán al cambio.
    - **5.3 Responsabilidades del usuario.**
      Objetivo: Hacer responsables a los usuarios para salvaguardar su información de autenticación.
        - **5.3.1 Uso de información secreta para la autenticación.**
          Control: Se exigirá a los usuarios seguir las prácticas de la organización en el uso de información secreta para la autenticación.
    - **5.4 Control de acceso a los sistemas y las aplicaciones.**
      Objetivo: Prevenir un acceso no autorizado a los sistemas y las aplicaciones.
        - **5.4.1 Restricción del acceso a la información.**
          Control: El acceso a las funciones de la información y al sistema de aplicación estará restringido de acuerdo con las políticas de control de acceso.
        - **5.4.2 Procedimientos seguros de inicio de sesión.**
          Control: Según lo requerido por la política de control de acceso, el acceso a los sistemas y aplicaciones será controlado por un procedimiento seguro de inicio de sesión.
        - **5.4.3 Sistema de gestión de contraseñas.**
          Control: El sistema de gestión de contraseñas será interactivo y asegurará contraseñas de calidad.
        - **5.4.4 Uso de programas de utilidad privilegiados.**
          Control: El uso de programas de utilidad que podrían ser capaces de predominar los controles de sistemas y aplicaciones serán restringidos y estrechamente controlados.
        - **5.4.5 Control de acceso al código fuente de los programas.**
          Control: El acceso al código fuente de los programas será restringido.
- **6. Criptografía.**

- **6.1 Controles criptográficos.**
  Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
  - **6.1.1 Política de uso de los controles criptográficos.**
    Control: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.
  - **6.1.2 Gestión de claves.**
    Control: Una política sobre el uso, la protección y la duración de las claves criptográficas será desarrolla e implementada a través de todo su ciclo de vida.

- **7. Seguridad física y ambiental**
  - **7.1 Áreas seguras.**
    Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a la información y a los servicios de procesamiento de información de la organización.
    - **7.1.1 Perímetro de seguridad física.**
      Control: Los perímetros de seguridad serán definidos y utilizados para proteger áreas que contengan tanto información sensible o crítica como a los servicios de procesamiento de información.
    - **7.1.2 Controles físicos de entrada.**
      Control: Las áreas seguras serán protegidas mediante controles de entrada adecuados para garantizar que se le permite el acceso únicamente al personal autorizado.
    - **7.1.3 Seguridad de oficinas, despachos e instalaciones**
      Control: La seguridad física para oficinas, despachos e instalaciones será diseñada y aplicada.
    - **7.1.4 Protección contra las amenazas externas y ambientales.**
      Control: La protección física contra los desastres naturales, ataques maliciosos o accidentes serán diseñados y aplicados.
    - **7.1.5 El trabajo en áreas seguras.**
      Control: Los procedimientos para trabajar en áreas seguras serán diseñados y aplicados.
    - **7.1.6 Áreas de carga y descarga.**
      Control: Los puntos de acceso tales como las áreas de carga y descarga y otros puntos donde gente no autorizada pueda entrar a la instalación deben ser controladas y, si fuese posible, aisladas de los servicios de procesamiento de la información para evitar un acceso no autorizado.
      *Protección auditiva, ergonomía (prevención de riesgos laborables). Ambiente en el trabajo (Ruido, Iluminación, Higiene, Vibraciones, Temperaturas).
  - **7.2 Equipamiento.**
    Objetivo: Evitar la pérdida, daño, robo o la puesta en peligro de los activos y la interrupción de las operaciones de la organización.
    - **7.2.1 Localización y protección de equipos.**
      Control: Los equipos deberán estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y oportunidades de acceso no autorizado.
    - **7.2.2 Servicios de soporte.**

Control: Los equipos deberán estar protegidos contra fallos de energía y otras interrupciones causadas por fallos en el apoyo a los servicios de soporte.

- **7.2.3 Seguridad del cableado.**
  Control: La energía y el cableado de las telecomunicaciones que transporta datos o apoya a los servicios de información deberá ser protegido contra la interceptación, interferencia o daños.
- **7.2.4 Mantenimiento de los equipos.**
  Control: Los equipos deben mantenerse correctamente para asegurar su continua disponibilidad e integridad.
- **7.2.5 Retirada de activos.**
  Control: Los equipo, la información o el software no serán retirados del sitio en el que estén sin una autorización previa.
- **7.2.6 Seguridad de los equipos y activos fuera de las instalaciones.**
  Control: La seguridad se aplicará a los activos de fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
- **7.2.7 Reutilización o retirada segura de los equipos.**
  Control: Todos los elementos del equipo contenidos en los medios de almacenamiento deberán ser verificados para garantizar que algún dato sensible y software con licencia ha sido eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
- **7.2.8 Equipo informático de usuario desatendido.**
  Control: Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada.
- **7.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.**
  Control: Se adoptará una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política de la pantalla clara para las instalaciones de procesamiento de la información.

- **8. Seguridad en las operaciones.**
  - **8.1 Responsabilidades y procedimientos de operación.**
    Objetivo: Asegurar operaciones correctas y seguras de los servicios de procesamiento de información.
    - **8.1.1 Procedimientos operativos documentados.**
      Control: Los procedimientos de operación deberán ser documentados y puestos a disposición de todos los usuarios que lo necesiten.
    - **8.1.2 Gestión de cambios.**
      Control: Los cambios en la organización, los procesos de negocio, servicios de procesamiento de la información y sistemas que afectan a la seguridad deberán ser controlados.
    - **8.1.3 Gestión de la capacidad.**
      Control: El uso de los recursos será supervisado, ajustado y las proyecciones hechas de las futuros requisitos de la capacidad para garantizar el funcionamiento del sistema requerido.
    - **8.1.4 Separación de entornos de desarrollo, prueba y operación.**

Control: Los entornos de desarrollo, pruebas y operativos serán separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.

- **8.2 Protección contra código malicioso.**
  Objetivo: Asegurar que las instalaciones de procesamiento de la información y la información están protegidos contra el código malicioso (malware).
  - **8.2.1 Controles contra el código malicioso.**
    Control: Controles de detección, prevención y recuperación para protegerse contra el malware se aplicarán, en combinación con el conocimiento del usuario correspondiente.
- **8.3 Copias de seguridad.**
  Objetivo: Protegerse contra la pérdida de datos.
  - **8.3.1 Copias de seguridad de la información.**
    Control: Las copias de seguridad de la información (back up), software e imágenes del sistema serán tomadas y probadas regularmente de acuerdo con una política de copias de seguridad acordada.
- **8.4 Registros y monitorización.**
  Objetivo: Registrar eventos y generar evidencia.
  - **8.4.1 Registro de eventos de actividad.**
    Control: Los registros de eventos graban las actividades del usuario, excepciones, fallos y eventos de seguridad de la información que se produzcan, cuidándose y revisándose regularmente.
  - **8.4.2 Protección de los registros de información.**
    Control: Los registros de servicios y de la información se protegerán contra la falsificación y el acceso no autorizado.
  - **8.4.3 Registros de actividad del administrador y operador del sistema.**
    Control: Las actividades del administrador y del gestor de las actividades del sistema serán registradas y dichos registros protegidos y regularmente revisados.
  - **8.4.4 Sincronización de relojes.**
    Control: Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad serán sincronizados con un solo tiempo de referencia.
- **8.5 Control del software de operación.**
  Objetivo: Asegurar la integridad de los sistemas de operación.
  - **8.5.1 Instalación del software en sistemas de operación.**
    Control: Los procedimientos serán implementados para controlar la instalación del software en sistemas de operación.
- **8.6 Gestión de la vulnerabilidad técnica.**
  (Adquisición, Desarrollo y Mantenimiento de Sistemas de Información)
  Objetivo: Prevenir la explotación de técnicas de vulnerabilidad.
  - **8.6.1 Gestión de las vulnerabilidades técnicas.**
    Control: La información acerca de las vulnerabilidades técnicas de los sistemas de información que será usada se obtendrá en el momento oportuno, la exposición de la organización a tales

vulnerabilidades evaluadas y tomando las medidas adecuadas para hacer frente a los riesgos asociados.

- **8.6.2 Restricciones en la instalación de software.**
  Control: Las normas que rigen la instalación de software por los usuarios serán establecidas e implementadas.

- **8.7 Consideraciones de las auditorías de los sistemas de información. (Cumplimiento)**
  Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas de operación.
  - **8.7.1 Controles de auditoría de los sistemas de información.**
    Control: Los requisitos y actividades de auditoría relacionadas con la verificación de los sistemas de operación serán cuidadosamente planeados y con el fin de minimizar las interrupciones en los procesos de negocio.

- **9. Seguridad en las comunicaciones.**
  - **9.1 Gestión de la seguridad en las redes.**
    Objetivo: Asegurar la protección de la información en redes y sus instalaciones de apoyo de procesamiento de la información.
    - **9.1.1 Controles de red.**
      Control: Las redes serán gestionadas y controladas para proteger la información en sistemas y aplicaciones.
    - **9.1.2 Servicios de seguridad en redes.**
      Control: Los mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red serán identificados e incluidos en los acuerdos de servicios de red, si estos servicios son proveídos por la empresa o subcontratados.
    - **9.1.3 Segregación de redes.**
      Control: Los grupos de servicios de la información, usuarios y sistemas de información serán segregados en redes.
  - **9.2 Transferencia de información.**
    Objetivo: Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad exterior.
    - **9.2.1 Políticas y procedimientos de transferencia de información.**
      Control: Las políticas formales de transferencias, procedimientos o controles estarán en su lugar para proteger la transferencia de información a través del uso de todo tipo de servicios de comunicación.
    - **9.2.2 Acuerdos de transferencias de información.**
      Control: Los acuerdos dirigirán una transferencia segura de información de negocio entre la organización y las partes externas.
    - **9.2.3 Correo electrónico.**
      Control: La información involucrada en correos electrónicos estará apropiadamente protegida.
    - **9.2.4 Acuerdos de confidencialidad y no divulgación.**
      Control: Los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información serán identificados, revisados regularmente y documentados.

- **10. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información**

- **10.1 Requisitos de seguridad de los sistemas de información.**
  Objetivo: Asegurar que la seguridad de la información es una parte integral de los sistemas de información a través de su entero ciclo de vida. Esto también incluye a los requisitos para los sistemas de información los cuales proporcionan servicio a través de redes públicas.
  - **10.1.1 Análisis y especificación de los requisitos de seguridad de la información.**
    Control: Los requisitos relacionados con la seguridad de la información serán incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.
  - **10.1.2 Seguridad de los servicios de las aplicaciones en redes públicas.**
    Control: La información involucrada en los servicios de aplicaciones que pasen a través de redes públicas, serán protegida de la actividad fraudulenta, disputa de contrato, la modificación y la divulgación no autorizada.
  - **10.1.3 Protección de los servicios de las aplicaciones en transacciones.**
    Control: La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir la transmisión incompleta, mal enrutamiento, alteración mensaje no autorizado, la divulgación no autorizada, la duplicación de mensajes no autorizada o la reproducción.
- **10.2 Seguridad en los procesos de desarrollo y soporte.**
  Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
  - **10.2.1 Política de desarrollo seguro.**
    Control: Las reglas para el desarrollo de software y sistemas se establecerán y aplicarán a los desarrollos dentro de la organización.
  - **10.2.2 Procedimientos de control de cambios en los sistemas.**
    Control: Los cambios en los sistemas dentro del ciclo de vida de desarrollo serán controlados por el uso de procedimientos formales de control de cambios.
  - **10.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma.**
    Control: Cuando las plataformas de operación, aplicaciones críticas de negocio son cambiadas serán revisadas y probadas para asegurar que no hay impacto negativo en las operaciones de la organización o de la seguridad.
  - **10.2.4 Restricciones a los cambios en los paquetes de software.**
    Control: Las modificaciones en los paquetes de software serán desalentadas y limitadas a los cambios necesarios y todos los cambios que serán estrictamente controlados.
  - **10.2.5 Principios de ingeniería en protección de sistemas.**
    Control: Los principios para una ingeniería segura de sistemas serán establecidos, documentados, mantenidos y aplicados en cualquier esfuerzo de implementación de sistemas de información.
  - **10.2.6 Seguridad en entornos de desarrollo.**

Control: La organización establecerá y protegerá apropiadamente la seguridad en entornos de desarrollo para sistemas de desarrollo y esfuerzos de integración que cubra por completo el ciclo de vida de desarrollo del sistema.

- **10.2.7 Externalización del desarrollo.**
  La organización supervisará y monitorizará la actividad del desarrollo del sistema externalizado.
- **10.2.8 Pruebas del sistema de seguridad.**
  Control: Las pruebas de la funcionalidad de seguridad se llevarán a cabo durante el desarrollo.
- **10.2.9 Pruebas de aceptación del sistema.**
  Control: Los programas de pruebas de aceptación y criterios relacionados serán establecidos para los nuevos sistemas de información, actualizaciones y nuevas versiones.

- **10.3 Datos de prueba.**
  Objetivo: Asegurar la protección de los datos usados para las pruebas.
  - **10.3.1 Protección de los datos en las pruebas.**
    Control: Los datos probados serán seleccionados cuidadosamente, protegidos y controlados.

- **11. Relaciones con proveedores.**
  - **11.1 Seguridad de la información en las relaciones con proveedores.**
    Objetivo: Asegurar la protección de los activos de la organización que son accesibles por los proveedores.
    - **11.1.1 Política de seguridad de la información para la relación con proveedores.**
      Control: Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización se acordarán con el proveedor y estarán documentados.
    - **11.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores.**
      Control: Todos los requisitos de seguridad de la información relevantes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de TI de infraestructura para la información de la organización.
    - **11.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.**
      Control: Los acuerdos con los proveedores deberán incluir requisitos para tratar los riesgos de seguridad de información asociados a la información, los servicios de tecnología de las comunicaciones y la cadena de suministro de productos.
  - **11.2 Gestión de la entrega del servicio de proveedores**
    Objetivo: Mantener un nivel de servicio acordado de seguridad de la información y servicio de entrega acorde con los acuerdos con proveedores.
    - **11.2.1 Monitorización y revisión de los servicios provistos.**
      Control: Las organizaciones deberán supervisar, revisar y auditar periódicamente la entrega del servicio de proveedores.
    - **11.2.2 Gestión de cambios en los servicios provistos.**

Control: Los cambios en la provisión de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, serán gestionados, teniendo en cuenta la criticidad de la información del negocio, sistemas y procesos que intervienen y la reevaluación de los riesgos.

- **12. Gestión de incidentes de seguridad de la información.**
  - **12.1 Gestión de incidentes de seguridad de la información y mejoras.**
    Objetivo: Garantizar un enfoque coherente y efectivo para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.
    - **12.1.1 Responsabilidades y procedimientos.**
      Control: Las responsabilidades y procedimientos de gestión serán establecidas para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
    - **12.1.2 Reportes de los eventos de seguridad de la información.**
      Control: Los eventos de seguridad de información serán comunicados a través de canales de gestión adecuadas tan pronto como sea posible.
    - **12.1.3 Reportes de las debilidades de la seguridad de la información.**
      Control: Los eventos de seguridad de información se comunicarán a través de canales de gestión adecuadas tan pronto como sea posible.
    - **12.1.4 Evaluación y decisión sobre los eventos de seguridad de la información.**
      Control: Los eventos de seguridad de información serán evaluados y se decidirá si han de ser clasificados como incidentes de seguridad de la información.
    - **12.1.5 Respuesta a los incidentes de seguridad de la información.**
      Control: Los incidentes de seguridad de información serán respondidos de acuerdo a los procedimientos documentados.
    - **12.1.6 Aprendizaje de los incidentes de seguridad de la información.**
      Control: Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se utilizarán para reducir la probabilidad o el impacto de los incidentes en el futuro.
    - **12.1.7 Recopilación de evidencias.**
      Control: La organización definirá y aplicará procedimientos para la identificación, recolección, adquisición y conservación de la información, que pueda servir como evidencia.
- **13. Seguridad de la Información en aspectos de la Gestión de la Continuidad Comercial.**
  - **13.1 Continuidad de la seguridad de la información.**
    Objetivo: La continuidad de la seguridad de la información será incrustada en los sistemas de gestión de continuidad de negocio de la organización.
    - **13.1.1 Planificación de la continuidad de la seguridad de la información.**

Control: La organización determinará sus necesidades de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

- **13.1.2 Implementación de la continuidad de la seguridad de la información.**
  Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.
- **13.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**
  Control: La organización verificará los controles de continuidad de la seguridad de la información establecidos e implementados a intervalos regulares con el fin de asegurarse de que son válidos y eficaces en situaciones adversas.

- **13.2 Redundancias.**
  Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de información.
  - **13.2.1 Disponibilidad de instalaciones para el procesamiento de la información.**
    Control: Las instalaciones de procesamiento de información se llevarán a cabo con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

- **14. Cumplimiento.**
  - **14.1 Cumplimiento de los requisitos legales y contractuales.**
    Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales en materia de seguridad de la información y de los requisitos de seguridad.
    - **14.1.1 Identificación de la legislación aplicable y requisitos contractuales.**
      Control: Todos los requisitos relevantes de estatutos legislativos, reglamentarios y contractuales y el enfoque de la organización para cumplir con estos requisitos deberán ser identificados de manera explícita, documentada y mantenidos para cada sistema de información y la organización.
    - **14.1.2 Derechos de propiedad intelectual (DPI).**
      Control: Los procedimientos apropiados se aplicarán para garantizar el cumplimiento con los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y uso de productos de software de propietarios.
    - **14.1.3 Protección de los registros.**
      Control: Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, en conformidad con los requisitos legislados, reglamentados, contractuales y de negocio.
    - **14.1.4 Protección de datos y privacidad de la información personal.**

Control: La privacidad y la protección de la información de identificación personal se garantizarán como requieran en la legislación y la reglamentación según se aplique.

- **14.1.5 Regulación de los controles criptográficos.**
  Control: Los controles criptográficos serán utilizados en cumplimiento de todos los acuerdos relevantes, la legislación y los reglamentos.

- **14.2 Revisiones de la seguridad de la información.**
  Objetivo: Garantizar la seguridad de la información que se implementa y opera de acuerdo con las políticas y procedimientos de la organización.
  - **14.2.1 Revisión independiente de la seguridad de la información.**
    Control: El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisarán de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
  - **14.2.2 Cumplimiento de las políticas y normas de seguridad.**
    Control: Los gerentes comprobarán periódicamente el cumplimiento de los procedimientos de procesamiento y la información dentro de su área de responsabilidad con las apropiadas políticas de seguridad, normas y otros requisitos de seguridad.
  - **14.2.3 Comprobación del cumplimiento.**
    Control: Los sistemas de información serán revisados por cumplimiento regularmente con las políticas de seguridad de la información de la organización y los estándares.

# Anexo 2 – Procesos y Métricas de la norma COPC PSIC

Definiremos tres grupos de procesos: Los PCRC (Procesos Clave Relacionados con el Cliente), los PCA (Procesos Clave de Apoyo) y las Métricas Clave de Resultado.

**PCRC (Procesos Clave Relacionados con el Cliente)** se pueden agrupar en dos tipos:

- **Transacciones en Tiempo Real**

  Se definen porque:

  - Hay un intercambio directo con el usuario final y el mismo está presente durante el tiempo en cola
  - El Usuario Final determina cuándo contactar al centro y el centro responde a esta demanda.
  - El centro tiene un tiempo limitado para atender la transacción antes que el usuario abandone.
  - Si la llamada no se responde en un tiempo razonable, aquellas no atendidas se consideran dentro de la tasa de abandono.

- **Transacciones Diferida:**

  Se definen porque el usuario final no participa activamente del tiempo en cola.

  - El centro determina cuándo procesar la transacción.
  - La duración del ciclo para transacciones diferidas usualmente se mide en horas o días.
  - Las transacciones que esperan ser procesadas se llaman pendientes.

  Los tipos de PCRCs que son transacciones diferidas son: E-mails; Web Mails; Cartas y Faxes; Devolución de llamadas (Callbacks); Procesamiento de mensajes de Correo de Voz; Escalamientos Internos (excepto transferencias en vivo); Excepciones; Procesamiento de pagos; La mayoría de las funciones Back Office; Procesamiento de Pedidos; Ensamblado del Producto, Retiro, Empaquetamiento; Transporte; Procesamiento de Devoluciones; Recepción de Material y Almacenamiento; Despacho de Servicio; Manejo de Casos; Activación de cuentas; Procesamiento de pedidos de Literatura de Campaña; Procesamiento de lista de No Llamar; Procesamiento de archivos del cliente; Procesamiento de correo; Recepción y Preparación de transacciones; Actualizaciones de la base de datos; Procesamiento de transacciones defectuosas o, transacciones que no se pueden manejar; Almacenamiento de transacciones; Búsqueda de transacciones; Provisión de Producto; Reabastecimiento de Materiales de Marketing.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad, Pendientes, Precisión del Error Crítico del Usuario Final, Precisión del Error Crítico del Negocio, Precisión del Error Crítico de Cumplimiento, Resolución en el Contacto, Ventas, Volumen y Eficiencia.

También hay procesos especializados que no son tiempo real o en diferido y disponen de métricas únicas, listados a continuación:

**a. Procesamiento de Escalamientos por fuera de la Entidad**

Son consultas que el PSIC no puede resolver y que debe derivar a un grupo o función externo a la entidad.

Se medirán mensualmente y abarcarán las siguientes: Tasa de escalamiento y Volumen.

**b. Gestión del IVR**

La provisión y mantenimiento de hardware y software del IVR utilizado para el direccionamiento de un usuario final a información automatizada o a la fila de atención de Agentes que sea apropiada.

Se medirán trimestralmente y abarcarán las siguientes: Tasa de autoservicio, Tasa de abandono, Tasa de salida y Precisión del ruteo.

**c. Cierre de contactos salientes**

Es la obtención de compromiso del Usuario Final (Por ejemplo: Ventas/Oportunidades de venta, referencias de producto, retenciones, promesas de afiliación, etc.) de parte de clientes internos o externos.

Se medirán mensualmente y abarcarán las siguientes: Éxito de completitud y Tasa de cierre.

**d. Procesamiento de contactos salientes con el Usuario Final**

Indicarán los intentos de contactar con Usuarios Finales usando métodos automatizados (marcador) o manuales.

Se medirán mensualmente y abarcarán las siguientes: Tasa de Conexión con la parte Correcta (RPC), Listado de pendientes, Precisión del Error Crítico del Usuario Final, Precisión del Error Crítico del Negocio, Precisión del Error Crítico de Cumplimiento, Coste por unidad, Tasa de RPC, Tasa de Ventas, Tasa de completitud, Utilización y AHT.

**e. Rastreo de prospectos**

Su misión será encontrar prospectos potenciales con números de teléfono y/o direcciones desconocidos.

Se medirá mensualmente y abarcará la siguiente: Tasa de éxito.

**f. Gestión global de casos**

Gestión de los casos hasta su completitud.

Concierne la medición y gestión de las interacciones que generalmente no serán resueltas en una sola transacción y donde el PSIC es responsable por gestionar la interacción con el usuario final hasta que sea resuelta.

1. Esto es distinto del manejo de llamadas típico, donde se espera que la mayoría de las transacciones sean resueltas en el primer contacto, y aquellos que impliquen múltiples contactos serían la excepción.

2. Cada evento dentro de un caso es medido cómo un PCRC distinto, y juntos se combina para formar el caso completo.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad en el cierre, Pendientes de caso, Precisión del Error Crítico del Usuario Final, Precisión del Error Crítico del Negocio, Precisión del Error Crítico de Cumplimiento, Resolución en el Contacto, Volumen y Eficiencia.

A continuación se explican todas las **métricas relacionadas con los PCRC**, como calcular su medición y el objetivo marcado, asociadas a esta norma:

- **Velocidad de Respuesta**: Se puede diferenciar de dos formas, la primera como el Nivel de Servicio, es decir, porcentaje de transacciones atendidas dentro del periodo de tiempo establecido como objetivo o la segunda como el Tiempo Medio de Espera (AWT) o Tiempo Medio de Respuesta (ASA), el tiempo medio utilizado en un periodo para que se atienda una llamada.

  El Nivel de Servicio debe estar basado en las transacciones ofrecidas a la cola de Agentes, no en las transacciones atendidas por la cola de Agentes.
  De usarse TME, debe aplicarse RUICA a la distribución de velocidad de respuesta cercana a la media.
  Donde no es apropiado o posible medir Nivel de Servicio o Tasa de Abandono para un programa como en una operación de cola compartida. Entonces el PSIC debe medir Cumplimiento de la Programación para cada locación que participa en la cola compartida.

  - Medición: Porcentaje de transacciones atendidas antes de un umbral objetivo; por ej., 40 segundos o tiempo promedio para atender todas las transacciones en un período (TME).
  - Objetivo: fijado en base a la expectativa del cliente y el tipo de servicio

- **Tasa de Abandono**: Es el % de transacciones abandonadas antes de ser atendidas por un Agente en vivo.

  Si hay un IVR o sistema de mensajes, entonces no se debe utilizar un umbral de abandono corto.
  Los objetivos de Tasa de abandono y Velocidad de respuesta deben ser matemáticamente consistentes.

  - Medición: El número de clientes que llaman y cortan después del IVR pero antes de hablar con un RAC en vivo expresado como un porcentaje de llamadas ofrecidas.
  - Objetivo: fijado en base a la expectativa del cliente y el tipo de servicio.

- **Puntualidad (On time):** Debe hacerse seguimiento del porcentaje de transacciones procesadas dentro del objetivo de duración de un ciclo.

  El objetivo de duración de un Ciclo es el objetivo de tiempo para procesar una transacción de punta a punta desde la perspectiva del usuario final.
  Donde no es apropiado o posible medir Puntualidad o Pendientes al nivel del sitio para un programa, como en una operación de cola compartida. Entonces el PSIC debe medir Cumplimiento de la Programación para cada localización participante en la cola compartida.

  - Medición: Se debe establecer la duración de ciclo y el objetivo de duración de ciclo antes de que se pueda medir la puntualidad.
    Puntualidad es el porcentaje de transacciones procesadas dentro del objetivo de duración de ciclo.
  - Objetivo: 95% para cualquier requisito de duración de Ciclo.

- **Pendientes:** Tiempo promedio de atraso de las transacciones no procesadas a tiempo.

  Promedio Ponderado de “fotos diarias”.

  - Medición: Tiempo promedio de atraso de las transacciones aún no procesadas, que están más allá del objetivo de duración de ciclo.
  - Objetivo: Tiempo promedio de atraso de 24 horas o un ciclo de atraso, el que sea más corto.

- **Tasa de autoservicio:** Número total de interacciones completadas utilizando la función de autoservicio dividido por el número total de transacciones ofrecidas que presentan la opción de autoservicio.

  - Medición: Número total de llamadas completadas por la opción del menú de autoservicio del IVR como porcentaje del total de llamadas respondidas por el IVR.
  - Objetivo: No está definido para el IVR.

- **Tasa de Conexión con la parte Correcta (RPC**): Conexiones con la parte correcta por intento.

  Se procesa un registro después de que se alcance a potenciales personas o el número de intentos repetidos se excedió o que la persona potencial es inalcanzable (por ejemplo: se fue, no hay número, desconocido, etc.)

  - Medición: Número de Partes Correctas alcanzado como porcentaje de registros procesados.
  - Objetivo: No está definido.

- **Listado de pendientes:** Tiempo promedio de atraso de la lista de Usuarios Finales que aún no se ha contactado o que no se ha intentado, al finalizar el tiempo requerido para ello.

  La completitud de la lista es o un objetivo definido por el Cliente o es definida internamente. Los pendientes de la lista permiten al equipo de llamadas salientes planear sus requisitos de planificación de personal y programar campañas futuras.

  - Medición: Se calcula comparando el número de grabaciones que fueron procesadas por período (normalmente día) contra el número que debe ser procesado por período para alcanzar la fecha de completitud de la lista.
  - Objetivo: Generalmente no debe ser mayor a un día de atraso.

- **Puntualidad en el cierre:** Es el % de casos cerrados dentro del objetivo de duración de ciclos.

  Se puede hacer seguimiento de Puntualidad para resolver si el proceso no requiere cierre de casos.

  - Medición: Porcentaje de casos cerrados dentro del objetivo de duración de ciclos dividido por el número de casos creados.
  - Objetivo: Un 95%.

- **Pendiente de casos:** Tiempo Promedio de Atraso para casos que no se han cerrado o resuelto al objetivo de duración de ciclos

  Medido mensualmente Promedio Ponderado de “fotos diarias”.

  - Medición: Tiempo promedio de atraso de las transacciones aún no procesadas, que están más allá del objetivo de duración de ciclo.
  - Objetivo: No está definido.

- **Precisión crítica para el Usuario Final:** Tasa de precisión de errores críticos que afectan al usuario final en las transacciones monitoreadas.

  Porcentaje de transacciones monitoreadas que no tienen un Error Crítico Usuario final.

Medido por unidad, donde unidad es igual a una transacción.

- Medición: Errores que son críticos desde la perspectiva del usuario final (Por ejemplo: información errónea, maltratar al cliente, como una falta de respeto o no resolver el problema del usuario final, etc.) Se calcula de la siguiente manera:

  (Transacciones sin ECUF / Transacciones Monitoreadas) %

- Objetivo: Cuando se miden satisfactorios e insatisfactorios: 95% (por Unidad); Cuando se miden sólo satisfactorios: 98% (por Unidad)

- **Precisión del Error Crítico para el Negocio:** Tasa de precisión de errores críticos que afectan al negocio en las transacciones monitoreadas.
  Porcentaje de transacciones monitoreadas que no tienen un Error Crítico para el Negocio.

  Medido por unidad, donde unidad es igual a una transacción.

  - Medición: Errores que son críticos desde la perspectiva del PSIC o del Cliente pero que no impactan negativamente en el Usuario Final. Se calcula de la siguiente manera:

    (Transacciones sin ECN / Transacciones Monitoreadas) %

  - Objetivo: 90%

- **Precisión del Error Crítico de Cumplimiento:** Tasa de precisión de errores críticos de cumplimiento en las transacciones monitoreadas.
  Porcentaje de transacciones monitoreadas que no tienen un Error Crítico de Cumplimiento

  Medido por unidad, donde unidad es igual a una transacción.

  - Medición: Errores asociados con el cumplimiento de normas Nacionales, Estatales, Federales, Autonómicas o Locales o cumplimiento con cualquier ente regulador de la industria. Se calcula de la siguiente manera:

    (Transacciones sin ECC / Transacciones Monitoreadas) %

  - Objetivo: 99.5%. Sin embargo esto varía con los requisitos del ente regulador

- **Resolución en el contacto:** Debe hacer el seguimiento de Resolución de Problemas, Resolución en el Primer Contacto o Resolución en la Primera Llamada.
  No hay una manera consistente en la industria de medir la Resolución en el Contacto.
  Los enfoques incluyen medir en una encuesta al usuario final, analizando las transacciones repetidas en la información del CRM o durante el monitoreo de transacciones.

- Medición: (Número de transacciones que se resolvieron / Número total de transacciones atendidas) % o (Número de transacciones que se resolvieron durante el primer contacto / Número total de transacciones atendidas) %
- Objetivo: No hay, pero deben ser consistentes con los Objetivos y Resultados de Satisfacción del Usuario final.

- **Tasa de escalamientos:** Es el porcentaje de las Transacciones que requieren escalamientos a una función externa.
  Escalamiento por fuera de la Entidad significa específicamente:
  - Que la responsabilidad por resolver la transacción pasó a otro grupo o función externa y no gestionada por la entidad.
  - Donde el PSIC tiene una definición de Entidad limitada, el PCRC "Procesando Escalamientos por fuera de la entidad" no aplica si el PSIC es capaz de influenciar el desempeño del grupo o función que reciba las transacciones escaladas.
  - Medición: (Número de transacciones que se escalaron / Transacciones manejadas) %
  - Objetivo: No está establecido.

- **Tasa de salida:** El porcentaje de personas que llaman, que contactan el IVR, realizan o no alguna tarea significativa, pero eligen salir hacia un Agente o salen por "Error out".
  Los "Opt Out" son aquellos que llaman y seleccionan una opción para ir directamente a un Agente sin seleccionar entre las opciones ofrecidas en el IVR. Los "Error Out" son aquellos que llaman y no seleccionan una opción válida en el IVR. Por ejemplo, seleccionan "4" cuando sólo hay opciones para 1, 2 y 3.

  - Medición: La Tasa de Salida se define como la suma de las tasas de "Opt Out" y "Error Out".
  - Objetivo: No está establecida para el IVR.

- **Precisión del ruteo:** Es el porcentaje de transacciones que son ruteadas correctamente según diseño del IVR.
  - Medición: Generalmente hay dos mediciones
    - ➔ La precisión Técnica mide el porcentaje de llamadas que son enviadas al perfil de agente que corresponda por diseño del IVR. Por ejemplo: El nodo 1 del IVR debería ser enviado a agentes con el set de perfil 1).
    - ➔ La precisión de Comportamiento mide el porcentaje de llamadas que fueron identificadas precisamente por el cliente usando el IVR. Por ejemplo: para una aerolínea, que porcentaje de llamadas de reservas internacionales fueron de clientes qué buscaban una reserva internacional.
  - Objetivo: No está establecida para el IVR.

- **Tasa de Éxito:** Es, por ejemplo, el porcentaje de prospectos (potenciales usuarios finales) encontrados.
  - Medición: Calculado como el número de prospectos rastreados exitosamente dividido por el número de prospectos intentados.
  - Objetivo: No está establecido.

- **Ventas:** Debe hacerse seguimiento de la tasa de conversión (por ejemplo, porcentaje de llamadas con una venta) o volumen de conversión (por ejemplo, dólares/euros vendidos).

  Los servicios que tienen un objetivo relacionado con los ingresos (por ejemplo: hacer citas, completar encuestas, salvar clientes, generar oportunidades de ventas), deben utilizar esta métrica.

  - Medición: Número de transacciones donde el objetivo de venta o ganancias es alcanzado (por ejemplo: se hace una venta o una cita) como un porcentaje del número total de transacciones atendidas o Valor total o volumen de ventas/ objetivo de ingresos alcanzado en cierto período.
  - Objetivo: Depende del Programa.

- **Éxito de completitud:** Valor de Ventas, número de oportunidades de ventas generadas, valor total de promesas, valor de producto, valor retenido.

  Se debe hacer seguimiento a dos niveles, al nivel del Agente individual y al nivel apropiado (por ejemplo: cliente, centro, tipo de producto, portfolio).

  - Medición: Valor o Volumen total del Objetivo de Ventas/Ingresos alcanzado en un período determinado.
  - Objetivo: Varían de programa a programa.

- **Tasa de cierre:** Porcentaje de ventas cerradas, ratio de promesas a ventas, porcentaje de promesas concretadas.

  Se debe hacer seguimiento de al menos una métrica para medir la efectividad del cierre. Por ejemplo: Porcentaje de Ventas cerradas, proporción respecto de ventas, porcentaje de compromisos canjeados.

  - Medición: Volumen total de transacciones cerradas exitosamente como porcentaje del número de transacciones gestionadas donde el cierre era posible.
  - Objetivo: Varían de programa a programa.

- **Utilización de agentes:** Porcentaje de tiempo pagado, que los agentes invierten en trabajo productivo o están disponibles para atender transacciones del cliente.

  Trabajo productivo incluye el tiempo de manejo de llamadas, tiempo de espera de una llamada, si se usa marcador (tiempo disponible) y tiempo utilizado en otro tipo de transacciones del cliente (por ejemplo, casos o correos), revisión de una grabación antes de llamada. El tiempo disponible es el tiempo en el que los agentes están esperando transacciones.

  - Medición: (Tiempo Productivo + Tiempo Disponible) / Horas Pagadas
  - Objetivo: Un 86%

- **Tiempo Medio de Manejo (Average Handle Time, AHT):** Es el tiempo promedio que lleva manejar una transacción en Tiempo Real, incluyendo todo tipo de trabajo llevado a cabo después de haberse desconectado del usuario final.

  Tiempo promedio utilizado por transacción respondida, sea hablando con el cliente (tiempo medio de conversación), en espera (hilo musical o silencio) con un cliente, o en tiempo posterior a la llamada (After Call Wait, ACW).

  - Medición: Tiempo Total de Manejo (incluido ACW) / Transacciones Manejadas
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieros similares.

- **Ocupación:** Debe hacerse un seguimiento del tiempo que el agente está ocupado en trabajo productivo como porcentaje del tiempo que está disponible para hacer trabajo productivo.

  La ocupación varía significativamente de programa a programa, dependiendo de un número de factores como reglas de planificación, horas de apertura, volúmenes de transacciones, etc.

  - Medición: Tiempo Productivo / (Tiempo Productivo + Tiempo Disponible)
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieras similares.

- **Coste por x:** Donde x puede ser (Transacción, Resolución, Cliente, Venta/Oportunidad de Venta/Retención, Incidente, Aplicación/Caso o Cualquier otro Factor.

  El numerador debería ser el coste directo asociado de proveer el servicio. No debería incluir costes asignados.

  El Denominador debería ser el número total de x (si x es transacciones, entonces éste es el número total de transacciones manejadas).

  - Medición: Costes Directos / Numero total de x
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieros similares.

- **Eficiencia:** Por ejemplo, el tiempo promedio de procesamiento por transacción, transacciones procesadas por agente en una hora, coste por transacción, etc.

Una métrica común usada para gestionar la eficiencia de las transacciones diferidas es el número de transacciones procesadas por período de tiempo dado (usualmente una hora o día de agente) en vez de medir el tiempo de manejo, ya que puede ser más difícil medir esto sin una herramienta especializada para hacer seguimiento de transacciones.

- Medición: No se requiere una métrica específica siempre y cuando se comparen unidades de entrada y salida o sea relevante para el Proceso Clave Relacionado con el Cliente que se está midiendo.
- Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieros similares.

- **Coste por unidad:** Por ejemplo, el coste por RPC (Conexión con la Parte Correcta), coste por venta, coste por llamada, coste por cuenta, coste por hora.

  El numerador debería ser el coste directo asociado con la provisión del servicio. No debería incluir costes asignados.

  El denominador debería ser el número total de x (si x es transacciones, entonces este es el número total de transacciones manejadas).

  - Medición: Costes asociados con la provisión de servicio / Número total de x
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieras similares.

- **Tasa de RPC** (Conexión con la Parte Correcta): Por ejemplo, RPCs por hora de trabajo.

  - Medición: Número de RPCs hecho / Número de horas de personal trabajadas
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieras similares.

- **Tasa de ventas:** Por ejemplo, ventas por hora, contactos por hora, acuerdos por hora, etc.

  - Medición: Número de Ventas | Contactos | Retenciones | Otros logrados / Número de horas de personal empleadas.
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieras similares.

- **Tasa de completitud:** Si el PSIC utiliza marcador automático.

  - Medición: Número real de intentos hechos / Total de registros
  - Objetivo: Son determinados correctamente con un objetivo de mejora continua y pueden basarse inicialmente en estimaciones de presupuesto o indicadores financieras similares.

- **Volumen:** Por ejemplo, el número de llamadas recibidas por período, número de transacciones escaladas, cantidad de casos recibidos por período, número de llamadas que aun no han sido atendidas, etc.
  No requieren ninguna métrica ni tienen un objetivo marcado.

**Los PCA (Procesos Clave de Apoyo)** se pueden dividir en dos secciones

- Como procesos internos:

**1. Telecomunicaciones (Tecnología).**

Provisión y mantenimiento de hardware, software y servicios de telecomunicaciones (por ejemplo: el servicio de larga distancia, el servicio de línea local, switchs, teléfonos de agentes, software de gestión de llamadas, etc.).

Se medirán mensualmente y abarcarán las siguientes: Disponibilidad/Acceso y Transacciones bloqueadas (esta tendrá una medición trimestral).

**2. Sistemas de Gestión de la Información (Tecnología).**

Provisión y mantenimiento del hardware y software de apoyo de los sistemas de información (por ejemplo: sistemas de gestión de pedidos, bases de conocimiento, terminales de agentes u ordenadores personales).

Se medirá mensualmente y abarcará la siguiente: Disponibilidad/Acceso.

**3. Gestión de la Base de Conocimiento (Tecnología).**

Mantener actualizadas y precisas las bases de conocimiento.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad, Precisión de la Base de Conocimiento y Satisfacción con la base de conocimiento.

**4. Provisión interna del Servicio de Asistencia (Helpdesk).**

Respuesta al pedido del personal para reparar (o agregar/ mover/ cambiar) telecomunicaciones o equipos de sistemas de información.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad y Calidad.

**5. Pronóstico de Volumen y AHT.**

Proyectar el volumen de transacciones para asegurar que se dispone de la suficiente capacidad para cumplir los requisitos de servicio en forma óptima y eficiente.

Se medirán mensualmente y abarcarán las siguientes: Precisión de Pronóstico de Volumen para Programación y Precisión de pronóstico de AHT para Programación.

**6. Búsqueda/Contratación.**

Obtener los recursos humanos necesarios para satisfacer las necesidades de dotación de la operación.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad y Calidad de Reclutamiento.

7. **Formación**.

Formación del personal en los requisitos de habilidades mínimas y conocimiento.

Se medirá mensualmente y abarcará la siguiente: Calidad de la Formación.

**8. Implementación de Nuevos programas.**

Puntualidad en el cumplimiento de los hitos de implementación.

Se medirá mensualmente y abarcará la siguiente: Puntualidad.

**9. Gestión de la planta.**

Asegurar que los agentes trabajan según su programación.

Se medirá mensualmente y abarcará la siguiente: Adhesión.

**10. Provisión de productos.**

Pedido de producto al proveedor del mismo con el fin de mantener un inventario suficiente, y provisión de productos necesarios para ensamblar otros productos o enviar productos a los usuarios finales.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad, Pedido en espera y Precisión.

**11. Reaprovisionamiento de Materiales de Marketing.**

Asegurarse que los materiales de marketing estén siempre actualizados.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad, Pendientes y Precisión.

**12. Control de inventarios.**

Mantenimiento preciso del inventario, tanto en el caso que pertenezca al cliente como al PSIC.

Se medirá mensualmente y abarcará la siguiente: Precisión en el recuento cíclico de inventario.

**13. Recepción y almacenamiento de materiales.**

Recepción de los materiales y almacenamiento de los mismos en sus lugares definitivos o transitorios.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad, Pedido en espera y Disponibilidad/Acceso.

**14. Gestión del marcador.**

Provisión y mantenimiento de hardware y software para apoyar la función del marcador automático del PSIC.

Se medirá mensualmente y abarcará la siguiente: Disponibilidad/Acceso.

- Y como procesos externos:

**15. Informes sobre el desempeño al Cliente.**

Reporte de la información tal como es requerida por los clientes. Comúnmente llamados reportes diarios, semanales o mensuales.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad y Precisión del Error Crítico.

**16. Facturación a Clientes.**

Facturación al cliente por los servicios prestados.

Se medirán mensualmente y abarcarán las siguientes: Puntualidad y Precisión Externa.

Seguidamente se explican todas las **métricas relacionadas con los PCA**, como calcular su medición y el objetivo marcado, asociadas a esta norma:

- **Disponibilidad/Acceso:** Por ejemplo, el porcentaje de tiempo que el sistema está en total funcionamiento, porcentaje de tiempo que las líneas están en total disponibilidad, porcentaje de tiempo que el marcador está en total funcionamiento

  Para la tecnología: debería ser calculado como el porcentaje de las horas que está abierto. Es aceptable reportar cada sistema por separado. De todas maneras esto debería ser combinado para crear una sola métrica para los cálculos de niveles.

  Para las telecomunicaciones (líneas): debería ser calculada como el porcentaje de horas en que las líneas están en total funcionamiento.

  Para el marcador: se debe calcular como un porcentaje de las horas abierto. Aplicable únicamente si el PSIC utiliza un marcador automático.

  - Medición: (Minutos de disponibilidad del switch|sistema|marcador / Total de minutos de las líneas en total funcionamiento) %

  - Objetivo: 99,6 %

- **Transacciones bloqueadas:** Por ejemplo la cantidad de llamadas no recibidas debido a limitaciones y/o configuración de redes, troncales o PBX.

  Si el reporte de bloqueo de llamadas no está disponible, la capacidad máxima de utilización mensual de las troncales puede ser reportada.

  Si los datos de satisfacción e insatisfacción del usuario final indican un problema con el acceso de los clientes, esta métrica debe ser reportada más frecuentemente.

  - Medición: (Número de llamadas que reciben un tono de ocupado / Total de llamadas ofrecidas) %

  - Objetivo: 0 %

- **Puntualidad (On line):** Por ejemplo puede referirse a: la puntualidad en el procesamiento de actualizaciones de la información dentro del objetivo de duración de ciclos, puntualidad por nivel de gravedad, porcentaje de solicitudes de contratación del personal completadas a la fecha objetivo, porcentaje de los componentes de programa entregados puntualmente, porcentaje de pedidos de productos entregados puntualmente, porcentaje de materiales de marketing

reaprovisionados puntualmente o puntualidad para el registro de recepción del material en el ordenador.

Cuando se trate de la provisión interna de Helpdesk, es aceptable establecer un objetivo de puntualidad para cada ticket basado en su severidad.

Con respecto a la búsqueda o contratación, contratar más personal del requerido no resulta en una puntualidad mayor al 100% el máximo es 100%.

En la Implementación de Nuevos programas, no es mejor práctica, pero cumple hacer seguimiento sólo de Puntualidad para la fecha acordada de "ir en vivo".

- Medición:
    - Gestión de la base del conocimiento = (Número de actualizaciones procesadas en tiempo objetivo / Total actualizaciones) %
    - Provisión interna del Servicio de Asistencia (Helpdesk) = (Tickets resueltos / Tiempo objetivo) %
    - Búsqueda/Contratación = Solicitudes de contratación cubiertas para la fecha objetivo (%)
    - Implementación de Nuevos programas = Hitos que son completados en la fecha planeada o antes (%)
    - Pedidos o Reaprovisionamiento de materiales de marketing = (Cantidad de pedidos entregados / Total de pedidos) % {Por ciclo de duración}
    - Recepción y almacenamiento de materiales = (Ítems registrados como procesados dentro del tiempo objetivo / Número total de ítems) %
- Objetivo:

No está definido para las actualizaciones.

Para la Provisión interna de Helpdesk, la Búsqueda/Contratación, la Implementación de Nuevos programas: generalmente 90% o más.

- **Adhesión:** Por ejemplo, la Adhesión a la Programación, Conformidad, Cumplimiento de la Programación, etc.

- Medición: No hay una métrica específica pero se pueden medir los siguientes ejemplos.

    - Cumplimiento de la Programación = Número correcto de agentes presentes en cada intervalo comparado con la programación

    - Adhesión a la Programación = adherencia de cada agente al programa tal como estaba previsto

    - Conformidad con la Programación = se cumplió con el total de horas programadas.

  - Objetivo: Dependerá del ejemplo concreto.

- **Pedido en espera:** Por ejemplo el tiempo promedio de atraso de materiales de marketing que fueron pedidos pero todavía no se recibieron.

  - Medición: Tiempo medio de Atraso de pedidos a procesar y que han sobrepasado el objetivo de duración de ciclo
  - Objetivo: No está definido.

- **Pendientes:** Por ejemplo la antigüedad de las unidades de almacenamiento que han sido pedidas pero aún no han sido recibidas, el tiempo promedio de atraso del producto ya recibido en el depósito pero que aún no ha sido ingresado en el sistema del PSIC o almacenado.

  Promedio ponderado de “fotos diarias”.

  - Medición: Tiempo medio de Atraso de transacciones o pedidos a procesar y que han sobrepasado el objetivo de duración de ciclo.
  - Objetivo: 24 horas o 1 ciclo de atraso, el que sea más corto.

- **Precisión de la Base de Conocimiento**: Por ejemplo la tasa de precisión de búsquedas en las que la información fue la correcta.

  Esta métrica puede basarse en datos muestreados.

  - Medición: No tiene.
  - Objetivo: No está definido.

- **Calidad**: Por ejemplo la precisión de la solución/reparación.

  Se deben desarrollar las reglas del negocio para que definan cuando un incidente se reabre.

  Si la calidad se mide a partir del monitoreo de transacciones, estos datos pueden ser muestreados.

- Medición: Número de tickets que no se reabren (%).
- Objetivo: No está definido.

- **Precisión de Pronóstico de Volumen para Programación**: Por ejemplo el Volumen de transacciones Reales contra el Volumen Pronosticado, a nivel del intervalo para el pronóstico desarrollado para crear programaciones para el personal existente.

  Debe tener en cuenta el tiempo de desfase operacional para la programación. Debe ser calculado a nivel del intervalo.
  - Medición: El % de intervalos donde el volumen de transacciones real está entre +x% y –y% del volumen pronosticado.
  - Objetivo: Varios objetivos dependiendo de la volatilidad de la tasa de llegada de transacciones.

- **Precisión de Pronóstico de AHT para Programación**: Por ejemplo el AHT real contra el AHT pronosticado a nivel diario para el pronóstico desarrollado para generar programaciones para el personal existente.

  Debe responder por el tiempo de desfase operacional para programación. Se reporta mensualmente basado en datos diarios.

  - Medición: El % de días donde el AHT real de las transacciones está entre +x% y –y% del pronóstico de AHT.
  - Objetivo: Varios objetivos dependiendo de la volatilidad de la tasa de llagada de transacciones.

- **Calidad de reclutamiento**: Por ejemplo la tasa de rotación entre el nuevo personal.

  Las cifras deberían ser reportadas en el mes de reclutamiento. Habrá una demora en el reporte, debido al desfase de 3 meses.

  - Medición: (Número de agentes nuevos todavía en el negocio después de 3 meses / total contratado en el mes) %
  - Objetivo: 80%

- **Calidad de la formación**: Por ejemplo el porcentaje del personal que pasa el monitoreo de transacciones 30 días después de completar la formación.

  Es mejor mirar el desempeño en el último monitoreo del período de 30 días.

  - Medición: (Número de agentes nuevos que aprueban el monitoreo al final de sus primeros 30 días en el puesto) %

- Objetivo: 90%

- **Precisión**: Por ejemplo el porcentaje de unidades de almacenamiento o de materiales de marketing entregadas en forma correcta o sin daños.

  - Medición: (Cantidad de pedidos entregados en forma correcta o sin daños / Total de pedidos realizados) %
  - Objetivo: 90%

- **Precisión en el recuento cíclico de inventario**: Por ejemplo la precisión en las unidades de almacenamiento.

  - Medición: Ninguna.
  - Objetivo: No está establecido.

- **Puntualidad**: Por ejemplo el porcentaje de informes enviados puntualmente, la puntualidad en el envío de la factura al cliente.

  Con respecto a las facturas, la fecha de envío límite se establecerá por políticas contables internas.

  - Medición:
    - Informes enviados al cliente a la fecha estipulada para el envío del informe o antes de la misma (%)
    - Porcentaje de facturas enviadas al cliente en la fecha estipulada para el envío o antes de la misma (%)
  - Objetivo:

    - Informes: A acordar con el cliente. Típicamente en el rango de 95% a 100% dependiendo del volumen de informes
    - Facturas: Típicamente 100% debido a la importancia del pago al PSIC externo.

- **Precisión del Error Crítico:** Por ejemplo el porcentaje de reportes sin errores marcados por el cliente.

  Se puede calcular por unidad o por oportunidad.

  - Medición: Reportes sin errores (%)
  - Objetivo: Dependiendo del método de cálculo y cantidad de informes, estará en un rango del 90% a 100%

- **Precisión externa**: Por ejemplo el valor de las notas de crédito.

El crédito debe reportarse para el mes de la facturación. Esto puede generar un desfase en los informes hasta que se conozcan todos los créditos.

- Medición: Notas de crédito respecto al valor facturado (%)

Objetivo: ≥ 98%

Por último se establecen las **Métricas Clave de Resultado** que no pertenecen a los PCRC o PCA:

**1. Satisfacción e insatisfacción del Usuario Final.**

Evaluar el grado de satisfacción/insatisfacción que el usuario final tiene con el servicio provisto por el PSIC.

Se medirán mensualmente y abarcarán las siguientes: Satisfacción Global del Usuario Final e Insatisfacción Global del Usuario Final.

**2. Satisfacción e insatisfacción del Cliente.**

Evaluar el grado de satisfacción/insatisfacción que el cliente tiene con el servicio provisto por el PSIC.

Se medirán mensualmente y abarcarán las siguientes: Satisfacción Global del Cliente y Puntualidad en la gestión de las quejas, que se medirá al menos anualmente.

3. **Rotación**.

Evaluar la tasa de desvinculaciones de personal para agentes y jefes de equipo.

Se medirán al menos trimestralmente y abarcarán las siguientes: Rotación de agentes y Rotación de jefes de equipo.

4. **Ausentismo**.

Calcular la cantidad de tiempo que se pierde debido al ausentismo no programado.

Se medirá al menos trimestralmente y abarcará la siguiente: Ausentismo de agentes.

Las métricas que las componen serán las siguientes:

- **Satisfacción global del Usuario Final:** Se debe hacer el seguimiento de la Satisfacción global del Usuario Final al nivel del programa, al nivel del cliente y a nivel de la entidad.

  El estándar COPC usa una escala de 5 puntos donde el punto medio es neutral. Se puede cumplir utilizando otras escalas. Si se utiliza otra escala, el PSIC debe definir la métrica basada en un número de boxes. Es también responsabilidad del PSIC demostrar que el objetivo es de alto desempeño.

  - Medición: Número de respuestas a las encuestas que puntúan Top Two Box a la satisfacción global como porcentaje de todas las encuestas respondidas recibidas.
  - Objetivo: 85% Top Two Box en una escala de 5 puntos donde el punto del medio es neutral.

- **Insatisfacción global del Usuario Final:** Se debe hacer el seguimiento de la Satisfacción global del Usuario Final al nivel del programa, al nivel del cliente y a nivel de la entidad.

  El estándar COPC usa una escala de 5 puntos donde el punto medio es neutral. Se puede cumplir utilizando otras escalas. Si se utiliza otra escala, el PSIC debe definir la métrica basada en un número de boxes. Es también responsabilidad del PSIC demostrar que el objetivo es de alto desempeño.

  - Medición: Número de respuestas a las encuestas que puntúan bottom box a la Satisfacción Global como porcentaje del total de encuestas completadas recibidas.

  Objetivo: 2% Bottom Box en una escala de 5 puntos donde el punto del medio es neutral.

- **Satisfacción global del Cliente:** Se debe hacer el seguimiento de la Satisfacción global del Usuario Final al nivel del programa, al nivel del cliente y a nivel de la entidad.

  Si se reciben muy pocas encuestas, es obligatorio reportar una puntuación promedio.

  - Medición: Número de respuestas a las encuestas que puntúan Top Two Box a la satisfacción global como porcentaje de todas las encuestas respondidas recibidas.
  - Objetivo: 80% Top Two Box en una escala de 5 puntos donde el punto del medio es neutral.

- **Puntualidad en la gestión de las quejas:** Se debe hacer el seguimiento de la puntualidad para resolver o de la puntualidad para responder a las quejas de los clientes.

  - Medición: Número de quejas respondidas o resueltas dentro de la duración de ciclo objetivo como un % del total de quejas recibidas.
  - Objetivo: <95% para cualquier ciclo.

- **Rotación de agentes:** Rotación anual del personal en puestos de agentes, calculada tanto al nivel del programa como al nivel de la entidad.

  Debe ser medida por persona, no por equivalencia de tiempo completo, es decir por el número de horas que trabaja cada persona.

  El cálculo anual debe estar basado en un mes o más de datos. Se recomienda que un mes de datos se use para programas de gran escala y hasta doce meses para programas más pequeños.

  El cálculo está basado en el nivel de la entidad en el número de personas que se fue de la Entidad. Al nivel del programa se basa en el número de personas que salió del rol en el programa (esto incluye ascensos a otro rol en el mismo programa).

  - Medición: Número de Agentes que se fueron y que fueron remplazados como % del total de Agentes.
  - Objetivo: Se determinan en base a un entendimiento de los costes de la rotación y el impacto en Servicio, Calidad y Costes.

- **Rotación de jefes de equipo:** Rotación anual de personal en puestos de jefes de equipo, calculada tanto al nivel del programa como al nivel de la entidad.

  Para programas pequeños con muy pocos jefes de equipo no se requiere la medición de rotación de jefes de equipo para ese programa.

  - Medición: No tiene una medida específica.
  - Objetivo: Se determinan en base a un entendimiento de los costes de la rotación y el impacto en Servicio, Calidad y Costes.

- **Ausentismo de agentes:** Por ejemplo el porcentaje de horas perdidas por la ausencia en el puesto de trabajo). Se debe medir al nivel del programa y a nivel de la entidad.

Incluye ausentismo a corto plazo por cualquier motivo. El ausentismo a corto plazo se define como el ausentismo por cualquier razón de aquel personal que estaba programado para trabajar.

No incluye el ausentismo a largo plazo. Los agentes se consideran ausentes a largo plazo cuando ya no se incluyen en la elaboración de la programación habitual.

- Medición: Esto se calcula como el número de horas perdidas a través de ausencias de corto plazo como un porcentaje de las horas programadas.
- Objetivo: No está definido para este tipo de métrica.