SERVICIO COMPLIANCE

POLÍTICAS Y PROCEDIMIENTOS

MEDIDAS PARA EL CUMPLIMIENTO NORMATIVO

Uno de los objetivos del Compliance es implementar medidas para prevenir, detectar y gestionar los riesgos asociados con el cumplimiento de las normas que afectan a las organizaciones. A fin de cumplir con este objetivo, en este documento se detallan las medidas y procedimientos que garantizan el cumplimiento normativo.

CONVERSIA

ÍNDICE DE CONTENIDOS

REGISTRO DE VERSIONES

Razón Social	NIF	Versión
SERVERA SL	B07020191	2.01
Acrónimo	**Fecha de creación**	
MCN_SERVERA SL	14 de septiembre de 2023	
DESCRIPCIÓN		
Medidas y Políticas para garantizar el cumplimiento normativo, así como establecer una cultura ética en las actuaciones de SERVERA SL		

1. OBJETO DEL DOCUMENTO

La evolución de la tecnología y el constante incremento del volumen, complejidad y variabilidad de las normas, así como, la creciente severidad de las consecuencias asociadas a su violación, ha provocado la expansión del Compliance a cualquier organización.

En este sentido, las organizaciones deberán estar atentas a lo previsto en las diversas leyes que les sean de aplicación, ya que pueden sufrir consecuencias tanto económicas como reputacionales derivadas de un incumplimiento normativo. Es por ello que, para prevenir, detectar y gestionar posibles riesgos y consecuencias negativas, así como para garantizar el cumplimiento de las normas que les son de aplicación, deberán aplicar medidas técnicas y organizativas.

El objeto del presente documento es definir y desarrollar aquellas medidas, políticas y procedimientos que deberá implementar SERVERA SL para cumplir con las normas que le son de obligado cumplimiento y así evitar los riesgos intrínsecos del desarrollo de su actividad. Las medidas que se establecen, serán consideradas de obligado cumplimiento para directivos, personas trabajadoras, voluntarias, así como para los demás agentes relacionados con SERVERA SL.

Del mismo modo, las medidas y políticas del presente documento, se adecuarán a las disposiciones vigentes de las siguientes materias:

- 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 y por el que se deroga la Directiva 95/46/CE.
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley orgánica 34/2002 de 11 de julio, Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 10/2021, de 9 de julio, de trabajo a distancia (en lo estrictamente relacionado con la protección de datos de carácter personal).
- Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo (en lo estrictamente relacionado con la protección de datos de carácter personal).
- Circular de la Fiscalía 1/2016, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.

Finalmente, el presente documento se mantendrá en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes o sustanciales en las actividades desarrolladas por SERVERA SL, las cuales puedan tener un impacto en el cumplimiento de las normativas aplicables a la organización.

2. IDENTIFICACIÓN DE LA ENTIDAD

Razón social	SERVERA SL
NIF	B07020191
Dirección	PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS)
Actividad profesional	SERVERA SL dedica su actividad principal a: SERVICIOS DE ALOJAMIENTO
Área geográfica de desarrollo	SERVERA SL desarrolla su actividad en el ámbito geográfico del territorio europeo.

SERVERA SL no dispone de filiales u otras entidades dentro de su estructura corporativa.

3. MEDIDAS Y POLÍTICAS PARA EL CUMPLIMIENTO NORMATIVO

Las distintas medidas y políticas especificadas en este documento tienen como finalidad establecer un conjunto de procedimientos que ayuden a prevenir, detectar y gestionar razonablemente los riesgos asociados con el cumplimiento de las normas que afectan a SERVERA SL, en el desarrollo de su actividad profesional o laboral.

A su vez, también pretende dotar a SERVERA SL de buenas prácticas sobre Compliance, las cuales promuevan una cultura organizativa que impulse comportamientos éticos y de cumplimiento de la ley.

Para ello, las medidas y políticas que se detallan garantizan el principio de proporcionalidad, es decir, se adaptan a las circunstancias internas y externas de SERVERA SL, estableciendo un sistema de gestión adecuado a sus particularidades.

SERVERA SL ha diseñado un registro de las actividades del tratamiento, un protocolo para el diseño de los flujos de operaciones de tratamiento de datos de carácter personal, una relación de los activos de información, así como diferentes procedimientos y políticas que deberán implementarse de manera adecuada en SERVERA SL para garantizar el cumplimiento normativo.

Asimismo, entre estas medidas, deberá establecerse la implementación y gestión de un canal de comunicación al efecto de facilitar:

- La detección y conocimiento por parte de la organización de cualquier incumplimiento de la normativa aplicable o del propio Sistema de Gestión de Compliance.
- La gestión de las violaciones de seguridad o el ejercicio de derechos de los interesados en materia de protección de datos.

Por último, la organización establecerá un Sistema Disciplinario para penalizar los incumplimientos normativos y del Sistema de Gestión de Compliance por parte de los integrantes de la organización.

3.1. REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

De conformidad con la normativa vigente y aplicable en materia de protección de datos, SERVERA SL y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) El nombre y los datos de contacto de SERVERA SL y, en su caso, del corresponsable, del representante de SERVERA SL, y de su Delegado de Protección de Datos (en adelante, DPD) si fuera necesaria su designación;

b) Los fines del tratamiento;

c) Una descripción de las categorías de interesados y de las categorías de datos personales;

d) Las categorías de destinatarios a quienes se han comunicado o se comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional, así como la documentación de garantías adecuadas cuando sea oportuno;

f) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Con el objeto de cumplir con esta obligación, SERVERA SL ha diseñado e implantado, un registro de las actividades de tratamiento de los datos personales de las que es responsable, y el mismo se mantiene actualizado.

Las actividades de tratamiento de datos, que se relacionan a continuación son responsabilidad de SERVERA SL, con domicilio en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), el responsable legal del cual es MARIA TERESA SERVERA GUAL con DNI 18221554B y teléfono de contacto 971585433.

SERVERA SL ha documentado el registro de las categorías de actividades de tratamiento de las que es responsable, aportando la siguiente información:

- El responsable del tratamiento.
- Las categorías de los interesados y las tipologías de datos personales a tratar.
- Los fines del tratamiento.
- Las categorías de destinatarios de los datos.
- Las transferencias de datos a un tercer país.
- Los plazos previstos para la supresión de las categorías de datos.
- Una descripción de las medidas técnicas y organizativas de seguridad aplicadas a las categorías de datos.

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

Datos de la entidad

Entidad	SERVERA SL
NIF	B07020191
Datos de contacto	info@hotelatolon.com

Operaciones en condición de Responsable del Tratamiento

Tratamiento	Gestión de las reservas alojamiento
Categoría de interesados	Clientes, Menores.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono, NIF, Dirección electrónica, Datos económicos o de seguros. Datos sensibles: Datos relativos a menores.
Finalidad del tratamiento	Registro y gestión de las reservas de alojamiento.
Categorías de destinatarios	Agencia Tributaria, Bancos y Cajas, Fuerzas y Cuerpos de Seguridad y autoridades competentes.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	3 años, Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos.

Tratamiento	Uso de aplicaciones de mensajería instantánea
Categoría de interesados	Clientes, Proveedores, Padres/Tutores, Personas trabajadoras.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono.
Finalidad del tratamiento	Realizar comunicaciones de carácter informativo a través de WhatsApp.
Categorías de destinatarios	No se realizan cesiones de datos.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	mientras se mantenga el consentimiento prestado, salvo obligación legal.

Tratamiento	Gestión Formulario web
Categoría de interesados	Usuarios web.
Tipología de datos	Datos básicos: Nombre y apellidos, Dirección electrónica, Dirección IP.
Finalidad del tratamiento	Atender sus consultas y/o solicitudes.
Categorías de destinatarios	No se realizan cesiones de datos.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	mientras se mantenga el consentimiento prestado.

Tratamiento	Gestión usuarios web
Categoría de interesados	Usuarios web.
Tipología de datos	Datos básicos: Nombre y apellidos, Dirección electrónica.
Finalidad del tratamiento	Captación, registro y tratamiento de datos del usuario.
Categorías de destinatarios	No se realizan cesiones de datos.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	mientras se mantenga el consentimiento prestado, salvo obligación legal.

Tratamiento	Instalación de cookies
Categoría de interesados	Usuarios web.
Tipología de datos	Datos básicos: Dirección electrónica, Dirección IP.
Finalidad del tratamiento	Gestión e instalación de las cookies .
Categorías de destinatarios	No se realizan cesiones de datos.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	mientras se mantenga el consentimiento prestado.

Tratamiento	Gestión económica y administrativa
Categoría de interesados	Clientes, Proveedores, Colaboradores, Padres/Tutores.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono, NIF, Dirección postal, Datos económicos o de seguros.
Finalidad del tratamiento	Gestión administrativa, facturación, contabilidad y obligaciones legales.
Categorías de destinatarios	Agencia Tributaria, Bancos, Cajas y Organismos y/o administración pública con competencia en la materia.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	5 años en cumplimiento de la ley tributaria y 10 años la documentación fiscal en cumplimiento de la L.O. 7/2012.

Tratamiento	Gestión de RRHH
Categoría de interesados	CANDIDATOS, Personas trabajadoras.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono, NIF, Dirección postal, Características personales, Dirección electrónica, Firma, Datos académicos, Datos profesionales/empleo, Imagen.
Finalidad del tratamiento	Captación, registro y tratamiento de datos de candidatos para finalidades de selección de personal y gestión, análisis y archivo de los currículos de los candidatos.
Categorías de destinatarios	No se realizan cesiones de datos.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	1 año.

Tratamiento	Gestión del cumplimiento normativo
Categoría de interesados	Clientes, Proveedores, Colaboradores, Padres/Tutores, Menores, Personas trabajadoras.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono, NIF, Dirección postal, Dirección electrónica, Firma, Datos profesionales/empleo, Datos económicos o de seguros. Datos sensibles: Datos relativos a menores.
Finalidad del tratamiento	Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad.
Categorías de destinatarios	Organismos y/o administración pública con competencia en la materia.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	conservación de las copias de los documentos hasta que prescriban las acciones para reclamarle una posible responsabilidad.

Tratamiento	Gestión de nóminas y contratos
Categoría de interesados	Personas trabajadoras.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono, NIF, Dirección postal, Nº Seguridad Social, Características personales, Datos académicos, Datos profesionales/empleo, Datos económicos o de seguros.
Finalidad del tratamiento	Confección de los contratos laborales de los trabajadores y de los recibos de salario, tramitación de expedientes, liquidación de Seguros Sociales, tramitación con las Mutuas y Organismos correspondientes, retención e ingresos a cuenta del IRPF de los trabajadores y profesionales y cualquier otra actividad propia de la gestión del personal.
Categorías de destinatarios	Seguridad Social, Aseguradoras, Mutuas, Bancos y Cajas.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	10 años, en cumplimiento de la Ley Orgánica 7/2012, de 27 de diciembre. Los datos económicos de esta actividad de tratamiento se conservarán al amparo de lo dispuesto en la Legislación Tributaria.

Tratamiento	Acciones comerciales y/o envíos publicitarios
Categoría de interesados	Clientes.
Tipología de datos	Datos básicos: Nombre y apellidos, Teléfono, Dirección postal, Dirección electrónica, Información comercial.
Finalidad del tratamiento	Captación, registro y tratamiento de datos con finalidades de publicidad y prospección comercial.
Categorías de destinatarios	No se realizan cesiones de datos.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	mientras se mantenga el consentimiento prestado.

Tratamiento	Control de acceso y presencialidad con sistema de fichaje
Categoría de interesados	Personas trabajadoras.
Tipología de datos	Datos básicos: Nombre y apellidos, Firma. Datos de carácter especial: Datos biométricos.
Finalidad del tratamiento	Registro de horas de inicio, pausa y finalización de la actividad laboral del empleado, el control de acceso a las instalaciones y garantizar su identidad en el acceso..
Categorías de destinatarios	Inspección de Trabajo y Seguridad Social.
Transferencia internacional	No se realizan transferencias internacionales de datos.
Medidas técnicas y organizativas	Previstas en el documento *6 Medidas para el cumplimiento normativo* y documento *7 Políticas para el cumplimiento de la normativa de seguridad.*
Plazos de supresión	Los registros serán conservados durante cuatro años, en cumplimiento de la Ley del Estatuto de los Trabajadores.

3.2. PROTOCOLO PARA EL DISEÑO DE LOS FLUJOS

Cualesquiera de los nuevos tratamientos, en particular si utiliza nuevas tecnologías, que por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, requerirá que SERVERA SL proceda a la realización de un análisis de riesgos de los tratamientos, un análisis de la necesidad de una Evaluación de Impacto de protección de datos y una Evaluación de impacto en el caso que este análisis previo así lo dictamine. Para un correcto desarrollo de la Evaluación de Impacto, SERVERA SL procederá a documentar el procedimiento de tratamiento de datos.

En el apartado *3.2.1. Procedimiento de generación de procesos de tratamiento de datos* se establece la metodología que seguirá SERVERA SL a fin de ejecutar nuevos procedimientos de tratamiento de datos de carácter personal.

En todo caso estos procedimientos serán supervisados y aprobados por el Delegado de Protección de Datos, o en su defecto por el Compliance Officer.

3.2.1. Procedimiento de generación de procesos de tratamiento de datos

La normativa vigente en materia de protección de datos establece que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, SERVERA SL realizará antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

En este sentido SERVERA SL recabará el asesoramiento del Delegado de Protección de Datos o en su defecto, del Compliance Officer.

SERVERA SL deberá proceder con la siguiente operativa cuando existan nuevas operaciones de tratamiento:

1. Creación de un equipo de trabajo

Previamente a cualquier acción se establecerá un equipo de trabajo. Este equipo de trabajo estará configurado como mínimo por los siguientes roles:

- Compliance Officer
- Responsable de área origen de la nueva operación de tratamiento

2. Análisis de la nueva operación de tratamiento

Una vez creado el equipo de trabajo, se establecerá un plan de acción, que como mínimo contendrá las siguientes acciones de análisis:

- Origen de los datos objeto de la nueva operación de tratamiento
- Tipología de datos
- Sistema de tratamiento de los datos
- Tratamientos y subtratamientos vinculados a la nueva operación

Elaborado y acordado el plan de acción a fin de analizar la nueva operación de tratamiento, este deberá ser aprobado por la dirección de SERVERA SL. Como fase ejecutiva de este paso, una vez obtenida la validación de la dirección de SERVERA SL se procederá a ejecutar el plan de acción.

3. Diseño del flujo del proceso de tratamiento de datos

Culminado el plan de acción previsto en el punto anterior se procederá a plasmar el procedimiento de tratamiento. Este contendrá como mínimo exigible la siguiente información:

- Origen de los datos
- Forma o formas de cumplimiento de las obligaciones de SERVERA SL ante los derechos de los interesados
- Descripción del tratamiento de datos
- Posibles comunicaciones de datos
- Categorías de datos objeto de tratamiento
- Plazos de conservación
- Plazos de bloqueo

4. Necesidad de Evaluación de Impacto

Con la información que disponemos, SERVERA SL realizará un análisis de la nueva operación de tratamiento con la finalidad de detectar si es necesario realizar una EIPD. Este análisis tendrá en cuenta lo establecido en la normativa aplicable y vigente en materia de protección de datos, así como, las directrices de los órganos competentes en dicha materia.

En todo caso, previo a la realización de una EIPD se deberá analizar detenida y responsablemente los nuevos tratamientos de datos personales que se vayan a llevar a cabo por parte de la entidad y así, detectar la necesidad o no, de realizar una EIPD, ya que no todos los tratamientos que lleven a cabo los responsables y encargados de tratamiento requerirán de una EIPD para cada una de las operaciones de tratamiento realizadas.

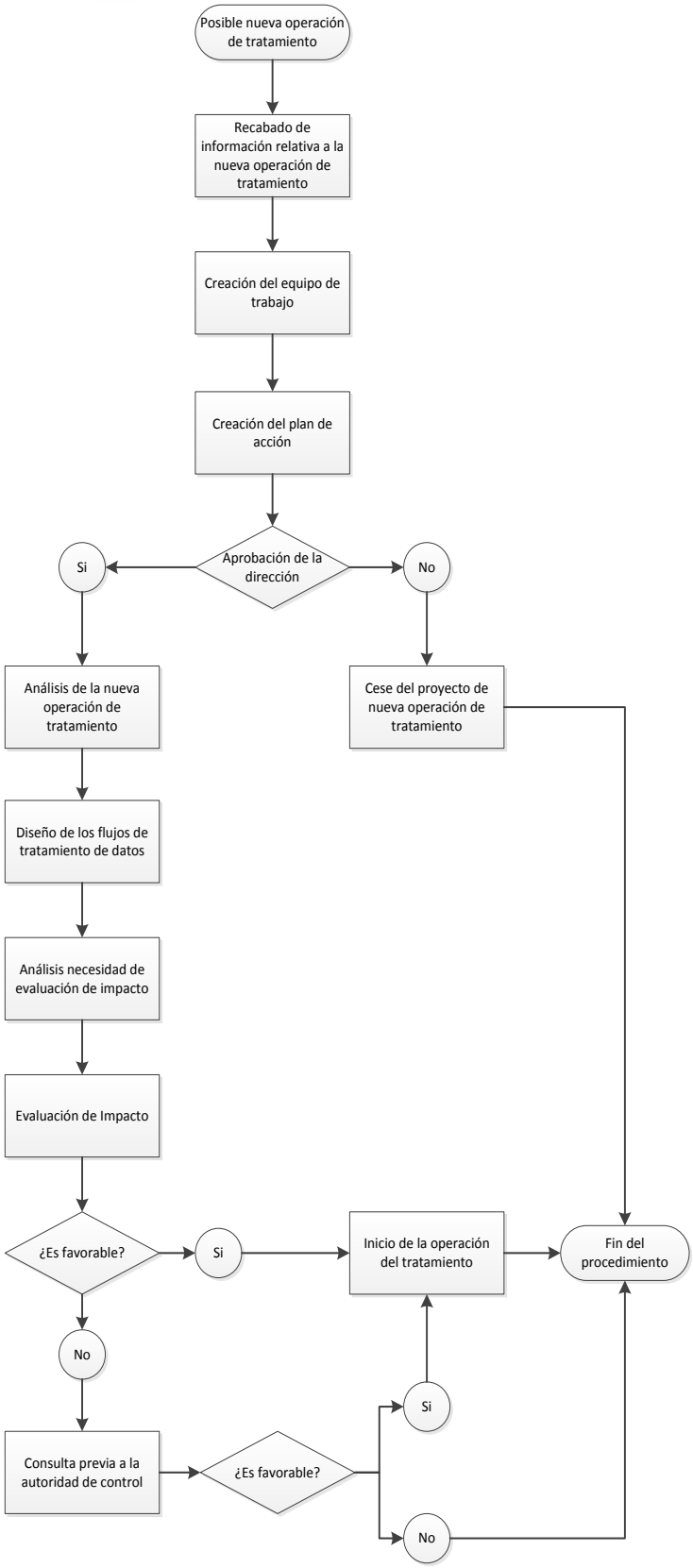
5. Evaluación de Impacto

Finalizadas las fases anteriores se procederá a la elaboración de una Evaluación de Impacto de la nueva operación de tratamiento, en caso de ser obligatoria. Esta puede ser realizada por el propio equipo de trabajo de acuerdo con lo establecido en el punto 1 o por parte de un equipo o empresa externos.

El resultado de esta evaluación será determinante para la puesta en producción de la nueva operación del tratamiento, pudiendo desembocar en dos situaciones:

- Evaluación de Impacto favorable, la nueva operación de tratamiento no conlleva riesgos altos. En este caso se procederá a iniciar la nueva operación de tratamiento.
- Evaluación de Impacto desfavorable, la nueva operación de tratamiento sí conlleva riesgos altos. Se deberá someter esta operación de tratamiento a consulta previa de la Autoridad de Control. En este caso, hasta obtener respuesta positiva de la Autoridad de Control, no se podrá iniciar la nueva operación de tratamiento.

A modo descriptivo, SERVERA SL ha diseñado un modelo gráfico del proceso a seguir para la iniciación de nuevas operaciones de tratamiento que entrañen riesgos elevados ante los derechos de los interesados.


Posible nueva operación de tratamiento
Recabado de información relativa a la nueva operación de tratamiento
Creación del equipo de trabajo
Creación del plan de acción
Aprobación de la dirección
Si
No
Análisis de la nueva operación de tratamiento
Cese del proyecto de nueva operación de tratamiento
Diseño de los flujos de tratamiento de datos
Análisis necesidad de evaluación de impacto
Evaluación de Impacto
¿Es favorable?
Si
Inicio de la operación del tratamiento
Fin del procedimiento
No
Si
Consulta previa a la autoridad de control
¿Es favorable?
No

3.3. ACTIVOS DE INFORMACIÓN

Los activos de información son los recursos que utiliza una organización para que ésta funcione y consiga los objetivos que se ha propuesto.

La gestión de activos de información involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio.

SERVERA SL deberá llevar a cabo un inventario de los activos de información que intervengan en las operaciones de tratamiento realizadas por SERVERA SL con el objetivo de proteger la información que resulta fundamental frente a cualquier situación que suponga un riesgo o amenaza.

Debido a que los activos de información son cambiantes, el inventario de activos deberá actualizarse cuando sea oportuno.

En el presente apartado, se identifican los activos de información más relevantes para el tratamiento de los datos de carácter personal. Asimismo, mencionar que no se trata de un análisis o identificación técnica sino de un estudio conceptual de los mismos.

A continuación, procederemos a identificar conceptualmente los sistemas y tecnologías de SERVERA SL:

INVENTARIO DE TECNOLOGÍAS DE INFORMACIÓN (activos de información)			

Nombre:	Sistema de copias de seguridad	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	Mensajería instantánea	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	Personaltec	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	Otec	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	Ecotec	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	Contec	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	Bectron	**Tipo:**	Software- Aplicaciones

Ubicación:	Dependencia Principal	**Responsable:**	

Nombre:	www.hotelatolon.com	**Tipo:**	Servicios
Ubicación:		**Responsable:**	

Nombre:	Responsable de Privacidad	**Tipo:**	Activos Humanos
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Memoria USB	**Tipo:**	Soportes de Información
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Ordenador de mesa	**Tipo:**	Hardware
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Pack ofimática	**Tipo:**	Software- Aplicaciones
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Material impreso	**Tipo:**	Datos - Información
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Red inalámbrica	**Tipo:**	Redes de comunicación
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Oficinas	**Tipo:**	Entorno - Infraestructura
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Archivadores	**Tipo:**	Entorno - Infraestructura
Ubicación:	Dependencia principal	**Responsable:**	

Nombre:	Router	**Tipo:**	Hardware
Ubicación:	Dependencia principal	**Responsable:**	

3.4. POLÍTICA DE PRIVACIDAD

3.4.1. Introducción

SERVERA SL deberá cerciorarse de que los datos personales del interesado sean tratados según los principios relativos al tratamiento:

- Tratados de manera lícita, leal y transparente en relación con el interesado (“licitud lealtad y transparencia”).
- Recogidos con fines determinados, explícitos y legítimos, no pudiendo ser tratados de manera incompatible con dichos fines (“limitación de la finalidad”).
- Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (“minimización de los datos”).
- Exactos y, si fuera necesario actualizados adoptándose las medidas técnicas y organizativas razonables para que se supriman o rectifiquen cuando sean inexactos con respecto a los fines para los que se tratan (“exactitud”).
- Mantenidos de forma que se permita la identificación durante no más tiempo de lo necesario para los fines del tratamiento (“limitación del plazo de conservación”).
- Tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas técnicas u organizativas apropiadas (“integridad y confidencialidad”).

Así, SERVERA SL será responsable del cumplimiento de lo dispuesto anteriormente y deberá poder acreditarlo con posterioridad (“responsabilidad proactiva”).

Del mismo modo, el tratamiento que realice la entidad solo será lícito si cumple al menos una de las siguientes condiciones (“licitud del tratamiento”):

- el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Dicha base legítima no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

Asimismo, sólo podrán tratarse datos personales que revelen el origen étnico o racial, opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física en los supuestos previstos en el artículo 9 del RGPD.

El tratamiento de los datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión Europea o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

SERVERA SL deberá incluir en los formularios que se usen para la recogida de datos personales, la información para dar cumplimiento al deber de informar recogido en los artículos 13 y 14 del Reglamento General de Protección de datos (en adelante RGPD).

En este sentido, y con la finalidad de adaptarse a la normativa aplicable y vigente en materia de protección de datos, cuando SERVERA SL obtenga los datos personales directamente de un interesado, tendrá que:

1- Facilitar la identidad y los datos de contacto del Responsable del Tratamiento y en su caso, de su representante, los datos de contacto del Delegado de Protección de Datos, en su caso y los fines del tratamiento a que se destinan los datos personales así como, la base jurídica del tratamiento.

2- Especificar los intereses legítimos del responsable o de un tercero cuando el tratamiento sea necesario para la satisfacción de esos intereses. Siempre que, sobre ellos no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

3- Facilitar los destinatarios o las categorías de destinatarios de los datos personales y en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión.

4- Indicar el plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinar el plazo de conservación.

5- Informar de la existencia del derecho a solicitar al Responsable del Tratamiento el acceso a los datos personales relativos al interesado, su rectificación o supresión (“derecho al olvido”), la limitación de su tratamiento o el derecho a oponerse al tratamiento, así como a la portabilidad de sus datos.

6- Informar sobre la posibilidad de retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada. Así como, poner en su conocimiento la posibilidad de presentar una reclamación ante una Autoridad de Control.

7- Especificar si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato y si el interesado está obligado a facilitar los datos personales e informar de las posibles consecuencias de no facilitar tales datos.

8- Informar sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, informar sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando SERVERA SL no obtenga los datos personales del interesado tendrá que facilitarle la información descrita en el apartado anterior. Así como, las categorías de datos personales que se traten, la fuente de la que proceden y, en su caso, si proceden de fuentes de acceso público.

Si SERVERA SL obtiene los datos de carácter personal directamente del interesado la información se debe poner a disposición de estos en el momento en que se soliciten los datos, previamente a la recogida o registro. En el caso que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, SERVERA SL informará a las personas interesadas dentro de un plazo razonable, pero en cualquier caso, antes de un mes desde que se obtuvieron los datos personales, en la primera comunicación con el interesado o antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Cuando SERVERA SL proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente.

3.4.2. Información básica de protección de datos

SERVERA SL deberá incluir en los formularios o documentos que se usen para la recogida de datos personales, inclusive los establecidos en la página web titularidad de SERVERA SL, la información para dar cumplimiento al deber de informar recogido en los artículos 13 y 14 del Reglamento General de Protección de Datos (en adelante RGPD), y, en caso de que sea necesario, hacer constar el consentimiento otorgado por el interesado.

Para hacer compatible la mayor exigencia de información que debe facilitarse al interesado cuyos datos de carácter personal van a tratarse se establece la posibilidad de presentar la información adoptando un modelo de información por capas o niveles, ello deberá estar en consonancia con que la información deberá proporcionarse con un lenguaje claro, sencillo y de forma concisa, transparente, inteligible y de fácil acceso.

El artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), regula la información básica que se requiere en una primera capa.

La información por capas consiste en:

- Presentación de Información básica (1ª capa): consiste en presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos.
- Remisión a Información adicional (2ª capa): Consiste en presentar de forma detallada y completa la información, en un medio adecuado, estructurado, conciso y preciso. La forma de presentar esta información adicional depende de las características del medio empleado para informar, se podrá presentar en formato papel o en formato electrónico.

Información Básica Sobre Protección De Datos - Gestión de las reservas alojamiento	
Responsable	SERVERA SL
Finalidad	Registro y gestión de las reservas de alojamiento.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

☐ He leído y acepto la información básica de protección de datos.

Nombre y apellidos del tutor legal:	Nombre y apellidos del menor:
DNI:	DNI:
Firma del tutor legal:	

Información Básica Sobre Protección De Datos - Uso de aplicaciones de mensajería instantánea	
Responsable	SERVERA SL
Finalidad	Realizar comunicaciones de carácter informativo a través de WhatsApp.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

☐ He leído y acepto la información básica de protección de datos.

Información Básica Sobre Protección De Datos - Gestión Formulario web	
Responsable	SERVERA SL
Finalidad	Atender sus consultas y/o solicitudes.

Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

☐ He leído y acepto la información básica de protección de datos.

Información Básica Sobre Protección De Datos - Gestión usuarios web	
Responsable	SERVERA SL
Finalidad	Captación, registro y tratamiento de datos del usuario.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

☐ He leído y acepto la información básica de protección de datos.

Información Básica Sobre Protección De Datos - Instalación de cookies	
Responsable	SERVERA SL
Finalidad	Gestión e instalación de las cookies .
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

☐ He leído y acepto la información básica de protección de datos.

Información Básica Sobre Protección De Datos - Gestión económica y administrativa	
Responsable	SERVERA SL

Finalidad	Gestión administrativa, facturación, contabilidad y obligaciones legales.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

Información Básica Sobre Protección De Datos - Gestión de RRHH	
Responsable	SERVERA SL
Finalidad	Captación, registro y tratamiento de datos de candidatos para finalidades de selección de personal y gestión, análisis y archivo de los currículos de los candidatos.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

Información Básica Sobre Protección De Datos - Gestión del cumplimiento normativo	
Responsable	SERVERA SL
Finalidad	Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

Nombre y apellidos del tutor legal:	Nombre y apellidos del menor:
DNI:	DNI:
Firma del tutor legal:	

Información Básica Sobre Protección De Datos - Acciones comerciales y/o envíos publicitarios	
Responsable	SERVERA SL
Finalidad	Captación, registro y tratamiento de datos con finalidades de publicidad y prospección comercial.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional.
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web, apartado Política de Privacidad.

☐ He leído y acepto la información básica de protección de datos.

☐ SI quiero recibir comunicaciones comerciales.

3.4.3. Información complementaria de protección de datos

INFORMACIÓN COMPLEMENTARIA CLIENTES

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

Gestión de las reservas alojamiento	**Finalidad:** Registro y gestión de las reservas de alojamiento. **Plazo de conservación:** 3 años, Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos. **Base legítima:** El consentimiento del interesado. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos y Cajas, Fuerzas y Cuerpos de Seguridad y autoridades competentes con la finalidad de cumplir con las obligaciones administrativas y de seguridad establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Uso de aplicaciones de mensajería instantánea	**Finalidad:** Realizar comunicaciones de carácter informativo a través de WhatsApp. **Plazo de conservación:** mientras se mantenga el consentimiento prestado, salvo obligación legal. **Base legítima:** El consentimiento del interesado.
Gestión económica y administrativa	**Finalidad:** Gestión administrativa, facturación, contabilidad y obligaciones legales. **Plazo de conservación:** 5 años en cumplimiento de la ley tributaria y 10 años la documentación fiscal en cumplimiento de la L.O. 7/2012. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos, Cajas y Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones tributarias y fiscales establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Gestión del cumplimiento normativo	**Finalidad:** Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad. **Plazo de conservación:** conservación de las copias de los documentos hasta que prescriban las acciones para reclamarle una posible responsabilidad. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Acciones comerciales y/o envíos publicitarios	**Finalidad:** Captación, registro y tratamiento de datos con finalidades de publicidad y prospección comercial. **Plazo de conservación:** mientras se mantenga el consentimiento prestado. **Base legítima:** El consentimiento del interesado.

☐ SI quiero recibir comunicaciones comerciales.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.
SERVERA SL informa que con la firma del presente documento otorga el consentimiento explícito para el tratamiento de los datos de las finalidades mencionadas anteriormente.

Nombre y apellidos:
DNI:
Firma:

INFORMACIÓN COMPLEMENTARIA MENORES

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

Gestión de las reservas alojamiento	**Finalidad:** Registro y gestión de las reservas de alojamiento. **Plazo de conservación:** 3 años, Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos. **Base legítima:** El consentimiento del interesado. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos y Cajas, Fuerzas y Cuerpos de Seguridad y autoridades competentes con la finalidad de cumplir con las obligaciones administrativas y de seguridad establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Gestión de las reservas online alojamiento	**Finalidad:** Registro y gestión de las reservas online de alojamiento. **Plazo de conservación:** 3 años, Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos. **Base legítima:** El consentimiento del interesado. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos y Cajas, Fuerzas y Cuerpos de Seguridad y autoridades competentes con la finalidad de cumplir con las obligaciones administrativas y de seguridad establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Gestión del cumplimiento normativo	**Finalidad:** Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad. **Plazo de conservación:** conservación de las copias de los documentos hasta que prescriban las acciones para reclamarle una posible responsabilidad. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

Nombre y apellidos del tutor legal:	Nombre y apellidos del menor:
DNI:	DNI:

Firma del tutor legal:	

INFORMACIÓN COMPLEMENTARIA PROVEEDORES

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

Uso de aplicaciones de mensajería instantánea	**Finalidad:** Realizar comunicaciones de carácter informativo a través de WhatsApp. **Plazo de conservación:** mientras se mantenga el consentimiento prestado, salvo obligación legal. **Base legítima:** El consentimiento del interesado.
Gestión económica y administrativa	**Finalidad:** Gestión administrativa, facturación, contabilidad y obligaciones legales. **Plazo de conservación:** 5 años en cumplimiento de la ley tributaria y 10 años la documentación fiscal en cumplimiento de la L.O. 7/2012. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos, Cajas y Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones tributarias y fiscales establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Gestión del cumplimiento normativo	**Finalidad:** Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad. **Plazo de conservación:** conservación de las copias de los documentos hasta que prescriban las acciones para reclamarle una posible responsabilidad. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

SERVERA SL informa que con la firma del presente documento otorga el consentimiento explícito para el tratamiento de los datos de las finalidades mencionadas anteriormente.

Nombre y apellidos:
DNI:
Firma:

INFORMACIÓN COMPLEMENTARIA PADRES/TUTORES

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

Uso de aplicaciones de mensajería instantánea	**Finalidad:** Realizar comunicaciones de carácter informativo a través de WhatsApp. **Plazo de conservación:** mientras se mantenga el consentimiento prestado, salvo obligación legal. **Base legítima:** El consentimiento del interesado.
Gestión económica y administrativa	**Finalidad:** Gestión administrativa, facturación, contabilidad y obligaciones legales. **Plazo de conservación:** 5 años en cumplimiento de la ley tributaria y 10 años la documentación fiscal en cumplimiento de la L.O. 7/2012. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos, Cajas y Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones tributarias y fiscales establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Gestión del cumplimiento normativo	**Finalidad:** Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad. **Plazo de conservación:** conservación de las copias de los documentos hasta que prescriban las acciones para reclamarle una posible responsabilidad. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

SERVERA SL informa que con la firma del presente documento otorga el consentimiento explícito para el tratamiento de los datos de las finalidades mencionadas anteriormente.

Nombre y apellidos:
DNI:
Firma:

INFORMACIÓN COMPLEMENTARIA COLABORADORES

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

Gestión económica y administrativa	**Finalidad:** Gestión administrativa, facturación, contabilidad y obligaciones legales. **Plazo de conservación:** 5 años en cumplimiento de la ley tributaria y 10 años la documentación fiscal en cumplimiento de la L.O. 7/2012. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos, Cajas y Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones tributarias y fiscales establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.
Gestión del cumplimiento normativo	**Finalidad:** Gestión y tramitación de las obligaciones y deberes que se deriven del cumplimiento de la normativa a la cual está sujeta la entidad. **Plazo de conservación:** conservación de las copias de los documentos hasta que prescriban las acciones para reclamarle una posible responsabilidad. **Base legítima:** El cumplimiento de una ley. **Cesiones:** sus datos serán comunicados en caso de ser necesario a Organismos y/o administración pública con competencia en la materia con la finalidad de cumplir con las obligaciones establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

INFORMACIÓN COMPLEMENTARIA CANDIDATOS

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

Gestión de RRHH	**Finalidad:** Captación, registro y tratamiento de datos de candidatos para finalidades de selección de personal y gestión, análisis y archivo de los currículos de los candidatos. **Plazo de conservación:** 1 año. **Base legítima:** El interés legítimo.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

3.4.4. Política de privacidad de la página web

POLÍTICA DE PRIVACIDAD DE www.hotelatolon.com

Datos del propietario de la web:

RAZÓN SOCIAL	SERVERA SL
NIF	B07020191
DOMINIO	www.hotelatolon.com
DIRECCIÓN POSTAL	PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS)
DIRECCIÓN ELECTRÓNICA	info@hotelatolon.com
TELÉFONOS	971585433
Nº REGISTRO/ DATOS ADICIONALES	

Protección de datos

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS), y que a continuación se relacionan sus respectivas finalidades, plazos de conservación y bases legitimadoras:

TRATAMIENTOS REALIZADOS	
Gestión de las reservas online alojamiento	**Finalidad**: Registro y gestión de las reservas online de alojamiento **Plazo de conservación:** 3 años, Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos**.** **Base legítima**: El consentimiento del interesado. **Tipología de Datos**: Datos básicos: Nombre y apellidos, Teléfono, NIF, Dirección electrónica, Datos económicos o de seguros

	Datos sensibles: Datos relativos a menores **Cesiones:** sus datos serán comunicados en caso de ser necesario a Agencia Tributaria, Bancos y Cajas, Fuerzas y Cuerpos de Seguridad y autoridades competentes con la finalidad de cumplir con las obligaciones administrativas y de seguridad establecidas en la normativa aplicable. Además, se informa que la base legitimadora de la cesión es el cumplimiento de una ley. el interés legítimo.
Gestión Formulario web	**Finalidad**: Atender sus consultas y/o solicitudes **Plazo de conservación:** mientras se mantenga el consentimiento prestado**.** **Base legítima**: El consentimiento del interesado. **Tipología de Datos**: Datos básicos: Nombre y apellidos, Dirección electrónica, Dirección IP
Gestión usuarios web	**Finalidad**: Captación, registro y tratamiento de datos del usuario **Plazo de conservación:** mientras se mantenga el consentimiento prestado, salvo obligación legal**.** **Base legítima**: El consentimiento del interesado. **Tipología de Datos**: Datos básicos: Nombre y apellidos, Dirección electrónica
Instalación de cookies	**Finalidad**: Gestión e instalación de las cookies **Plazo de conservación:** mientras se mantenga el consentimiento prestado**.** **Base legítima**: El consentimiento del interesado. **Tipología de Datos**: Datos básicos: Dirección electrónica, Dirección IP

Derechos de los interesados

SERVERA SL informa a los Usuarios que, podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad, oposición al tratamiento de sus datos de carácter personal y el derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles, ante el Responsable del Tratamiento, así como a la retirada del consentimiento prestado.

- **Derecho de Acceso**: Es el derecho del usuario a obtener confirmación sobre si se están tratando sus datos y, en tal caso, los concretos datos personales tratados y la información legal del tratamiento (finalidades, base legitimadora, plazos de conservación, cesiones, origen de los datos, etc.).

- **Derecho de Rectificación**: Es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. En relación a la página web, sólo podrá satisfacerse en relación a aquella información que se encuentre bajo el control del sitio web, por ejemplo, eliminar comentarios publicados en la propia página, imágenes o contenidos web donde consten datos de carácter personal del usuario.

- **Derecho a la Limitación de tratamiento**: Es el derecho a que se limiten los fines del tratamiento previstos de forma original por el responsable del tratamiento en determinados supuestos.

- **Derecho de Supresión**: Es el derecho a suprimir los datos de carácter personal del usuario, a excepción de lo previsto en el propio RGPD (libertad de expresión e información, obligaciones de conservación, formulación, ejercicio o defensa de reclamaciones, etc.).

- **Derecho a la Portabilidad**: El derecho a recibir los datos personales que el usuario haya facilitado, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable cuando

el tratamiento está basado en el consentimiento o en la ejecución de un contrato y se efectúe por medios automatizados.

- **Derecho de Oposición**: Es el derecho del usuario a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese el tratamiento de los mismos por parte del sitio web cuando el tratamiento esté basado en el interés legítimo o el interés público o cuando se trate de tratamientos de mercadotecnia directa.

- **Derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles**: Cuando el tratamiento no es necesario para la celebración o ejecución de un contrato, ni está autorizada por el Derecho de la Unión Europea o de los Estados miembros ni se basa en el consentimiento, tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos o le afecte significativamente de modo similar.

- **Derecho a retirar el consentimiento**: Para cualquier tratamiento basado en su consentimiento, tiene derecho a retirarlo, en cualquier momento y de manera gratuita.

Para ejercer cualquiera de los derechos en materia de protección de datos descritos anteriormente deberá seguir las siguientes indicaciones:

- Presentación de un escrito a la dirección PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS) (a la atención de SERVERA SL) o bien a través de correo electrónico a por correo electrónico a info@hotelatolon.com .
- El escrito remitido por el titular de los datos personales (interesado/a) que solicite el ejercicio de derechos deberá tener en cuenta lo siguiente:
    - Deberá identificarse fehacientemente y, en el caso de que concurran dudas sobre la identidad del solicitante, se le solicitará que subsane la petición (p. ej. solicitando más información, como el número de DNI, el documento del DNI, el correo electrónico que aportó, etc.)
    - La solicitud puede realizarla el representante, legal o voluntario, cuando éste esté debidamente identificado y autorizado por el titular de los datos (mediante una autorización expresa del titular para ejercer los derechos personalísimos regulados en la normativa en materia de protección de datos personales).
    - Petición en que se concreta la solicitud (Derecho/s que se pretende/n ejercer). Si no hace referencia a un tratamiento concreto se le facilitará respuesta en relación a todos los tratamientos que afectan a sus datos de carácter personal. Si solicita información de un tratamiento en concreto, sólo la información de éste. Si lo solicita por teléfono se le indicará que lo haga por escrito y se le informará de cómo lo puede hacer y la dirección a la que tiene que enviarlo. Nunca se le dará información por teléfono.
    - Dirección postal o electrónica a efectos de notificaciones.
    - Documentos acreditativos de la petición que formula, en caso de que sean necesarios.
    - La persona solicitante debe utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

Por último, le informamos que tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos en caso de que tenga conocimiento o considere que un hecho pueda suponer un incumplimiento de la normativa aplicable en materia de protección de datos.

SERVERA SL se compromete a adoptar las medidas técnicas y organizativas necesarias, acorde al nivel de riesgos que acompañan los tratamientos realizados por éstas e indicados en el apartado de los términos y condiciones de uso, de forma que garanticen su integridad, confidencialidad y disponibilidad.

Última actualización: 14 de septiembre de 2023

3.4.5. Política de privacidad redes sociales

POLÍTICA DE PRIVACIDAD REDES SOCIALES www.hotelatolon.com

De conformidad con lo establecido en la normativa vigente y aplicable de protección de datos de carácter personal y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), SERVERA SL informa a los usuarios, que ha procedido a crear un perfil en la/s Red/es Social/es Facebook, Instagram, con la finalidad principal de publicitar sus productos y servicios.

Datos de SERVERA SL:

- NIF: B07020191
- DIRECCIÓN: PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS)
- CORREO ELECTRÓNICO: info@hotelatolon.com .

El usuario dispone de un perfil en la misma Red Social y ha decidido unirse a la página creada por SERVERA SL, mostrando así interés en la información que se publicite en la Red. Al unirse a nuestra página, nos facilita su consentimiento para el tratamiento de aquellos datos personales publicados en su perfil.

El usuario puede acceder en todo momento a las políticas de privacidad de la propia Red Social, así como configurar su perfil para garantizar su privacidad.

SERVERA SL tiene acceso y trata aquella información pública del usuario, en especial, su nombre de contacto. Estos datos, sólo son utilizados dentro de la propia Red Social. No son incorporados a ningún sistema de tratamiento.

Derechos de los interesados

En relación a los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, de los que usted dispone y que pueden ser ejercitados ante SERVERA SL, de acuerdo con la RGPD, debe tener en cuenta los siguientes matices:

- Derecho de Acceso: Es el derecho del usuario a obtener información sobre sus datos concretos de carácter personal y del tratamiento que se haya realizado o realice, así como de la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.
- Derecho de Rectificación: Es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. Sólo podrá satisfacerse en relación a aquella información que se encuentre bajo el control de SERVERA SL, por ejemplo, eliminar comentarios publicados en la propia página, imágenes o contenidos web donde consten datos de carácter personal del usuario.
- Derecho a la Limitación de tratamiento: Es el derecho a que se limiten los fines del tratamiento previstos de forma original por el responsable del tratamiento.
- Derecho de Supresión: Es el derecho a suprimir los datos de carácter personal del usuario, a excepción de lo previsto en el propio RGPD o en otras normativas aplicables que determinen la obligatoriedad de la conservación de los mismos, en tiempo y forma.
- Derecho de portabilidad: El derecho a recibir los datos personales que el usuario, haya facilitado, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable.

- Derecho de Oposición: Es el derecho del usuario a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese el tratamiento de los mismos por parte de SERVERA SL.

SERVERA SL realizará las siguientes actuaciones:

- Acceso a la información pública del perfil.
- Publicación en el perfil del usuario de toda aquella información ya publicada en la página de SERVERA SL.
- Enviar mensajes personales e individuales a través de los canales de la Red Social.
- Actualizaciones del estado de la página que se publicarán en el perfil del usuario.

El usuario siempre puede controlar sus conexiones, eliminar los contenidos que dejen de interesarle y restringir con quién comparte sus conexiones, para ello deberá acceder a su configuración de privacidad.

Publicaciones

El usuario, una vez unido a la página de SERVERA SL, podrá publicar en ésta última comentarios, enlaces, imágenes o fotografías o cualquier otro tipo de contenido multimedia soportado por la Red Social. El usuario, en todos los casos, debe ser el titular de los mismos, gozar de los derechos de autor y de propiedad intelectual o contar con el consentimiento de los terceros afectados. Se prohíbe expresamente cualquier publicación en la página, ya sean textos, gráficos, fotografías, vídeos, etc. que atenten o sean susceptibles de atentar contra la moral, la ética, el buen gusto o el decoro, y/o que infrinjan, violen o quebranten los derechos de propiedad intelectual o industrial, el derecho a la imagen o la Ley. En estos casos, SERVERA SL se reserva el derecho a retirar de inmediato el contenido, pudiendo solicitar el bloqueo permanente del usuario.

SERVERA SL no se hará responsable de los contenidos que libremente ha publicado un usuario.

El usuario debe tener presente que sus publicaciones serán conocidas por los otros usuarios, por lo que él mismo es el principal responsable de su privacidad.

Las imágenes que puedan publicarse en la página no serán almacenadas en ningún sistema de tratamiento por parte de SERVERA SL, pero sí que permanecerán en la Red Social.

Concursos y promociones

SERVERA SL se reserva el derecho a realizar concursos y promociones, en los que podrá participar el usuario unido a su página. Las bases de cada uno de ellos, cuando se utilice para ello la plataforma de la Red Social, serán publicadas en la misma. Cumpliendo siempre con la LSSI-CE y con cualquier otra norma que le sea de aplicación.

La Red Social no patrocina, avala ni administra, de modo alguno, ninguna de nuestras promociones, ni está asociada a ninguna de ellas.

Publicidad

SERVERA SL utilizará la Red Social para publicitar sus productos y servicios, en todo caso, si decide tratar sus datos de contacto para realizar acciones directas de prospección comercial, será siempre, cumpliendo con las exigencias legales de la normativa en materia de protección de datos y de la LSSI-CE.

No se considerará publicidad el hecho de recomendar a otros usuarios la página de SERVERA SL para que también ellos puedan disfrutar de las promociones o estar informados de su actividad.

A continuación, detallamos el enlace a la política de privacidad de la Red Social:

- Facebook: https://es-es.facebook.com/privacy/explanation
- Instagram: http://instagram.com/about/legal/privacy/

Última actualización: 14 de septiembre de 2023

3.5. VIDEOVIGILANCIA

Según lo estipulado en la normativa vigente y aplicable en protección de datos, se consideran datos personales toda información sobre una persona física identificada o identificable (el interesado) entendiendo como persona física a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador.

Las imágenes, consideradas información gráfica o fotográfica, se establecen como un dato de carácter personal en virtud de la normativa aplicable y vigente en protección de datos. Por tanto, la captación y en su caso la grabación, de información personal en forma de imágenes cuando su uso afecta a personas identificadas o identificables, se considera un dato de carácter personal.

Las entidades podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como las de sus instalaciones.

Asimismo, el tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia. Asimismo, el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar quedará exceptuado y se regirá por las disposiciones correspondientes.

En consecuencia, la utilización de videocámaras y cámaras o cualquier otro medio técnico análogo para fines de vigilancia repercute sobre las libertades y derechos fundamentales de las personas, siendo obligatorio fijar unas garantías.

En lo que respecta a los derechos de las personas trabajadoras, la instalación de las cámaras de videovigilancia en los centros de trabajo respetará siempre el derecho a la propia imagen, así como la intimidad de las personas trabajadoras, aunque el tratamiento se limitará a las finalidades previstas por el Estatuto de los Trabajadores, y/o en todo caso a finalidades legítimas reconocidas por la normativa vigente y aplicable.

Las entidades podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de las personas trabajadoras previstas en el artículo 20.3 del Estatuto de los Trabajadores, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Las entidades deberán de informar con carácter previo, y de forma expresa, clara y concisa, a las personas trabajadoras y, en su caso, a sus representantes, acerca de esta medida.

En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de las personas trabajadoras, tales como vestuarios, aseos, comedores y análogos.

La utilización de sistemas similares para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y adoptando las garantías oportunas. La supresión de los sonidos conservados por estos sistemas de grabación se realizará en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

El Responsable o Encargado del Tratamiento deberá respetar los siguientes principios cuando trate datos con fines de videovigilancia:

- Debe existir una relación de proporcionalidad entre la finalidad perseguida, que en todo caso deberá ser legítima, y el modo en el que se traten los datos.
- Debe informarse sobre la captación y/o grabación de las imágenes.
- La instalación de cámaras o videocámaras sólo es admisible cuando no exista un medio menos

invasivo u intrusivo a la intimidad de las personas.

- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos. Asimismo, podrían tomarse imágenes parciales y limitadas de vías públicas cuando resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.
- En cualquier caso, el uso de sistemas de videovigilancia deberá ser respetuoso con los derechos de las personas y el resto del ordenamiento jurídico.
- Las imágenes serán suprimidas en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.
- Debe adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Asimismo, cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

Las especiales características que se dan en la videovigilancia comportan el diseño de procedimientos específicos para informar a las personas cuyas imágenes se capten. Se debe colocar, al menos, un distintivo informativo ubicado en las zonas de videovigilancia, en un lugar suficientemente visible, tanto en espacios abiertos como cerrados. Para cumplir con el deber de información, el distintivo informativo debe identificar:

- La existencia del tratamiento.
- La identidad de los responsables.
- Posibilidad de ejercitar los derechos en materia de Protección de Datos.

También podrá incluirse en el distintivo informativo un código de conexión o dirección de internet a esta información.

Por otro lado, el Responsable del Tratamiento deberá disponer de un impreso con toda la información necesaria para cumplir con el deber de información y transparencia.

3.6. POLÍTICA DE COOKIES

Debe tenerse en cuenta que, la utilización de las cookies en los equipos terminales de los usuarios tiene implicaciones relevantes en relación con la protección de datos. Y es que, mediante la utilización de cookies las entidades obtienen datos relacionados con los usuarios que posteriormente podrán ser utilizados. Es por ello, que se determina la necesidad de informar al usuario de la utilización de cookies para que conozcan el tratamiento de datos llevado a cabo.

SERVERA SL debe realizar un análisis exhaustivo de las Cookies que, a través de su página web, pueden ser instaladas en los dispositivos informáticos de los usuarios. Conocida la finalidad de las mismas, SERVERA SL debe cumplir con la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE), la normativa en materia de protección de datos y con las recomendaciones que la Agencia Española de Protección de Datos ha publicado en su Guía sobre el uso de Cookies.

Es necesario determinar que, quedan exceptuadas de la presente política las cookies utilizadas para las siguientes finalidades:

- Permitir únicamente la comunicación entre el equipo del usuario y la red.
- Estrictamente prestar un servicio expresamente solicitado por el usuario.

Es importante decir que, SERVERA SL podrá utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización.

La información relativa a las cookies debe mostrarse siguiendo los siguientes requisitos:

- La información o la comunicación debe ser concisa, transparente e inteligible.
- Se ha de utilizar un lenguaje claro y sencillo, evitando el uso de frases que induzcan a confusión o desvirtúen la claridad del mensaje.
- La información ha de ser de fácil acceso.

Se recomienda el uso de avisos de privacidad por niveles, es decir, que contengan la información en capas, de modo que se permita al usuario ir a aquellos aspectos del aviso que sean de mayor interés para él, evitando así la fatiga informativa, y ello sin perjuicio de que la totalidad de la información se encuentre disponible en un único lugar o en un documento completo al que se pueda acceder fácilmente si el interesado desea consultarlo en su totalidad.

SERVERA SL realizará de forma periódica la revisión de los posibles cambios que pudieran producirse en la gestión y uso de cookies con la finalidad de actualizar la información mostrada a los usuarios relativa a las cookies.

3.6.1. Información previa a la política de cookies

La información sobre las cookies facilitada en el momento de solicitar el consentimiento debe ser suficientemente completa para permitir a los usuarios entender sus finalidades y el uso que se les dará.

En la información previa se deberá incluir la siguiente información:

- Identificación del responsable del sitio web.
- Identificación de las finalidades de las cookies que se utilizarán.
- Información sobre si las cookies son propias o de terceros.
- Información genérica sobre el tipo de datos que se van a tratar en caso de que se elaboren perfiles.
- Modo en el que el usuario puede aceptar, configurar y rechazar la utilización de cookies.
- Un enlace claramente visible dirigido a la información complementaria y más detallada (política de cookies).

Esta información se facilitará antes del uso de las cookies a través de un formato que sea visible para el usuario y que deberá mantenerse hasta que el usuario preste el consentimiento o lo rechace.

Será necesario que la información de la primera capa se complete con un sistema o panel de configuración en el que el usuario pueda optar entre aceptar o no las cookies de forma granular.

En este sentido, a continuación le facilitamos aquella información que SERVERA SL debe escoger e insertar en su página web, dependiendo de las Cookies que disponga, mediante una barra de encabezamiento o una ventana emergente:

INFORMACIÓN PREVIA - POLÍTICA DE COOKIES

Utilización de cookies propias técnicas

Este sitio web utiliza Cookies propias para recopilar información con la finalidad técnica, no se recaban ni ceden sus datos de carácter personal sin su consentimiento.

Asimismo, se informa que este sitio web dispone de enlaces a sitios web de terceros con políticas de privacidad ajenas a SERVERA SL.

ACEPTAR MÁS INFO

Utilización de cookies propias y de terceros técnicas

Este sitio web utiliza Cookies propias y de terceros para recopilar información con la finalidad técnica, no se recaban ni ceden sus datos de carácter personal sin su consentimiento.

Asimismo, se informa que este sitio web dispone de enlaces a sitios web de terceros con políticas de privacidad ajenas a SERVERA SL.

ACEPTAR MÁS INFO

Al pulsar **MÁS INFO**, se deberá dirigir al usuario al apartado 2. *Política de cookies* y no deberá existir un panel de configuración, ya que estas se instalarán para el correcto funcionamiento de la página.

Utilización de cookies propias y de publicidad comportamental

Este sitio web utiliza Cookies propias para recopilar información con la finalidad de mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias en base a un perfil elaborado a partir de sus hábitos de navegación. El usuario tiene la posibilidad de obtener más información y configurar sus preferencias AQUÍ.

Necesarias por motivos técnicos ☑ Publicidad ☐

ACEPTAR TODO RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias, terceros y de publicidad comportamental

Este sitio web utiliza Cookies propias y de terceros, para recopilar información con la finalidad de mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias, en base a un perfil elaborado a partir de sus hábitos de navegación. El usuario tiene la posibilidad de obtener más información y configurar sus preferencias AQUI.

Necesarias por motivos técnicos ☑ Publicidad ☐

ACEPTAR TODO RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias, terceros, publicidad y análisis

Este sitio web utiliza Cookies propias y de terceros, para recopilar información con la finalidad de mejorar nuestros servicios, para mostrarle publicidad relacionada con sus preferencias, así como analizar sus hábitos de navegación. El usuario tiene la posibilidad de obtener más información y configurar sus preferencias AQUÍ.

Necesarias por motivos técnicos ☑ Publicidad ☐

Análisis ☐

ACEPTAR TODO RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias técnicas y de análisis

Este sitio web utiliza Cookies propias para recopilar información con la finalidad de mejorar nuestros servicios y así como el análisis de sus hábitos de navegación. El usuario tiene la posibilidad de configurar sus preferencias AQUI.

Necesarias por motivos técnicos ☑ Análisis ☐

ACEPTAR TODO RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias, terceros, técnicas y de análisis

Este sitio web utiliza Cookies propias y de terceros para recopilar información con la finalidad de mejorar nuestros servicios y así como el análisis de sus hábitos de navegación. El usuario tiene la posibilidad de configurar sus preferencias AQUI.

Necesarias por motivos técnicos ☑ Análisis ☐

ACEPTAR TODO RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias, terceros y de análisis, dirigidas a usuarios menores de 14 años

Si tienes menos de 14 años, pide a tu padre, madre o tutor que lea este mensaje.

Utilizamos cookies propias y de terceros para saber cómo utilizas nuestro sitio web y hacer estadísticas. Más información.

Tu padre, madre o tutor puede pulsar “aceptar” si consiente que utilicemos todas las cookies, o configurarlas o rechazar su uso AQUÍ.

ACEPTAR

PANEL DE CONFIGURACIÓN

Cuando se pulse Configuración personalizada o **AQUÍ**, se deberá insertar un link que se dirija a un panel de configuración en el que el usuario pueda optar entre aceptar o no las cookies de forma granular:

SERVERA SL informa al usuario de que tiene la posibilidad de configurar sus preferencias en referencia a la instalación de cookies:

Utilización de cookies propias de publicidad comportamental o utilización de cookies propias y de terceros de publicidad comportamental

Puede habilitar y deshabilitar las cookies según sus finalidades:

- **Técnicas**: son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan. — Aceptar — Rechazar
- **Publicidad comportamental:** son aquellas que almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo. — Aceptar — Rechazar

ACEPTAR TODO — RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias de análisis o utilización de cookies propias y de terceros de análisis

Puede habilitar y deshabilitar las cookies según sus finalidades:

- **Técnicas**: son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan. — Aceptar — Rechazar
- **Analíticas**: son aquellas que permiten al responsable de las mismas el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. — Aceptar — Rechazar

ACEPTAR TODO — RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Utilización de cookies propias, terceros de análisis y publicidad comportamental

Puede habilitar y deshabilitar las cookies según sus finalidades:

• **Técnicas**: son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan.	Aceptar	Rechazar
• **Analíticas**: son aquellas que permiten al responsable de las mismas el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas.	Aceptar	Rechazar
• **Publicidad comportamental:** son aquellas que almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.	Aceptar	Rechazar

ACEPTAR TODO RECHAZAR TODO

GUARDAR CONFIGURACIÓN

Al pulsar “ACEPTAR TODO” se aceptará la instalación de todas las cookies y al pulsar “RECHAZAR TODO” se rechazarán todas las cookies.

Al pulsar “GUARDAR CONFIGURACIÓN”, se guardará la selección de cookies que el usuario haya realizado. Si no se ha seleccionado ninguna opción, pulsar este botón equivaldrá a rechazar todas las cookies.

Por último, recuerde que debe actualizar la tabla del documento Política de cookies, indicando las Cookies que su página web instala con la navegación por parte del usuario.

3.6.2. Política de cookies

SERVERA SL deberá facilitar a los usuarios información clara y completa sobre la utilización de cookies y, en particular, sobre los fines del tratamiento de los datos.

En la política de cookies se deberá facilitar al usuario la siguiente información:

- Definición y función genérica de las cookies.
- Información sobre el tipo de cookies que se utilizan y su finalidad.
- Identificación de quien utiliza las cookies.
- Información sobre la forma de aceptar, denegar o revocar el consentimiento para el uso de cookies.
- En su caso, información sobre las transferencias de datos a terceros países realizadas por el editor.
- En caso de que sea oportuno, informar sobre la elaboración de perfiles.
- Periodo de conservación de los datos personales o criterios utilizados para determinar el plazo de conservación.

A continuación SERVERA SL, establece la política de cookies la cual deberá estar accesible para los usuarios de la página web:

POLÍTICA DE COOKIES

Conforme a lo dispuesto en el artículo 22.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) vigente, SERVERA SL debe cumplir con la obligación de informar sobre las cookies que utiliza y sus finalidades.

Este sitio web utiliza cookies y/o tecnologías similares que almacenan y recuperan información cuando navegas. Las cookies permiten a una página web, entre otras cosas, almacenar y recuperar información sobre los hábitos de navegación de un Usuario o de su equipo y, dependiendo de la información que contenga y de la forma en que utilice su equipo, pueden utilizarse para reconocer al Usuario.

Las cookies son esenciales para el funcionamiento de internet, aportando innumerables ventajas en la prestación de servicios interactivos, facilitándole al Usuario la navegación y usabilidad de nuestra web.

El usuario puede modificar la configuración personalizada AQUÍ.

La información que le proporcionamos a continuación le ayudará a comprender los diferentes tipos de cookies:

TIPOS DE COOKIES		
SEGÚN LA ENTIDAD QUE LAS GESTIONE	COOKIES PROPIAS	Son aquellas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario
	COOKIES DE TERCERO	Son aquellas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos a través de las cookies.
SEGÚN EL PLAZO DE TIEMPO QUE PERMANEZCAN ACTIVADAS	COOKIES DE SESIÓN	Son aquellas diseñadas para recabar y almacenar datos mientras el usuario accede a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (por ejemplo, una lista de productos adquiridos) y desaparecen al terminar la sesión
	COOKIES PERSISTENTES	Son aquellas en las que los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.
SEGÚN SU FINALIDAD	COOKIES TÉCNICAS	Son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan
	COOKIES DE PERSONALIZACIÓN	Permiten aplicar características propias para la navegación del usuario por el website (Ej. idioma).
	COOKIES DE ANÁLISIS	Son aquellas que permiten al responsable de estas el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están

		vinculadas, incluida la cuantificación de los impactos de los anuncios. La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.
	COOKIES PUBLICITARIAS	Permiten al editor incluir en la página web espacios publicitarios, según el contenido de la propia web.
	COOKIES DE PUBLICIDAD COMPORTAMENTAL	Son aquellas que almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.

Adicionalmente, SERVERA SL informa de manera más detallada de las cookies que utiliza sus titulares, el uso o finalidad concreta, los plazos de conservación, así como de las posibles Transferencias Internacionales de datos de cada una de ellas utilizadas en nuestra página web:

COOKIES PROPIAS				
Tipo	**Titular**	**Cookie**	**Finalidad**	**Conservación**
Técnicas				
Personalización				
Análisis				
Publicidad/ Publicidad comportamental				

COOKIES DE TERCEROS				
Tipo	**Titular**	**Cookie**	**Finalidad**	**Conservación**
Técnicas				
Personalización				
Análisis				
Publicidad/ Publicidad comportamental				

Puede informarse de las transferencias internacionales a terceros países que, en su caso, realizan los TERCEROS, identificados en esta política de cookies, en sus correspondientes políticas (hacer click encima del titular de la cookie).

SERVERA SL informa de manera más exhaustiva la información relativa a las transferencias internacionales derivadas de la utilización de cookies propias:

TRANSFERENCIAS INTERNACIONALES			
Titular	**Cookie**	**País de la transferencia**	**Régimen aplicado**

Téngase en cuenta que, si acepta las cookies de terceros, deberá eliminarlas desde las opciones del navegador o desde el sistema ofrecido por el propio tercero.

A continuación, le proporcionamos los enlaces de diversos navegadores, a través de los cuales podrá modificar la configuración de su navegador sobre el uso de cookies:

- **Firefox*:*** *http://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-que-los-sitios-we*
- **Chrome*:*** *http://support.google.com/chrome/bin/answer.py?hl=es&answer=95647*
- **Internet Explorer*:*** *http://windows.microsoft.com/es-es/internet-explorer/delete-manage-cookies#ie=ie-10*
- **Microsoft Edge**: https://support.microsoft.com/es-es/microsoft-edge/eliminar-las-cookies-en-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09
- **Safari*:*** *https://support.apple.com/kb/ph17191?locale=es_ES*

- **Opera*:*** *https://help.opera.com/en/latest/web-preferences/#cookies*

Para conocer más información sobre el tratamiento de datos personales, le recomendamos visitar nuestro apartado "*Política de Privacidad*".

Última actualización: 14 de septiembre de 2023

3.7 GESTIÓN DEL CANAL ÉTICO

Un Canal Ético (o canal de Denuncias) es un sistema interno de comunicación, que la organización pone a disposición de las personas trabajadoras y de los terceros con los que mantiene relaciones profesionales y/o comerciales para que puedan informar sobre incumplimientos o irregularidades de los que hayan tenido conocimiento y que contravengan la normativa vigente y aplicable a la organización, el SGC y sus políticas y/o procedimientos.

El establecimiento de un Canal Ético en la organización es un elemento fundamental para la eficacia del Sistema de Gestión de Compliance, ya que permite prevenir, detectar y actuar contra aquellas conductas que puedan suponer la materialización de incumplimientos e infracciones.

Es por ello, que SERVERA SL en el marco de su Sistema de Gestión de Compliance implementará un Canal Ético, así como su protocolo de funcionamiento y las pautas de actuación en caso de materialización de una infracción de la normativa tanto interna como externa aplicable a la organización.

Es necesario que tanto en la recepción de comunicaciones a través del Canal Ético, como en caso de materialización de una infracción se sigan los procedimientos y operativas que se establecen a continuación para asegurar que se garantizan todos los derechos de las personas implicadas y a la vez la entidad recaba todas las evidencias de su buen proceder.

3.7.1. Protocolo de funcionamiento del Canal Ético

1. Introducción

SERVERA SL, en el marco de la correcta implementación del Sistema de Gestión de Compliance deberá instaurar y trasladar los principios generales de actuación, los valores éticos de comportamiento y las políticas y procedimientos, todos ellos de obligado cumplimiento, a todos los integrantes de la entidad sin excepción, así como a los terceros con los que se relaciona en el desarrollo de su actividad profesional.

Además, SERVERA SL dotará a la organización de las estructuras de Compliance correspondientes para la eficaz implementación del SGC y dar cumplimiento a las distintas funciones y responsabilidades que se desprenden del mismo.

SERVERA SL, en el marco de lo anterior, y teniendo en cuenta que los Sistemas de Compliance deben posibilitar la detección de conductas contrarias a los principios generales de actuación y a los valores éticos establecidos en el mismo SGC, deberá implementar los procedimientos adecuados para el establecimiento, funcionamiento y gestión de un Canal Ético.

El Canal Ético de SERVERA SL será el mecanismo eficaz y de confianza para la comunicación interna de circunstancias que puedan suponer la materialización de incumplimientos del propio SGC, de las políticas y procedimientos que lo integran, de los principios y valores que de él se desprenden, así como de la normativa a la que pretende dar cobertura.

Así pues, a continuación se establecen al detalle el contenido de Canal Ético de SERVERA SL fijando el procedimiento de comunicación y gestión de las comunicaciones, así como, la provisión y protección de los derechos y garantías de todos los sujetos intervinientes en el proceso.

2. Objeto de las comunicaciones

La función fundamental del establecimiento de un Canal Ético en SERVERA SL es la recepción de comunicaciones de buena fe y sobre la base de indicios razonables sobre aquellas circunstancias, hechos o comportamientos que puedan suponer la materialización de infracciones, irregularidades, incumplimientos o debilidades del SGC, de cualquiera de sus políticas y procedimientos y/o de la normativa a la que pretende dar cobertura el mismo así como aquellos que puedan suponer la materialización de un incumplimiento normativo en la entidad.

Se entiende que una comunicación es de buena fe cuando quien la realiza tiene motivos razonables, para creer, en base de la información de la que disponga en el momento de la denuncia, que los hechos que comunica son ciertos.

Se entiende por infracción, irregularidad o incumplimiento:

- Los actos u omisiones reales o potenciales, que ya hayan ocurrido o que muy probablemente puedan ocurrir.

- Los actos u omisiones que la persona denunciante tenga motivos o indicios para considerar infracciones.

- El intento de ocultar infracciones, irregularidades o incumplimientos, se considerará una infracción en sí misma.

Tendrán consideración de infracción, irregularidad o incumplimiento las conductas anteriores independientemente de si perjudican a la organización, a sus miembros, a terceras personas o a las administraciones públicas.

3. Comunicaciones no sujetas al Canal Ético

Aquella información que esté completamente disponible al público, rumores y habladurías no confirmadas no se considerarán infracciones o irregularidades susceptibles de comunicación a través del Canal Ético.

Tampoco lo serán aquellas reclamaciones interpersonales que afecten solamente a la persona comunicante, como pueden ser los conflictos interpersonales entre el denunciante y otros miembros de la organización así como cualquier otra duda, queja o consulta sobre su situación laboral que deberán ser encauzadas por los procedimientos correspondientes distintos al Canal Ético.

Las comunicaciones de mala fe, falsas o malintencionadas podrán dar lugar a las correspondientes sanciones, sin perjuicio de las responsabilidades civiles e incluso penales que puedan derivarse según la normativa vigente y aplicable.

4. Mecanismos de comunicación

SERVERA SL podrá habilitar los siguientes medios para instrumentar las comunicaciones mencionadas anteriormente:

- Correo electrónico específico: info@hotelatolon.com
- Formularios específicos según el tipo de comunicación que la organización pondrá a disposición de las personas interesadas y una vez cumplimentados deberán ser entregados al Compliance Officer (Véase *Modelo de comunicación de indicio o sospecha de incumplimiento*).
- Formulario web habilitado en la sede electrónica de la organización.

  El Formulario web Canal Ético deberá estar disponible en un apartado visible y de fácil acceso en la página web. Deberá quedar introducido por la finalidad y procedimiento que seguirá la comunicación así como contener la cláusula de protección de datos correspondiente por si el comunicante se identifica.

  Asimismo, deberá permitir incluir los datos personales de quien realiza la comunicación por si la persona comunicante quiere identificarse, posibilitar a la misma trasladar cuál es su relación con la entidad y los hechos que quiere notificar, entre otros, datos de las personas involucradas, fechas, relación de los hechos, etc. (véase ejemplo en el documento *Formulario web – Canal Ético).*

SERVERA SL permite realizar tanto de forma anónima como confidencial las comunicaciones sobre posibles infracciones normativas y del SGC y sus medidas, políticas y procedimientos. Es por ello que se establecen las siguientes medidas para instrumentar las comunicaciones de forma anónima:

- Habilitar un buzón ético o de denuncias en la organización donde depositar la comunicación.
- Enviar la comunicación mediante correo postal a la atención del Compliance Officer a la dirección de la organización (PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS)).

En caso de que no utilice el *Modelo de comunicación de indicio o sospecha de incumplimiento* la información mínima que deberá trasladar es la siguiente:

- Fecha del día que se presenta la comunicación.
- Hechos objeto de denuncia:

- Datos de la persona o personas involucradas en los hechos.
- Fecha de los hechos denunciados.
- Relación de los hechos a denunciar.

En todo caso, tanto si se realiza la comunicación de forma anónima como confidencial, en el momento de realizar la comunicación se deberán aportar los medios de prueba de los que se disponga para acreditar los hechos comunicados.

Por último, aquellas comunicaciones realizadas a través de un medio distinto a los anteriores se tendrán por no efectuadas.

5. Destinatarios del Canal Ético

La utilización del Canal Ético está destinado a los miembros que integran la organización, eso es, las personas trabajadoras, los miembros del órgano de gobierno, las personas propietarias de la organización así como las personas voluntarias y aquellas en prácticas, si las hubiere, con independencia de su modalidad contractual, posición que ocupen o el ámbito geográfico en el que desempeñen su trabajo.

Asimismo, el uso del Canal Ético también está reservado a aquellos terceros, personas físicas o jurídicas, con las que se relaciona la organización en su actividad profesional, entre ellos: clientes, prestadores de servicio, proveedores, contratistas, asesores, subcontratistas y personal, miembros o cargos de las administraciones públicas además de cualquier persona que trabaje bajo la supervisión y dirección de las anteriores.

Finalmente, el Canal Ético también está orientado a aquellas personas cuya relación laboral o profesional con la organización no ha comenzado, pero que han tratado con la misma mediante procesos de selección o de negociación precontractual.

6. Gestión

La gestión del Canal Ético corresponde al Compliance Officer de SERVERA SL.

6.1. Recepción

Las comunicaciones se recibirán a través de cualquier de los canales que la organización haya establecido.

El Compliance Officer, independientemente del canal utilizado, realizará un estudio preliminar de la comunicación para que se le dé el cauce correspondiente:

1. Si la comunicación sí revela una infracción o irregularidad relacionada con el Sistema de Gestión de Compliance o con el cumplimiento normativo dentro de la entidad, se gestionará con lo establecido en el presente Protocolo.
2. Si la comunicación revela una irregularidad no relacionada con el Sistema de Gestión de Compliance o con el cumplimiento normativo dentro de la entidad, la misma será remitida al órgano, área o persona de SERVERA SL correspondiente para que le dé el cauce correspondiente.
3. Si la comunicación no revela ninguna infracción o irregularidad en ninguna materia o es totalmente infundada, ésta será archivada y desestimada, dando por finalizada la tramitación de la misma.
4. Si la comunicación es relativa a una incidencia o violación de la seguridad de los datos se gestionará de acuerdo con lo establecido en el apartado *3.7. Gestión de incidencias y violaciones de seguridad de los datos del presente documento.*

5. Si la comunicación es relativa a un ejercicio de derechos en materia de protección de datos se gestionará de acuerdo con lo establecido en el apartado *3.8. Gestión de derechos de los interesados del presente documento.*

En todo caso, si la comunicación recibida a través del Canal Ético, independientemente del medio utilizado, se trata de una de las tres primeras, será registrada de acuerdo con el *Modelo de resolución ante la comunicación de indicio o sospecha de infracción* juntamente con su número de referencia con la finalidad de poder identificarla a lo largo de toda su gestión para iniciar los pasos que se detallan a continuación:

En un plazo no superior a siete días naturales de la recepción de la comunicación, se trasladará acuse de recibo al comunicante confirmando la recepción de la misma; informándole de sus derechos en materia de protección de datos, en caso de que no se haya realizado previamente; e indicándole, siempre de forma justificada, si se continuará la tramitación mediante el Protocolo de funcionamiento del Canal Ético, si se remitirá a otro órgano, área o persona de SERVERA SL porque la comunicación no está relacionada con el SGC o si, por el contrario, la comunicación es desestimada por no considerarse una infracción.

considere que puede estar sujeto a un conflicto de interés, lo pondrá en conocimiento del órgano de gobierno y se abstendrá de participar en la gestión de la comunicación.

En función de la gravedad de los hechos comunicados y de los sujetos de la organización implicados, el Compliance Officer valorará la conveniencia de informar al órgano de gobierno de SERVERA SL sobre los mismos.

6.2. Tramitación

Si se ha determinado que la comunicación debe seguir la vía establecida en el presente Protocolo se iniciará la investigación de los hechos trasladados en la denuncia con la finalidad de comprobar la veracidad y exactitud de los mismos.

Durante la fase de investigación, si se estima oportuno, se adoptarán las medidas cautelares necesarias para evitar la reiteración de los hechos denunciados mientras tiene lugar la investigación, así como para asegurar los medios probatorios.

Para ello, en esta fase de investigación, si se considera necesario, se podrá solicitar información adicional a la persona que ha realizado la comunicación y, si se considera oportuno, entrevistarse con la misma.

En relación con la persona o personas denunciadas, se les informará de la existencia de la denuncia al inicio de la fase de investigación. En casos excepcionales, cuando exista riesgo de que tal comunicación ponga en peligro la propia investigación, la notificación al denunciado podrá retrasarse mientras exista dicho riesgo.

Asimismo, se comunicarán al denunciado los hechos objeto de investigación y se le invitará a que exponga su versión completa de los mismos, dándole la posibilidad de aportar los medios de prueba pertinentes, sin perjuicio de la posibilidad de que presente alegaciones por escrito. Finalmente, se le informará sobre el tratamiento de sus datos personales en relación con la comunicación.

Del mismo modo, podrán entrevistarse a los testigos y/o las personas afectadas por el contenido de la comunicación. En este sentido, todos los miembros de SERVERA SL deberán colaborar lealmente en las investigaciones con la debida reserva, discreción y confidencialidad sobre la información trasladada. Igualmente, se procederá a informar a los mismos sobre sus derechos en materia de protección de datos.

La fase de investigación no podrá ser, salvo casos excepcionales, debido a la complejidad de la misma o el número de personas implicadas, superior a tres meses. Asimismo, si los hechos comunicados revisten de especial gravedad se dará la celeridad oportuna a la comunicación.

De todas las actuaciones que forman parte de la investigación se levantará acta escrita.

El denunciante de buena fe tendrá derecho, en cualquier momento, a estar informado del estado de la tramitación de su denuncia.

Asimismo, durante todo el proceso de gestión y tramitación de la comunicación, especialmente en la fase de investigación, se garantizará, en todo momento, el derecho a la intimidad, a la defensa y a la presunción de inocencia de las personas investigadas.

7. Garantías del procedimiento

SERVERA SL garantiza la confidencialidad o el anonimato, según corresponda, de las personas que hagan uso del Canal Ético además de una gestión de todos los datos de carácter personal de los intervinientes en el procedimiento de acuerdo con la normativa vigente y aplicable en materia de protección de datos.

Asimismo, la organización prohíbe cualquier tipo de represalia contra aquellas personas que realicen comunicaciones de buena fe y sobre la base de indicios razonables a través del Canal Ético.

7.1. Confidencialidad

La identidad de las personas que realizan la comunicación no será divulgada ni, en su caso, la de las personas cuya conducta o actuación pudiera ser mencionada en las mismas. Además, tampoco se permitirá el acceso a la información de las comunicaciones por parte de personas no autorizadas. No obstante, el acceso a dichas información será lícito por parte de personas distintas a las que reciben y realizan su seguimiento cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procesos judiciales que, en su caso, puedan proceder.

Para asegurar el cumplimiento de lo anterior, las personas que gestionen el Canal Ético o en su caso puedan tener conocimiento del contenido de las comunicaciones, estarán sujetas a un compromiso de confidencialidad.

La confidencialidad de la comunicación y de su procedimiento solamente podrá cesar en aquellos casos que sea requerido por la autoridad competente y/o exista una obligación necesaria y proporcionada.

La organización garantizará el que el acceso al contenido de las comunicaciones y de su investigación así como el almacenamiento de la información se realiza de forma segura y diligente.

7.2. Protección de datos

Los datos de la persona que realice la comunicación y de las personas involucradas en los hechos trasladados serán tratados de acuerdo con la normativa vigente y aplicable en materia de protección de datos.

El acceso a los datos contenidos en el sistema de gestión del Canal Ético quedará limitado exclusivamente a quienes desarrollen las funciones de control interno y de cumplimiento, o a los encargados de tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Los datos personales serán conservados en el sistema únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos trasladados.

En todo caso, transcurridos tres meses desde la introducción de los datos, la organización procederá a su supresión del sistema, salvo que la finalidad de conservación sea dejar evidencia del funcionamiento eficaz del Canal Ético y del Sistema de Gestión de Compliance de la organización. Los datos de las comunicaciones que hayan sido archivadas solamente podrán constar de forma anonimizada.

Asimismo, SERVERA SL no recopilará datos personales cuya pertinencia no resulte manifiesta para tratar una denuncia específica, si se recopilan por accidente, se eliminarán sin dilación indebida.

7.3. No represalias

SERVERA SL asegura la inexistencia de represalias contra las personas denunciantes que de buena fe hubieran comunicado a través del Canal Ético alguna infracción e irregularidad.

Así pues, quedará prohibido cualquier trato desfavorable causado por una acción u omisión que se produzca en el contexto laboral o contractual y que cause un perjuicio no justificado al comunicante de una infracción.

Por lo tanto, queda prohibida cualquier acción disciplinaria o despido a los miembros profesionales de la organización que realicen una comunicación a través del Canal Ético.

Asimismo, las situaciones de discriminación, acoso o amenaza por el hecho de haber realizado una comunicación serán sancionadas debidamente por la organización.

8. Conclusión y respuesta del procedimiento

Una vez concluida la fase de investigación de los hechos se procederá a la apertura de la fase de conclusión y respuesta.

Si de la fase de investigación se constata la comisión de una infracción, el Compliance Officer elaborará un informe, que será trasladado al órgano de gobierno, con:

- Los hechos objeto de investigación.
- Las posibles vulneraciones del Sistema de Gestión de Compliance y/o de sus políticas y procedimientos.
- Explicación detallada de las acciones de investigación llevas a cabo.
- Propuesta de resolución.
- Medidas a adoptar en caso de incumplimientos e irregularidades que variarán en función de la severidad del caso, pudiendo incluir la adopción de medidas disciplinarias establecidas en el Sistema Disciplinario, que pueden ir desde la amonestación hasta el despido disciplinario; las medidas para evitar que los hechos vuelvan a ocurrir y; en su caso, la comunicación de los hechos a las autoridades administrativas y/o judiciales pertinentes.

En caso de que en la comunicación recibida hubiera involucrado algún tercero con el que la organización mantiene relaciones profesionales o comerciales, se estudiarán las medidas que contractualmente estén previstas en las relaciones con las mismas.

Si de la fase de investigación se constata que los hechos no son constitutivos de una infracción, igualmente se elaborará el informe con el contenido detallado anteriormente y con la propuesta de archivo de la comunicación.

En todo caso, tanto si se considera que se ha producido una infracción como si se considera que los hechos denunciados carecen de fundamento, el informe estará debidamente argumentado y justificado.

El informe podrá elaborarse siguiendo el *Modelo de resolución ante la comunicación de indicio o sospecha*. El presente modelo es modificable y no vinculante, podrá ser modificado o ampliado según las necesidades del caso.

Una vez el informe sea trasladado al órgano de gobierno, este lo ratificará realizando las modificaciones que crea oportunas, su resultado será trasladado a la persona denunciada y, si procede, se adoptarán las medidas disciplinarias pertinentes y se comunicarán a las autoridades oportunas.

Finalmente, en función de cada supuesto y siempre y cuando se garanticen los derechos de las partes afectadas, se comunicará al denunciante el resultado de la investigación.

9. Asesoramiento

La organización prestará asesoramiento a cualquiera de los destinatarios del Canal Ético que planteen dudas o inquietudes relacionadas con el mismo. Dichas dudas o inquietudes se trasladarán a la organización mediante el propio Canal Ético.

10. Conocimiento

La existencia del Canal Ético, la obligatoriedad de acudir al mismo en caso de indicios razonables de irregularidades y su funcionamiento se comunicará y divulgará a todas las personas trabajadoras de SERVERA SL sin excepción mediante el Código de Conducta y poniendo a disposición de los mismos el presente Protocolo.

Para las personas que se incorporen en la organización se realizará la misma comunicación anexando el Código de Conducta al contrato asumiendo así el compromiso de poner en conocimiento de la organización las irregularidades de las que puedan tener conocimiento.

Asimismo, la existencia del Canal Ético y la obligatoriedad de acudir en mismo en caso de conocimiento de infracciones relacionadas con la organización y/o sus miembros será trasladada a los distintos grupos de interés de la organización, esto es, proveedores, prestadores de servicio, clientes, contratistas, subcontratistas, asesores y cualquier otro tercero que se relacione de alguna forma con SERVERA SL.

MODELO DE COMUNICACIÓN DE INDICIO O SOSPECHA DE INCUMPLIMIENTO

MODELO DE COMUNICACIÓN DE INCICIO O SOSPECHA DE INCUMPLIMIENTO	
Fecha de la denuncia*	
Datos del denunciante (Nombre y apellidos, DNI/NIE, dirección y teléfono y/o correo electrónico)	
Relación del denunciante con la organización	
Hechos objeto de denuncia* (Datos de la persona o personas involucradas en los hechos, fecha de los hechos, relación de los hechos)	
Listado de los medios de prueba adjuntados	

Nota: Los campos con asterisco son obligatorios

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS),

- **Finalidad:** Gestionar la denuncia formulada.
- **Plazo de conservación:** Cuando finalice el motivo de la misma SERVERA SL mantendrá sus datos personales bloqueados durante los plazos de prescripción legal o reclamaciones. Transcurridos los plazos de prescripción legal destruiremos sus datos.
- **Base legítima:** Consentimiento del interesado e interés legítimo.
- **Cesiones:** No se cederán datos a terceros, salvo obligación legal.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

Firma:

MODELO DE RESOLUCIÓN ANTE LA COMUNICACIÓN DE INDICIO O SOSPECHA DE INCUMPLIMIENTO

MODELO DE RESOLUCIÓN ANTE LA COMUNICACIÓN DE INDICIO O SOSPECHA DE INCUMPLIMIENTO	
NÚMERO DE EXPEDIENTE	
FECHA DE RECEPCIÓN DE LA DENUNCIA	
HECHOS OBJETO DE INVESTIGACIÓN	
MEDIOS DE PRUEBA APORTADOS	
VALORACIÓN INICIAL DE LOS HECHOS	No infracción/archivo de la comunicación. No infracción SGC remisión a otra área o departamento. Sí infracción SGC.
En caso de infracción o incumplimiento del SGC.	
PRECEPTO VULNERADO DEL SGC	
VALORACIÓN ADOPCIÓN MEDIDAS CAUTELARES	
ACTUACIONES DE INVESTIGACIÓN	
RESULTADO DE LA INVESTIGACIÓN	
PROPUESTA DE RESOLUCIÓN Y MEDIDAS A DOPTAR	
FECHA DE RESOLUCIÓN	

FORMULARIO WEB -CANAL ÉTICO

SERVERA SL en el marco de su firme compromiso con el cumplimiento normativo y con su Sistema de Gestión de Compliance ha habilitado el presente Canal Ético con la finalidad de proporcionar a todas las personas que se relacionan con la organización, tanto miembros integrantes de la misma como terceros, un canal de comunicación que sirva de instrumento para trasladar cualquier posible infracción, irregularidad, incumplimiento o comportamiento contrario a la ética, la legalidad y/o a los procedimientos del Sistema de Gestión de Compliance de la organización.

Las reclamaciones interpersonales, las quejas, rumores, habladurías o consultas sobre las relaciones con la organización no son comunicaciones susceptibles de ser transmitidas mediante este canal.

SERVERA SL garantiza la confidencialidad, el anonimato y la inexistencia de represalias o consecuencias negativas contra la persona que hubiera puesto los hechos en conocimiento, salvo que la investigación interna determine que la denuncia es falsa o haya sido realizada con temerario desprecio hacia la verdad, mala fe o abuso de derecho.

Asimismo, SERVERA SL se compromete a gestionar con la celeridad y diligencia debida las comunicaciones recibidas mediante el presente formulario.

Para más información sobre la utilización del Canal Ético puede ponerse en contacto con nosotros mediante el siguiente correo electrónico info@hotelatolon.com .

FORMULARIO WEB - CANAL ÉTICO	
Nombre y apellidos	Campo opcional
DNI/NIE	Campo opcional
Dirección	Campo opcional
Teléfono y/o correo electrónico	Campo opcional
Relación con la organización*	
Hechos objeto de denuncia* (Datos de la persona o personas involucradas en los hechos, fecha de los hechos, relación de los hechos)	
Adjuntar documentación	Examinar... No se ha seleccionado ningún archivo

Nota: Los campos con asterisco son obligatorios

De conformidad con la normativa vigente y aplicable en protección de datos de carácter personal, le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de SERVERA SL con NIF B07020191 y domicilio social sito en PASEIG MARITIM 42,07559 CALA BONA(ILLES BALEARS),

- **Finalidad:** Gestionar su comunicación, adoptar las medidas correctivas correspondientes y, en caso de ser necesario, informarle sobre el resultado del procedimiento.
- **Plazo de conservación:** los datos serán conservados durante el plazo estrictamente necesario para esclarecer los hechos denunciados. En todo caso transcurridos tres (3) meses se procederá a la destrucción de los datos facilitados salvo que sean investigados en un entorno legal distinto.
- **Base legítima:** Consentimiento del interesado.
- **Cesiones:** No se cederán datos a terceros, salvo obligación legal.

De acuerdo con los derechos que le confiere la normativa vigente y aplicable en protección de datos podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de sus datos de carácter personal así como la revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico info@hotelatolon.com. Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

En último lugar, el/la denunciante/da otorga el consentimiento explícito para el tratamiento de los datos mencionados anteriormente.

☐ He leído y acepto la política de protección de datos para que se gestionen mis datos para el Canal Ético.

3.7.2. Pautas de actuación en caso de comisión de un delito

1. Introducción

En caso de que SERVERA SL tenga conocimiento de la comisión de un delito en el seno de su organización, ya sea a raíz de una comunicación recibida a través del Canal Ético o bien conocida directamente por el órgano de gobierno o el Compliance Officer en el marco de sus funciones de máximos garantes del cumplimiento normativo dentro de la organización, la entidad deberá reaccionar de forma rápida y transparente para tomar el control de la situación, corregirla y gestionar las consecuencias, tratando de reducir sus efectos adversos a través de las siguientes acciones:

2. Acciones a nivel interno

- **Comunicación del hecho delictivo**: todas las personas relacionadas con la organización, tanto los miembros de la misma, como aquellos terceros con los que se mantienen relaciones comerciales o profesionales tienen el deber de comunicar a la organización mediante el Canal Ético habilitado los hechos delictivos e incluso las situaciones de sospecha o posibilidad de que se produzcan en el seno de la entidad.
- **Traslado a la persona u órgano responsable**: la comisión de un hecho delictivo o la posibilidad de perpetrarse debe comunicarse a través de los canales habilitados para que así, la persona designada por la organización pueda analizar los hechos y poner en marcha el conjunto de acciones que convengan en cada caso.
- **Análisis de las causas por las que no se ha podido evitar o prevenir el hecho delictivo**: es esencial determinar qué debilidades tiene la organización así como, el Sistema de Gestión de Compliance que han posibilitado la comisión del delito concreto.
- **Análisis de los hechos:** para poder averiguar si pueden estar produciéndose otras irregularidades similares y si pudieran llegar a producirse otros delitos.
- **Revisión inmediata de las medidas del Sistema de Gestión de Compliance:** adoptar nuevas medidas o intensificar las existentes para que, en un futuro, sí sean eficaces para evitar el tipo de delito cometido.
- **Revisión del análisis de riesgos:** especialmente, en el ámbito del tipo delictivo que ha sido violentado. Será fundamental actualizar el análisis de riesgos para el delito que se haya cometido teniendo en cuenta las circunstancias de comisión del mismo, eso es, su gravedad, su extensión en la organización, el número de personas implicadas, la intensidad del delito, la frecuencia y duración del mismo.
- **Aplicación de medidas disciplinarias:** imponer las medidas disciplinarias al autor del delito previstas en el Sistema Disciplinario de la organización, en el Convenio Colectivo de aplicación y el Estatuto de los Trabajadores. La aplicación del Sistema Disciplinario es un elemente esencial para demostrar la eficacia del Sistema de Gestión de Compliance y trasladar el mensaje inequívoco de tolerancia cero ante conductas delictivas.
- **Adopción de medidas que contribuyan a la reparación o disminución del daño causado:** la organización deberá adoptar las medidas a su alcance para disminuir el daño, corregir o paliar sus efectos.
- **Información documentada** que acredite la naturaleza de las no conformidades detectadas y las acciones que se han adoptado así como los resultados de las acciones correctivas adoptadas.

3. Acciones orientadas a las autoridades y tribunales

- **Denuncia de los hechos a las autoridades:** detectar las conductas delictivas que se cometen en la organización así como poner el delito en conocimiento de la autoridad competente confirma el

compromiso de la organización con una cultura de cumplimiento normativo y de que el Sistema de Gestión de Compliance funciona de forma eficiente.

- **Colaboración con las autoridades**: cooperar con las autoridades en el esclarecimiento del delito de forma activa y aportar pruebas esenciales, así como los resultados de la investigación interna para esclarecer las responsabilidades penales derivadas del delito.

- **Conservación de toda la documentación**: conservar la documentación relativa a todas las comunicaciones recibidas, así como las investigaciones que se hayan desprendido de las mismas es esencial para poder demostrar, que aunque los hechos no hayan llegado ante las autoridades, el Sistema de Gestión de Compliance es eficaz.

3.8. GESTIÓN DE INCIDENCIAS Y VIOLACIONES DE SEGURIDAD DE LOS DATOS

1. Incidentes y violaciones en la seguridad de la información

SERVERA SL ha establecido un conjunto de responsabilidades y procedimientos en cuanto a gestión, para tener la garantía de efectuar una respuesta rápida y eficiente ante un incidente de seguridad de la información

Para ello, la organización ha tenido en cuenta, principalmente, las siguientes directrices:

- Con respecto de responsabilidades para la gestión eficiente:
    - Procedimientos para la monitorización, detección, análisis y comunicación de incidentes de seguridad de la información. Además del registro de actividades de gestión de incidentes.
    - Procedimientos para la respuesta. Considerando aquellos como el escalado en la comunicación hacia personas internas y externas. Para personas externas se considera, además, el Delegado de Protección de Datos (DPD) en caso de tener asignada una persona que ocupe dicho rol, o bien, la propia Autoridad de Control.
    - Ninguna persona trabajadora, contratista o tercero debería comprobar, en ningún caso, un punto débil. En caso de hacerlo se podría interpretar como un uso indebido del sistema y podría derivar responsabilidades legales.

- A nivel de comunicación se han establecido:
    - Canales de comunicación adecuados y un formulario de comunicación de eventos de seguridad para formalizar el proceso y garantizar que se cumplen todas las acciones necesarias en caso de eventos de seguridad.
    - Procedimientos relativos comportamiento a adoptar ante un incidente de seguridad y a la comunicación efectiva hacia el punto de contacto para adoptar acciones coordinadas
    - Procesos de retroalimentación para que toda persona que haya notificado un evento de seguridad, una vez se haya tratado y cerrado el incidente, sea informada de los resultados. El conocimiento obtenido se utilizará para reducir la probabilidad o el impacto de posibles incidentes futuros.

Se consideran eventos o incidentes de seguridad de la información, principalmente, los siguientes:

- Quebrantamiento de las expectativas de integridad, confidencialidad y disponibilidad de la información. También se considerará el quebrantamiento de la seguridad física.
- Errores humanos o incumplimiento de las políticas o directrices.
- Cambios incontrolados o comportamientos anómalos de los sistemas, software o hardware.
- Violaciones de acceso.

En caso de incidente o violación de la seguridad de la información, SERVERA SL determinará si la continuidad de la seguridad de la información se enmarca dentro de la continuidad del negocio, o bien, dentro del plan de recuperación de desastres. La continuidad del negocio engloba la totalidad de la organización mientras que el plan de recuperación de desastres sólo se ocupa de la infraestructura tecnológica. Para ello, SERVERA SL ha establecido, documentado, implementado procesos, procedimientos y controles para la continuidad del negocio.

SERVERA SL ha establecido en los apartados *3.8.1. Procedimiento para la gestión de las violaciones de seguridad de los datos* y *3.8.2. Procedimiento de comunicación interna ante una violación de seguridad de los datos*, procedimientos que establecen las pautas para la gestión de las violaciones de seguridad de los datos así como, el canal de comunicación con el Delegado de Protección de Datos, en su defecto el Compliance Officer, el cual será el responsable de atender cualquier incidente de seguridad que afecte a los datos de carácter personal.

3.8.1. Procedimiento para la gestión de las violaciones de seguridad de los datos

1. Alcance y objetivos

Según el artículo 4 del Reglamento General de Protección de Datos una violación de la seguridad de datos personal es *"toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;".* Por ende, solo se aplicará este procedimiento en aquellos incidentes de seguridad que se vean afectados datos de carácter personal.

El presente procedimiento tiene por objeto pautar la gestión de las violaciones de seguridad en cuanto afecten a datos de carácter personal, de conformidad con la normativa aplicable y vigente en materia de protección de datos, específicamente, para el cumplimiento de lo dispuesto en los artículos 33 y 34 del Reglamento General de Protección de Datos. El procedimiento trata de garantizar la confidencialidad, integridad y disponibilidad de los datos en un proceso de mejora continua.

El procedimiento pretende facilitar a SERVERA SL un plan de actuación para enfrentarse a las brechas y así paliar o aminorar las consecuencias negativas. A modo de ejemplo:

- Se ha realizado una clasificación de mecanismos de detección e identificación de las brechas.
- Se establecen tipologías de brechas teniendo en cuenta su peligrosidad.
- Se tiene en cuenta un plan de actuación.
- Se establece un proceso de notificación en aquellos casos en que sean necesario.

En la medida en que la organización esté preparada para afrontar la gestión de un incidente de seguridad permitirá responder de forma rápida, ordenada y eficaz al evento, minimizando las consecuencias del mismo sobre la propia organización y terceras partes implicadas. El nivel de respuesta a un incidente de seguridad dependerá del tamaño de la organización, del tipo de datos y la complejidad del tratamiento.

El presente procedimiento se mantendrá en todo momento actualizado por el Delegado de Protección de Datos y en su defecto, por el Compliance Officer. Debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en la organización del mismo o en la organización de SERVERA SL.

Del mismo modo, el procedimiento, se adecuará en todo momento, a las disposiciones vigentes en materia de privacidad de los datos de carácter personal, tanto a nivel nacional como a nivel europeo.

2. Formas de detección de una brecha

SERVERA SL podrá identificar un incidente de seguridad de la información mediante fuentes internas o, bien, fuentes externas:

- Fuentes internas

Se pueden considerar las siguientes fuentes de información:

- Notificaciones de usuarios/ personas trabajadoras: presencia de archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información. En caso de que la detección se realice por parte del personal de SERVERA SL deberá tener en cuenta el procedimiento establecido en el apartado *3.8.2. Procedimiento de comunicación interna de las violaciones de seguridad de los datos.*
- Alertas generadas por software antivirus.
- Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
- Anomalías de tráfico de red o picos de tráfico en horas inusuales.
- Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.

- Fuentes externas

Es posible que la detección de incidentes se produzca por la comunicación de un tercero como:

- Proveedores de servicios informáticos.
- Proveedores de servicios de internet.
- Fabricantes de soluciones de seguridad.
- Clientes.
- Distintos organismos públicos a través de comunicación o notificación que realicen a la empresa los como el Instituto Nacional de Cyberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), Fuerzas y Cuerpos de Seguridad del Estado.
- Medios de comunicación mediante información publicada.

3. Identificación y registro

Una vez que SERVERA SL haya detectado la violación de seguridad, deberá determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal, y por tanto, constituye una “brecha de los datos de carácter personal” descrita en el RGPD, y el nivel de riesgo al que se enfrenta SERVERA SL.

Una vez identificado el incidente es necesario contar con medios para documentar el seguimiento del mismo, quedando anotados todos los aspectos del incidente en un registro de incidencias.

En particular, SERVERA SL deberá mantener como mínimo un registro documental de los incidentes de seguridad que hayan afectado a los datos de carácter personal, incluyendo el tipo de incidente, descripción del mismo, gravedad, estado y medidas adoptadas para su resolución. Por otra parte, una de las ventajas de disponer de este registro documental de incidencias es que, en ocasiones, incidentes de pequeña entidad pueden revelar la ocurrencia de un problema mayor previamente no identificado.

Por ende, SERVERA SL documentará, en el Registro de violaciones de seguridad de datos, cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en la normativa aplicable y vigente en materia de protección de datos. (Véase *Modelo de Registro de violaciones de seguridad de datos*).

4. Clasificación de violaciones de seguridad

Una vez detectado e identificado un incidente de seguridad es necesario entrar en la fase de análisis que permitirá a SERVERA SL recabar información y clasificar el incidente con mayor precisión.

Los factores que se pueden considerar a la hora de establecer criterios de clasificación son, entre otros:

- Tipo de amenaza: código dañino, intrusiones, fraude, etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.
- Contexto u origen de la amenaza: interna o externa.
- Categoría de seguridad de los sistemas y datos afectados.
- El perfil de los usuarios afectados.
- Número y tipología de los sistemas afectados.
- Impacto del incidente en la organización y en los derechos y libertades de los afectados.
- Requerimientos legales y regulatorios.

4.1. Tipos de brechas de seguridad

Una brecha de seguridad se puede clasificar en una o varias de las siguientes categorías:

- Brecha de confidencialidad: Tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella. La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegalmente a la información.
- Brecha de integridad: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al individuo.
- Brecha de disponibilidad: su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

5. Valoración del alcance de la brecha

Una vez clasificada la violación de la seguridad, SERVERA SL procederá a su valoración para determinar cuál es el riesgo de vulnerar los derechos y libertades de los interesados. La peligrosidad dependerá de los siguientes factores:

- La categoría o nivel de criticidad respecto a la seguridad de los sistemas afectados. Siguiendo la clasificación genérica, podemos distinguir entre:
    - Crítico (afecta a datos valiosos, gran volumen y en poco tiempo)
    - Muy Alto (Cuando dispone de capacidad para afectar a información valiosa, en cantidad apreciable)
    - Alto (Cuando dispone de capacidad para afectar a información valiosa)
    - Medio (Cuando dispone de capacidad para afectar a un volumen apreciable de información)
    - Bajo (Escasa o nula capacidad para afectar a un volumen apreciable de información).
- Naturaleza, sensibilidad y categorías de los datos personales afectados:
    - Datos de escaso riesgo: datos de contacto, de educación, familiares, profesionales, biográficos.

    - Datos de comportamiento: localización, tráfico, hábitos y preferencias.
    - Datos financieros: transacciones, posiciones, ingresos, cuentas, facturas.
    - Datos sensibles: de salud, biométricos, datos relativos a la vida sexual, etc.
- Datos legibles/ilegibles: Datos protegidos mediante algún sistema de seudonimización (por ejemplo, cifrado o hash).
- Volumen de datos personales: expresados en cantidad (registros, ficheros, documentos) y/o en periodos de tiempo (una semana, un año, etc.).
- Facilidad de identificación de individuos: facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha.
- Severidad de las consecuencias para los individuos:
    - Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.).
    - Media: Las personas pueden encontrar inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.).
    - Alta: Las personas pueden enfrentar consecuencias importantes, que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.).
    - Muy alta: Las personas pueden enfrentar consecuencias significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.).
- Características especiales de los individuos: Si afectan a individuos con características especiales o con necesidades especiales.
- Número de individuos afectados: Dentro de una escala determinada, por ejemplo, más de 100 individuos.
- Características especiales del responsable del tratamiento (de la entidad en sí): En base a la actividad de la entidad.
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El número y tipología de los sistemas afectados.
- Los requerimientos legales y regulatorios: Notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación a Fuerzas y Cuerpos de Seguridad del Estado en caso de delito.

El impacto que la brecha puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los Servicios, la conformidad legal y/o la imagen pública va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. En este aspecto diferenciamos entre los siguientes impactos:

- Bajo (perjuicio limitado)
- Medio (perjuicio grave)
- Alto (perjuicio muy grave)

5.1. Notificación de la brecha a la autoridad de control

Independientemente de las comunicaciones internas, SERVERA SL deberá notificar las violaciones de seguridad a la autoridad de control correspondiente, en caso de que sea oportuno. Según la normativa aplicable y vigente en materia de protección de datos, una violación de la seguridad de los datos personales se deberá notificar a la autoridad de control en caso que se considere probable que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de las personas físicas. Esta notificación, a la autoridad de control, deberá realizarse sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella. En caso de que la notificación a la autoridad de control no tenga lugar en el plazo de 72 horas, en el momento de efectuarse deberá ir acompañada de los motivos de la dilación. Notificación de una violación de la seguridad de los datos personales a la autoridad de control, del RGPD:

La notificación de la violación de seguridad deberá contener, como mínimo:

a) descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicación del nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) descripción de las posibles consecuencias de la violación de la seguridad de los datos personales;

d) descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

5.2. Comunicación de la brecha a los interesados

Independientemente de las comunicaciones internas, SERVERA SL deberá comunicar las violaciones de seguridad a los afectados en caso de que sea oportuno. Según la normativa aplicable y vigente en materia de protección de datos, una violación de la seguridad de los datos personales se deberá comunicar a los interesados en caso de que se considere probable que dicha violación de la seguridad constituya un alto riesgo para los derechos y libertades de las personas físicas. Esta comunicación, a los interesados, deberá realizarse sin dilación indebida.

La comunicación al interesado contendrá como mínimo la información y las medidas que se describen a continuación:

a) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

b) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

c) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

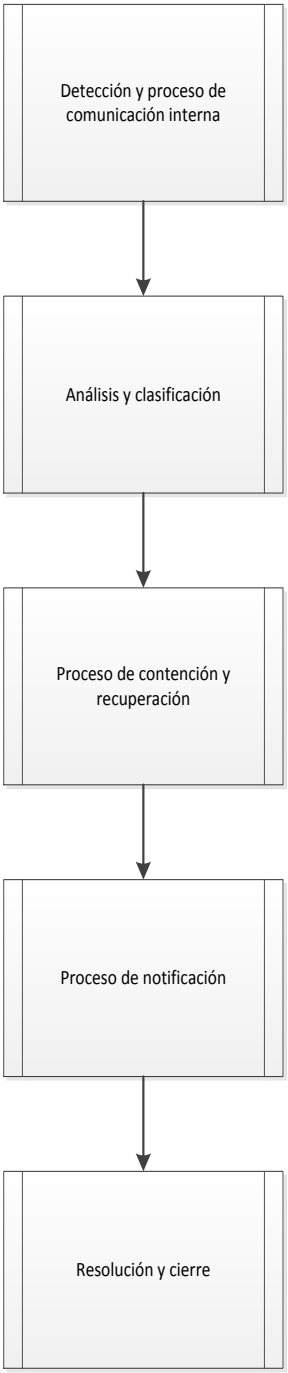
Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga.

6. Contención de la violación de la seguridad y recuperación del sistema

SERVERA SL deberá garantizar la aplicación de las medidas dirigidas a contener la violación de la seguridad y a recuperar el sistema en su funcionamiento habitual. Dentro de esta fase tenemos los procesos de contención y de recuperación:

- Proceso de contención: tiene como objetivo contener el incidente, tras lo cual se erradica la situación generada por el mismo. Cuando se ha conseguido contener el incidente, la erradicación puede ser necesaria para solventar determinados efectos del incidente de seguridad, como por ejemplo, eliminar un malware o desactivar de cuentas de usuario vulneradas.
- Proceso de recuperación: tiene como objetivo el restablecimiento del servicio en su totalidad confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa. Esto puede implicar la adopción no solo de medidas activas, sino también implementando controles periódicos y eficaces que permitan el seguimiento pormenorizado de los procesos de mayor riesgo.

7. Flujo del procedimiento de gestión de las violaciones de seguridad de los datos personales



REGISTRO DE VIOLACIONES DE SEGURIDAD DE LOS DATOS

REGISTRO DE VIOLACIONES DE SEGURIDAD						
Código de entrada	**Año**	**Tipo de incidente**	**Información afectada**	**Número de registros afectados**	**Notificación ante la AEPD/ Comunicación afectados**	**Dpto. Gestión**

3.8.2. Procedimiento de comunicación interna ante una violación de seguridad de los datos

1. Alcance y objetivo

El presente procedimiento tiene por objeto pautar la gestión de las violaciones de seguridad en cuanto afecten a datos de carácter personal, de conformidad con la normativa aplicable y vigente en materia de protección de datos. Específicamente, para el cumplimiento de lo dispuesto en los artículos 33 y 34 del Reglamento General de Protección de datos. El procedimiento trata de garantizar la confidencialidad, integridad y disponibilidad de los datos en un proceso de mejora continua.

El presente procedimiento se mantendrá en todo momento actualizado por el Delegado de Protección de Datos y en su defecto, por el Compliance Officer y debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en la organización del mismo o en la organización de SERVERA SL.

Del mismo modo, el procedimiento, se adecuará en todo momento, a las disposiciones vigentes en materia de privacidad de los datos de carácter personal, tanto a nivel nacional como a nivel europeo.

El alcance o ámbito de aplicación del presente procedimiento es para los miembros de la entidad, incluyendo al personal de la compañía que trabaje de manera itinerante. El procedimiento deberá ser conocido por el personal de SERVERA SL y será considerado de obligado cumplimiento para todo el personal que detecta una violación de seguridad que afecte a datos de carácter personal.

2. Detección y comunicación interna

Cuando algún miembro de la organización haya detectado e identificado una brecha de seguridad será necesaria poner en marcha este procedimiento para la comunicación interna de las violaciones de seguridad con la finalidad de solucionar el incidente.

SERVERA SL ha establecido un canal fluido de comunicación para que el personal que detecte cualquier brecha o violación en la seguridad de los datos personales y la misma pueda afectar al cumplimiento de la normativa vigente y aplicable en protección de datos, pueda comunicarla con la máxima diligencia posible. El procedimiento de comunicación será el siguiente:

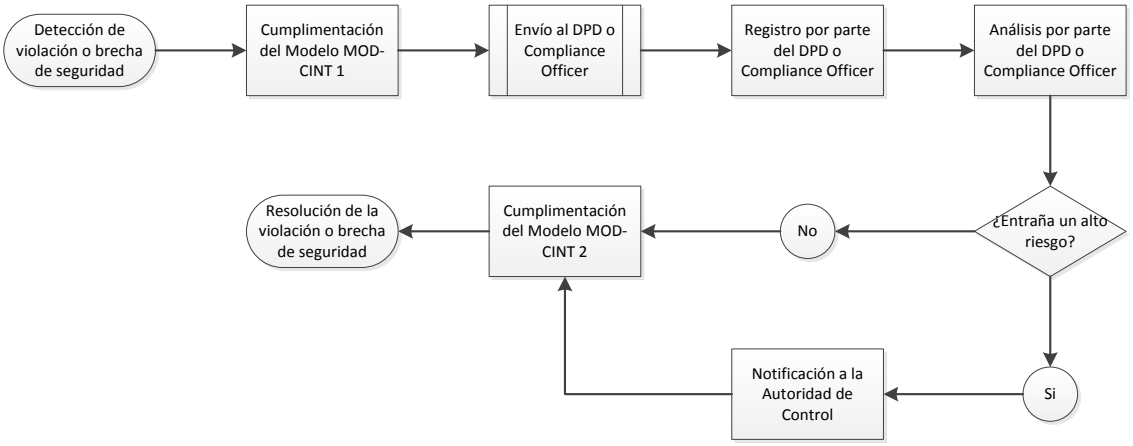
1) Remisión del *Modelo de Comunicación Interna* por parte del miembro de la organización. Una vez cumplimentado el Modelo de Comunicación Interna, la persona comunicante deberá remitirlo al Delegado de Protección de Datos (en adelante DPD), o en su defecto al Compliance Officer, adjuntando toda la documentación que considere relevante, en relación a la operación comunicada.
2) El Compliance Officer registrará la comunicación realizada indicando hora, fecha y lugar de presentación de la comunicación. Todas las comunicaciones internas que se realicen por parte de los directivos, miembros o agentes de SERVERA SL, quedarán registradas por orden numérico de entrada seguido del año en que se realice la comunicación. Dicho registro de entrada será la que se corresponderá con el número de comunicación. (véase apartado *3.8.1. Procedimiento para la gestión de las violaciones de seguridad de los datos*)
3) El Compliance Officer podrá requerir a la persona comunicante información más detallada sobre la operación comunicada, si ello resultase necesario para un análisis más detallado de la misma.
4) El Compliance Officer realizará las actuaciones pertinentes para la detección, identificación, clasificación y valoración de la brecha de seguridad en atención al procedimiento establecido en el apartado *3.7.1. Procedimiento para la gestión de las violaciones de seguridad de los datos.*
5) El Compliance Officer emitirá un informe de resolución y cierre de la violación de la seguridad a través del *Modelo de resolución ante la violación de seguridad de los datos.*

Dicho Informe de resolución recopilará toda la información y documentación relativa a la brecha de manera que se facilite el estudio y revisión por terceros, o la dirección de SERVERA SL. El Informe recopilará:

- Alcance e impacto del incidente.
- Controles preventivos existentes.
- Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución de la brecha.
- Acciones tomadas para la prevención de futuras brechas.
- Impacto en la resolución del incidente de las acciones de respuesta tomadas.
- Acciones definidas para el seguimiento.

Los informes sobre las brechas y su impacto son una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

SERVERA SL ha establecido un flujo para la comunicación de la violación de la seguridad al Compliance Officer:



3. Cumplimentación formulario de comunicación de la violación de seguridad

El Modelo de Comunicación Interna (MOD-CINT1) deberá contener la siguiente información:

- Registro de entrada – día – mes – año – hora
- Identificación del sujeto que realiza la comunicación (persona física/persona jurídica)
- Relación que mantiene con la empresa (cargo/rol)
- Descripción de la duda, sugerencia o comunicación
- Si se trata de un indicio o sospecha de una violación de seguridad de los datos personales, se deberá de describir:
    a) La violación de seguridad de los datos producida
    b) Lugar, fecha y hora de la violación de la seguridad de los datos personales
    c) Las consecuencias probables de la violación de seguridad de los datos personales (en caso de conocerse)

    Asimismo, deberán señalarse las medidas adoptadas o propuestas para poner remedio a la violación de seguridad de los datos personales (en caso de conocerse). Indicar medidas tendentes a atenuar los posibles efectos negativos de la violación de seguridad de los datos personales.
- Relación de documentación adjuntada

- Otros comentarios
- Firma/sello del comunicante

Todas las comunicaciones internas que se realicen al Compliance Officer, por parte de los directivos, miembros o agentes relaciones con la entidad, quedarán registradas por orden numérico de entrada seguido del año en que se realice la comunicación. Dicho registro de entrada será la que se corresponderá con el número de comunicación.

Una vez recibida la comunicación, la persona trabajadora quedará liberado totalmente de cualquier responsabilidad al respecto y será plena responsabilidad del Compliance Officer proceder a su inmediato análisis o comprobación para determinar la relación de los hechos u operaciones comunicadas.

El resultado del análisis de la violación de la seguridad deberá realizarse a través de la cumplimentación del modelo de resolución (MOD-CINT2), que deberá contener la siguiente información:

- Nº de comunicación – día – mes – año – hora
- A quien se dirige (persona que ha efectuado la comunicación)
- Datos de referencia de la comunicación
- Conclusiones del análisis de la operación
- Acciones efectuadas
- Firma del DPD o Compliance Officer

4. Entrada en vigor y actualización

La presente política entrará en vigor con efectos vinculantes para todos sus destinatarios desde la aprobación por parte del órgano de gobierno del Sistema de Gestión de Compliance y permanecerá mientras no se apruebe su actualización, revisión o derogación.

MODELO DE COMUNICACIÓN DE LA VIOLACIÓN DE SEGURIDAD

COMUNICACIÓN INTERNA VIOLACIÓN DE SEGURIDAD
ENTRADA: …….. DÍA: …….. MES:…… AÑO: …… HORA: ……
IDENTIFICACIÓN DEL EMPLEADO QUE REALIZA LA COMUNICACIÓN: Nombre y Apellidos: DNI/NIE: Cargo: 1. DESCRIPCIÓN DE DUDA, SUGERENCIA, COMUNICACIÓN: 1. COMUNICACIÓN DE VIOLACIÓN DE SEGURIDAD DE LOS DATOS PERSONALES 2.1.-Descripción de la violación producida: 2.2.- Describir las consecuencias probables de la violación de seguridad de los datos personales (en caso de conocerse): 2. RELACIÓN DE DOCUMENTACIÓN ADJUNTADA: 1.-…….. 2.-…….. 3.-…… 3. OTROS COMENTARIOS
Firma/sello del comunicante

MODELO DE RESOLUCIÓN ANTE LA VIOLACIÓN DE SEGURIDAD

INFORME DE RESOLUCIÓN DE LA VIOLACIÓN DE SEGURIDAD
ENTRADA: ……..…..…….. DÍA: ……..…… MES:……..…… AÑO: …… HORA: ……..……
Nº COMUNICACIÓN: DIRIGIDO A: Nombre y Apellidos: DNI/NIE: Cargo: 2. DATOS DE REFERENCIA DE LA COMUNICACIÓN 3. CONCLUSIONES DEL ANÁLISIS DE LA OPERACIÓN 4. ACCIONES EFECTUADAS
Firma

3.9. GESTIÓN DE DERECHOS DE LOS INTERESADOS

En la normativa vigente y aplicable de protección de datos se regula tanto los derechos que puede ejercer el interesado como los mecanismos de ejercicio de tales derechos ante el Responsable del Tratamiento de los datos.

Los derechos que puede ejercer el interesado son los siguientes:

1. Derecho de Acceso a los datos personales

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a obtener copia de los mismos de manera sencilla y gratuita. Ello implica tener acceso a la siguiente información sobre su tratamiento:

a) Fines del tratamiento.

b) Categorías de datos que se traten.

c) Destinatarios o categorías de destinatarios a los que se comunicarán o se prevén comunicar.

d) El plazo de conservación o, en su defecto, los criterios utilizados para determinarlo.

e) El derecho a solicitar la rectificación, supresión de datos o la limitación u oposición al tratamiento.

f) El derecho a poner una reclamación ante la autoridad de control.

g) El origen de los datos cuando no se hayan obtenido directamente del interesado.

h) Existencia de decisiones automatizadas, incluida la elaboración de perfiles.

i) Transferencias internacionales de datos a un tercer país u organización internacional, así como las garantías de las mismas.

2. Derecho de Rectificación de datos personales

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Al ejercer el derecho de rectificación, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

3. Derecho de Supresión y derecho al Olvido

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento;

c) el interesado se oponga al tratamiento;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Cuando haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, el responsable del tratamiento adoptará medidas razonables con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado, para que se suprima cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Lo establecido anteriormente no se aplicará cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

4. Derecho de Limitación del Tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando el tratamiento de datos personales se haya limitado, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

Todo interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

5. Derecho a la Portabilidad de los datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento, cuando:

a) el tratamiento esté basado en el consentimiento o en un contrato y

b) el tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad de los datos, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

El ejercicio del derecho se entenderá sin perjuicio del derecho de supresión de los datos. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

El derecho de portabilidad de los datos no afectará negativamente a los derechos y libertades de otros.

6. Derecho de Oposición al tratamiento

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

A más tardar en el momento de la primera comunicación con el interesado, el derecho de oposición al tratamiento será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

En el contexto de la utilización de servicios de la sociedad de la información, el interesado podrá ejercer su derecho a oponerse por medios automatizados.

Cuando los datos personales se traten con fines de investigación científica, histórica o fines estadísticos, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

7. Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles

Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Ello no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

En los casos a que se refiere las letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

3.9.1. Procedimiento de atención de los derechos

1. Objeto y alcance

El objeto del presente procedimiento es establecer las pautas para la atención y gestión de los derechos de los interesados de conformidad con la normativa aplicable y vigente en materia de protección de datos. Específicamente, para el cumplimiento de lo dispuesto en los artículos 15 al 22 del Reglamento General de Protección de datos y los artículos 12 al 18 de la Ley Orgánica de Protección de Datos y Garantías de los Derechos digitales. Este procedimiento se ha confeccionado teniendo en cuenta las operaciones de tratamiento realizadas por SERVERA SL, en especial atención a las categorías de interesados de las operaciones de tratamiento. El procedimiento, deberá ser conocido por el personal de SERVERA SL y será considerado de obligado cumplimiento para todo el personal que reciba un ejercicio de derecho de un interesado.

El presente documento se mantendrá en todo momento actualizado por el Delegado de Protección de Datos y en su defecto, por el Compliance Officer. Debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en la organización del mismo o en la organización de SERVERA SL.

Del mismo modo, el documento, se adecuará en todo momento, a las disposiciones vigentes en materia de privacidad de los datos de carácter personal, tanto a nivel nacional como a nivel europeo.

2. Ejercicio de derechos

Los derechos que puede ejercer el interesado de los datos son los siguientes:

- Derecho de acceso: Es el derecho del interesado a obtener del Responsable del Tratamiento confirmación de si se están tratando o no datos personales que le conciernen, y en caso de que se confirme el tratamiento se le deberá de facilitar el acceso a los datos y a la información que dispone.
- Derecho de rectificación: El interesado tendrá derecho a obtener del Responsable del Tratamiento sin demora injustificada la rectificación de los datos personales que le conciernen cuando tales datos resulten inexactos. Habida cuenta de los fines para los cuales se hayan tratado los datos, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular por medio de la entrega de una declaración adicional.
- Derecho a la limitación del tratamiento: Es el derecho a obtener del Responsable del Tratamiento la limitación del tratamiento de datos personales.
- Derecho a la supresión (“derecho al olvido”): Hace referencia al derecho del interesado a obtener del Responsable del Tratamiento la supresión de los datos personales que le conciernan sin demora injustificada.
- Derecho a la portabilidad de los datos: Consiste en el derecho a recibir los datos personales que le incumban, que haya facilitado a un Responsable del Tratamiento, en un formato estructurado y de uso habitual y de lectura mecánica y a transmitirlos a otro Responsable del Tratamiento sin que lo impida el Responsable del Tratamiento al que se hubieran facilitado los datos.
- Derecho de oposición: El interesado podrá oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento para el cumplimiento de un interés público o para la satisfacción de un interés legítimo, inclusive la elaboración de perfiles sobre la base de dichas disposiciones.
- Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles: El interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

En materia de protección de datos de carácter personal, debemos tener en cuenta los siguientes criterios comunes que serán de aplicación a cualquier ejercicio de derechos conferidos por esta normativa:

- El ejercicio es gratuito (salvo en los excepcionales casos determinados expresamente por la ley, como solicitudes manifiestamente infundadas o excesivas).
- El Responsable del Tratamiento está obligado a informar sobre los medios y canales para ejercer estos derechos, debiendo ser accesibles.
- Puede ser ejercido por el propio interesado o por medio de su representante legal o voluntario.
- Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.
- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.
- Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

3. Solicitud

SERVERA SL establece que toda solicitud deberá ir acompañada de la siguiente información:

- Nombre, apellidos del interesado y copia del DNI. En los excepcionales casos en que se admita la representación, será también necesaria la identificación por el mismo medio de la persona que le representa, así como el documento acreditativo de la representación. La fotocopia del DNI podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.
- Petición en que se concreta la solicitud. (Ejercicio que se solicita o información a la que se quiere acceder). Si no hace referencia a un fichero concreto se le facilitará toda la información que se tenga a su nombre. Si solicita información de un fichero en concreto, sólo la información de este fichero. Si solicita información relativa a un tercero nunca se podrá facilitar. Si lo solicita por teléfono se le indicará que lo haga por escrito y se le informará de cómo lo puede hacer y la dirección a la que tiene que enviarlo. Nunca se le dará información por teléfono.
- Domicilio a efecto de notificaciones.
- Fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula.

Se ha habilitado un modelo de ejercicio de derechos que podrá ser proporcionado a aquellos interesados que pretendan ejercer un derecho.

Asimismo, SERVERA SL establece un canal de comunicación para recibir y atender de forma efectiva los derechos de los interesados.

4. Plazos de respuesta

SERVERA SL dispone de un plazo de un mes para resolver el ejercicio de los derechos anteriormente indicados. Dicho plazo podrá prorrogarse otros dos meses en caso de que sea necesario, teniendo en cuenta la complejidad y el número de solicitudes. SERVERA SL informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el

interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

SERVERA SL soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

5. Régimen sancionador

La importancia de la implementación del procedimiento de gestión y atención de derechos de los interesados responde a la obligatoriedad de atender los derechos de los interesados en el tiempo y forma oportunos. De otra forma se estaría vulnerando las disposiciones de la normativa aplicable y vigente en materia de protección de datos. Específicamente, la LOPDGDD dispone de un régimen sancionador en el cual se establecen algunas infracciones en materia de derechos de los interesados. A modo ejemplificativo se enumeran las siguientes infracciones:

- La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.
- El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

6. Entrada en vigor y actualización

La presente política entrará en vigor con efectos vinculantes para todos sus destinatarios desde la aprobación por parte del órgano de gobierno del Sistema de Gestión de Compliance y permanecerá mientras no se apruebe su actualización, revisión o derogación.

MODELO DE DOCUMENTO PARA EL EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS

Responsable del Tratamiento:

Nombre y Apellidos del solicitante:
DNI:

Nombre y Apellidos del representante:
DNI:

Solicito:
Que, de acuerdo con lo establecido en la normativa aplicable y vigente en materia de protección de datos ejerzo:

- ☐ Derecho Acceso
- ☐ Derecho de Rectificación
- ☐ Derecho de Limitación de tratamiento
- ☐ Derecho de Supresión (“derecho al olvido”)
- ☐ Derecho de Portabilidad
- ☐ Derecho de Oposición/revocación

Motivación y especificación de la solicitud:

Documentación adjunta (marcar la que proceda):

- ☐ Copia del DNI o pasaporte
- ☐ Título que acredita la representación, en caso de que sea necesario
- ☐ Otra documentación acreditativa:

Dirección a efectos de notificaciones:

Localidad y fecha

Firma del solicitante

3.10. POLÍTICA INTERNA DE DESCONEXIÓN DIGITAL

1. Introducción

La política de desconexión digital pretende dar cumplimiento a las previsiones del artículo 88 de la LOPDGDD. De conformidad con el mencionado artículo el personal tendrá derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la entidad y los representantes de las personas trabajadoras.

La entidad, previa audiencia de los representantes de las personas trabajadoras, elaborará una política interna dirigida al personal, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio de la persona trabajadora vinculado al uso con fines laborales de herramientas tecnológicas.

2. Antecedentes

En diciembre de 2018, entró en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), por la que se modifica, entre otras disposiciones legales, el Texto Refundido de la Ley del Estatuto de los Trabajadores (en adelante ET), mediante la inclusión de un nuevo artículo, el 20 bis en el cual se reconoce el derecho a la desconexión digital. Adicionalmente, el artículo 88 de la LOPDGDD regula el derecho a la desconexión digital en el ámbito laboral a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto del tiempo de descanso, permisos y vacaciones, así como de la intimidad personal y familiar.

Por tanto, con la finalidad de dar respuesta a las estipulaciones del artículo 20 bis del ET y el artículo 88 de la LOPDGDD, SERVERA SL establece la siguiente política interna reguladora del derecho a la desconexión digital para las personas trabajadoras.

3. Objetivo

La presente política tiene por objeto el establecimiento de medidas que tiendan a asegurar el respeto del tiempo de descanso y vacaciones de las personas trabajadoras, así como el respeto a su intimidad familiar y personal.

El objetivo de la presente política es reconocer el derecho a la desconexión digital como elemento fundamental para:

- Lograr una ordenación del tiempo de trabajo en aras del respeto de la vida privada y familiar;
- Mejorar la conciliación de la vida personal, familiar y laboral;
- Contribuir a la optimización de la salud laboral.

4. Ámbito de aplicación

Esta política interna será de aplicación a las personas trabajadoras de SERVERA SL, incluidas las que ocupen puestos directivos, con la excepción de aquellas personas trabajadoras que disponen de un complemento de

disponibilidad o de similar naturaleza. Esta política también se aplicará en los supuestos de realización total o parcial del trabajo a distancia.

La presente política se deberá revisar periódicamente o cuando existan cambios significativos en la estructura y/u organización de SERVERA SL.

5. Principios en materia de desconexión digital

SERVERA SL se compromete a impulsar medidas para garantizar el derecho a la desconexión digital atendiendo a los siguientes principios:

- Respetar el tiempo de descanso, permisos y vacaciones de las personas trabajadoras;
- Mejor la ordenación del tiempo de trabajo en aras del respeto de la vida privada y familiar;
- Potenciar el derecho a la conciliación de la actividad laboral y la vida personal y familiar;
- Realizar acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.

Adicionalmente, SERVERA SL implantará y coordinará el trabajo a distancia desde el respeto y reconocimiento del derecho a la desconexión digital de las personas trabajadoras, de acuerdo al art. 88 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

6. Medidas para la desconexión digital

1) SERVERA SL garantizará a las personas trabajadoras el derecho a la desconexión digital una vez finalizada la jornada laboral. Estas tendrán derecho a no responder a ninguna comunicación, independientemente del medio utilizado, una vez finalizada su jornada laboral, salvo que concurran las circunstancias señaladas en el apartado 6) de la presente política.
2) Las personas trabajadoras se deberán comprometer al uso adecuado de los medios informáticos y tecnológicos que SERVERA SL pudiera haber puesto a su disposición, de conformidad con las recomendaciones de protección de datos y seguridad de la información para el personal.
3) Los responsables sobre un equipo de personas se abstendrán de requerir respuesta en las comunicaciones enviadas a las personas trabajadoras fuera de horario de trabajo o próximo a su finalización, siempre que pudieran suponer para los destinatarios de las mismas la realización de un trabajo efectivo que previsiblemente pueda prolongarse e invadir su tiempo de descanso. Por ello, las personas destinatarias de la comunicación tendrán derecho a no responder a la misma hasta el inicio de la siguiente jornada laboral.

   En este sentido, en caso de enviar una comunicación que pueda suponer respuesta fuera del horario establecido al efecto, el remitente asumirá expresamente que la respuesta podrá esperar a la jornada laboral siguiente.
4) La convocatoria de reuniones de trabajo, tanto a nivel interno como las que se lleven a cabo con clientes, así como la formación obligatoria, se realizarán teniendo en cuenta el tiempo aproximado de duración y, preferiblemente, no se extenderán hasta más tarde de la finalización de la jornada ordinaria de trabajo, a fin de que no se vea afectado el tiempo de descanso de las personas trabajadoras. Con carácter excepcional, y siempre que concurran las circunstancias establecidas en el apartado 6) de la presente política, el apartado anterior no será de aplicación.
5) SERVERA SL garantizará a las personas trabajadoras el derecho a la desconexión digital durante el periodo que duren sus vacaciones, días de asuntos propios, descanso diario y semanal, permisos, incapacidades o excedencias.

6) Se excluye la aplicación del derecho a desconexión digital a aquellas personas trabajadoras que perciban un complemento de “disponibilidad” u otro de similar naturaleza por el cual la persona trabajadora deberá atender las comunicaciones de la entidad.

   Asimismo, no serán de aplicación las medidas que garantizan el derecho a la desconexión digital en los casos en que concurran circunstancias de causa de fuerza mayor o que supongan un grave o inminente perjuicio empresarial o del negocio, cuya urgencia necesita de una respuesta inmediata.

   En dichos supuestos, si SERVERA SL requiere una respuesta de la persona trabajadora, una vez finalizada su jornada laboral, contactará con aquella preferiblemente por teléfono para comunicarle la situación de urgencia.

7) SERVERA SL implementará medidas de sensibilización sobre el derecho a la desconexión digital. Para lo cual se pondrá a disposición de las personas trabajadoras, toda la información y/o formación que precisen para la comprensión y posterior aplicación de las medidas protectoras del derecho a la desconexión digital.

   Corresponde a quienes tengan la responsabilidad sobre un equipo y/o superiores jerárquicos de las personas trabajadoras, fomentar la utilización responsable de las tecnologías con el propósito de dar cumplimiento al derecho a la desconexión digital.

8) El ejercicio del derecho a desconexión digital no repercutirá negativamente en el desarrollo profesional de las personas trabajadoras.

Con todo ello, SERVERA SL reconoce y formaliza el derecho a la desconexión digital como un derecho, aunque no como una obligación, aplicable a todas las personas trabajadoras. Esto implica expresamente que, aquellas personas trabajadoras que realicen comunicaciones fuera de la jornada laboral podrán hacerlo con total libertad; sin embargo, deben asumir que no tendrán respuesta alguna hasta el día hábil posterior. Las únicas excepciones serían las reconocidas en el apartado 6) de la presente política.

7. Entrada en vigor y actualización

La presente política entrará en vigor con efectos vinculantes para todos sus destinatarios desde la aprobación por parte del órgano de gobierno del Sistema de Gestión de Compliance y permanecerá mientras no se apruebe su actualización, revisión o derogación.

3.11. SISTEMA DISCIPLINARIO

1. Introducción

La finalidad fundamental del Sistema de Gestión de Compliance de SERVERA SL es promover e instaurar una cultura de respeto y cumplimiento de la ley entre todas las personas que integran la misma, así como entre todas aquellas con las que se relaciona.

Por ello el SGC implementado en la organización cuenta con políticas, procedimientos y medidas de vigilancia y control para prevenir cualquier actuación contraria a la normativa vigente y aplicable a la organización y garantizar la legalidad de los actos de los miembros profesionales de la organización así como de los directivos.

Así pues, en el contexto de lo anterior, el presente Sistema Disciplinario es una de las medidas imperativas con la que debe contar la organización en el marco de una implementación eficaz de su SGC.

Por lo tanto, la finalidad del presente Sistema Disciplinario es sancionar el quebrantamiento de las normativas, procedimientos y políticas internas implementadas mediante el SGC. De esta manera, se pretende contribuir a evitar la transgresión de las normativas aplicables a SERVERA SL así como las políticas y procedimientos internos establecidos actuando como un mecanismo de ejemplaridad, corrección y solución.

El presente Sistema Disciplinario no sustituye el régimen disciplinario establecido en la organización ni en el Convenio Colectivo aplicable, en el Estatuto de los Trabajadores o en los regímenes específicos aplicables, sino que los completa con la finalidad de favorecer la prevención de conductas contrarias a la ley en la entidad por parte de sus miembros profesionales.

2. Facultad disciplinaria

La legitimidad de la organización para establecer el Sistema de Gestión de Compliance, sus medidas, procedimientos y políticas de obligado cumplimiento así como el presente Sistema Disciplinario se desprende del Estatuto de los Trabajadores.

Dicho texto, en el primer apartado de su artículo 1 fija el trabajo por cuenta ajena "…dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o empresario."

Por otro lado, en su artículo 5.c) expone el deber básico de las personas trabajadoras de "Cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas".

Por su parte, el artículo 20.1 del mismo texto establece que las personas trabajadoras tendrán la obligación de "realizar el trabajo convenido bajo la dirección del empresario o persona en quien este delegue."

Asimismo, el mismo artículo 20.2 instaura que: "…el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquel en el ejercicio regular de sus facultades de dirección."

Igualmente, el artículo 54 declara que: "Se considerarán incumplimientos contractuales: la indisciplina o desobediencia en el trabajo, la transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo".

Finalmente, el artículo 58 del mismo Estatuto de los Trabajadores determina que: "Los trabajadores podrán ser sancionados por la dirección de las empresas en virtud de incumplimientos laborales, de acuerdo con la

graduación de faltas y sanciones que se establezcan en las disposiciones legales o en el convenio colectivo que sea aplicable".

Así pues, de acuerdo con la normativa citada, el órgano de gobierno o la dirección de la organización puede reputar como incumplimiento laboral sancionable aquellas actuaciones laborales de los miembros profesionales de la organización que realicen en el desarrollo de sus funciones y sean contrarias a las disposiciones legales aplicables, al Convenio Colectivo, o a cualquier política o normativa interna de la organización relacionada con el SGC.

3. Destinatarios

El Sistema Disciplinario de la organización será aplicable a todas las personas trabajadoras de SERVERA SL, es decir, a aquellas personas que tienen una relación laboral con la misma.

Así pues, no estarán sujetas por el mismo, las personas que tengan una vinculación mercantil o civil con la entidad, como puede ser el caso de los administradores o socios de la entidad.

No obstante, para aquellas personas y organizaciones fuera del alcance del presente Sistema Disciplinario, la organización prevé que conozcan y acepten de forma fehaciente los principios de actuación recogidos en el SGC así como las posibles acciones en caso de incumplimiento.

4. Deberes/actuaciones

A continuación se detallan las características básicas de las conductas que eventualmente darían lugar a la aplicación del presente Sistema Disciplinario:

- Falta de seguimiento del Sistema de Gestión de Compliance.
- Falta de seguimiento de las medidas, políticas y procedimientos del SGC.
- Falta de seguimiento de los principios de ética, integridad, legalidad y transparencia.
- Falta de seguimiento del Código de Conducta.
- Falta de comunicación a través del Canal Ético de las infracciones o posibles infracciones del SGC y/o de la legalidad.
- Adopción de represalia o sanción a la persona que hubiera realizado una comunicación a través del Canal Ético.
- Realización de una comunicación con conocimiento de su falsedad o menosprecio a la verdad a través del Canal Ético.
- Falta de colaboración en la investigación de los hechos comunicados a través del Canal Ético.
- Las conductas que contribuyan a impedir o dificultar las infracciones respecto al SGC.
- Las conductas delictivas vinculadas a la actividad laboral desarrollada por la organización.
- Las infracciones en materia de protección de datos vinculadas a la actividad laboral desarrollada por la organización.

Además, ninguna persona integrante de SERVERA SL podrá realizar conductas contrarias al SGC o que contravengan lo establecido en las leyes vigentes y aplicables amparándose en el desconocimiento de los mismos o en una orden de un tercero, de un compañero/a o de un superior jerárquico.

Asimismo, hay que tener en cuenta que unos mismos hechos cometidos por una persona trabajadora o voluntaria pueden ser constitutivos de infracción administrativa o de delito, pero no de una infracción laboral sancionable y viceversa.

5. Sanciones

Las sanciones que corresponderán a las conductas anteriormente descritas serán calificadas por la organización como leves, graves o muy graves, teniendo en cuenta las circunstancias y particularidades concretas de cada caso. Las sanciones, que pueden ir desde la amonestación al despido disciplinario, dependerán entre otros, de la gravedad de la conducta, la reiteración de la misma, la reincidencia o los daños causados a la organización.

La determinación de la infracción y de las sanciones se realizará de acuerdo con el Convenio Colectivo aplicable y/o en su defecto por lo previsto en el Estatuto de los Trabajadores y en el resto de legislación aplicable.

Las sanciones se impondrán sin perjuicio de las acciones y sanciones administrativas o penales que, en su caso, puedan también resultar de aplicación.

6. Imposición de la sanción

El órgano o persona de la organización competente para la imposición de la sanción es el órgano de gobierno o la dirección de la organización.

El procedimiento a seguir para la imposición de la sanción disciplinaria, así como la iniciación y desarrollo del expediente disciplinario, en caso de que corresponda, así como la imposición y comunicación de la sanción, se realizará de acuerdo con lo estipulado en los acuerdos internos con los representantes de las personas trabajadoras, el Convenio Colectivo aplicable, el Estatuto de los Trabajadores y el resto de legislación aplicable.

Asimismo, en todo expediente disciplinario constará:

- La decisión de incoar un expediente, por parte de la organización.
- La notificación a la persona trabajadora de la incoación, de manera fehaciente, mediante el "pliego de cargos", como escrito en el que se hacen constar por parte de la organización los hechos o conductas que han dado lugar a la incoación del expediente y su imputación a la persona trabajadora o voluntaria, así como, el plazo del que dispone para presentar las alegaciones y las proposiciones de prueba.

Una vez recibido el pliego de cargos, la persona trabajadora o voluntaria, dentro del plazo concedido, podrá realizar su escrito de alegaciones o "pliego de descargos", como escrito en el que haga constar las argumentaciones que en su defensa realiza, en contestación y en relación con el contenido del pliego de cargos, pudiendo proponer la realización de aquellas diligencias de prueba que estime oportunas para poder dar veracidad o apoyar a sus alegaciones.

Igualmente, todas las actuaciones realizadas en virtud del presente Sistema Disciplinario respetarán en todo momento los derechos fundamentales de los miembros de la organización y asegurarán un tratamiento correcto e imparcial de los que se sospeche que hayan cometido algún incumplimiento de las directrices y normas a las que están sujetos.

La terminación del expediente se dará una vez valorado todo el expediente:

- Con la decisión de la organización de sancionar.
- Con el archivo o la decisión de la organización de no sancionar.

7. Prescripción

En relación con la prescripción de las faltas cometidas también será de aplicación lo dispuesto en el Convenio Colectivo y el resto de aplicación vigente y aplicable en la materia.

8. Comunicación

El presente Sistema Disciplinario será difundido a todas aquellas personas de la organización a las que les será de aplicación.

9.Entrada en vigor y actualización

El presente protocolo entrará en vigor con efectos vinculantes para todos sus destinatarios desde la aprobación por parte del órgano de gobierno del Sistema de Gestión de Compliance y permanecerá mientras no se apruebe su actualización, revisión o derogación.

CONVERSIA

info@conversia.es | T. 902 877 192 | www.conversia.es