

Gobierno Corporativo de TI

Guía breve de Autoevaluación



ISACA[®] Capítulo de Madrid

Cuadernos de ISACA Madrid. Nº 1

Reconocimientos

El Capítulo de Madrid de ISACA (183) desea reconocer la labor de:

Coordinación

Miguel García Menéndez, CGEIT, CISM, CISA, Atos Consulting

Autoría

M^a Cristina Bausá Rosa, CGEIT, CISA, CISM, CIA, Mazars Auditores

M^a José Carmona Carmona, CISA, Telecinco

M^a Jesús Casado Robledo, CGEIT, CISA, Intervención General de la Administración del Estado

Juan José Huerta Díaz, CGEIT, CISM, CISA, Mutua Madrileña

Revisores expertos (miembros de la “Comisión para el estudio y el desarrollo del Buen Gobierno Corporativo de las TIC, dentro de las organizaciones”)

Alberto Javier Arroyo Jávega, Alamcia

Dr. Carlos Bachmaier Johanning, CGEIT, CISM, CISA, Loterías y Apuestas del Estado

Dr. José Manuel Ballester Fernández, CGEIT, CISM, CISA, Temanova-Alintec

José Fernando Carvajal Vión, CGEIT, CISM, CISA, Indra

José Antonio Castrillo Nuevo, CGEIT, CISM, CISA, Aventia

Juan Fernández Corral, PMP, Hitachi Consulting

Antonio Folgueras Marcos, CISA, CGEIT, Universidad Carlos III de Madrid

Luís Fuente Simón, CGEIT, Junta de Castilla y León

Adolfo Hernández Lorente, CISA, Écija Abogados

Beatriz Jiménez Martín, CGEIT, CISA, Fomento de Construcciones y Contratas

Samuel Linares Fernández, CGEIT, CISM, CISA, Grupo Intermark

Gonzalo Martínez Rioja, CISA, CISM, Ferrovial

Javier Ángel Moreno Montón, CGEIT, CISM, CISA, Grupo Eptisa

Manolo Palao García-Suelto, CGEIT, CISM, CISA, Personas y Técnicas: Soluciones

Julio Sáiz Rodríguez, CISA, Adecco

Junta Directiva del Capítulo de Madrid de ISACA (183)

Alejandro Rembado Mendizábal, CGEIT, Telefónica, Presidente

Fernando Hervada Vidal, CGEIT, CISA, CIA, ENDESA, Vicepresidente

Ramiro Mirones Gómez, CISA, CISM, Ernst & Young, Secretario

Jesús Bermejo Izquierdo, CISA, CISM, MA, CajaMadrid, Tesorero

Elena Maestre García, CISA, CISM, PricewaterhouseCoopers, Vocal

Julio San José, CISA, CISM, Bankinter, Vocal

Luís Manuel Carro, CISA, Deloitte, Vocal

Manuel Mendiola Antona, CISA, CISM, CIA, KPMG, Vocal

Javier Galiana Ferrándiz, CIA, CISA, Liberty Seguros, Vocal

Miguel García Menéndez, CGEIT, CISM, CISA, Atos Consulting, Vocal

Prof. Dr. José Domingo Carrillo Verdún, Universidad Politécnica de Madrid, Vocal

José Manuel Vidal Formoso, CISA, BBVA, Presidente anterior

Contenidos

RECONOCIMIENTOS.....	3
CONTENIDOS	4
1 INTRODUCCIÓN	5
2 OBJETIVO	5
3 CUESTIONARIO DE AUTOEVALUACIÓN. ESTRUCTURA.....	5
3.1 BLOQUE I. SOBRE EL PAPEL DEL CONSEJO DE ADMINISTRACIÓN/COMITÉ DE DIRECCIÓN EN RELACIÓN A TI 6	
3.2 BLOQUE II. SOBRE LA FUNCIÓN DE TI	6
3.3 BLOQUE III. SOBRE LOS PRINCIPIOS GENERALES QUE HAN DE REGIR EL GOBIERNO CORPORATIVO DE TI....	6
3.3.1 PRINCIPIO DE RESPONSABILIDAD.....	6
3.3.2 PRINCIPIO DE ESTRATEGIA	6
3.3.3 PRINCIPIO DE ADQUISICIÓN (INVERSIÓN)	6
3.3.4 PRINCIPIO DE RENDIMIENTO	7
3.3.5 PRINCIPIO DE CONFORMIDAD	7
3.3.6 PRINCIPIO DE CONDUCTA HUMANA	7
4 CUMPLIMENTACIÓN DEL CUESTIONARIO DE AUTOEVALUACIÓN	7
ANEXOS	9
ANEXO I: CUESTIONARIO DE AUTOEVALUACIÓN	9
ANEXO II: RIESGOS Y CONTROLES	18

1 INTRODUCCIÓN

El **Gobierno Corporativo de las Tecnologías de la Información y las Comunicaciones (TIC/TI)** constituye una disciplina relativamente nueva, con apenas una década de vida desde la aparición de las primeras referencias bibliográficas sobre el tema. Ello unido al, cada vez más creciente, interés que la Gobernanza de TI suscita en el mercado, han servido de incentivo para el lanzamiento de la presente **Guía breve de Autoevaluación**.

La iniciativa, gestada en el seno de la *Comisión para el estudio y el desarrollo del Buen Gobierno Corporativo de las TIC, dentro de las organizaciones del Capítulo de Madrid de ISACA*, no tiene otra finalidad que la de servir de puerta de entrada a la Gobernanza de TI para aquellos individuos que quieran comenzar a aproximarse a los problemas que las TIC plantean a las organizaciones y a los mecanismos que han de ponerse en marcha para atajar y superar tales retos.

Basada en la norma *ISO/IEC 38500:2008. Corporate Governance of Information Technology* y otro material bibliográfico de ISACA/ITGI, la *Guía* ofrece una lista de puntos de verificación que permitirá realizar autoevaluaciones sobre el grado de Gobierno TIC adoptado por las organizaciones.

2 OBJETIVO

El objetivo de la *Guía* será, por tanto, proporcionar a los consejeros-administradores y resto de individuos con responsabilidades sobre la evaluación, dirección y supervisión del uso de las TIC en sus organizaciones, una herramienta que les permita conocer el estado del marco de Gobierno Corporativo de las TIC, vigente en las mismas.

Adicionalmente, se pretenden atajar las principales barreras a la adopción de mecanismos de Buen Gobierno Corporativo de TI: el desconocimiento de los referidos mecanismos y de los beneficios de su adopción; y, la falta de concienciación sobre la necesidad de disponer de ellos.

La *Guía* podrá ser utilizada en cualquier tipo de organización, independientemente de su tamaño, o de su naturaleza, pública o privada.

3 CUESTIONARIO DE AUTOEVALUACIÓN. ESTRUCTURA

La herramienta que se ha dispuesto para permitir conocer el estado del marco de Gobierno Corporativo de TI dentro de una organización es un cuestionario de autoevaluación.

Este cuestionario ha sido dividido en los siguientes bloques:

- Bloque I. Sobre el papel del Consejo de Administración/Comité de Dirección en relación a TI.
- Bloque II. Sobre el papel de la Función de TI en el proceso de transformación del negocio.
- Bloque III. Sobre los principios generales que han de regir el Gobierno Corporativo de TI.
 - Principio de responsabilidad.
 - Principio de estrategia.
 - Principio de adquisición (inversión).
 - Principio de rendimiento.
 - Principio de conformidad.
 - Principio de conducta humana.

Cada uno de estos bloques se describe, en mayor detalle, a continuación.

3.1 BLOQUE I. SOBRE EL PAPEL DEL CONSEJO DE ADMINISTRACIÓN/COMITÉ DE DIRECCIÓN EN RELACIÓN A TI

La evaluación de un marco de Gobierno Corporativo de TI ha de pasar, necesariamente, por un análisis del papel que juega el Consejo de Administración/Comité de Dirección, u órgano equivalente, en relación a la dirección y control de las TI, y su uso, en el seno de la organización. Ello habrá de permitir obtener una imagen del lugar que ocupa la Gobernanza TIC en el escenario general de Gobierno Corporativo.

3.2 BLOQUE II. SOBRE EL PAPEL DE LA FUNCIÓN DE TI EN EL PROCESO DE TRANSFORMACIÓN DEL NEGOCIO

El segundo bloque del cuestionario trata de ofrecer una perspectiva sobre una serie de aspectos generales de la Función de TI, dentro de la entidad (comunicación con el Consejo de Administración/Comité de Dirección, comunicación con los empleados, percepción de las áreas usuarias, etc.), en relación a su papel en los procesos de transformación de la propia organización.

3.3 BLOQUE III. SOBRE LOS PRINCIPIOS GENERALES QUE HAN DE REGIR EL GOBIERNO CORPORATIVO DE TI

En este tercer, y último, bloque se hace un recorrido por los seis principios generales del Buen Gobierno Corporativo de TI, según recoge la norma ISO/IEC 38500:2008 -responsabilidad, estrategia, adquisición, rendimiento, conformidad y conducta humana-.

Dentro del cuestionario, se dedica un subapartado a cada uno de los citados principios.

3.3.1 PRINCIPIO DE RESPONSABILIDAD

El Bloque III del cuestionario comienza con una serie de preguntas relativas al principio general de responsabilidad, en relación al uso de las TI.

Se intenta evaluar si las responsabilidades de cada individuo, o grupo de personas, dentro de la organización, en relación a las TI, están definidas. Cada miembro de la organización debe conocer, comprender y aceptar sus responsabilidades; y disponer de la debida autoridad, en función del papel que desempeñe, para ejecutarlas.

Las responsabilidades han de estar claramente definidas, tanto a nivel interno (miembros de los órganos de gobierno, alta dirección y resto de personal), como hacia el exterior (diferentes grupos con intereses en la organización).

3.3.2 PRINCIPIO DE ESTRATEGIA

Las preguntas planteadas en este apartado ayudan a evaluar si la planificación estratégica del negocio de la organización tiene en cuenta y está coordinada con las capacidades actuales y futuras (infraestructuras, recursos humanos, etc.) de las TI.

Al mismo tiempo, se trata de evaluar si la estrategia de TI extiende la estrategia del negocio, esto es, si se satisfacen las necesidades actuales, y previstas, reflejadas en el plan estratégico de la organización.

3.3.3 PRINCIPIO DE ADQUISICIÓN (INVERSIÓN)

Las adquisiciones (inversiones) en TI ocupan el tercer apartado de este Bloque III. Se pretende evaluar si las adquisiciones de TI se realizan siguiendo un criterio valido, sobre la base de un análisis

apropiado y continuo, con decisiones claras y transparentes. Ha de existir un adecuado equilibrio entre beneficios, oportunidades, costes y riesgos, tanto a corto, como a largo plazo. Las soluciones de TI deben ser consideradas como parte del negocio ya que su razón de ser será facilitar la transformación de la organización y de sus procesos.

3.3.4 PRINCIPIO DE RENDIMIENTO

Se trata de evaluar si las áreas e infraestructuras de TI están suficientemente dimensionadas para dar soporte a la organización, cubriendo sus necesidades actuales y futuras, y ofreciendo unos servicios con la calidad adecuada. Se hace precisa la existencia de mecanismos de medida, para garantizar la supervisión constante y continuada del rendimiento y la fiabilidad de las TI.

3.3.5 PRINCIPIO DE CONFORMIDAD

La Función de TI debe cumplir y contribuir al cumplimiento, por parte de la organización, de todas las regulaciones (legales o normativas) aplicables. Las políticas y prácticas al respecto deberán estar claramente definidas, implantadas y exigidas.

Debido al creciente número de requisitos normativos a que deben dar respuesta las organizaciones en el actual entorno globalizado -nacidos, en gran parte, de los escándalos corporativos producidos en los últimos años-, las direcciones de las organizaciones y los grupos con intereses en ellas, en general, demandan un mayor control, una mayor garantía del cumplimiento con leyes y reglamentos, y una mayor adhesión a las buenas prácticas del Gobierno Corporativo por parte de sus entornos operativos.

Aplicar un Buen Gobierno Corporativo de TI requerirá alcanzar un equilibrio adecuado entre rendimiento y conformidad.

3.3.6 PRINCIPIO DE CONDUCTA HUMANA

Finalmente, el cuestionario ayuda a evaluar si las políticas, prácticas y decisiones en torno a TI muestran respeto por el componente humano de la organización, incluyendo las necesidades actuales, y emergentes, de toda la gente involucrada.

Cualquier decisión relevante, o cambio organizativo, en torno a TI puede suponer un cambio cultural significativo en el comportamiento de las organizaciones, de sus clientes y socios de negocios. Para evitar posibles temores y mitigar la más que probable resistencia, debe existir un compromiso explícito por parte de la Organización (de la Dirección de la Organización) y han de comunicarse sus objetivos, en relación con posibles decisiones o cambios.

4 CUMPLIMENTACIÓN DEL CUESTIONARIO DE AUTOEVALUACIÓN

Como se ha indicado, el objetivo de este cuestionario es permitir una autoevaluación del estado en que se encuentra el actual marco de Gobierno Corporativo de TI, dentro de una organización.

El presente documento va acompañado de una herramienta informática en la que se diferencian los siguientes módulos:

1. Información del Encuestado.

Información sobre la dimensión y tipo de empresa, que servirá para aportar mayor calidad a los resultados de la encuesta pudiendo extraer conclusiones a nivel sectorial, tamaño de empresa, etc.

2. Cuestionario de autoevaluación (propriadamente dicho).

Para cada pregunta se ofrecerán cuatro posibles respuestas. A saber:

- **Si:** Se está de acuerdo / Cumple la pregunta planteada.

- **No:** No se está de acuerdo / No cumple la pregunta planteada.
- **No Aplica:** La pregunta planteada no es de aplicación a la organización objeto de evaluación.
- **No Sabe / No Contesta:** Se desconoce la respuesta.

3. Auto-informe.

Tras finalizar la cumplimentación del cuestionario, la propia herramienta podrá generar un informe de observaciones y recomendaciones a aplicar.

El cuestionario, basado en la herramienta Excel de Microsoft, requiere, para su correcta ejecución, que se habilite la ejecución de macroinstrucciones.

ANEXOS

ANEXO I: CUESTIONARIO DE AUTOEVALUACIÓN

En las páginas que siguen se detallan las preguntas para cada bloque del cuestionario.

BLOQUE I. Sobre el papel del Consejo de Administración/Comité de Dirección en relación a TI	
1.1	¿Está definida, documentada y publicada la misión de la organización?
1.2	¿Está creada, documentada y publicada la estructura organizativa?
1.3	¿Se asignan responsabilidades a todos los niveles de la estructura organizativa?
1.4	¿Se han asignado responsabilidades al Comité de Dirección? ¿Están entre tales responsabilidades las relativas a la supervisión de las TI?
1.5	¿En el Comité de Dirección están representados todos los departamentos de la organización, ya sean de negocio o tecnológicos?
1.6	¿El Comité de Dirección define los objetivos a conseguir en el corto y medio plazo, teniendo en cuenta las necesidades y e intereses de la organización?
1.7	¿Las personas destinadas en los distintos departamentos conocen cuáles son sus responsabilidades, las entienden y las aceptan?
1.8	¿Se asignan los recursos necesarios a todos los departamentos?
1.9	¿Se verifica que los recursos asignados se utilizan adecuadamente?
1.10	¿El Comité de Dirección es consciente y trasmite a los departamentos de negocio lo importante que es su participación en todas las etapas de la informatización de los procesos de negocio?
1.11	¿El respaldo del Comité de Dirección se refleja en la asignación de los recursos necesarios y en el control posterior del uso de los mismos?
1.12	¿Se aporta información al Comité de Dirección sobre los avances tecnológicos que pueden aportar ventajas competitivas en los procesos de negocio?
1.13	¿Se elaboran informes sobre la contribución de TI a la generación de valor para los procesos de negocio? ¿El Comité de Dirección los conoce y entiende?
1.14	¿Se informa al Comité de Dirección de los riesgos asociados al uso de la TI?
1.15	¿Se ha definido un Marco de Gestión del Riesgo Corporativo, que permita identificar, evaluar y gestionar todo el espectro de riesgos que afecte a la organización?
1.16	El Comité de Dirección, ¿ha identificado el “apetito” al riesgo de la organización? Esto es, ¿se ha definido el nivel de riesgo que la organización está dispuesta a asumir para las diferentes categorías de riesgos: estratégicos, operacionales, de información (<i>reporting</i>) y de cumplimiento?

BLOQUE II. Sobre el papel de la Función de TI en el proceso de transformación del negocio	
2.1	¿Está definida, documentada y publicada la misión del área de TI, dentro de la organización?
2.2	¿Está creada, documentada y publicada la estructura organizativa del área de TI?
2.3	¿Se asignan responsabilidades a todos los niveles de la estructura organizativa del área de TI?
2.4	¿Se dispone de una metodología para la ejecución de los proyectos de transformación de los procesos de negocio, que facilite la reutilización de elementos y la reducción del tiempo de ejecución?
2.5	¿Se elaboran informes sobre el seguimiento de la ejecución de los proyectos de transformación de los procesos de negocio?
2.6	¿El Comité de Dirección conoce y entiende las desviaciones recogidas en esos informes?
2.7	¿Se identifican los factores que han propiciado las desviaciones?
2.8	¿Se adoptan las medidas necesarias para eliminar las desviaciones?
2.9	¿El día a día obliga a tomar demasiadas decisiones a corto plazo que pueden afectar a dirección estratégica y, por tanto a la consecución de los objetivos a medio y largo plazo?
2.10	¿Está definida, documentada y publicada la política -y normativa afín- sobre el uso adecuado de las TI por todos los empleados de la organización?
2.11	¿Los empleados conocen y aceptan las consecuencias del incumplimiento de la política/normativa?
2.12	¿En función de los cambios tecnológicos introducidos en la organización se actualiza la política/normativa de uso de las TI?
2.13	¿Se difunden los cambios introducidos para que los empleados los conozcan y asuman?
2.14	¿Se dispone de los recursos necesarios (presupuesto, formación, tiempo,...) antes de abordar un proceso de cambio tecnológico?
2.15	¿Existe un plan de formación y concienciación continuas, dirigido a todos los empleados, de forma que se entienda el proceso de cambio y se favorezca su participación activa?
2.16	¿Se transmite la necesidad de los cambios como una aportación de valor que garantiza la continuidad de la organización en el tiempo?
2.17	¿Los empleados perciben que su actuación individual contribuye a la culminación con éxito del proceso de cambio?
2.18	¿Existe un sistema de comunicación fluido de la marcha del proceso de cambio?
2.19	¿Están los usuarios satisfechos con el desempeño de TI de la organización?

BLOQUE III. Principio de RESPONSABILIDAD	
3.1	¿La estructura organizativa asegura una cierta independencia de la Función de TI?
3.2	¿Se han definido roles en los que recaiga la planificación y dirección de TI?
3.3	¿Se han definido las funciones y obligaciones para cada rol, con respecto a sistemas de información, control interno y seguridad?
3.4	¿Se han definido responsabilidades respecto a la propiedad de los datos y los sistemas?
3.5	¿Se controla que los roles y responsabilidades se cumplan? ¿Se realiza un seguimiento?
3.6	¿Se ha establecido la debida segregación de funciones entre desarrollo, operación, seguridad y control interno?
3.7	¿Se considera la competencia del personal, antes de asignar un determinado rol?
3.8	¿Existen políticas para revisar la definición de funciones y responsabilidades de cada rol?
3.9	¿Existen políticas que limiten qué funciones se pueden desempeñar por personal externo?
3.10	¿Los diferentes roles disponen de autoridad suficiente para ejercer las funciones encomendadas?
3.11	¿La función de Sistemas de Información presenta informes periódicos al Comité de Dirección respecto a los resultados del desempeño?
3.12	¿Existe una política que defina las pautas mínimas para las relaciones con terceros?
3.13	¿Se disponen los recursos suficientes para las actividades encomendadas?

BLOQUE III. Principio de ESTRATEGIA	
4.1	¿Participa el Responsable de TI en el Comité de Dirección?
4.2	Dentro del Comité de Dirección ¿Los representantes de los departamentos tecnológicos tienen la posibilidad de participar activamente en la toma de decisiones relativas a la estrategia?
4.3	¿Conoce el Responsable de TI los planes a corto y largo plazo de la organización?
4.4	¿Los planes a corto y largo plazo de TI van alineados con los planes a corto y largo plazo de la organización?
4.5	¿Se utilizan indicadores clave de desempeño y/o factores críticos de éxito para medir los resultados de TI en el logro de los objetivos de la organización?
4.6	¿Se hace un seguimiento de los indicadores definidos que nos ayude a la toma de decisiones sobre TI?
4.7	¿Se elevan los resultados al Comité de Dirección?
4.8	¿Se dispone una metodología para formular y modificar planes, y que incluya el estudio de factibilidad, los riesgos y la sincronización con los objetivos de la organización?
4.9	¿Los proyectos de transformación del negocio, con base en TI, están soportados por la suficiente información y documentación?
4.10	¿Los planes TI de alto nivel están aprobados por el Comité de Dirección?

BLOQUE III. Principio de ADQUISICIÓN (INVERSIÓN)	
5.1	¿Las adquisiciones de TI se basan en el análisis continuo de la dirección estratégica y los planes a corto y largo plazo definidos?
5.2	¿Se dispone de un Plan de Infraestructura Tecnológica?
5.3	¿Se revisa o actualiza periódicamente el Plan de Infraestructura Tecnológica?
5.4	¿Se consideran las tendencias y regulaciones presentes y futuras durante el mantenimiento del Plan de Infraestructura Tecnológica?
5.5	¿Se evalúa el impacto frente a una adquisición tecnológica?
5.6	Durante la evaluación del plan tecnológico, ¿se evalúan aspectos de contingencia (redundancia, adecuación y capacidad evolutiva de la infraestructura)?
5.7	¿Se planifica el mantenimiento de la infraestructura?
5.8	¿Están definidos entornos separados de prueba y producción?
5.9	¿El proceso de adquisición de la infraestructura tecnológica está en línea con las aplicaciones críticas del negocio y con la arquitectura tecnológica?
5.10	¿Participan en el proceso de adquisición/inversión Consejo de Administración/Comité de Dirección/TI/Usuarios?

BLOQUE III. Principio de RENDIMIENTO	
6.1	¿La infraestructura y los recursos de TI disponibles son suficientes para lograr los objetivos estratégicos de la empresa?
6.2	¿Se consensuan los niveles de servicio entre los departamentos usuario y los de sistemas?
6.3	¿Se realizan auditorias periódicas que verifiquen la eficacia y eficiencia de los procesos de TI?
6.4	¿Se calculan las desviaciones sobre los niveles de servicio acordados?
6.5	¿Se hace un seguimiento de la implementación de las recomendaciones?
6.6	La dirección obtiene informes independientes del cumplimiento de los objetivos de rendimiento (efectividad y eficiencia) de las TI
6.7	La dirección recibe informes del desempeño de las TI desde el punto de vista de negocio, en los que se vea que se satisfacen sus necesidades
6.8	Existe una planificación de capacidad de TI (tanto tecnológica como humana) que garantice el servicio tanto presente como futuro.
6.9	¿Se supervisa que el uso de las TI por parte de los empleados sea el adecuado?
6.10	¿Son conscientes los empleados de que un uso inadecuado de los recursos afecta al rendimiento?
6.11	¿Existen ANS que garanticen el rendimiento de TI con los diferentes departamentos de la organización?
6.12	¿Hay un seguimiento periódico de los servicios externalizados, incluyendo: Procesos de TI, Desarrollos de Software e Infraestructuras?
6.13	Existen procedimientos de control que garanticen la confidencialidad, disponibilidad e integridad de los datos contenidos en los SI.
6.14	¿Está definido, documentado y se mantiene actualizado un plan de actuación ante contingencias que garantice que se van a mantener los niveles de servicio acordados?
6.15	¿Los empleados del departamento de TI disponen de las capacidades suficientes para recuperar un servicio en el menor tiempo posible?
6.16	¿Se dispone de alguna alternativa en caso de que esa persona no esté disponible?
6.17	¿En caso de detectar desviaciones en el cumplimiento de los niveles de servicio acordados se adoptan medidas correctoras?

BLOQUE III. Principio de CONFORMIDAD	
7.1	¿Se conocen y aplican las normas y regulaciones de carácter general que son de obligado cumplimiento? (nacionales e internacionales)
7.2	¿Se conocen y aplican las normas y regulaciones sectoriales que son de obligado cumplimiento?
7.3	¿Se redactan, actualizan y divulgan cláusulas a incorporar en los contratos con objeto de garantizar la confidencialidad y privacidad de la información que un tercero utilice en la ejecución del trabajo contratado?
7.4	¿Se redactan, actualizan y divulgan cláusulas a incorporar en los contratos con objeto de proteger la propiedad intelectual?
7.5	¿Se redactan, actualizan y divulgan cláusulas a incorporar en los contratos indicando qué se ha de hacer con la información manejada durante el período de ejecución del trabajo objeto del contrato?
7.6	¿Cuándo se incorpora nuevo personal a la organización en el contrato se le informa del uso que ha de hacer de los recursos que se ponga a su disposición para la realización de su trabajo, así como, las consecuencias de un uso indebido de los mismos?
7.7	¿Se han implementados controles para verificar el cumplimiento de las obligaciones derivadas de la normativa?
7.8	¿En los contratos celebrados con terceros se incluye una cláusula que indique el derecho de la organización a someter a una auditoría a dicho tercero con objeto de verificar que se cumplen los extremos recogidos en el contrato?
7.9	¿Se realizan auditorías, internas o externas, de forma periódica, para verificar que se cumple internamente la normativa obligatoria?
7.10	¿Se hace un seguimiento de las correcciones de las no conformidades recogidas en el informe de auditoría?
7.11	¿Se llevan a cabo campañas de sensibilización del personal de forma que cada empleado tome conciencia de que todo lo que hace en la organización afecta a la imagen de la misma?
7.12	¿Se informa al personal de que el mal uso de las tecnologías de la organización puede hacer incurrir a ésta en responsabilidad legal?
7.13	¿Se realizan campañas de formación dirigidas al personal para dar a conocer la normativa y la regulación aplicables?
7.14	¿Se preparan los sistemas informáticos para su adecuación continua a los preceptos legales, de forma que esa automatización facilite el cumplimiento por parte de los empleados?

BLOQUE III. Principio de CONDUCTA HUMANA	
8.1	¿Existen políticas para la contratación y conservación del personal?
8.2	¿Se realiza una evaluación del desempeño laboral y de las capacidades del personal?
8.3	¿Se ha realizado una valoración de la dependencia de individuos claves?
8.4	¿Existen políticas o procedimientos que prevengan dichas dependencias?
8.5	¿Existen políticas donde se definan como se deben llevar a cabo los cambios de puestos de los empleados?
8.6	¿Existen políticas donde se definan como se deben llevar a cabo la extinción de la relación laboral con los empleados?
8.7	¿En la realización de los proyectos de TI se mantiene el compromiso de las partes interesadas?
8.8	¿Se transfiere el conocimiento a la gerencia de negocio y a los usuarios finales cuando finaliza un proyecto de TI?
8.9	¿Se motiva a las personas y se les hace partícipe del objetivo desde el principio y se les permite participar en la toma de la decisión más adecuada?
8.10	¿Se llevan a cabo iniciativas de sensibilización y de formación de todos y cada uno de los implicados con las Tecnologías de la Información?
8.11	¿Cuándo se producen cambios en las Tecnologías de la Información, se evalúa el impacto que el cambio producirá a nivel individual para todos los involucrados?
8.12	¿Se involucra a las personas y se busca la sincronización con la estrategia corporativa?
8.13	¿Se identifican los riesgos con los proveedores que puedan afectar al funcionamiento de las Tecnologías de la Información?
8.14	¿Se cuenta con personal suficiente y con los conocimientos técnicos necesarios para el desarrollo de las tareas?
8.15	¿La organización de TI y sus procesos son desarrollados y mantenidos de manera que se detecten las necesidades y requerimientos del personal a todos los niveles?
8.16	¿Se realiza una gestión de los recursos humanos de manera que se explique cómo debe ser el comportamiento de los individuos de manera que se sincronice con los objetivos y metas corporativas?

ANEXO II: RIESGOS Y CONTROLES

En la siguiente tabla se muestran los riesgos asociados a cada pregunta si la respuesta ha sido un “No”. También se proponen controles que mitigan los riesgos identificados.

BLOQUE I. Sobre el papel del Consejo de Administración/Comité de Dirección en relación a TI		
	Riesgos	Controles
1.1	<ul style="list-style-type: none"> Indefinición estratégica. Desorientación en la definición de los objetivos de negocio. Desubicación sectorial. 	<ul style="list-style-type: none"> Definición de la misión de la organización. Definición de los objetivos estratégicos.
1.2	<ul style="list-style-type: none"> Imposibilidad de asignar responsabilidades Solapamiento de competencias. Duplicidad de esfuerzos. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa
1.3	<ul style="list-style-type: none"> Desconocimiento de las obligaciones y responsabilidades. Incumplimiento normativo y regulatorio. 	<ul style="list-style-type: none"> Definición de las consecuencias por incumplimientos de las responsabilidades. Formación y concienciación en materia normativa y regulatoria.
1.4	<ul style="list-style-type: none"> Vacío directivo. Dirección sin rumbo. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa
1.5	<ul style="list-style-type: none"> Toma de decisiones incompleta. Dificultad en la conciliación de los intereses de la gestión y de la TI. 	<ul style="list-style-type: none"> Modificación del Comité para que estén representados los departamentos de gestión y los departamentos técnicos.
1.6	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio 	<ul style="list-style-type: none"> Definición de planes directores plurianuales.
1.7	<ul style="list-style-type: none"> Desorientación en la ejecución de las tareas asignadas. Resultados individuales no contribuyen a la consecución de los objetivos de negocio. Divulgación no autorizada de información. Posibilidad de comprometer la imagen de la organización. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. Campañas de concienciación para crear cultura corporativa.
1.8	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. Aumento del estrés en los trabajadores. Personal descontento y desmotivado. Conflictos laborales. 	<ul style="list-style-type: none"> Asignación de los recursos en función de los proyectos del plan director. Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros.
1.9	<ul style="list-style-type: none"> Gestión de recursos ineficiente. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros.
1.10	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. Sistemas que no satisfacen los requerimientos del negocio. Dificultad para conciliar intereses heterogéneos. 	<ul style="list-style-type: none"> Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio.
1.11	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. Gestión de recursos ineficiente. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros.

BLOQUE I. Sobre el papel del Consejo de Administración/Comité de Dirección en relación a TI		
	Riesgos	Controles
1.12	<ul style="list-style-type: none"> Desaprovechamiento de oportunidades asociadas al uso de la TI. Pérdida de mercado. Capacidad de respuesta limitada a los cambios del entorno. 	<ul style="list-style-type: none"> Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo.
1.13	<ul style="list-style-type: none"> Falta de inversión en TI. Innovación insuficiente. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio.
1.14	<ul style="list-style-type: none"> Decisiones temerarias o erróneas. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio
1.15	<ul style="list-style-type: none"> No conseguir identificar todos los eventos que puedan afectar a la consecución los objetivos. 	<ul style="list-style-type: none"> Cada área debe identificar y gestionar los riesgos que le afectan. Creación de un comité de riesgos formado por la alta dirección que evalúe periódicamente el control del riesgo.
1.16	<ul style="list-style-type: none"> No alcanzar los objetivos planeados para cada una de las cuatro categorías: estrategia, operación, reporting y cumplimiento. 	<ul style="list-style-type: none"> La dirección debe establecer la zona de confort para cada categoría de riesgos. Las diferentes áreas deberán evaluar los riesgos y tomar las acciones necesarias que permitan mantener los riesgos identificados en la zona de confort (apetito).

BLOQUE II. Sobre la Función de TI		
Riesgos		Controles
2.1	<ul style="list-style-type: none"> • Que no exista una alineación estratégica de TI con el negocio. • Que TI no aporte el valor que la organización espera. • Imposibilidad de medir el desempeño 	<ul style="list-style-type: none"> • Herramientas que permitan asignar responsabilidad y ayudar a medir el desempeño. • Definir indicadores
2.2	<ul style="list-style-type: none"> • Dificultad para establecer metas y estrategias en la dirección de TI. • No tener adaptada la estructura organizativa a los objetivos de negocio. • Dificultad de adaptarse a los cambios en la organización. 	<ul style="list-style-type: none"> • Implantar un proceso para revisar la estructura organizativa de TI de forma periódica, para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y los cambios que se vayan produciendo.
2.3	<ul style="list-style-type: none"> • Uso ineficiente de recursos. • Desaprovechamiento de las sinergias. • Limitaciones a la innovación. • Inmadurez de los procesos. 	<ul style="list-style-type: none"> • Implantación de una metodología adecuada a los proyectos que se realizan. • Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.
2.4	<ul style="list-style-type: none"> • Imposibilidad de implantar estándares de trabajo. 	<ul style="list-style-type: none"> • Implantación de una metodología adecuada a los proyectos que se realizan. • Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.
2.5	<ul style="list-style-type: none"> • Imposibilidad de definir y aplicar medidas correctivas. 	<ul style="list-style-type: none"> • Elaboración de informes ejecutivo redactado en un lenguaje que entienda la Dirección.
2.6	<ul style="list-style-type: none"> • Ineficiencia en la gestión de los recursos. 	<ul style="list-style-type: none"> • Implantación de una metodología adecuada a los proyectos que se realizan. • Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización
2.7	<ul style="list-style-type: none"> • Perpetuación de las desviaciones. • Imposibilidad de crecimiento. • Limitación de abordar proyectos innovadores o, simplemente, nuevos proyectos. 	<ul style="list-style-type: none"> • Implantación de una metodología adecuada a los proyectos que se realizan. • Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización
2.8	<ul style="list-style-type: none"> • Ineficiencia ante nuevas necesidades. • Pérdida de competitividad. • Merma de la capacidad de reacción. • Pérdida de oportunidades. 	<ul style="list-style-type: none"> • Campañas de formación sobre gestión de recursos, en general y del tiempo en particular.
2.9	<ul style="list-style-type: none"> • Comprometer el buen nombre de la organización. • Incumplimiento normativo y regulatorio. • Repercusiones legales para la organización. • Divulgación no autorizada de información sensible. 	<ul style="list-style-type: none"> • Elaboración, divulgación y actualización de la política de uso de los recursos de TI.

BLOQUE II. Sobre la Función de TI		
	Riesgos	Controles
2.10	<ul style="list-style-type: none"> • Comprometer el buen nombre de la organización. • Incumplimiento normativo y regulatorio. • Repercusiones legales para la organización. • Divulgación no autorizada de información sensible. 	<ul style="list-style-type: none"> • Definición de las consecuencias por incumplimientos de las responsabilidades. • Definición de la estructura organizativa. • Definición de las funciones de cada unidad organizativa • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Campañas de concienciación para crear cultura corporativa.
2.11	<ul style="list-style-type: none"> • Comprometer el buen nombre de la organización. • Incumplimiento normativo y regulatorio. • Repercusiones legales para la organización. • Divulgación no autorizada de información sensible. 	<ul style="list-style-type: none"> • Elaboración, divulgación y actualización de la política de uso de los recursos de TI.
2.12	<ul style="list-style-type: none"> • Comprometer el buen nombre de la organización. • Incumplimiento normativo y regulatorio. • Repercusiones legales para la organización. • Divulgación no autorizada de información sensible. 	<ul style="list-style-type: none"> • Elaboración, divulgación y actualización de la política de uso de los recursos de TI.
2.13	<ul style="list-style-type: none"> • El cambio no llega a realizarse por falta de recursos. • Implementación ineficaz e ineficiente del cambio. 	<ul style="list-style-type: none"> • Asignación de los recursos en función de los proyectos del plan director. • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros.
2.14	<ul style="list-style-type: none"> • No aprovechamiento de las oportunidades asociadas al cambio por falta de recursos. • Rechazo de los cambios aunque supongan mejoras. 	<ul style="list-style-type: none"> • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio.
2.15	<ul style="list-style-type: none"> • Percepción del cambio como un obstáculo. • Rechazo del cambio y se dejan llevar por la inercia. 	<ul style="list-style-type: none"> • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio.
2.16	<ul style="list-style-type: none"> • Percepción del cambio como un obstáculo. • Rechazo del cambio y se dejan llevar por la inercia. 	<ul style="list-style-type: none"> • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio. • Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. • Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo.
2.17	<ul style="list-style-type: none"> • No se detectan desviaciones. • No se consiguen los objetivos definidos. 	<ul style="list-style-type: none"> • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio.

BLOQUE II. Sobre la Función de TI		
	Riesgos	Controles
2.18	<ul style="list-style-type: none">• Gestión de recursos ineficientes.• Descoordinación en las actuaciones de los distintos departamentos.	<ul style="list-style-type: none">• Establecer un estándar de trabajo basado en herramientas colaborativas.
2.19	<ul style="list-style-type: none">• Falta de apoyo de los usuarios a futuros proyectos.• Los usuarios perciben las TI como un obstáculo y no como una ayuda.	<ul style="list-style-type: none">• Realización de encuestas a los usuarios.• Comparar los resultados de las encuestas con el uso de la TI y con los objetivos definidos por la gestión en el plan director.

BLOQUE III. Principio de RESPONSABILIDAD		
	Riesgos	Controles
3.1	<ul style="list-style-type: none"> Inexistencia de segregación de funciones. Toma de decisiones limitadas e influenciadas 	<ul style="list-style-type: none"> Establecer segregación de funciones y de dependencias en la definición de la estructura organizativa.
3.2	<ul style="list-style-type: none"> Cualificación y habilidades inadecuadas o incompletas de las personas competentes en la toma de decisiones de TI. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa
3.3	<ul style="list-style-type: none"> Falta de segregación de funciones. Influencia de la coyuntura en la toma de decisiones. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa. Definición de las consecuencias por incumplimientos de las responsabilidades.
3.4	<ul style="list-style-type: none"> Dificultad para definir el procedimiento de gestión de identidades. 	<ul style="list-style-type: none"> Definición de las funciones de cada unidad organizativa. Definición de las consecuencias por incumplimientos de las responsabilidades
3.5	<ul style="list-style-type: none"> Incumplimiento normativo y regulatorio. Gestión ineficiente de los permisos de acceso. Imposibilidad de imputar responsabilidades. 	<ul style="list-style-type: none"> Realización de auditorías periódicas.
3.6	<ul style="list-style-type: none"> Posibilidad de cambios no autorizados. Se facilita el uso indebido de los sistemas. Aumento de la probabilidad de que un sistema pase a producción con alguna vulnerabilidad de seguridad. 	<ul style="list-style-type: none"> Establecer segregación de funciones y dependencias en la definición de la estructura organizativa. Realización de auditorías para verificar la aplicación práctica de la segregación de funciones.
3.7	<ul style="list-style-type: none"> Personal con capacidades o habilidades inadecuadas a las necesidades de desempeño del rol. 	<ul style="list-style-type: none"> Formación al personal. Mantenimiento actualizado de los curriculum de los empleados. Consulta de los curriculum antes de asignar nuevos roles a los empleados. Fomentar la aplicación de la inteligencia emocional en las relaciones humanas.
3.8	<ul style="list-style-type: none"> Incumplimiento normativo y regulatorio. Ejercicio de funciones ineficaz. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa. Establecer segregación de funciones y de dependencias en la definición de la estructura organizativa. Realización de auditorías periódicas. Realización de auditorías para verificar la aplicación práctica de: Establecer segregación de funciones y dependencias en la definición de la estructura organizativa.
3.9	<ul style="list-style-type: none"> Pérdida del conocimiento. 	<ul style="list-style-type: none"> Definición de las tareas que puede desempeñar el personal externo. No externalizar funciones o tareas de control y de toma de decisiones. Crear equipos mixtos de trabajo en los que las tomas de decisiones estén asignadas al personal de la organización. Concienciar al personal interno del incumplimiento de los controles anteriores.
3.10	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. Falta de autonomía en la toma de decisiones. 	<ul style="list-style-type: none"> Establecer segregación de funciones y de dependencias en la definición de la estructura organizativa.

BLOQUE III. Principio de RESPONSABILIDAD		
	Riesgos	Controles
3.11	<ul style="list-style-type: none"> • Pérdida del apoyo de la Dirección. • Imposibilidad de justificar la necesidad de nuevos recursos. • Imposibilidad de explicar el aporte de valor de la TI. 	<ul style="list-style-type: none"> • Realizar los informes ejecutivos en un lenguaje cercano a la Dirección. • Informar a la Dirección objetivamente sobre las ventajas competitivas del uso de las TI y de los riesgos asociados.
3.12	<ul style="list-style-type: none"> • Incumplimiento normativo y regulatorio. • Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> • Definición de los criterios a aplicar en los contratos suscritos con terceros. • Materialización de los criterios en cláusulas contractuales. • Incorporación obligatoria de las cláusulas en los contratos celebrados por todos los departamentos de la organización.
3.13	<ul style="list-style-type: none"> • Incumplimiento de los objetivos de negocio. • Aumento del estrés del personal. • Tensiones laborales. • A medio y largo plazo posible desaparición de la organización. 	<ul style="list-style-type: none"> • Asignación de los recursos en función de los proyectos del plan director. • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. • Formación y concienciación para crear cultura de organización.

BLOQUE III. Principio de ESTRATEGIA		
	Riesgos	Controles
4.1	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. Falta de apoyo de la Dirección. 	<ul style="list-style-type: none"> Modificación del Comité para que estén representados los departamentos de gestión y los departamentos técnicos.
4.2	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. 	<ul style="list-style-type: none"> Que los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité de dirección. Que los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Implantación de una metodología adecuada a los proyectos que se realizan. Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.
4.3	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. 	<ul style="list-style-type: none"> Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo.
4.4	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. 	<ul style="list-style-type: none"> Verificar la coherencia entre el segundo control 1.12 (Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo) y el control 1.6.(Definición de planes directores plurianuales)
4.5	<ul style="list-style-type: none"> Desconocimiento del cumplimiento de los objetivos de negocio. Gestión ineficiente de los recursos de TI. Coste excesivo. 	<ul style="list-style-type: none"> Definición de indicadores que permitan verificar el alcance de los objetivos de negocio.
4.6	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. Falta de apoyo de la Dirección. 	<ul style="list-style-type: none"> Comprobar que se definen y aplican los planes directores plurianuales.
4.7	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. Falta de apoyo de la Dirección. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio.
4.8	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. Falta de apoyo de la Dirección. Desconocimiento del cumplimiento de los objetivos de negocio. Gestión ineficiente de los recursos de TI. Coste excesivo. 	<ul style="list-style-type: none"> Implantación de una metodología adecuada a los proyectos que se realizan. Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.

BLOQUE III. Principio de ESTRATEGIA		
	Riesgos	Controles
4.9	<ul style="list-style-type: none"> Desconocimiento del cumplimiento de los objetivos de negocio. Gestión ineficiente de los recursos de TI. Coste excesivo. 	<ul style="list-style-type: none"> Implantación de una metodología adecuada a los proyectos que se realizan. Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.
4.10	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. Falta de apoyo de la Dirección. 	<ul style="list-style-type: none"> Definición de los objetivos estratégicos. Definición de los planes directores plurianuales. Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo.

BLOQUE III. Principio de ADQUISICIÓN (INVERSIÓN)		
	Riesgos	Controles
5.1	<ul style="list-style-type: none"> • Dimensionamiento inadecuado de la TI. • Falta de alineación de los objetivos de TI con los objetivos de negocio. 	<ul style="list-style-type: none"> • Definición de los objetivos estratégicos • Definición de planes directores plurianuales. • Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. • Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo.
5.2	<ul style="list-style-type: none"> • Lentitud en la respuesta a las necesidades de los usuarios. • Dificultad de escalabilidad. • Pérdida de oportunidades por no prever las necesidades futuras y poder aprovechar la innovación tecnológica. 	<ul style="list-style-type: none"> • Definición de planes directores plurianuales.
5.3	<ul style="list-style-type: none"> • Lentitud en la respuesta a las necesidades de los usuarios. • Dificultad de escalabilidad. • Pérdida de oportunidades por no prever las necesidades futuras y poder aprovechar la innovación tecnológica 	<ul style="list-style-type: none"> • Definición de planes directores plurianuales. • Verificar la coherencia entre el segundo control 1.12 (Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo) y el control 1.6. (Definición de planes directores plurianuales). • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros • Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. • Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. • Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio. • Elaboración de informes ejecutivos redactados en un lenguaje que entienda la Dirección.

BLOQUE III. Principio de ADQUISICIÓN (INVERSIÓN)		
	Riesgos	Controles
5.4	<ul style="list-style-type: none"> Imposibilidad de adoptar soluciones innovadoras. Limitaciones en la escalabilidad. Incumplimiento normativo y regulatorio. 	<ul style="list-style-type: none"> Definición de planes directores plurianuales. Verificar la coherencia entre el segundo control 1.12 (Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo) y el control 1.6. (Definición de planes directores plurianuales). Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros <ul style="list-style-type: none"> Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio. Elaboración de informes ejecutivos redactados en un lenguaje que entienda la Dirección. Conocimiento y aplicación de la normativa general y sectorial.
5.5	<ul style="list-style-type: none"> Impacto negativo en el funcionamiento de los sistemas existentes. 	<ul style="list-style-type: none"> Elaboración de informes ejecutivos redactados en un lenguaje que entienda la Dirección
5.6	<ul style="list-style-type: none"> Discontinuidad del servicio. A medio y largo plazo posible desaparición de la organización. 	<ul style="list-style-type: none"> Elaboración, revisión y actualización del plan de continuidad de negocio
5.7	<ul style="list-style-type: none"> Que existan procesos de negocio críticos soportados por infraestructura obsoleta. No conocer los componentes de infraestructura que ya no se puedan soportar 	<ul style="list-style-type: none"> El departamento de TI deberá establecer un plan de mantenimientos de infraestructura. Definir indicadores que permitan conocer el estado de las infraestructuras.
5.8	<ul style="list-style-type: none"> Interrupciones en las aplicaciones provocadas por no haber realizado pruebas anteriormente a la puesta en producción. Aplicaciones que no satisfacen los objetivos planificados 	<ul style="list-style-type: none"> Definir una metodología de pruebas que permita probar que los cambios en las aplicaciones o infraestructuras cumplen con los objetivos marcados y están libres de errores. Realizar revisiones a posteriori de la implantación en el entorno de producción.
5.9	<ul style="list-style-type: none"> Adquisición de plataformas no adecuadas a las aplicaciones del negocio y con la infraestructura técnica ya en producción. 	<ul style="list-style-type: none"> Establecer un plan de adquisición de tecnología alineado con las infraestructuras ya implantadas en la organización.
5.10	<ul style="list-style-type: none"> Adquirir o invertir en algo que no responde a los requerimientos del negocio. 	<ul style="list-style-type: none"> Definir procedimientos y estándares de adquisición Realizar cuestionarios que permita medir el porcentaje de satisfacción de todos los implicados en la nueva adquisición.

BLOQUE III. Principio de RENDIMIENTO		
	Riesgos	Controles
6.1	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. Aumento del estrés del personal. Tensiones laborales. A medio y largo plazo posible desaparición de la organización. 	<ul style="list-style-type: none"> Definición de planes directores plurianuales. Verificar la coherencia entre el segundo control 1.12 (Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo) y el control 1.6. (Definición de planes directores plurianuales). Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio. Elaboración de informes ejecutivos redactados en un lenguaje que entienda la Dirección Asignación de los recursos en función de los proyectos del plan director. Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros
6.2	<ul style="list-style-type: none"> Falta de alineación de los objetivos de TI con los objetivos de negocio. Falta de apoyo de la Dirección. 	<ul style="list-style-type: none"> Verificar la coherencia entre el segundo control 1.12 (Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo) y el control 1.6.(Definición de planes directores plurianuales)
6.3	<ul style="list-style-type: none"> Gestión de los recursos ineficiente. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. Realización de auditoría para verificar la efectividad y eficiencia de los procesos de TI.
6.4	<ul style="list-style-type: none"> Desconocimiento del cumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> Definición de indicadores que permitan verificar el alcance de los objetivos de negocio. Realizar seguimiento del cumplimiento del control 1.6.
6.5	<ul style="list-style-type: none"> Se perpetúan las no conformidades detectadas. 	<ul style="list-style-type: none"> Realización de auditorías de seguimiento.

BLOQUE III. Principio de RENDIMIENTO		
	Riesgos	Controles
6.6	<ul style="list-style-type: none"> • Subjetividad al tomar decisiones. • Dificultad para detectar un posible uso ineficiente de recursos. • Dificultad de detectar el exceso de recursos en algunas áreas y escasez en otras. Es decir, dificultad de detectar una asignación inadecuada de recursos. 	<ul style="list-style-type: none"> • Encargar auditorías a empresas externas.
6.7	<ul style="list-style-type: none"> • Incumplimiento de los objetivos de negocio. • Satisfacción parcial de las necesidades o requerimientos definidos por los usuarios. 	<ul style="list-style-type: none"> • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros • Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. • Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo. • Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio.
6.8	<ul style="list-style-type: none"> • Falta de personal. • Distribución inadecuada de personal. • Personal sin la formación adecuada. • Dependencia de otras empresas 	<ul style="list-style-type: none"> • Asignación de los recursos en función de los proyectos del plan director. • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros..
6.9	<ul style="list-style-type: none"> • Incumplimiento normativo y regulatorio. • Uso ineficiente de los recursos. • Inversiones innecesarias. 	<ul style="list-style-type: none"> • Automatización de todas las limitaciones recogidas en la política de uso de los recursos de TI. • Aplicar técnicas de observación para el resto.
6.10	<ul style="list-style-type: none"> • Uso ineficiente de los recursos. 	<ul style="list-style-type: none"> • Campañas de formación y concienciación.
6.11	<ul style="list-style-type: none"> • Falta de alineación de los objetivos de TI con los objetivos de negocio. 	<ul style="list-style-type: none"> • Establecimiento de ANS consensuados entre los departamentos de gestión y los de TI. • Resolución de los posibles conflictos de intereses.
6.12	<ul style="list-style-type: none"> • Falta de alineación de los objetivos de TI con los objetivos de negocio.. • Gestión ineficiente del coste. • Incumplimiento de la empresa contratada de los ANS. 	<ul style="list-style-type: none"> • Presentación de informes por parte de la empresa externa. • Encuestas a los destinatarios de los servicios contratados. • Comparación de los resultados de los informes y las encuestas con objeto de obtener una visión completa y tomar decisiones objetivas

BLOQUE III. Principio de RENDIMIENTO		
	Riesgos	Controles
6.13	<ul style="list-style-type: none"> • Incumplimiento normativo y regulatorio. • Perjuicio a terceras personas o entidades. 	<ul style="list-style-type: none"> • Formación y concienciación en materia de seguridad de la información. • Elaboración, y publicación de procedimientos • Implementación de gestión de identidades a partir de los procedimientos. • Implantación de medidas de seguridad que garanticen la disponibilidad e integridad. • Configurar los sistemas para asignar prioridades a los trabajos, clasificándolos por niveles de importancia. • Comprobar que se definen planes directores plurianuales..
6.14	<ul style="list-style-type: none"> • Discontinuidad del servicio. • A medio y largo plazo posible desaparición de la organización. 	<ul style="list-style-type: none"> • Elaboración, revisión y actualización del plan de continuidad de negocio. • Realización de pruebas periódicas del plan con objeto de corregir desviaciones o proceder a su actualización en caso de haber introducido cambios en la gestión o en la tecnología.
6.15	<ul style="list-style-type: none"> • Discontinuidad del servicio. • A medio y largo plazo posible desaparición de la organización. 	<ul style="list-style-type: none"> • Asignación de los recursos en función de los proyectos del plan director. • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. • Formación al personal.
6.16	<ul style="list-style-type: none"> • Discontinuidad del servicio. 	<ul style="list-style-type: none"> • Disponer, al menos, de dos personas que tengan una capacitación similar.
6.17	<ul style="list-style-type: none"> • Discontinuidad del servicio. • A medio y largo plazo posible desaparición de la organización. 	<ul style="list-style-type: none"> • Obtener informes periódicos. Con base en los resultados comprobar si los ANS son realistas y adecuados. • Mantener reuniones periódicas con los departamentos afectados con objeto de corregir las desviaciones y adaptar los ANS a los cambios tecnológicos y a los requerimientos de los usuarios. • Establecimiento de ANS consensuados entre los departamentos de gestión y los de TI. • Resolución de los posibles conflictos de intereses.

BLOQUE III. Principio de CONFORMIDAD		
	Riesgos	Controles
7.1	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. Cese obligado de la actividad. 	<ul style="list-style-type: none"> Estudio de las normas de obligado cumplimiento. Establecer referencias cruzadas entre todas ellas. Actualizar las referencias cruzadas cuando cambie alguna de las normas. Identificar los procesos de negocio a los que afecta. Formar en esta materia a los responsables de los procesos de negocio afectados. Realizar auditorías de cumplimiento.
7.2	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. Cese obligado de la actividad. 	<ul style="list-style-type: none"> Estudio de las normas de obligado cumplimiento. Establecer referencias cruzadas entre todas ellas. Actualizar las referencias cruzadas cuando cambie alguna de las normas. Identificar los procesos de negocio a los que afecta. Formar en esta materia a los responsables de los procesos de negocio afectados. Realizar auditorías de cumplimiento.
7.3	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. Cese obligado de la actividad. 	<ul style="list-style-type: none"> Definición de los criterios a aplicar. Materialización de los criterios en cláusulas contractuales. Incorporación obligatoria de las cláusulas en los contratos celebrados por todos los departamentos de la organización..
7.4	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. 	<ul style="list-style-type: none"> Definición de los criterios a aplicar para proteger el material con derechos de autor. Materialización de los criterios en cláusulas contractuales. Incorporación obligatoria de las cláusulas en los contratos celebrados por todos los departamentos de la organización..
7.5	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. Cese obligado de la actividad. 	<ul style="list-style-type: none"> Definición de los criterios a aplicar. Materialización de los criterios en cláusulas contractuales. Incorporación obligatoria de las cláusulas en los contratos celebrados por todos los departamentos de la organización..

BLOQUE III. Principio de CONFORMIDAD		
	Riesgos	Controles
7.6	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. Cese obligado de la actividad. 	<ul style="list-style-type: none"> Definición de las consecuencias por incumplimiento de responsabilidades. Asignación de los recursos en función de los proyectos del plan director. Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. Elaboración, divulgación y actualización de la política de uso de los recursos de TI. Definición de las consecuencias por incumplimientos de las responsabilidades. Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. Campañas de concienciación para crear cultura corporativa.
7.7	<ul style="list-style-type: none"> Sanciones. Pérdida de credibilidad. Pérdida de clientes. Daño a la imagen. 	<ul style="list-style-type: none"> Realización de auditorías periódicas.
7.8	<ul style="list-style-type: none"> Sanciones por incumplimiento de las normas por los terceros contratados. Pérdida de control. 	<ul style="list-style-type: none"> Incorporar cláusulas que contemplen este extremo en los contratos.
7.9	<ul style="list-style-type: none"> Sanciones. Pérdida de credibilidad. Pérdida de clientes. Daño a la imagen. 	<ul style="list-style-type: none"> Realización de auditorías periódicas.
7.10	<ul style="list-style-type: none"> Se perpetúan las no conformidades detectadas. 	<ul style="list-style-type: none"> Realizar seguimiento de la aplicación de las recomendaciones de los informes de auditoría..
7.11	<ul style="list-style-type: none"> Sanciones que afecten a la situación patrimonial de la organización. Pérdida de credibilidad. Cese obligado de la actividad. 	<ul style="list-style-type: none"> Campañas de formación sobre gestión de recursos, en general y del tiempo en particular. Formación al personal. Mantenimiento actualizado de los curriculum de los empleados. Consulta de los curriculum antes de asignar nuevos roles a los empleados.

BLOQUE III. Principio de CONFORMIDAD		
	Riesgos	Controles
7.12	<ul style="list-style-type: none"> • Sanciones que afecten a la situación patrimonial de la organización. • Pérdida de credibilidad. • Cese obligado de la actividad. 	<ul style="list-style-type: none"> • Definición de la estructura organizativa. • Definición de las funciones de cada unidad organizativa • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Campañas de concienciación para crear cultura corporativa.
7.13	<ul style="list-style-type: none"> • Sanciones que afecten a la situación patrimonial de la organización. • Pérdida de credibilidad. • Cese obligado de la actividad. 	<ul style="list-style-type: none"> • Campañas de formación y concienciación en materia normativa y regulatoria.
7.14	<ul style="list-style-type: none"> • Sanciones que afecten a la situación patrimonial de la organización. • Pérdida de credibilidad. • Cese obligado de la actividad. 	<ul style="list-style-type: none"> • Configuración de los sistemas. • Auditorías de los sistemas.

BLOQUE III. Principio de CONDUCTA HUMANA		
Riesgos		Controles
8.1	<ul style="list-style-type: none"> • Pérdida del conocimiento. 	<ul style="list-style-type: none"> • Partiendo de la misión, objetivos estratégicos, estructura y de las consecuencias del incumplimiento de responsabilidades elaborar la política de contratación y conservación del personal. • Formación al personal. • Mantenimiento actualizado de los curriculum de los empleados. • Consulta de los curriculum antes de asignar nuevos roles a los empleados. • Fomentar la aplicación de la inteligencia emocional en las relaciones humanas.
8.2	<ul style="list-style-type: none"> • Personal inseguro. • Personal descontento. • Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> • Formación al personal. • Mantenimiento actualizado de los curriculum de los empleados. • Consulta de los curriculum antes de asignar nuevos roles a los empleados. • Fomentar la aplicación de la inteligencia emocional en las relaciones humanas..
8.3	<ul style="list-style-type: none"> • Discontinuidad de procesos clave del negocio. • Pérdidas económicas. • Pérdida de conocimiento. • Pérdida de credibilidad. 	<ul style="list-style-type: none"> • Identificación de los roles críticos. • Disponer, al menos, de dos personas que tengan una capacitación similar. • Revisión periódica de las relaciones de dependencia y su criticidad, con el objetivo de mantener las estrictamente necesarias.
8.4	<ul style="list-style-type: none"> • Discontinuidad de procesos clave del negocio. • Pérdidas económicas. • Pérdida de conocimiento. • Pérdida de credibilidad. 	<ul style="list-style-type: none"> • Identificación de los roles críticos. • Disponer, al menos, de dos personas que tengan una capacitación similar. • Revisión periódica de las relaciones de dependencia y su criticidad, con el objetivo de mantener las estrictamente necesarias.
8.5	<ul style="list-style-type: none"> • Discontinuidad de procesos clave del negocio. • Pérdidas económicas. • Pérdida de conocimiento. • Pérdida de credibilidad. 	<ul style="list-style-type: none"> • Formación al personal. • Mantenimiento actualizado de los curriculum de los empleados. • Consulta de los curriculum antes de asignar nuevos roles a los empleados. • Fomentar la aplicación de la inteligencia emocional en las relaciones humanas.
8.6	<ul style="list-style-type: none"> • Discontinuidad de procesos clave del negocio. • Pérdidas económicas. • Pérdida de conocimiento. • Pérdida de credibilidad. 	<ul style="list-style-type: none"> • Elaboración de cláusulas a incorporar en los contratos. • Comunicación directa de RRHH al personal que gestiona identidades o definir un perfil para RRHH en la aplicación de gestión de identidades para que recojan la baja al mismo tiempo que el personal recoge el papel de finalización de la relación laboral.

BLOQUE III. Principio de CONDUCTA HUMANA		
	Riesgos	Controles
8.7	<ul style="list-style-type: none"> • Incumplimiento de los objetivos de negocio. • Satisfacción parcial de las necesidades o requerimientos definidos por los usuarios. 	<ul style="list-style-type: none"> • Definición de las funciones de cada unidad organizativa • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Campañas de concienciación para crear cultura corporativa. • Asignación de los recursos en función de los proyectos del plan director. • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no se definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio. • Implantación de una metodología adecuada a los proyectos que se realizan. • Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.
8.8	<ul style="list-style-type: none"> • Discontinuidad de procesos clave del negocio. • Pérdida de conocimiento. 	<ul style="list-style-type: none"> • Implantación, aplicación de una metodología adecuada a los proyectos que se realizan, pues en una metodología la transferencia de conocimientos es una de las tareas que se contempla.

BLOQUE III. Principio de CONDUCTA HUMANA		
	Riesgos	Controles
8.9	<ul style="list-style-type: none"> • Desmotivación del personal. • Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> • Definición de las funciones de cada unidad organizativa • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Campañas de concienciación para crear cultura corporativa. • Asignación de los recursos en función de los proyectos del plan director. • Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no se definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio. • Implantación de una metodología adecuada a los proyectos que se realizan. • Revisar la metodología con objeto de llegar al nivel óptimo de madurez para que pueda convertirse en un estándar de obligado cumplimiento por todos los departamentos de la organización.
8.10	<ul style="list-style-type: none"> • Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> • Campañas de formación y concienciación.
8.11	<ul style="list-style-type: none"> • Rechazo del cambio. 	<ul style="list-style-type: none"> • Definición de la estructura organizativa. • Definición de las funciones de cada unidad organizativa • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Campañas de concienciación para crear cultura corporativa. • Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. • Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio.

BLOQUE III. Principio de CONDUCTA HUMANA		
	Riesgos	Controles
8.12	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> Definición de las funciones de cada unidad organizativa Transmitir a los departamentos de gestión que si no definen adecuadamente sus requerimientos la inversión en tecnología y el esfuerzo de los departamentos tecnológicos no sirven de nada. Como consecuencia no se alcanzan los objetivos de negocio. Los departamentos tecnológicos tengan el mismo peso que los departamentos de gestión en el Comité. Los departamentos tecnológicos conozcan las estrategias y los objetivos de negocio a medio y largo plazo.
8.13	<ul style="list-style-type: none"> Discontinuidad de procesos clave del negocio. Pérdidas económicas. Pérdida de conocimiento. Pérdida de credibilidad. 	<ul style="list-style-type: none"> Revisión anual de los recursos disponibles en cada departamento o en el proveedor en el que están externalizados los servicios, con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros Los departamentos tecnológicos o los proveedores en los que están externalizados los servicios conozcan las estrategias y los objetivos de negocio a medio y largo plazo. Elaboración de informes periódicos con el aporte de valor y riesgo asociado, utilizando un lenguaje cercano al negocio.
8.14	<ul style="list-style-type: none"> Falta de personal. Distribución inadecuada de personal. Personal sin la formación adecuada. Dependencia de otras empresas. Pérdida del conocimiento. 	<ul style="list-style-type: none"> Asignación de los recursos en función de los proyectos del plan director. Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros. Formación al personal. Mantenimiento actualizado de los curriculum de los empleados. Consulta de los curriculum antes de asignar nuevos roles a los empleados. Fomentar la aplicación de la inteligencia emocional en las relaciones humanas. Cualificación y habilidades multidisciplinares.
8.15	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> Definición de planes directores plurianuales. Asignación de los recursos en función de los proyectos del plan director. Revisión anual de los recursos disponibles en cada departamento con objeto de evitar la existencia de recursos ociosos en unos departamentos y carencias en otros.

BLOQUE III. Principio de CONDUCTA HUMANA		
	Riesgos	Controles
8.16	<ul style="list-style-type: none"> Incumplimiento de los objetivos de negocio. 	<ul style="list-style-type: none"> Definición de la estructura organizativa. Definición de las funciones de cada unidad organizativa Recordatorios periódicos de la misión, responsabilidad de cada puesto de trabajo. Campañas de concienciación para crear cultura corporativa. Realización de auditorías periódicas. Establecer segregación de funciones y dependencias en la definición de la estructura organizativa. Formación al personal. Mantenimiento actualizado de los curriculum de los empleados. Consulta de los curriculum antes de asignar nuevos roles a los empleados. Fomentar la aplicación de la inteligencia emocional en las relaciones humanas.. Formación al personal. Disponer, al menos, de dos personas que tengan una capacitación similar.