Manual
Formación Básica ISO

2017

1. LOS SISTEMAS DE GESTIÓN SEGÚN NORMAS ISO

Los Sistemas de Gestión tienen el fin de mejorar el funcionamiento de la empresa en diferentes ámbitos y hacen que clientes, proveedores, trabajadores, becarios... estén satisfechos con del desarrollo del trabajo.

TCP-UST Global cuenta con los siguientes Sistemas de Gestión implantados y certificados:

- Calidad y según norma ISO 9001
- Medio Ambiente según norma ISO 14001
- Seguridad de la Información, según norma ISO 27001
- Servicio, según norma ISO 20000-1

Todos los Sistemas de Gestión están implantados en base a normas ISO se basan en el Ciclo de Deming:

- **Plan:** Se planifica la implantación y provisión de la gestión del servicio.
- **Do:** Se implantan los objetivos y el plan de gestión.
- **Check:** Se monitoriza, mide y revisan los objetivos y el plan de gestión.
- **Act:** Mejorar la eficacia y la eficiencia de la entrega, prestación y gestión del servicio.

2. PARTES COMUNES A TODOS LOS SISTEMAS DE GESTIÓN DE TCP-UST Global

Documentación de los Sistemas de Gestión

- **Política:** Intenciones globales y orientación de la organización tal y como se expresa formalmente por la Dirección.
- **Manual:** Se describe cada uno de los Sistemas de Gestión de la empresa. Se incluyen la estructura organizativa de la empresa y las responsabilidades de las partes funcionales y debe hacer referencia a los procedimientos y otra documentación relevante del sistema.

- **Procedimientos:** Documento donde se describe detalladamente la forma de llevar a cabo una actividad o un proceso. Todos los procedimientos del Sistema son codificados al inicio con *PE/XX Nombre del Procedimiento*.

- **Registros:** Documentos que presentan resultados obtenidos y/o proporcionan evidencias de actividades desempeñadas. En este tipo de documento se recogen los datos críticos derivados de la ejecución de procesos, actividades y operaciones.

No Conformidades, Acciones Correctivas y Preventivas

Las No Conformidades son una herramienta útil para la detección de fallos actuales o futuros y la mejora de cualquiera de los Sistemas de Gestión de la empresa. Su objetivo no es responsabilizar a usuarios particulares sino resolver situaciones que pueden causar conflictos o quejas. Cualquier trabajador puede comunicar una No Conformidad a través del correo electrónico: calidad@tcpsi.es

Auditorías

Es el proceso sistemático, independiente y documentado mediante el cual se recogen las evidencias necesarias para determinar y evaluar si se está procediendo según se documentaron los Sistemas de Gestión. Este proceso verifica si se están cumpliendo las normas implantadas. Las auditorias pueden ser internas o externas, siendo esta última realizada por un Organismo Independiente que emite las certificaciones de los Sistemas de Gestión implantados.

3. SISTEMA DE GESTIÓN DE CALIDAD Y MEDIO AMBIENTE (ISO 9001 Y 14001)

La calidad es la manera de proporcionar a los clientes productos y/o servicios que cumplan, de forma constante, sus necesidades y expectativas logrando su satisfacción y la mejora de los procesos de la organización, sin olvidar que se ha de ser lo más sostenible ambientalmente posible.

Los principios básicos de Calidad son los siguientes:

- Organización enfocada al cliente
- Liderazgo y participación del personal
- Enfoque basado en procesos y gestión basada en sistemas
- Mejora continua y toma de decisiones basada en hechos
- Relación mutuamente beneficiosa con el proveedor

Buenas Prácticas Ambientales

Han de conocerse y ser aplicadas correctamente por todos los trabajadores de la organización. Se centran en los siguientes aspectos:

Ahorro en consumos de agua, luz, papel y tóner
Gestión correcta de residuos

Puedes consultar el documento completo en el Sistema de Gestión Documental (*Links en apartado 6*), pero de todas formas a continuación recordamos las prácticas ambientales más importantes en el día a día en las oficinas:

Consumo de papel: Trata de realizar sólo las fotocopias/impresiones necesarias y tiende a hacerlas prioritariamente por ambas caras.

Residuos: Aplica la teoría de las '3Rs': Reducir, Reutilizar y Reciclar.
Minimiza el uso de las papeleras y recicla correctamente cada residuo en su contenedor:

- Contenedor azul: Sólo papel usado, no lo mezcles con otros residuos.
- Contenedor amarillo: bolsas, vasos, latas/bricks, y demás envoltorios plásticos.

→ **No olvides separar el tapón de plástico y echarlo al contenedor solidario.**

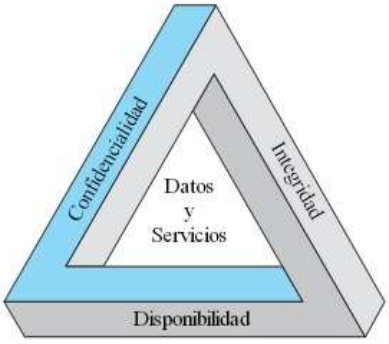
Consumos de luz y agua:

- En tu puesto de trabajo, configura el ahorro de energía en el ordenador y apágalo al terminar tu jornada laboral.

- Ajusta los termostatos en temperaturas de Confort (22º) y recuerda apagar aire acondicionado/calefacción si eres el último en salir de las oficinas.
- En el baño, cierra el grifo mientras te enjabonas o cepillas los dientes, usa el botón pequeño de la cisterna siempre que sea posible y apaga las luces al salir.

4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001)

Su objetivo es asegurar de cara al mercado, a nuestros clientes y a nuestros empleados, que hacemos una adecuada gestión de la seguridad de nuestros sistemas de información. Aunque es imposible garantizar la seguridad absoluta de un sistema informático, el objetivo es minimizar los riesgos existentes. La información es el activo más importante de la empresa, es lo que nos diferencia de la competencia y nos da nuestra identidad. La seguridad es un proceso continuo que debe garantizar estos tres pilares básicos:



- **Confidencialidad:** La información es accesible sólo por personas autorizadas.

- **Integridad:** La información es completa y exacta.

- **Disponibilidad:** La información es accesible en el momento en que se necesita.

Siempre teniendo en cuenta el cumplimiento de leyes, normas y reglamentos a las que está sujeta la empresa.

Todos los empleados son responsables durante su trabajo diario de mantener los niveles adecuados de seguridad en su puesto de trabajo. Como guía para ello se tiene el documento de **Buenas Prácticas en Seguridad de la Información**.

Buenas Prácticas en Seguridad de la Información

Han de conocerse y ser aplicadas correctamente por todos los trabajadores de la organización:

Contraseñas Seguras: Cada usuario es responsable de la confidencialidad de su contraseña y es conveniente tener en cuenta los siguientes aspectos:

- Más de 8 caracteres, con mayúsculas y minúsculas, números y, si es posible, símbolos especiales.
- Que sea fácil de recordar para y SÓLO por el usuario.
- No se han de revelar NUNCA las contraseñas a nadie, ni siquiera al administrador.
- No revelar contraseñas por teléfono, e-mail, etc.
- No apuntar sus contraseñas en papel o en documentos de texto sin proteger.
- Utilizar salvapantallas automático con contraseña.
- No usar la misma contraseña para todo.

Seguridad de los Datos: No dejar información valiosa expuesta a pérdida o divulgación:

- Trabajar en la unidad de red para mayor seguridad ya que es sobre la que se realizan las copias de seguridad. La información que no se encuentra allí (unidad C, escritorio…) no se podrá replicar.
- Cada usuario es responsable de la información que se encuentra en su equipo.
- Los datos ya utilizados han de borrarse, tanto en equipos como en otros soportes (CD, papel…)

Navegación por Internet:

- Se ha de tener cuidado de revisar la configuración de su ordenador antes de conectar a Internet. Es imprescindible que sea consciente de las carpetas/recursos que comparte.
- Apagar el ordenador cuando no esté en su puesto de trabajo.
- Respetar las licencias de software.
- Configurar el navegador para que pregunte si se permite el “contenido activo”.
- Ser selectivo respecto a qué sitios web se permite el acceso desde cada ordenador y ser crítico sobre los programas que se descargan de la web y con los programas P2P.
- Antes de descargar un software que se necesite utilizar, hay que asegurarse que el sitio de origen es fiable y no va a contener software malicioso.

Correo electrónico:

Si alguna de las siguientes situaciones se cumple, se ha de borrar el e-mail:

- El remitente es desconocido o es conocido, pero no habitual, y resulta raro (viene en idioma diferente, usa caracteres extraños…).
- El campo “asunto” no tiene sentido.
- El correo contiene enlace y no se está seguro de a dónde le direccionará en Internet.
- El e-mail como tal es sospechoso.

Seguridad Física:

- Hay que acceder y salir del edificio SIEMPRE por el torno de la planta baja y usando la tarjeta de acceso personalizada. En caso de olvido de la misma, el conserje del edificio le entregará una provisional para esa jornada.
- El acceso físico a las oficinas de personas no pertenecientes a la empresa o colaboradores no habituales se hará siempre acompañado desde su entrada hasta su salida por alguien de la organización. No facilitar la entrada a personas no identificadas.
- Si se viaja a menudo con portátil, la mejor opción es usar herramientas de encriptación.
- Se ha de guardar la documentación en papel con información relevante en lugar seguro (bajo llave), no dejándola en mesas o estanterías de forma descontrolada.
- Retirar inmediatamente sus documentos de las impresoras o faxes, cuando los utilice.
- Hacer uso de las destructoras cuando haya que deshacerse de papel con información sensible.

Estas pautas se complementan con las que pueden encontrarse en el Sistema de Gestión Documental (*Links en apartado 6 del documento*).

5. SISTEMA DE GESTIÓN DE SERVICIO (ISO 20000-1)

La ISO 20000-1 es la manera óptima de gestionar servicios TI a través de un código de buenas prácticas con reconocimiento Internacional (ITIL) y un Sistema de Gestión certificable. Actualmente se contemplan 13 procesos, los cuales están estructurados en 4 grupos: Procesos de Provisión del Servicio, Procesos de Control, Procesos de Resolución y Procesos de Relaciones.

Procesos de Provisión del Servicio

Este grupo de procesos es uno de los más importantes ya que nos ofrece herramientas para gestionar de manera adecuada todo lo relacionado con la prestación del servicio. Los procesos de este grupo son:

- **Gestión de la Capacidad:** La compañía necesita los recursos necesarios para proporcionar el servicio: Personas, equipos, comunicaciones, etc. pero también tiene que estar preparada para una posible sobrecarga de trabajo o para un incremento de las prestaciones del servicio que se le ofrece al cliente.

- **Gestión de la Continuidad y Disponibilidad del Servicio:** Es necesario identificar posibles escenarios de desastre, y por cada escenario se tienen que establecer estrategias de contingencia, con el objetivo de hacer frente a posibles problemas de continuidad. Además, para controlar que cumplimos con las condiciones establecidas en los acuerdos con nuestros clientes calcularemos y revisaremos la disponibilidad del servicio.

- **Gestión del Nivel de Servicio:** Es necesario definir acuerdos para establecer claramente qué tipo de servicio se ofrece y bajo qué condiciones. Es muy importante establecer reuniones periódicas con cada parte afectada para comprobar el correcto cumplimiento con todos los acuerdos.

- **Informe de Servicio:** Es necesario definir informes periódicos en los que se proporcionará información detallada acerca del estado del servicio. Es importante realizar y cumplir un plan de entregas al cliente para que tenga información detallada acerca del servicio averías, actualizaciones, cambios en operaciones, mantenimiento, mejoras, caídas del servicio, etc.).

- **Gestión de la Seguridad:** Es necesario establecer medidas de seguridad para proteger la información contra amenazas. Este punto es coincidente con el alcance de la Norma ISO 27001.

- **Presupuesto y Contabilidad:** El dinero es fundamental en la gestión de un servicio, por lo que es necesario controlar costes y beneficios, ya que necesitamos saber si el servicio es rentable o si es necesario realizar una nueva inversión. Han de conocerse los costes de los recursos, activos y equipamiento, tanto actual como futuro.

Con todos estos procesos podremos:

- Gestionar posibles sobrecargas de trabajo.
- Mantener el servicio operativo o a unos niveles aceptables.
- Establecer contractualmente las condiciones del servicio, para que de esta manera quede claro qué se le ofrece al cliente y bajo qué condiciones.
- Informar periódicamente al cliente sobre el estado del servicio.
- Establecer medidas de seguridad para proteger la información.
- Controlar gastos y la rentabilidad del servicio.

Puede ampliarse información sobre estos procesos o los del resto de grupos (Control, Resolución y Relación) en el Sistema de Gestión Documental (*Links en el apartado 6*).

6. REPOSITORIO DE DOCUMENTACIÓN Y CONCLUSIONES

Toda la documentación referente a las Normas ISO (Manual, Política, Buenas Prácticas, Formación y otros documentos relevantes) se puede consultar en cualquier momento en el **Sitio: Quality & Processes Department** de:

- **GDOC**, si estás en las oficinas de Madrid:
  http://gdoc/share/page/site/ope-procesos/dashboard

- **GDEX**, si estás fuera (cliente, otras oficinas…):
  http://gdex.tcpsi.com:8082/share/page/site/quality-processes-department/dashboard

Existe más información y documentación de los sistemas de gestión que está accesible bajo petición justificada. Para ello, o si se tiene alguna consulta o sugerencia sobre cuestiones relativas a las normas o sobre la documentación, te facilitamos el siguiente correo electrónico para que contacten con vosotros:

Quality & Processes Department

calidad@tcpsi.es

Es de vital importancia que todo el personal sea consciente de la implantación de las normas ISO en la organización y colabore cumpliendo las políticas y buenas prácticas asociadas.

¡Muchas gracias por el tiempo dedicado!