POLÍTICA DE CALIDAD Y MEDIO AMBIENTE

En **TECNITIA** tenemos la filosofía de lograr la confianza de nuestros clientes, satisfaciendo las necesidades informáticas para la mejora y el desarrollo de los negocios de todos nuestros clientes

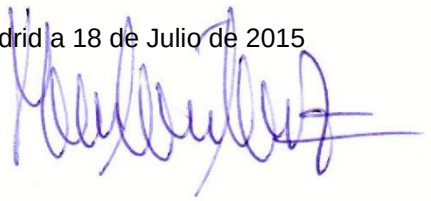
Nuestra filosofía de trabajo está orientada hacia la calidad total y en consecuencia a la satisfacción del cliente, y es por ello que en **TECNITIA** hemos decidido dar un paso más e implantar un Sistema de Gestión de Calidad basado en la norma **UNE-EN ISO 9001:2015** e **ISO 14001:2015**.

Para asegurar la calidad, tanto frente a terceros como internamente, la dirección junto a los responsables y empleados altamente cualificados con los que cuenta **TECNITIA** ha planificado un conjunto de acciones y sistemas que deben proporcionar la confianza adecuada frente a nuestros clientes y que se definen a continuación en nuestra Política de Calidad y Medio Ambiente.

- Conocer y satisfacer las necesidades y expectativas de nuestros clientes, garantizando un compromiso de cumplir los requisitos establecidos por los clientes y prevención de la contaminación.
- Cumplir con la legislación vigente que sea aplicable a las actividades y servicios desarrollados, los requisitos propios que nuestra organización suscriba, así como del cumplimiento de otras exigencias establecidas por terceras partes.
- Potenciar la eficacia de los recursos humanos y tecnológicos para asegurar la calidad de los trabajos y proyectos. Contamos con un equipo humano altamente experimentado en la dirección y ejecución de los proyectos, así como con todos los medios técnicos necesarios.
- Involucrar a nuestro personal, con sus aportaciones en la consecución de la Mejora Continua, y a través del perfeccionamiento de la capacitación profesional de nuestro personal mediante programa de formación continua ofrecido.
- Mejorar continuamente la eficacia del sistema de gestión, para garantizar nuestra permanente adecuación a las exigencias de un mercado cada vez más competitivo y un entorno en constante evolución.
- Compromiso de protección del medio ambiente y prevención de la contaminación.

Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y mantenida al día en todos los niveles de la organización.

Madrid a 18 de Julio de 2015



Fdo. Felipe Aceitón Muñoz

En representación de TECNITIA

POLÍTICA DE GESTIÓN DE SERVICIOS

El objeto de esta política es alcanzar una gestión de servicios adecuada en **TECNITIA**, mediante un Sistema de Gestión de Servicios basado en la norma **ISO/IES 20000:2011** y en nuestro **Catálogo de Servicios**:

Para ello, la Dirección de **TECNITIA** emplea los medios y recursos técnicos, productivos, financieros y humanos, en una única estructura y dirección competitiva de toma de decisiones acorde con los siguientes compromisos:

- Cumplir con los requisitos legales, o de otro tipo que la organización suscriba, que sean aplicables en base a nuestra actividad.
- Establecer la **mejora continua** como principio fundamental de actuación en nuestros procesos y en nuestras relaciones con las partes interesadas.
- Alcanzar y mejorar la **satisfacción del cliente**. Nuestra orientación está claramente dirigida a las necesidades de nuestros Clientes, aportando eficiencia, eficacia y productividad con nuestro trabajo, solventando sus necesidades tecnológicas y proporcionando una flexibilidad y escalabilidad en nuestras soluciones, todo ello teniendo la innovación como prioridad.
- Garantizar en todo momento el cumplimiento de los acuerdos de nivel de servicio fijados a través de una eficaz **gestión de los servicios.** Dicha gestión de servicios es un pilar estratégico fundamental de la empresa.
- Asegurar la **seguridad de la información** propia y de nuestros clientes.
- Desarrollar y mantener un **programa de formación, concienciación y capacitación tecnológica** para todos los empleados.
- Establecer **colaboraciones estratégicas** con nuestros proveedores para crear interacciones mercantiles de mejora de los servicios prestados, que creen valor añadido para ambas partes.
- Situar la empresa a la vanguardia de las **mejores prácticas de responsabilidad social corporativa** y adoptar un conjunto de **compromisos éticos, sociales y tecnológicos**. Estamos convencidos de que, además de resultar básico para cumplir el interés social de la empresa, es parte fundamental de su estrategia de excelencia y de mejora de su competitividad.

Madrid a 25 de Enero de 2017

Fdo. Felipe Aceitón Muñoz

En representación de TECNITIA

La dirección de **TECNITIA**, consciente de la necesidad de promover, mantener y mejorar el enfoque hacia el cliente en todas sus actividades, ha implantado un Sistema de Gestión Integrado (SGI) conforme al estándar cuyo **objetivo** final es asegurar que entendemos y compartimos las necesidades y metas de nuestros clientes, intentando prestar servicios que cumplan sus expectativas trabajando en la mejora continua. Manifiesta expresamente su compromiso de potenciar la **Seguridad y Ciberseguridad** de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, a mantener alta nuestra competitividad en los servicios y productos de **Servicio de Mantenimiento, Soporte, Operación y Administración de infraestructura y aplicaciones informáticas. Proyectos de transformación digital de infraestructuras y aplicaciones informáticas. Servicios de Cloud Privada, Hibrida y Publica, Housing y Hosting. Servicio de Diseño, Arquitectura y Desarrollo de soluciones software**.

MISIÓN y OBJETIVOS:

- Fomentar la mejora continua de los servicios y soporte al cliente.
- Continuar el posicionamiento de **TECNITIA** como referente en el sector.
- Proporcionar soluciones de software para transformar los datos y la información para ayudar en la toma de decisiones de nuestros clientes.
- Proporcionar a los clientes el equipo más profesional y disponer de forma inmediata y durante el tiempo necesario de técnicos altamente cualificados, expertos en las disciplinas requeridas y acostumbrados a trabajar en equipo.
- Tener una prestación del servicio basada en nuestro compromiso con la mejora continua de nuestros sistemas, con la seguridad y ciberseguridad de la información como pilar central y por defecto.

Nuestra misión y los objetivos los conseguiremos a través de:

- Un sistema de objetivos, métricas e indicadores de mejora continua, seguimiento, medición de nuestros procesos internos, así como de la satisfacción de nuestros clientes. Estableciendo y supervisando el cumplimiento de los requisitos contractuales para asegurar un servicio eficaz y seguro.
- Formando y concienciando continuamente a nuestro equipo para tener el mayor grado de profesionalidad y especialización posible, además teniendo nuestras infraestructuras en un estado adecuado y en concordancia con los requerimientos de nuestros clientes.
- Con un procedimiento seguro de gestión de adquisición de productos.
- Cumpliendo las exigencias de la legislación vigente, especialmente con el GDPR y el cumplimiento de nuestra Documentación de Seguridad.
- Introduciendo los procesos de mejora continua que permitan un avance permanente en nuestra gestión de Seguridad de la Información.
- Gestionando y elaborando planes para la gestión y tratamiento de los riesgos con una metodología de análisis y gestión de riesgos utilizada, basada en estándares.
- Gestionando las comunicaciones internas y externas e información almacenada y en tránsito.
- Asegurando la interconexión con otros sistemas de información.
- Gestionando y monitorizando la actividad con la gestión de logs.
- Con especial atención a la gestión de incidentes de seguridad.
- Asegurando la continuidad y disponibilidad del negocio y de los servicios.
- Asegurar que nuestros Activos y Servicios cumplen con las medidas del ENS de Nivel ALTO para las dimensiones de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.

Además, estos principios se deberán contemplar en las siguientes **áreas de seguridad**:

- **Física**: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información, así como los accesos físicos.

- **Lógica**: Incluyendo los aspectos de protección de aplicaciones, redes, comunicación electrónica, sistemas informáticos y con los accesos lógicos.
- **Político-corporativa**: Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal.

El objetivo último de la seguridad de la información es asegurar que una organización pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Roles o funciones de seguridad:

Responsable de la Información: determinará los requisitos de la información tratada.

- Implantar y mantener el Sistema de Gestión Integrado (SGI) mejorando continuamente su eficacia.
- Implantar y mantener el ENS mejorando continuamente su eficacia.
- Supervisar los procedimientos y las instrucciones técnicas.
- Aplicar las medidas y seguimientos indicados por el DPO.
- Realizar el seguimiento y verificar la implantación y eficacia de todas las acciones correctoras y preventivas establecidas.
- Asegurar que el sistema implantado cumple con la norma establecida.
- Analizar los datos obtenidos en el Sistema de Gestión Integrado (SGI) y ENS y proponer mejoras.
- Elaborar el plan anual de auditorías internas.
- Participar en la toma de decisiones en la revisión por la dirección.
- Gestión de No Conformidades de seguridad.
- Participar en Auditoria Externas.
- Responsable de los datos privados de la empresa en cuanto a su pérdida, el robo y la desactualización.
- Cumplir con el manual de buenas prácticas de seguridad de la información.
- Imparte los programas de formación para que el personal sepa cómo actuar en el supuesto de que se produzca contingencias.
- Mantener actualizados los medios de contacto con las autoridades.
- Lleva el inventario de soportes que contienen datos de carácter personal.
- Analiza los informes de auditoría y elevan las conclusiones al responsable de los datos.
- Convoca las reuniones del CSI.
- Genera las actas de reunión del CSI.
- Gestiona las no conformidades, acciones correctivas y acciones preventivas de SI.
- Mantiene los documentos del SGI.
- Mantiene y despliega la política de seguridad de **TECNITIA** así como el resto de las políticas al personal implicado en cada una de ellas.
- Responsable de la gestión de la auditoría de seguridad de protección de datos y RGPD.
- Supervisa las tareas de LOPD del DPO.
- Confecciona los documentos de seguridad de **TECNITIA**.
- Elabora los acuerdos para el tratamiento de datos por terceros.
- Atiende incidencias en materia de protección de datos.
- Se encarga de contactar con las autoridades en caso necesario.
- Aplicación y supervisión del cumplimiento de las políticas del SGI.
- Mantenimiento y aplicación del Documento de Aplicabilidad del SGI

Responsable de sistemas: Determina los requisitos de los servicios prestados.

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del RSI.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

Responsable de Seguridad de la Información: Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

- Responsable de la ciberseguridad.
- Supervisar el Manual de Seguridad, los procedimientos y las instrucciones técnicas.
- Responsabilidad general de administrar la implementación de las prácticas de seguridad.
- Asegurar que el sistema implantado cumple con la norma establecida.
- Analizar los datos obtenidos en el Sistema de Gestión de Seguridad de la Información y ENS y proponer mejoras.
- Participar en la toma de decisiones en la revisión por la dirección.
- Participar en Auditoria Externas.
- Responsable del riesgo de la intrusión física de los dispositivos de la empresa.
- Cumplir con el manual de buenas prácticas de seguridad de la información.
- Segregación de tareas y entornos.
- Comunicar cualquier emergencia de incendio, inundación o avería de los equipos de climatización que pueda activar el PCN.
- Revisa el Plan de Continuidad del negocio.
- Verifica el funcionamiento del Plan de Continuidad de Negocio.
- Controla el acceso de personas a los locales donde están instalados los sistemas.
- Supervisa las incidencias de seguridad producidas.
- Realiza y custodia las copias de seguridad.
- Genera los planes de tratamiento de gestión de riesgo y supervisa su implantación.

- Actualiza el análisis de riesgos.
- Supervisa la recogida de métricas.
- Realiza las revisiones de seguridad del SGI.
- Mantiene el Plan de Continuidad de Negocio.
- Incorpora en el registro de incidencias las medidas correctoras.
- Aplicación y supervisión del cumplimiento de las políticas de SGI.

Responsable del Servicio: Determina los niveles de seguridad de los servicios.

- Garantizar el cumplimiento de los objetivos y métricas establecidos para el servicio (SLAs).
- Organización diaria de los recursos.
- Responsable de la pérdida y robo de información de los servicios y soluciones informáticas para clientes y usuarios en general.
- Cumplir con el manual de buenas prácticas.
- Determina los requisitos de los servicios prestados.
- Programar, dirigir, coordinar, supervisar y controlar todas las actividades del servicio.
- Revisión y cumplimiento de los informes de los servicios.

El Comité de Seguridad de la Información (CSI) de **TECNITIA** alcanza a toda la empresa, es el mecanismo de coordinación y resolución de conflictos, entre otras funciones:

- Designación y/o renovación de los cargos de seguridad, así como sus funciones y responsabilidades.
- Crear, planificar, implementar e integrar la dirección estratégica de la organización y alinearla con el SGSI.
- Conocimiento del mercado TIC y nuevas tecnologías y su aplicación en la compañía.
- Dirección y supervisión de los distintos proyectos de seguridad de la compañía.
- Participar y promover el cumplimiento de la política de seguridad de la información de la organización.
- Velar por el cumplimiento de disposiciones legales y normas de las administraciones públicas y de régimen interno relativas a seguridad de la información.
- Aprobación del SGSI, así como sus cambios y nuevas versiones.

Componen el CSI:

- Responsable del Servicio.
- Responsable de Sistemas.
- Responsable de Seguridad de la información.

Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y tenida al día en todos los niveles de la organización.

Madrid a 28 de Marzo de 2022

Fdo. Felipe Aceitón Muñoz

En representación de TECNITIA