POLÍTICA DE GESTIÓN DE AUDIFILM

Audifilm Consulting S.L.U. (AUDIFILM) es una empresa especializada en el diseño, desarrollo, implementación y soporte de soluciones profesionales en el campo de las Tecnologías de la Información.

AUDIFILM (www.audifilm.com) desarrolla actualmente sus actividades, integrada en la estructura local de Grupo AL, optimizando las sinergias que brinda la capacidad de evolución del Grupo.

AUDIFILM tiene una dilatada y especial vinculación histórica al sector de la Administración Pública, debido a su presencia en ella desde inicios de los años 80. Ha desarrollado Genesys, un Sistema de Información para la Administración Pública, orientado a resolver mediante las Tecnologías de la Información, las necesidades de Gestión de la Administración.

Los Recursos Humanos de AUDIFILM constituyen uno de sus más sólidos pilares. En los departamentos Comercial, de Consultoría, I+D, Soporte y Administración, trabaja un equipo de personas altamente cualificadas.

Mediante la aplicación de un sistema de Gestión, basado en los requisitos de las normas UNE-EN-ISO 9001, UNE-EN-ISO 14001 y UNE-EN-ISO 27001 Y ENS (Esquema nacional de seguridad, Real Decreto 3/2010) se persigue lograr una mejora continua en la calidad de los servicios y el desempeño ambiental de las actividades de nuestra organización, así como un compromiso continuo de mejora técnica de nuestros sistemas, activos y procesos, y el de nuestros proveedores, para procurar una continua adaptación a las necesidades tecnológicas de nuestros clientes. Dentro del ámbito ambiental, la Dirección se compromete a proteger el medioambiente, incluyendo la prevención de la contaminación.

Para ello, AUDIFILM CONSULTING S.L.U. considera la base de esta Política, como pilares básicos de la organización para alcanzar la mejora continua de la eficacia de dicho sistema de Gestión, las siguientes directrices, que servirán de base al establecimiento de nuestros objetivos anuales:

- *Asegurar la **satisfacción de sus clientes** basándose en un trato siempre correcto y en un esfuerzo continuo en la prestación del servicio en base a sus requisitos y a nuestros compromisos desactualización y mejora de los cursos que impartimos.*
- *Cumplir con los **requisitos de los clientes y de sus grupos de interés**, así como con los requisitos legales y reglamentarios que afecten a la realización y prestación de los servicios prestados*
- *Cumplir con los **requisitos legales** que le son de aplicación, así como con aquellos requisitos que la organización suscriba evaluando continuamente dicho cumplimiento, en todas sus áreas de actividad.*
- *Evaluar de forma concienzuda **los riesgos de la Empresa**, analizando los posibles riesgos de todos y cada uno de los procesos de la organización y de los activos de información, previendo y evitando de esta manera desviaciones, tomando las oportunas decisiones para minimizar posibles no conformidades*
- ***Mejorar de forma continua la calidad** en la prestación de nuestros servicios y nuestro comportamiento frente a los impactos ambientales que genera nuestra actividad, así como* en la forma en que tratamos la información de nuestros clientes. *Mediante el establecimiento de **objetivos y metas para conseguirlo**.*

- *Mejorar continuamente los procesos y servicios como instrumento fundamental para el incremento de la eficacia, eficiencia, competitividad y fidelización del cliente.*

- *Mejorar permanentemente la **competitividad de nuestros servicios**, haciendo participe a nuestros clientes en todo momento de los mismos y adaptando continuamente nuestros servicios a sus necesidades, intentando colaborar mediante nuestros servicios a unas correctas políticas de gestión también entre nuestros clientes.*

- *Velar por una **continua y permanente actualización de nuestros recursos**, tanto tecnológicos como, sobre todo, de nuestro **personal,** fomentando políticas de información y formación continua profesional que les permitan avanzar en sus conocimientos al ritmo que lo hace nuestro sector. fomentando la conciencia de la Calidad, a fin de incrementar la competencia de los empleados.*

- *Establecer y revisar regularmente los Objetivos, acordes con los compromisos que se asumen en esta declaración, fortaleciendo el **compromiso y participación de todo el personal** en el desarrollo y consecución de los Objetivos.*

- *Garantizar la **mejora continua**, manteniendo el Sistema de forma eficaz y efectivo para constatar el compromiso con los clientes, buscando para ello una mejor organización interna del trabajo.* y en la forma en que tratamos la información de nuestros clientes.

- *Fomentar la sensibilización ambiental de nuestro personal, clientes, comerciales, proveedores, colaboradores, mediante el establecimiento de prácticas ambientales, formando e informando para conseguir la disminución de los gastos energéticos y la gestión correcta de los residuos ambientales, todo ello encaminado hacia la mejora ambiental.*

- *Lograr que la **seguridad de la información y el respeto a los datos personales sean una constante**:*

    - *Preservando la confidencialidad de la información y evitando su divulgación y el acceso por personas no autorizadas.*

    - *Manteniendo la integridad de la información procurando su exactitud y evitando su deterioro.*

    - *Asegurando la disponibilidad de la información en todos los soportes y siempre que sea necesaria.*

- *La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad y confidencialidad de su información y aún más la de sus clientes.*

Esta Política será revisada para su continua adecuación anualmente por la dirección, así como los objetivos y metas de la empresa, y comunicada a todo el personal de la organización encontrándose a disposición del público bajo solicitud de cualquier parte interesada.

Respecto al Esquema Nacional de Seguridad (ENS), la empresa tiene en cuenta los siguientes aspectos y directrices:

ALCANCE

En el caso de la norma ISO 27001, esta política se aplica a los DISEÑO Y DESARROLLO DE SISTEMAS DE INFORMACIÓN PARA LA ADMINISTRACIÓN PÚBLICA. PRESTACIÓN DE SERVICIOS DE CONSULTORÍA, IMPLANTACIÓN, PUESTA EN MARCHA, SOPORTE Y FORMACIÓN PARA LA ADMINISTRACIÓN PÚBLICA.

Por otro lado, de cara al Esquema Nacional de Seguridad el alcance es:

SISTEMA DE INFORMACIÓN DE ADMINISTRACIÓN ELECTRÓNICA QUE DA SOPORTE A LOS SERVICIOS DE SOFTWARE PARA LA ADMINISTRACIÓN PÚBLICA, DE ACUERDO CON LA CATEGORIZACIÓN DEL SISTEMA VIGENTE

MISIÓN

La misión de AUDIFILM es prestar servicios relacionados con el diseño, desarrollo, implementación y soporte de soluciones profesionales en el campo de las Tecnologías de la Información.

La empresa tiene como objetivo proveer soluciones aptas para que sus clientes dispongan de unos productos y servicios eficaces y de alta calidad, ofreciéndose también como el socio ideal para hacer frente a la ejecución del ciclo total de un proyecto. En definitiva, proporcionar servicios profesionales con la máxima calidad posible, por lo que exige a sus empleados que tomen todas las medidas necesarias parar garantizar la integridad de la información de la compañía y sus sistemas de comunicaciones, siguiendo los procedimientos y guías implantados en su SGSI.

Esta política aplica al uso de los sistemas de información y de comunicaciones de la empresa, así como a los datos y la información que se almacenen u originen de estos sistemas.

MARCO NORMATIVO

AUDIFILM se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código de Comercio, Código Civil, etc.) o específico, como por ejemplo la siguiente:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- ISO 9001:2015, Sistemas de Gestión de la Calidad.
- ISO 14001:2015, Sistemas de Gestión Ambiental.
- Real Decreto 1720/2007 de 21 de diciembre por el que se desarrolla la LOPD
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Guías de la serie 800 CCN-STIC, como, guías de la estructuración documental.

ORGANIZACIÓN DE LA SEGURIDAD

4.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Calidad y Seguridad estará formado por la Dirección, el Responsable de Seguridad y por representantes de otras áreas de la organización afectadas. La composición del Comité de Seguridad de la Información de AUDIFILM es la siguiente:

- Responsable de la información
- Responsable del Servicio
- Responsable del Sistema
- Responsable de Seguridad
- Delegado de Protección de Datos

Dentro de esta estructura, el Secretario del Comité de Calidad y Seguridad tendrá como funciones la preparación de las reuniones, la difusión de sus resultados y el seguimiento de los acuerdos alcanzados.

El Comité de Calidad y Seguridad reportará al Comité de Dirección.

El Comité de Calidad y Seguridad, por lo que se refiere al SGSI de AUDIFILM y al cumplimiento de lo dispuesto en el ENS, tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la normativa de seguridad de la información
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la gestión de incidentes de seguridad.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

4.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga la norma ISO 27001 y el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar o promover la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad, con la colaboración del Coordinador del CCA.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema, con el auxilio del resto del Comité de Calidad y Seguridad.
- La especificación de requisitos de seguridad corresponde a los responsables de la información y de los servicios, junto con el responsable del registro de actividades si hubiera datos de carácter personal. La operación corresponde a los responsables de los sistemas, mientras que la supervisión corresponde al responsable de la seguridad y al técnico de seguridad.

La descripción concreta de las responsabilidades puede consultarse en el documento: PS01_SEGURIDAD DE LA INFORMACIÓN.

Por su parte, el personal de la empresa tiene identificadas y comunicadas sus responsabilidades en relación a la seguridad de la información entre las que se destacan:

- Comunicar las incidencias de seguridad mediante los canales establecidos.
- Aplicar los mecanismos establecidos para el intercambio de información entre el personal, clientes y proveedores.

Cualquier asignación de tareas y responsabilidades de seguridad de la información será aprobada por el Comité de Seguridad.

DATOS DE CARÁCTER PERSONAL

AUDIFILM, trata datos de carácter personal, por lo que mantiene un “Registro de actividades del tratamiento”, al que tendrán acceso sólo las personas autorizadas, en el que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de AUDIFILM se ajustarán a los niveles de seguridad

requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro.

OBLIGACIONES DEL PERSONAL

Todos los trabajadores de AUDIFILM tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Calidad y Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de AUDIFILM, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

TERCERAS PARTES

Las terceras partes relacionadas con AUDIFLM, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando AUDIFILM utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Esta Política será revisada para su continua adecuación anualmente por la dirección, así como los objetivos y metas de la empresa, y comunicada a todo el personal de la organización.

En Girona a 02 de noviembre de 2022

35071848E PEDRO ESCALONA (R: B83998740)
Firmado digitalmente por 35071848E PEDRO ESCALONA (R: B83998740)
Fecha: 2022.11.02 16:25:14 +01'00'

Pedro Escalona

Director Gerente

44593467D DIEGO CAMBLO (R: B83998740)
Firmado digitalmente por 44593467D DIEGO CAMBLO (R: B83998740)
Nombre de reconocimiento (DN): 2.5.4.13=Notario: JOSE ANGEL GOMEZ MORAN ETCHART/Núm Protocolo: 585/Fecha Otorgamiento: 23-03-2017, cn=44593467D DIEGO CAMBLO (R: B83998740), givenName=DIEGO, sn=CAMBLO GIMENEZ, serialNumber=IDCES-44593467D, 2.5.4.97=VATES-B83998740, ou=DIRECCION GENERAL, o=AUDIFILM CONSULTING S.L.U., c=ES
Fecha: 2022.11.02 08:35:20 +01'00'

Diego Cambló Giménez

CEO/Responsable de la Información/Responsable de servicios