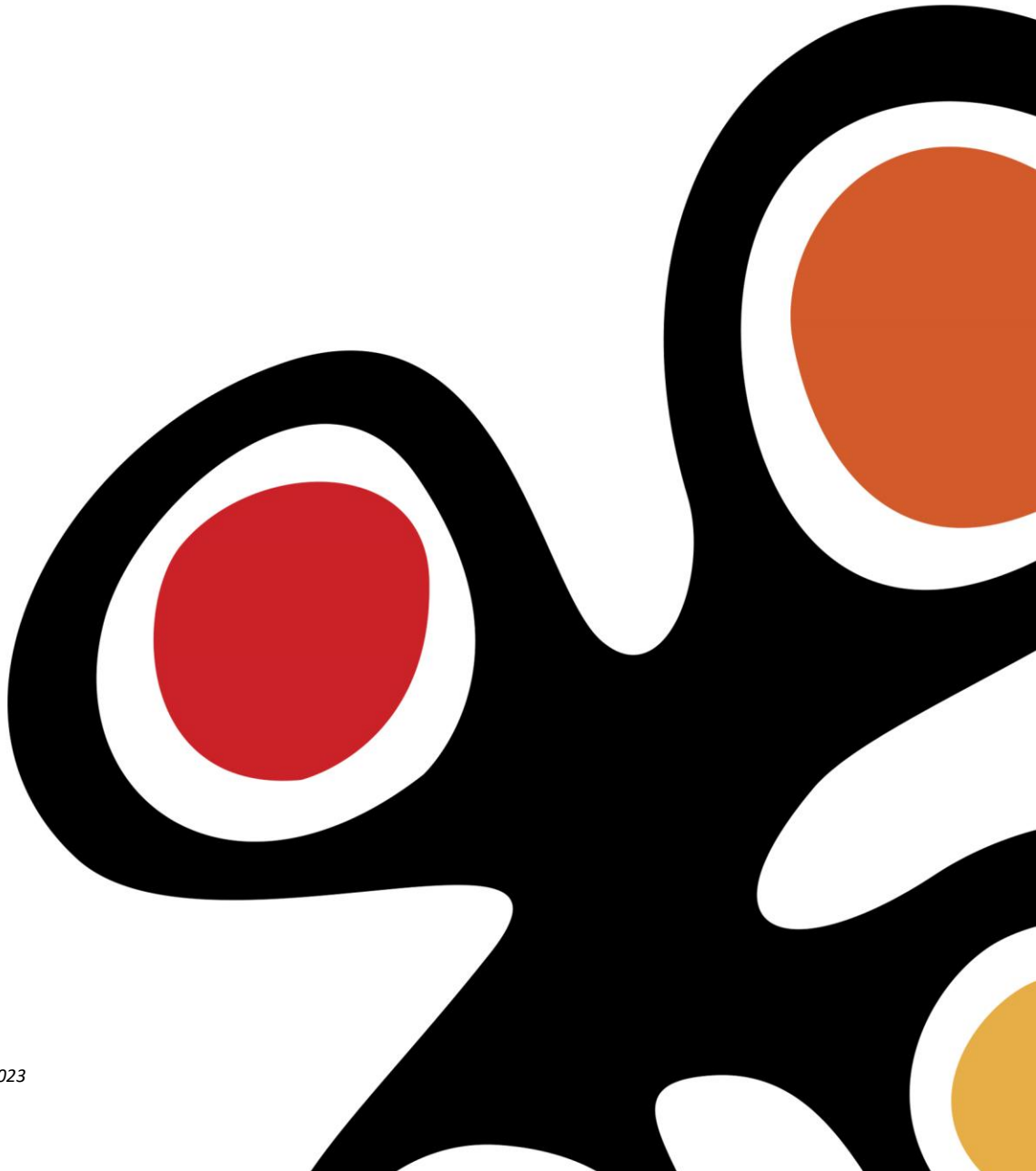
Política de Calidad



Fecha de Última Modificación: 19/01/2023

Nota sobre confidencialidad

Contenido

1 Introducción

La Calidad es un factor estratégico para la competitividad y la satisfacción de nuestros clientes y por lo tanto, desde el Departamento de Calidad trabajamos diariamente para conseguir la mejora continua de los servicios que ofrecemos. En Solutio somos conscientes de que la calidad abarca y es aplicable a todos nuestros procesos. Es por ello, que nuestro sistema tiene un enfoque global, integrado, comprometido con la Seguridad de la Información, la Calidad, el Medioambiente y la Gestión de Servicios tal y como recoge nuestras Políticas del Sistema de Gestión Integrado (*QMS – Quality Management System*).

2 Políticas de Calidad

2.1 Política de Calidad y Medioambiente

Esta Política se establece como marco en el que se debe llevar a cabo dicha actividad de Calidad y Medioambiente, de manera que se garantice a los clientes y demás partes interesadas el compromiso adquirido por la entidad a través de su SGI, por lo que su alcance son todas las actividades relacionadas con las líneas de negocio de gestión.

Los principios que rigen las actuaciones que la entidad sigue en materia de Calidad y Medioambiente son los siguientes:

- La constante preocupación por la satisfacción del Cliente.
- La consecución de los Objetivos de Calidad y Medio Ambiente, con el compromiso de la mejora permanente del Sistema Integrado de Gestión, involucrando a todo el personal de la empresa.
- La adecuación de los Recursos Humanos a estos Objetivos, mediante la formación que resulte necesaria para la consecución de los objetivos previstos en materia de calidad y medio ambiente.
- La mejora continua:
    - De los productos y servicios ofrecidos procurando alcanzar la máxima satisfacción del cliente, dentro del marco legal establecido y vigente en cada momento.
    - De la gestión y del comportamiento medioambiental, mediante la prevención y el análisis de las causas últimas de problemas surgidos, no limitándose sólo a la detección de estos.
    - De la satisfacción del cliente, mediante las actuaciones necesarias para fomentar la comunicación de todas aquellas necesidades o sugerencias de mejora que permitan prestar un servicio de mayor calidad.

- El compromiso de la protección del medio ambiente, implantando las medidas necesarias para prevenir la posible contaminación de suelos, atmósfera o aguas, en el proceso de toma de decisiones, en la planificación y en la ejecución de las actividades, de manera que sean ejecutadas de una manera respetuosa con el entorno que nos rodea.

- El cumplimiento de la legislación vigente aplicable en los ámbitos nacional, autonómico y local y, en el caso concreto de la reglamentación medioambiental, con especial hincapié en los aspectos relativos a la atmósfera, agua y residuos, de manera que se garantice que la actividad empresarial se lleva a cabo de acuerdo con esas exigencias, estableciendo así un compromiso con todas las partes interesadas.

- El compromiso de cumplimiento de otros requisitos que la organización suscriba en relación con sus aspectos ambientales.

- El análisis y la valoración de las actuaciones realizadas hasta el momento, evidenciándolas mediante registros cuyas conclusiones ayuden al fomento de la mejora continua del sistema de gestión.

- El comportamiento ético profesional en todos los niveles de la organización, en el desarrollo de productos y en la gestión con clientes y proveedores.

- La difusión de la Política de Calidad y Medio Ambiental todas las personas que conforman el equipo humano de la organización en todos los niveles, así como la comprensión de esta.

Sobre la base de esta Política y anualmente, la Dirección aprobará los objetivos y metas para la organización, de manera que se establezcan las líneas de mejora de la organización para ese período. Dichos objetivos serán revisados anualmente.

2.2 Política del Sistema de Gestión Seguridad de la Información

El propósito de esta Política de la Seguridad de la información es preservar los activos de información de SOLUTIO, de manera que esté protegida contra pérdidas de disponibilidad, confidencialidad, trazabilidad, autenticidad e integridad.

Es por ello que ha desarrollado e implantado un Sistema de Gestión de Seguridad de la Información, en conformidad con los requisitos de la norma UNE-ISO/IEC 27001 y con los requisitos del Esquema Nacional de Seguridad como soporte organizativo y metodológico, para emprender el camino de la mejora continua a través de los siguientes principios:

- La información está protegida contra pérdidas de disponibilidad, confidencialidad, trazabilidad, autenticidad e integridad.

- La información está protegida contra accesos no autorizados.

- Se cumplen los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.

- Se desplegarán los recursos necesarios para alcanzar los objetivos y las metas.

- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- Su cumplen los requisitos legales aplicables.
- El responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- Los responsables de cada área de negocio serán los encargados de implementar esta Política y sus correspondientes procedimientos dentro de su área.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto de trabajo.
- Es política de SOLUTIO implementar, mantener y realizar un seguimiento del SGI.

La Dirección de SOLUTIO, se compromete a liderar este proceso y a asignar los recursos necesarios para cumplir con los requisitos establecidos en el Sistema de Gestión de Servicios de TI, satisfacer las exigencias de los clientes y conseguir los objetivos fijados.

La presente política es conocida y suscrita por todo el personal de SOLUTIO contemplado en el alcance, de acuerdo con las exigencias de la Dirección. Esta política será revisada con una periodicidad máxima anual, y sus cambios deberán ser aprobados por la Dirección General de la organización.

2.3 Política del Sistema de Gestión de Servicios de TI

SOLUTIO considera que la provisión de servicios a nuestros clientes es una parte fundamental de nuestro negocio, y por ello la Gestión de Servicios ocupa un lugar destacado dentro de sus objetivos, alineada con la estrategia definida para el desarrollo del negocio. Es por ello que ha desarrollado e implantado un Sistema de Gestión de Servicios, en conformidad con los requisitos de la norma UNE-ISO/IEC 20000-1 como soporte organizativo y metodológico, para emprender el camino de la mejora continua a través de los siguientes principios:

- Asegurar que los servicios están alineados con las necesidades de nuestros clientes y usuarios.
- El cumplimiento de los requisitos de negocio, los legales y los reglamentarios
- Disposición de personal técnicamente competente y debidamente adiestrado para llevar a cabo las tareas con las garantías de calidad exigibles.
- La participación activa de todo el personal basada en el concepto de autogestión del puesto de trabajo y en la formación continua.
- El establecimiento de las medidas necesarias para prevenir, estudiar y eliminar, siempre que ello sea posible, los factores que puedan afectar de un modo negativo a la gestión de los servicios de TI.
- El establecimiento de objetivos anuales y la asignación de los recursos, tanto técnicos como materiales y humanos, para su realización, que garantice la mejora continua de los niveles de calidad deseados.

- Mejorar la comunicación entre el personal que participa en la prestación de servicios y los clientes y usuarios de dichos servicios.
- Mejorar la eficacia y eficiencia de los procesos internos de prestación de los servicios TI

La Dirección de SOLUTIO, se compromete a liderar este proceso y a asignar los recursos necesarios para cumplir con los requisitos establecidos en el Sistema de Gestión de Servicios de TI, satisfacer las exigencias de los clientes y conseguir los objetivos fijados.

La presente política es conocida y suscrita por todo el personal de SOLUTIO contemplado en el alcance, de acuerdo con las exigencias de la Dirección. Esta política será revisada con una periodicidad máxima anual, y sus cambios deberán ser aprobados por la Dirección General de la organización.

2.4 Política de Uso Aceptable

La intención del área de Calidad con la publicación de esta Política de Uso Aceptable no es la de imponer restricciones que sean contrarias a la cultura establecida de apertura, confianza e integridad de la empresa. Grupo Solutio está comprometido a proteger a empleados, socios y a la empresa de acciones ilegales o perjudiciales que podrían ser realizadas por individuos, ya sea de manera intencional o no.

Los sistemas relacionados con Internet, Intranet, Sistemas Corporativos, incluyendo, pero no limitado al hardware (equipos portátiles, ordenadores, móviles), software, sistemas operativos, medios de almacenamiento, cuentas de correo electrónico, servicios de navegación, son propiedad de la empresa. Estos sistemas deben ser utilizados para fines meramente profesionales, en el curso de las operaciones habituales de trabajo.

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Los puestos de trabajo deberán permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
- Además, el material deberá guardarse en lugar cerrado cuando no se esté utilizando.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.

- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red o los sistemas de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

Asimismo, los usuarios deberán de tener en cuenta las siguientes medidas de seguridad, durante el tratamiento de la información y el uso de los sistemas de TI:

- Cualquier persona que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia
- Cada equipo informático de usuario/a estará bajo la responsabilidad de algún usuario/a autorizado/a que tratará de proteger, en la medida de sus posibilidades, la confidencialidad de la información de SOLUTIO y, especialmente de los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido.
- Cuando la persona responsable de un equipo informático lo abandone temporalmente deberá dejarlo en un estado que impida la visualización de los datos protegidos, por ejemplo, a través de un protector de pantalla. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente. Si el abandono del equipo se produjera debido a la finalización de su turno de trabajo, el usuario o usuaria procederá al cierre completo de la sesión del sistema
- Se deben retirar de las impresoras y demás periféricos de salida todos los documentos que contengan información del Grupo conforme se vayan imprimiendo.
- Ningún usuario o usuaria podrá utilizar dispositivos extraíbles (CD, DVD, USB, etc.) ni almacenar información en ellos, sin la previa autorización del Responsable de Seguridad.
- Los soportes que contengan información deberán estar claramente identificados con una etiqueta externa que indique (directa o indirectamente) de qué fichero se trata y qué tipo de datos contiene.
- Se deberán guardar los soportes que contengan información en lugar seguro y bajo llave, o en salas, despachos, etc., con acceso restringido, cuando no sean usados, especialmente fuera de la jornada laboral.

- Ningún usuario o usuaria debe instalar ni ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar cualquiera de los recursos informáticos. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente.

- Queda terminantemente prohibido la modificación de la configuración de cualquier software ya sea sistema operativo o aplicaciones, establecida, por defecto, en el equipo informático por el Responsable de Seguridad, sin su previa autorización.

- El uso del correo electrónico e Internet debe limitarse a las funciones propias del puesto de trabajo.

- No se debe de responder a correos falsos, ni a cadenas de correos para evitar que la dirección de correo electrónico se difunda. Tampoco se deben abrir ficheros adjuntos sospechosos procedentes de desconocidos o que no se hayan solicitado

- Si se detectan virus en los archivos o correos recibidos o durante la navegación por Internet, hay que ponerlo en conocimiento del Responsable de Seguridad.

- Se asignarán contraseñas a todos los usuarios del sistema como medio de validación de su identidad. El procedimiento de asignación de contraseñas se realiza mediante la entrega personal por parte del Responsable de Informática, que es el encargado de comunicar el usuario y la clave para el acceso a los sistemas.

- La contraseña estará compuesta por un mínimo de 6 caracteres, (combinando caracteres alfabéticos y numéricos) y no se deberá revelar mediante ningún concepto, ni se deberá mantener por escrito o a la vista de terceras personas.

- Es recomendable cambiar las contraseñas con una periodicidad semestral. Asimismo, es necesario que los equipos dispongan de protectores de pantalla que se activen a los diez minutos de inactividad, siendo necesaria una contraseña de desbloqueo.

- La contraseña no debe contener el identificador o nombre de usuario de la cuenta, o cualquier otra información personal que sea fácil de conocer (cumpleaños, nombres de hijos, cónyuges...). Tampoco una serie de letras dispuestas adyacentemente en el teclado (123456, qwerty...).

- No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea. Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberán considerarse en peligro.

- No compartir las contraseñas en Internet, por correo electrónico ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que te soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla.

- Si un usuario o usuaria tiene sospecha fundada de que su acceso autorizado está siendo o puede ser utilizado por otra persona, estará obligado a cambiar su contraseña para lo cual contactará con el Responsable de Seguridad o Informática, para comunicar la incidencia.

- No se podrá utilizar ningún acceso autorizado de otro usuario o usuaria, aunque lo autorice la persona propietaria.

- Ningún usuario o usuaria debe intentar acceder a áreas restringidas de los sistemas de información propios o de terceras personas, distintos de los que le hayan sido asignados.

- Todos los empleados deberán devolver los activos de información propiedad de SOLUTIO una vez finalizado el periodo de su utilización, contrato o acuerdo.

2.4.1 Política de dispositivos móviles

En cuanto al uso de los dispositivos móviles (portátiles, teléfonos inteligentes, tablets), se deberá de tener en cuenta:

SOLUTIO, pondrá a disposición de los empleados autorizados, terminales móviles con la finalidad de facilitar el desarrollo de su actividad profesional. Por motivos, principalmente de seguridad, no se autoriza el uso de los mismos con fines personales o de ocio, y su uso deberá de ajustarse a lo expuesto en la presente Política.

Los teléfonos móviles, serán asignados por los responsables definidos, siendo estos los únicos autorizados para la gestión y distribución de los mismos. Se mantendrá, por parte de los responsables, un Inventario actualizado de los dispositivos facilitados. Tras su asignación, el teléfono móvil estará bajo la custodia del usuario, quien será responsable del cumplimiento de las medidas que se contemplan a continuación:

- La sustracción o pérdida de los teléfonos móviles se ha de poner inmediatamente en conocimiento del personal responsable de SOLUTIO para la adopción de las medidas que correspondan, según el procedimiento de gestión de incidencias. En general, los usuarios de estos dispositivos se responsabilizarán de que no serán usados por terceras personas ajenas a la entidad o no autorizadas para ello.

- Se reducirá en la medida de lo posible la información almacenada en los dispositivos móviles, autorizándose el acceso/uso del correo electrónico, agenda de contactos, y otras tareas que no requieran el uso de información confidencial o relevante de SOLUTIO: calendario, gestión de tareas, etc. No se deberán almacenar documentos con información confidencial o de uso interno en el dispositivo.

- En la medida de los posible, se cuidará la privacidad en el acceso a Internet a través del dispositivo, reduciendo el acceso a lo estrictamente necesario para cumplir con las finalidades profesionales, y teniendo en cuenta aspectos como no habilitar las opciones tipo “Recordar contraseñas” en los formularios web, o borrando periódicamente el historial de navegación. Se minimizará la conexión a redes externas o públicas, que no puedan asegurar un nivel de seguridad adecuado para la información intercambiada

- Cualquier cambio en la configuración del dispositivo por parte de los usuarios (instalación de nuevo software, o cambio en la configuración de privacidad que se contempla en esta política), requerirá la autorización/supervisión de los responsables definidos.

- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá a SOLUTIO, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo/dispositivo a su estado original para que pueda ser asignado a un nuevo usuario.

- El usuario se responsabilizará de mantener la configuración de la privacidad del dispositivo según los requisitos que se indican a continuación, para lo cual se accederá a la opción Seguridad del menú de “Ajustes”:

    a. El bloqueo de dispositivos (“Bloqueo de Pantalla”) se configurará de modo que se requiera el uso de un código PIN o contraseña de al menos 4 caracteres (Se recomienda el uso de contraseña de 6 caracteres, alfanuméricos, y con caducidad al menos anual).

b. Se configurará el dispositivo de modo que se bloquee automáticamente tras, como máximo, 10 minutos de inactividad.

c. Se deshabilitarán las opciones de “Mostrar Contraseñas”, e instalar “Apps de origen desconocido”, y se mantendrá activada la opción de “Verificar Aplicaciones”.

2.4.2 Incumplimiento de la Política de uso aceptable

Todos los usuarios de **SOLUTIO** están obligados a cumplir lo prescrito en la presente Política de uso aceptable.

En el supuesto de que un usuario no observe alguno de los preceptos señalados en la presente política de uso aceptable, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario