PROTOCOLOS PROTECCIÓN DE DATOS

ELECTRA DE ZAS, SL

V.1.- 06.03.2025

ÍNDICE DE CONTENIDO

1.- IDENTIFICACIÓN DEL PROYECTO

CÓDIGO	**2024.01.3518**
DESCRIPCIÓN	Se trata de reflejar la implantación de medidas y protocolos de seguridad en materia de protección de datos para minimizar o eliminar los riesgos detectados.
ENTIDAD RESPONSABLE	ELECTRA DE ZAS, SL
EQUIPO DESARROLLADOR	Errebe Consultores Empresariales S.L lopd@rbsoluciones.com www.rbsoluciones.com
FECHA DEL INFORME	06 de marzo de 2025
VERSIÓN DEL INFORME	V.1

2.- OBJETIVO

El presente documento pretende recoger todos los protocolos de seguridad aplicados en la entidad para garantizar la seguridad de la información que se trata.

Las medidas de seguridad a implantar vendrán determinadas por el riesgo que conlleve el tratamiento de los datos personales tal y como establece el Reglamento EU 2016/679.

3.- ÁMBITO DE APLICACIÓN

En el presente documento será de aplicación tanto a los medios técnicos como a los humanos:

- Personal con acceso a datos autorizado.
- Recursos protegidos. Entendiendo por recursos protegidos cualquier parte componente del sistema de información. Es decir, los programas, soportes y equipos empleados para el almacenamiento y tratamiento de los datos de carácter personal.

Los recursos que quedan protegidos son:

- Los centros de trabajo donde se encuentren ubicados o se almacenen los soportes que contengan datos de carácter personal.
- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a los datos personales.
- Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones.
- Los sistemas informáticos, o aplicaciones establecidas para acceder a los datos.

4.- REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El art.5 del RGPD establece los principios relativos al tratamiento de datos personales:

- Licitud, lealtad y transparencia: Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.
- Limitación de la finalidad: Los datos se deben recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
- Minimización de datos: Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Exactitud: Los datos deben ser exactos y, si fuera necesario, actualizados. Además, se establece que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación si los datos son inexactos con respecto a los finales para los que se tratan.
- Limitación del plazo de conservación: Los datos deben ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.
- Integridad y confidencialidad: Los datos deben ser tratados de tal manera que se garantice una seguridad adecuada mediante la aplicación de medidas de control apropiadas.

Estos son los principios que se han tenido en cuenta a la hora de determinar qué datos se van a recoger de los interesados.

La normativa, establece en su artículo 30.1 que "*cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad".*

Para la redacción del Registro de actividades del tratamiento, este documento seguirá las directrices marcadas por el artículo 30 del RGPD.

Contenido:

- Nombre y datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- Los fines del tratamiento.
- Una descripción de la categoría de interesados.
- Categorías de datos personales tratados.
- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- 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 y, en el caso de las transferencias indicadas en el artículo 49.1, la documentación de garantías adecuadas.
- Los plazos previstos para la supresión de los datos.
- Una descripción general de medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.1.

Asimismo, la normativa establece en su art. 30.2 *"Cada encargado y, en su caso, el representante del encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable".*

Para la redacción del Registro de actividades del tratamiento, este documento seguirá las directrices marcadas por el artículo 30 del RGPD.
Contenido:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos
- las categorías de tratamientos efectuados por cuenta de cada responsable
- en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas
- Una descripción general de medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.

En el ANEXO I**"**: A. REGISTRO DE ACTIVIDADES DEL RESPONSABLE DE TRATAMIENTO, se refleja el detalle de los registros de actividades de tratamiento de ELECTRA DE ZAS, SL
En el ANEXO II: B. REGISTRO DE ACTIVIDADES DEL ENCARGADO DE TRATAMIENTO, se refleja el detalle de los registros de actividades de tratamiento de ELECTRA DE ZAS, SL.

El personal con acceso a datos no podrá recopilar ni tratar otra tipología de datos ni con otras finalidades, plazos u otras condiciones reflejadas en el registro de actividades.

5.- ANÁLISIS DE RIESGOS

El 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, en adelante Reglamento General de Protección de datos, establece en su artículo 32, que versa sobre la seguridad del tratamiento de los datos, que el responsable de tratamiento aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Siguiendo las indicaciones del citado artículo, las medidas de seguridad incluirán:

- La seudonimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Dado que las actividades de tratamiento de ELECTRA DE ZAS, SL, no requieren una Evaluación de Impacto de Protección de Datos, se realiza un análisis de riesgos básico para determinar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados.

Este Análisis de Riesgos permitirá identificar las posibles amenazas y evaluar los riesgos para establecer las medidas de seguridad que permitan tratar a los mismos.

El análisis de riesgos constará de:

1. Descripción de las actividades de tratamiento.
2. Identificación de Riesgos.
3. Implantación de medidas de seguridad.

5.1.- DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO - ANÁLISIS DEL CICLO DE LA VIDA

El objetivo de este apartado es recoger toda la información que permita identificar todas las posibles amenazas y valorar los riesgos a los están expuestos los datos personales tratados por ELECTRA DE ZAS, SL.

En el ANEXO II: DESCRIPCIÓN DEL SISTEMADE TRATAMIENTO se documenta la descripción de las actividades de tratamiento.

Para entender el anexo, previamente se definen las 5 etapas del ciclo de la vida de los datos.

1.- ENTRADA DE DATOS: Se trata de identificar el origen de los datos. Analizar y detallar de qué forma llegan al responsable, si se obtienen del propio interesado o bien de terceros, qué medios se utilizan para su recogida y la legitimación para su tratamiento que puede estar basada en el consentimiento expreso, en una obligación legal o bien en un interés legítimo.

2.- ALMACENAMIENTO: Se trata de las operaciones y tecnologías que permiten conservar la información para recuperarla posteriormente. Aquí se debe concretar la ubicación de la información, es decir, si se trata de un almacenamiento en la nube o en sistemas propios. También donde están situados geográficamente

3.- TRATAMIENTO: Las operaciones realizadas sobre los datos personales, ya sean por procedimientos de datos automatizados o manuales.

4.- ACCESO, CESIÓN O COMUNICACIÓN: Tiene que ver con las funciones o permisos de los diferentes usuarios del sistema, que se resumen en la posibilidad de consultar y modificar datos. En esta etapa se debe tener en cuenta también que, en ocasiones es necesaria la cesión o comunicación de los datos personales a un tercero no relacionado con el responsable de tratamiento, ya sea persona física o jurídica. Se trata de los encargados de tratamiento.

5.- DESTRUCCIÓN: una vez dejan de ser necesarios los datos personales, deben ser eliminados de los sistemas informáticos o archivos físicos de forma que resulten irrecuperables. En esta

etapa deben explicarse los plazos de conservación de la información y describir los procesos de supresión.

Los elementos intervinientes en estas etapas del ciclo de la vida se pueden clasificar en las siguientes categorías:

1.- ACTIVIDADES DE TRATAMIENTO SOBRE LOS DATOS DE CARÁCTER PERSONAL: se trata de nombrar la finalidad sobre el tratamiento de los datos personales de un determinado colectivo de personas. Por ejemplo: la gestión de clientes para la prestación del servicio contratado, la gestión de clientes con fines de prospección comercial, …

2.- DATOS: Se identificarán los datos tratados en cada etapa del ciclo de la vida. Para establecer medidas de seguridad adecuadas, se tendrán en cuenta y se especificarán los datos especialmente sensibles.

3.- INTERVINIENTES: En cada ciclo de la vida, pueden existir distintos intervinientes: empleados que formen parte de la entidad o encargados de tratamiento.

4.- TECNOLOGÍA: se identificarán los sistemas tecnológicos que tratan y/o almacenan los datos de carácter personal y que intervienen en el ciclo de vida de la información.

Tras la revisión del ANEXO II: DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO, podemos identificar los riesgos asociados.

5.2.- IDENTIFICACIÓN DE RIESGOS

El objetivo de la identificación de riesgos es la búsqueda, reconocimiento y descripción de todos los posibles puntos de peligro tanto internos como externos.

Dado que se ha determinado que, ELECTRA DE ZAS, SL no necesita realizar una EIP, las actividades de tratamiento donde se puede aplicar el enfoque de gestión de riesgos por defecto se situarán siempre en un nivel de riesgo no elevado.

En el ANEXO III: GESTIÓN DE RIESGOS del presente Protocolo de Protección de Datos, se detalla la relación de riesgos identificados tras el análisis de la descripción de las actividades de tratamiento.

5.3.- IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD

Tras el análisis de la descripción de las actividades de tratamiento y haber detectado los posibles riesgos que pueden afectar la seguridad de los datos tratados por ELECTRA DE ZAS, SL, se establecen protocolos de protección de datos y medidas de seguridad técnicas que permitirán minimizar o eliminar los riesgos detectados.

6.- PROTOCOLOS DE PROTECCIÓN DE DATOS

Como protocolos de protección de datos, entendemos los procedimientos o pasos a seguir en los momentos de recogida, almacenamiento, tratamiento, cesión y destrucción de datos de carácter personal, para dar cumplimiento a la normativa de protección de datos.

6.1.- NOMBRAMIENTO DE UN COORDINADOR DE PROTECCIÓN DE DATOS

COORDINADOR DE PROTECCIÓN DE DATOS

Es importante destacar que, en ningún caso, el hecho de designar un Coordinador de Protección de Datos exime de responsabilidad al responsable de tratamiento. Es un puesto que no contempla la actual normativa en protección de datos y que únicamente se designa como medida de seguridad con el fin de coordinar el cumplimiento de los protocolos recomendados.

Así, el Coordinador de Protección de Datos será el encargado de coordinar las medidas de seguridad y protocolos de protección de datos que se definen en el presente documento.

El Coordinador firmará el documento **001 - NOMBRAMIENTO DE COORDINADOR DE PROTECCIÓN DE DATOS** con el fin de que estar informado de sus tareas como tal.

6.2.- PROTOCOLOS DE INFORMACIÓN/CONSENTIMIENTO DE LOS INTERESADOS.

Siguiendo las indicaciones de los artículos 13 y 14 del Reglamento General de Protección de datos, y el artículo 11 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, deberá informarse a toda persona que facilite sus datos de carácter personal de:

- Nombre del Responsable de Tratamiento.
- Finalidad con la que se tratarán los datos personales.
- El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
- La posibilidad de ejercitar los derechos en protección de datos.
- La identidad y datos de contacto del responsable del tratamiento.
- Los datos de contacto del Delegado de Protección de Datos, en su caso.
- La base jurídica o legitimación para el tratamiento.
- El plazo o los criterios de conservación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles.
- La previsión de transferencias a Terceros Países.
- El derecho a presentar una reclamación ante las Autoridades de Control.

Y además, en el caso de que los datos no se obtengan del propio interesado:

- El origen de los datos.
- Las categorías de los datos.

En relación al consentimiento para el tratamiento de datos de carácter personal, debe ser:

- Inequívoco y explícito: manifestado de manera clara por el interesado.

- Se solicitará consentimiento expreso para cada uno de los tratamientos de datos específicos: prestación de servicio, uso de fotografías, publicaciones en redes sociales o publicidad.

Para informar a los interesados y obtener el consentimiento probado para el tratamiento de sus datos de carácter personal, se redactan cláusulas informativas para todas las Entradas registradas en el Análisis del Sistema de Tratamiento de ELECTRA DE ZAS, SL.

CLIENTES/CLIENTES POTENCIALES

009A – CLÁUSULA INFORMACIÓN BÁSICA DE PROTECCIÓN DE DATOS: Esta cláusula se anexará a documentos que se faciliten a los clientes, como puedan ser las facturas.

009B – CLÁUSULA DE INFORMACIÓN AVANZADA DE PROTECCIÓN DE DATOS: Esta cláusula estará a disposición de cualquier cliente que la solicite. Se hará referencia a la misma en la cláusula de información básica y se incluirá en documentos de firma de aceptación de servicio por parte del cliente.

CON SOLICITANTES DE EMPLEO

007 – MODELO RESPUESTA A CURRÍCULUMS: este documento deberá entregarse a firmar a los candidatos que entregan su currículum.

- Currículums recibidos en mano: se les entregará el documento para que puedan firmarlo dejando constancia de la lectura y conformidad del mismo.
- Currículums recepcionados por correo ordinario, o que dejan en el buzón de correo ordinario de la entidad: En caso de que el candidato indique una dirección de correo electrónico, podremos enviar el "Modelo de respuesta a currículums" por correo electrónico. De lo contrario, conservaremos el currículum junto con el sobre sellado por el servicio de correos, que acreditará la forma en la que el currículum ha llegado a las instalaciones.

CUANDO LA VÍA DE ENTRADA DE INFORMACIÓN ES UNA PÁGINA WEB

Al abrirse la página web, lo primero que deberá visualizar el visitante es un banner informativo y de obtención de consentimiento sobre el uso de cookies, ya sean propias o de terceros.

El banner dará la opción directa de rechazar, aceptar o configurar las cookies aceptadas.

Además:

1.- Podrán rechazarse todas las cookies no esenciales en un solo clic. Las cookies esenciales para el funcionamiento de la página web no necesitan consentimiento, por lo que son las únicas que pueden estar marcadas por defecto.

2.- El usuario deberá tener claro cuáles son las cookies esenciales para la navegación web. En el apartado de configuración de cookies y en la política de cookies, deberá detallarse claramente cuales son esenciales y cuáles no.

3.- En la configuración de cookies, todas las opciones no necesarias, tendrán que estar desactivadas por defecto. Serán los usuarios quienes activen cada cookie que deseen habilitar.

4.- Hay que evitar cualquier práctica que pueda dar lugar a engaño. Los botones de aceptar y rechazar cookies serán claramente visibles y no deberán utilizarse colores o tamaños de fuente que dificulten su identificación.

5.- Deberá incluirse un mecanismo sencillo para que los usuarios puedan retirar su consentimiento al uso de cookies en cualquier momento.

6.- Se incluirá además un enlace a la política de cookies al completo que incluye la totalidad de información avanzada sobre cookies.

Tras cumplimentar el formulario de contacto y antes de poder enviar la información cumplimentada, el usuario deberá aceptar **017 - POLÍTICA PROTECCIÓN DE DATOS PARA PAGINA WEB**. La aceptación se realizará marcando una casilla "Acepto la política de protección de datos".

WEB QUE INCLUYE CORREO ELECTRÓNICO: Se incluirá en la página web un enlace o bien directamente el texto de **017 - POLÍTICA PROTECCIÓN DE DATOS PARA PAGINA WEB.** Se incluirá además, un enlace a pie de página de la web y siempre de forma visible y cercana a la zona en la que se visualiza el correo electrónico de contacto.

Asimismo, en un lugar visible de la web se incluirá el texto de la cláusula: **017 - AVISO LEGAL**, la cual debe figurar en la misma debido a ser una web corporativa.

6.3.- PROVEEDORES – ENCARGADOS DE TRATAMIENTO

Los proveedores a los que, para una correcta prestación del servicio, sea necesario dar acceso o comunicar datos de carácter personal, tienen la consideración de Encargados de Tratamiento y por tanto habrá que estar al día con lo dispuesto en el RGPD.
Para ello, se seguirán las siguientes normas de actuación:

- Previo a la contratación del servicio, se exigirá al Encargado de Tratamiento un certificado o alguna justificación que acredite que cumple con la normativa de protección de datos vigente.
- Nos aseguraremos también de que los productos y servicios contratados cumplen con los requisitos de seguridad establecidos por la empresa.
- Se formalizará un **013 – CONTRATO DE ENCARGADO DE TRATAMIENTO** con cada uno de los proveedores que tengan acceso o se les comuniquen datos de carácter personal.

En caso de que el proveedor facilite un contrato de servicios que regule las medidas de seguridad y protocolos de protección de datos a seguir, será revisado previamente por el Coordinador de Protección de Datos, para verificar que cumple con los requisitos establecidos en el RGPD.
En todo caso, el contenido mínimo del Contrato de Encargado de Tratamiento, o la cláusula de protección de datos del Contrato de Prestación de Servicios tendrá el siguiente contenido mínimo marcado por el artículo 28.3 del RGPD.

6.4.- ATENCIÓN DERECHOS PROTECCIÓN DE DATOS

Los interesados que hayan facilitado datos de carácter personal a ELECTRA DE ZAS, SL, podrán acceder, rectificar o suprimir los datos erróneos, solicitar la limitación del tratamiento de sus datos así como oponerse o retirar el consentimiento en cualquier momento, solicitar la portabilidad de los mismos o requerir la tutela de la Agencia Española de Protección de Datos.

Para dar cumplimiento a las obligaciones establecidas por la actual normativa de protección de datos, ELECTRA DE ZAS, SL en las cláusulas informativas se informa de las direcciones físicas y electrónicas en las que se pueden solicitar y/o presentar los citados formularios.

Además, para facilitar el ejercicio de los derechos de protección de datos, en caso de que así lo solicite el interesado, se entregará el formulario **018 – EJERCICIO DE DERECHOS PERSONALES**. El solicitante podrá cumplimentar el formulario y presentarlo adjuntando una copia de su DNI.

Pero no será imprescindible que el interesado cumplimente el citado formulario. Será admitida cualquier solicitud presentada por las vías de las que se informa en las cláusulas informativas básica y avanzada de protección de datos. Eso sí, siempre se exigirá una copia del DNI.

DETALLE Y PROCEDIMIENTO DE RESPUESTA PARA CADA UNO DE LOS DERECHOS

El plazo máximo para informar al interesado sobre las actuaciones derivadas de su petición es de un mes, pero siempre se tratará de dar respuesta en el menor plazo posible y sin dilación indebida.

En caso de solicitudes especialmente complejas, podrá extenderse a dos meses, pero se notificará esa ampliación en plazo de un mes.

Si la solicitud no tuviera lugar, se informará igualmente al interesado de ello, motivando la negativa, dentro del plazo de un mes desde la solicitud.

Derecho de Acceso: el interesado solicita información sobre los datos de carácter personal que están siendo tratados, el origen de los mismos, así como las comunicaciones de datos que se hayan realizado o puedan realizarse en un futuro. Podrá facilitársele todos los datos de base del afectado y también copias o documentos de los datos objeto del tratamiento.

Derecho de Rectificación: el interesado tiene derecho a solicitar que se rectifiquen sus datos de carácter personal cuando estén incompletos o incorrectos. Teniendo en cuenta que el hecho de no actualizar los datos, puede acarrear consecuencias negativas para la calidad de la prestación del servicio o para la correcta relación con el interesado, se gestionará de inmediato la rectificación de los datos erróneos o desactualizados.

Derecho de supresión: el afectado podrá solicitar que se eliminen la totalidad de sus datos de carácter personal.

Si los datos cancelados hubieran sido cedidos o comunicados a un tercero, se deberá notificar la solicitud de cancelación al cesionario en el mismo plazo de 10 días hábiles.

La cancelación de los datos una vez cumplida la finalidad para la que fueron recopilados, dará lugar al bloqueo de los mismos, conservándose únicamente a disposición de las

Administraciones Públicas, Jueces y Tribunales, para atender las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Derecho al olvido: el afectado podrá solicitar que se eliminen sus datos personales de los buscadores de Internet.

Para facilitar el ejercicio del derecho al olvido, se informará al solicitante de las URL´s de los principales buscadores de Internet, en las que podrá acceder de forma directa a los formularios de solicitud de derecho al olvido.

Limitación de tratamiento: el interesado podrá solicitar la limitación de tratamiento en los siguientes supuestos:

- El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.
- Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

Durante la duración de la limitación del tratamiento solo se podrán tratar los datos afectados:

- Con el consentimiento del afectado.
- Para la formulación, el ejercicio o la defensa de reclamaciones.
- Para proteger los derechos de otra persona física o jurídica.
- Por razones de interés público importante de la Unión o del Estado miembro correspondiente.

Derecho de oposición: Cuando no resulte necesario el consentimiento del interesado para tratar sus datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento.

Derecho a la portabilidad: El derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso en la que la persona interesada tiene derecho a recibir los datos personales que le afectan que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y de lectura mecánica, y transmitirlos a otro responsable, si se cumplen los requisitos siguientes:

- El tratamiento esté basado en el consentimiento o en un contrato.
- El tratamiento se haga por medios automatizados.
- Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan incluidos los datos derivados de la propia actividad del interesado. Esto supone que no es aplicable a los datos de terceras personas que un

interesado haya facilitado a un responsable. Como tampoco se aplicaría si el interesado solicita la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

Incluye el derecho a que los datos se transmitan directamente de responsable a responsable, cuando sea técnicamente posible.

Para dar respuesta siguiendo las indicaciones del Reglamento General de Protección de Datos, se utilizarán los modelos de respuesta: **019 – MODELOS DE RESPUESTA A SOLICITUDES DE DERECHOS DE DATOS PERSONALES.**

6.5.- RECURSOS HUMANOS

Evitar el error humano es clave para proteger los sistemas y la información. Por ello es importante tomar medidas de seguridad en la gestión de recursos humanos.

El protocolo a seguir será:

INFORMACIÓN AL PERSONAL: El personal con acceso a datos firmará el documento: **002 – PROTECCIÓN DE DATOS – PERSONAL CON ACCESO A DATOS.** El presente documento contiene:

- Acuerdo de confidencialidad para informar al interesado sobre su obligación de guardar secreto profesional, sus obligaciones en el uso de Internet y correo electrónico.
- Circular sobre implantación de medidas de seguridad para trabajadores, en la que se informa al interesado de las medidas de seguridad y protocolos en protección de datos que debe seguir en su puesto de trabajo.
- Información sobre el tratamiento de sus datos personales, para explicar al interesado el uso que se realiza de sus datos personales así como de sus derechos en materia de protección de datos.

PLAN DE FORMACIÓN Además de informar al personal con acceso a datos sobre las medidas de seguridad y procedimientos en materia de protección de datos, es recomendable establecer actividades, cursos, sesiones formativas, … para mantener a la plantilla que accede a datos personales, concienciada y formada en todo momento en aspectos relativos a la seguridad de la información.

CONCESIÓN AUTORIZADA DE LOS PERMISOS DE ACCESO. Se dará de alta al nuevo usuario en los sistemas de acuerdo con las políticas de control de acceso correspondientes. En este punto, se realizan las siguientes acciones: entregar las tarjetas de acceso físico; asignar las cuentas de correo electrónico; conceder los permisos de acceso a servicios, aplicativos y recursos compartidos; asignar el puesto de trabajo, los dispositivos y equipos. Para completar este punto es conveniente tener en cuenta lo detallado en el apartado 7. MEDIDAS TÉCNICAS DE SEGURIDAD.

FIN CONTRATO DEL PERSONAL: Una vez que el empleado finalice contrato, se revocarán todos los permisos de acceso, se eliminarán sus cuentas de correo electrónico y se cancelarán sus permisos de acceso a sistemas y aplicaciones.

7.- MEDIDAS TÉCNICAS DE SEGURIDAD

Entendemos por medidas técnicas de seguridad las acciones concretas a realizar en soportes automatizados y no automatizados para conseguir salvaguardar la integridad y confidencialidad de los datos personales.

7.1.- CONTROL DE ACCESOS

En el ciclo de la vida de los datos personales, hemos visto que existen "Intervinientes" que recogen, almacenan, tratan, comunican y destruyen la información.

A continuación, se define la política de seguridad a seguir para evitar tanto accesos de personal no autorizado, es decir posibles intrusismos por parte de asaltantes ajenos a la entidad, como protocolos para controlar y permitir el acceso a los intervinientes autorizados.

Se detectan dos tipos de Intervinientes autorizados en ELECTRA DE ZAS, SL: Personal laboral y Encargados de Tratamiento.

ENCARGADOS DE TRATAMIENTO

En el caso de los Encargados de Tratamiento, formalizarán su compromiso de dar cumplimiento a la política de protección de datos mediante la firma del Contrato de encargado de tratamiento, siguiendo el protocolo establecido en el apartado 6.3 del presente manual.

En general, será el personal autorizado de ELECTRA DE ZAS, SL, quien entregue la información al encargado de tratamiento, por lo que únicamente le remitirá la información concreta que necesitan para la prestación del servicio contratado.

Los métodos de envío de información:

- Informatizada: correo electrónico.
- Manual: en sobre cerrado, para evitar la pérdida accidental de documentos durante el traslado de los mismos.

En caso de que el Encargado de Tratamiento necesite una conexión directa o un acceso directo a los sistemas de información se atendrá a las medidas de seguridad establecidas para el personal laboral de ELECTRA DE ZAS, SL.

Se detalla en el ANEXO IV DETALLE DE MEDIDAS TÉCNICAS DE SEGURIDAD, el detalle de Encargados de Tratamiento existentes para cada actividad de tratamiento.

PERSONAL LABORAL

En cuanto al personal, la información será accesible únicamente por las personas que lo necesiten para el desarrollo de sus funciones y únicamente en el grado de acceso que necesiten.

En el momento de su incorporación, al personal que necesite acceso a la información, se le hará entrega de un usuario y una contraseña de acceso a los sistemas informáticos, que serán personales e intransferibles.

El responsable inmediato de la nueva incorporación, informará al Coordinador de Protección de Datos de los permisos que se le deben otorgar a la nueva incorporación: sistema de acceso al correo electrónico, acceso a programas informáticos para almacenamiento, tratamiento de datos personales,…

El interesado en solicitar el alta/modificación y baja de las autorizaciones de acceso a los datos, el interesado deberá solicitarlo formalmente y de forma directa y por escrito al su responsable directo, quien lo pondrá en conocimiento del Coordinador de Protección de Datos.

En caso de vacaciones, ausencias por enfermedad, etc. El interesado deberá solicitar nuevos accesos, quedando totalmente prohibida la cesión de contraseñas para acceso a soportes y/o soportes.

En los casos en que algún interviniente necesite un acceso extraordinario, se registrará en el ANEXO IV, dentro del apartado 3.- REGISTRO DE SOLICITUDES DE ACCESO EXTRAORDINARIO.

En el ANEXO IV: DETALLES DE MEDIDAS TÉCNICAS DE SEGURIDAD se incluye la relación de personal con acceso a datos autorizado para cada Actividad de Tratamiento. En esta relación se detallan las fases de tratamiento para las que tienen permiso (entrada, almacenamiento, tratamiento, cesión y destrucción).

La relación de Intervinientes se actualizará periódicamente en función de las incorporaciones/bajas de personal con acceso a datos, o según los cambios de contratación de servicios con encargados de tratamiento, y se revisará de forma anual mediante los puntos de control y/o auditorías de protección de datos.

7.2.- GESTIÓN DE SOPORTES

La relación de soportes que almacenan datos de carácter personal queda inventariada en el ANEXO IV.

IDENTIFICACIÓN

Los soportes que contienen datos de carácter personal, tanto en formato automatizado como manual, quedan identificados en su carátula. Con una descripción sencilla pero identificadora de su contenido.

CUSTODIA

Durante el tiempo que el soporte esté en uso, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas, por eso se les ha informado de las medidas de seguridad que deben cumplir para una correcta custodia de los soportes que almacenan información:

- Cierre de sesión en caso de abandono temporal del puesto de trabajo.
- Apagado del equipo en el momento de finalizar la jornada de trabajo.

- Dejar el puesto de trabajo recogido, de forma que todo documento que contenga datos personales quede archivado en su lugar correspondiente mientras no se esté utilizando.
- Evitar que la información manejada durante el tiempo de trabajo sea visualizada por personal no autorizado o por personal ajeno a la entidad.

ALMACENAMIENTO

El archivo de los soportes o documentos se realiza de acuerdo con los criterios establecidos por el Responsable de tratamiento. Se elegirá un método de archivo que permita localizar fácilmente la información y que garantice la correcta conservación de los documentos.

El almacenamiento de soportes estará protegido.

DISTRIBUCIÓN DE SOPORTES

Los métodos de envío de información:

- Informatizada: correo electrónico.
- Manual: en sobre cerrado, para evitar la pérdida accidental de documentos durante el traslado de los mismos.

PLAZOS DE CONSERVACIÓN DE LA INFORMACIÓN

La información se conservará durante el tiempo estrictamente necesario para prestar el servicio y dar cumplimiento a la normativa.

Una vez finalizada la relación, se conservarán para dar cumplimiento a las posibles exigencias legales por parte de la Administración Pública. Se tendrá en cuenta la siguiente tabla que refleja los plazos de prescripción de las distintas materias:

MATERIA	PRESCRIPCIÓN	NORMATIVA
Contable y mercantil.	6 años	Art. 30CC
Fiscal. Liquidar o exigir el pago de deudas tributarias.	4 años	Art. 66 Ley 58/2003
Fiscal. Comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación.	10 años	Art. 66 bis Ley 58/2003
Laboral. Infracciones.	3 años	Art. 4.1 Real Decreto Legislativo 5/2000

MATERIA	PRESCRIPCIÓN	NORMATIVA
Seguridad Social. Infracciones.	4 años	Art. 4.2 Real Decreto Legislativo 5/2000.
Prevención de Riesgos Laborales. Infracciones.	5 años	Art. 4.3 Real Decreto Legislativo 5/2000.
Delitos contra la Hacienda Pública y la Seguridad Social.	10 años	Art. 131 Ley Orgánica 10/1995.

DESTRUCCIÓN/REUTILIZACIÓN DE SOPORTES AUTOMATIZADOS

Los soportes informáticos que puedan contener información que contenga datos de carácter personal como CD´s, USB´s, discos duros extraíbles o incluso ordenadores que contengan discos de almacenamiento, se destruyen siguiendo las siguientes pautas:

- Todos los soportes informáticos removibles reutilizables deberán ser formateados (siempre que resulte posible) y entregados para su reutilización al Coordinador de protección de datos.
- Todos los soportes informáticos que vayan a ser desechados, serán formateados y entregados al Coordinador de protección de datos que procederá a la total destrucción de los mismos.
- La entrega o destrucción de ordenadores obsoletos será comunicada al Coordinador de protección de datos para que se elimine de forma segura toda la información contenida en dicho ordenador. En caso de que en el ordenador no se pudiera eliminar la información, se desmontarán los discos duros para proceder a una destrucción segura.

DESTRUCCIÓN DE SOPORTES NO AUTOMATIZADOS

Todos los soportes no automatizados que puedan contener información que contenga datos de carácter personal como documentos en papel, copias en papel, microfilms, cintas de audio o video y, en general cualquier tipo de soporte del que se pueda extraer la información, deberán ser eliminados o destruidos de acuerdo con las siguientes pautas:

- Ningún soporte deberá dejarse sin ser destruido previamente de forma que quede ilegible e irrecuperable.
- Aquellos soportes que vayan a ser desechados deberán depositarse en los contenedores señalados para proceder posteriormente a la incineración del contenido de los mismos.

7.3.- MEDIDAS DE PROTECCIÓN DE SOPORTES Y APLICACIONES

En el ANEXO IV se realiza un inventariado de los soportes de almacenamiento tanto de información automatizada como no automatizada, así como un inventariado del sistema de

almacenamiento de las aplicaciones o programas informáticos que realizan tratamiento de datos de carácter personal.

A continuación se detallan las medidas técnicas concretas a seguir para la protección de la información:

7.3.1. - POLÍTICA DE CONTRASEÑAS

REQUISITOS MÍNIMOS	Número de caracteres: 7 Tipo de caracteres: ALFANUMERICOS Periodo cambio: ANUALMENTE Nº intentos fallidos: NO
PROCEDIMIENTO DE DISTRIBUCIÓN DE CONTRASEÑAS	El Coordinador de protección de datos será el encargado de informar al interesado de su usuario y contraseñas de acceso a los distintos soportes y aplicaciones informáticas. Se realiza de forma personal y directa. Una vez entregada, el receptor deberá memorizarla y destruir el medio por el cual se le informó de la misma.
ALMACENAMIENTO	Las contraseñas, por motivos de seguridad, no se almacenan. Cada persona deberá ser responsable de recordar sus contraseñas de acceso. Una vez se entrega al interesado.
USO PERSONAL E INTRANSFERIBLE	La contraseña es de uso personal e intransferible. En caso de ausencia de alguno de los trabajadores por vacaciones, baja laboral… la contraseña no será facilitada a terceros.

7.3.2. - POLÍTICA DE COPIAS DE SEGURIDAD

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

PERIODICIDAD DE LA COPIA	SEMANAL
SOPORTE EN QUE SE REALIZA	DISCO DURO
ALMACENAMIENTO	EN LAS INSTALACIONES
SE ALMACENAN CIFRADAS	SI
REVISIÓN DEL PROCEDIMIENTO	Semestralmente se verificará el correcto funcionamiento de las copias de seguridad y de recuperación de datos.

En tratamientos manuales, la realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo la autorización del Responsable de Tratamiento, que se puede solicitar a través del Coordinador de protección de datos.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida, siguiendo las medidas de seguridad establecidas en el apartado 7.2 Gestión de Soportes.

7.4. - MEDIDAS DE CIBERSEGURIDAD

Del mismo modo que ha evolucionado la tecnología que utilizamos para desarrollar el trabajo en la empresa, lo ha hecho la ciberdelincuencia.

Las bases de datos de las empresas guardan una gran cantidad de información, tanto datos personales como datos bancarios. Con el fin de obtener esta información, los ciberdelincuentes buscan explotar las vulnerabilidades que nuestros equipos puedan presentar.

Para cumplir con la normativa vigente de Protección de Datos, las empresas deben tener un antivirus y un sistema operativo actualizados.

Las medidas de ciberseguridad deben aplicarse a la totalidad de los equipos y dispositivos corporativos y deben contar con las medidas necesarias para prevenir, detectar y contener cualquier tipo de amenaza a la que se vea expuesta nuestra organización.

En la actualidad, existen distintos tipos de sistemas operativos. El principal problema es que su soporte puede estar obsoleto si este sistema es muy antiguo. Por lo tanto, se mantendrá actualizado el sistema operativo para proteger nuestros equipos de posibles amenazas que puedan surgir.

ANTIVIRUS	WINDOWS DEFENDER
SISTEMA OPERATIVO	WINDOWS
REVISIÓN DE ACTUALIZACIONES	Mensualmente se verificará que las actualizaciones estén correctamente instaladas en los equipos informáticos.

7.5. - RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL RESPONSABLE DE TRATAMIENTO

Se contempla la posibilidad del trabajo fuera de las instalaciones por parte del personal, por lo que, habrá que atenerse a lo dispuesto en la Ley 10/2021 de 9 de julio, de trabajo a distancia.

MEDIDAS PARA GARANTIZAR EL DERECHO A LA INTIMIDAD Y PROTECCIÓN DE DATOS DEL EMPLEADO:

Los empleados que desarrollen sus funciones en la modalidad de distancia y/o teletrabajo, tendrán derecho a la intimidad y protección de datos en su ámbito de trabajo, al igual que aquellos que desarrollan su trabajo presencialmente.

- Todos los trabajadores que realicen teletrabajo, recibirán un ACUERDO DE TRABAJO A DISTANCIA en el que consta:

- Art. 7.1 a) Un inventario de los equipos y herramientas facilitados para el desarrollo del trabajo a distancia, la vida útil o periodo máximo de renovación de los mismos. estimada de los mismos
- Art. 7.1 h) Los medios de control empresarial de la actividad.
- Art. 7.1 i) Procedimiento a seguir en el caso de producirse dificultades técnicas que impidan el normal desarrollo del trabajo a distancia.
- Art. 7.1 j) Instrucciones dictadas por la empresa, en materia de protección de datos, específicamente aplicables en el trabajo a distancia.
- Art. 7.1 k) Instrucciones dictadas por la empresa, sobre seguridad de la información, específicamente aplicables en el trabajo a distancia.

La empresa establece como medidas de vigilancia y control para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, las siguientes:

- Control horario mediante fichaje tal y como establece el Real Decreto Ley 8/2019
- El artículo 20.3 del Estatuto de los trabajadores habilita al empresario a controlar el correo electrónico y accesos a Internet que él otorga a los trabajadores para el desarrollo de sus funciones. Por ello le informamos de que su cuenta de correo electrónico laboral y consultas web con medios de la empresa y durante la jornada laboral no son privadas y podrán ser consultada por parte de la entidad.

MEDIDAS ADICIONALES PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN DURANTE EL TELETRABAJO

Los soportes y aplicaciones utilizadas en formato de teletrabajo, tienen implantadas las mismas medidas técnicas de seguridad que los soportes y aplicaciones utilizadas en los centros de trabajo, por ello habrá que atenerse a las medidas de seguridad y protocolo de tratamiento de datos personales detallados en el presente Protocolo de Protección de Datos.

En concreto, para el tratamiento de datos que se realiza durante las jornadas de teletrabajo, es importante tener en cuenta las siguientes instrucciones:

- Sólo los medios aprobados por la entidad pueden ser usados para llevar a cabo sus actividades. En ningún caso el trabajador podrá utilizar herramientas propias o personales para el desempeño del trabajo.
- Será siempre la entidad quien aporte al trabajador los medios necesarios para el correcto desempeño de su labor, con el fin de garantizar la seguridad de la información que se trata con los mismos.
- El transporte de los dispositivos se realizará en maletines u otros medios que permitan proteger los dispositivos de golpes accidentales.
- Todos los dispositivos y medios facilitados al trabajador llevarán implantadas las medidas técnicas de seguridad detalladas en el Protocolo de Protección de Datos de la entidad.

INSTRUCCIONES ESPECÍFICAS SOBRE PROTECCIÓN DE DATOS

Se considerará Información confidencial la información de propiedad de la empresa y la información que genere la persona trabajadora en virtud del contrato de trabajo.

La persona trabajadora debe guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle, comprometiéndose a no divulgar dicha Información confidencial, por ningún medio físico o electrónico, así como a no publicarla ni ponerla a disposición de terceros, a no ser que cuente con el consentimiento de la empresa

La persona trabajadora se obliga a respetar la legislación en materia de protección de datos, las políticas de privacidad y de seguridad de la información que la empresa ha implementado, como también a:

- Utilizar los datos de carácter personal a los que tenga acceso único y exclusivamente para cumplir con sus obligaciones para con la empresa.
- A no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.
- El acceso a los diferentes entornos y sistemas informáticos de la persona trabajadora será efectuado siempre y en todo momento bajo el control y la responsabilidad de la misma, siguiendo los procedimientos establecidos por la entidad.
- A proteger la información contenida en dispositivos automatizados frente a posibles accesos de terceros no autorizados, cerrando sesión o bien apagándolos al acabar la jornada laboral.
- A proteger la información contenida en soportes no automatizados. Así, queda prohibido almacenar información en soporte papel. Aquella documentación que deba ser almacenada en el domicilio del trabajador por resultar imposible conservarla en otro formato, se protegerá archivándola en un lugar privado y seguro frente a terceros no autorizados y se entregará/enviará a las instalaciones de la entidad a la mayor brevedad posible.
- Cumplir con las medidas de seguridad que la empresa haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso.
- Atenerse a las medidas de seguridad recogidas en el Protocolo de Protección de Datos que la entidad mantendrá a disposición del trabajador siempre que lo necesite.

PROTOCOLO FRENTE A DIFICULTADES TÉCNICAS QUE IMPIDAN EL NORMAL DESARROLLO DEL TRABAJO A DISTANCIA

- INCIDENCIAS DETECTADAS POR EL TRABAJADOR:

El trabajador podrá ponerlas en conocimiento de la entidad a través de su responsable inmediato.

- Se utilizará el correo electrónico para comunicar la incidencia formalmente.
- En caso de que la incidencia impida el uso del correo electrónico, podrá comunicarse de forma telefónica o utilizando algún otro medio que garantice que la entidad queda informada de manera inmediata.
- El plazo para comunicar la incidencia es inmediato. Es decir, la incidencia debe comunicarse tan pronto como se detecte.

- INCIDENCIAS DETECTADAS POR LA ENTIDAD:

La entidad comunicará la incidencia a los trabajadores aportando instrucciones de actuación claras y precisas.

- Se utilizará el correo electrónico para comunicar la incidencia formalmente.
- En caso de que la incidencia impida el uso del correo electrónico, podrá comunicarse de forma telefónica o por otros medios que garanticen que los trabajadores son informados de manera inmediata.
- El plazo para comunicar la incidencia es inmediato.
- Cuando la incidencia afecte al trabajo de los empleados impidiendo el desarrollo del mismo, éstos recibirán instrucciones concretas sobre qué hacer mientras la incidencia se resuelve.
- Una vez resuelta la incidencia, nuevamente se reportará a los empleados, aportando nuevas instrucciones a aplicar en sus medios de trabajo o bien herramientas nuevas, según resulte necesario en cada caso.

El hecho de que una incidencia ajena al trabajador impida el correcto desarrollo y rendimiento en su trabajo, no repercutirá en su salario.

En caso de que la incidencia no pueda resolverse antes de las 24 horas, la entidad podrá solicitar a los trabajadores que desarrollen su jornada en su centro de trabajo asignado, hasta que la incidencia se resuelva.

8.- PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se entiende por “incidencia de seguridad” cualquier incumplimiento del protocolo de seguridad de protección de datos, o cualquier anomalía que afecte o pueda afectar a la seguridad de la información.

El procedimiento a seguir para la notificación de incidencias será:

Notificación al Coordinador de Protección de Datos en caso de que la incidencia sea comunicada por un tercero, en la que se hagan constar los siguientes datos:

- Identificación clara del tipo de incidencia producida.
- Descripción detallada de la Incidencia:
  - Intervenciones de personas que hayan podido tener relación con la producción de la incidencia.
  - Momento –día y hora- de su producción.
  - Persona que notifica la incidencia.
  - Persona a la que se le comunica la incidencia.
  - Efectos derivados de la incidencia.

Solicitar al coordinador un acuse de recibo en el que se haga constar que ha recibido la notificación de la incidencia y que contiene todos los extremos mencionados anteriormente.

En caso de que resulte necesario aplicar procedimientos de recuperación de datos será necesaria la autorización por escrito del responsable de tratamiento.

En el ANEXO V estará disponible el Registro de Incidencias, el modelo de solicitud de autorización para recuperación de datos, así como el registro de recuperación de datos.

8.1.- PROCEDIMIENTO DE MEDIDAS A SEGUIR ANTE UNA INCIDENCIA O BRECHA DE SEGURIDAD

Tras haberse producido la brecha de seguridad, el coordinador en protección de datos, junto con las personas responsables o quién el mismo determine, analizarán la situación acontecida para adoptar las medidas oportunas para erradicar la situación y emprender las acciones de recuperación necesarias.

A continuación, procedemos a explicar las medidas necesarias para llevar a cabo un óptimo procedimiento.

MEDIDAS DE CONTENCIÓN

Las medidas de contención que seguiremos podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la resolución del incidente.

Las medidas de contención más sencillas las podrá iniciar el propio usuario, por lo contrario, las medidas más complejas serán llevadas a cabo por personal especializado en seguridad informática de la empresa.

Las medidas que se tomarán serán:

- Impedir el acceso al origen de la difusión: dominios, puertos, servidores, la fuente o los destinatarios de la difusión. Dependiendo del vector de ataque, impedir el acceso al origen: dominios, conexiones, equipos informáticos o conexiones remotas, puertos, parches, actualización del software de detección (antivirus, IDS, etc.) bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.
- Anular y/o modificar todas las contraseñas de carácter lógico y físico de los usuarios con acceso a información relevante.
- Hacer una copia del sistema y analizarlo utilizando herramientas que permitan extraer la información de los discos y memorias del sistema, sin alterar el estado de los mismos.
- Aislar el sistema utilizado para revelar los datos, con el fin de realizar un análisis que le permita buscar datos ocultos, dañados o eliminados más tarde.
- Si se detecta que los datos han sido difundidos a servidores públicos, solicitar al propietario o a la persona responsable del mantenimiento o programación informática, que elimine los datos difundidos.
- Controlar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales (FB, Twitter, etc.) así como los comentarios y reacciones de los usuarios de Internet.

MEDIDAS DE ERRADICACIÓN

Ante brechas de seguridad de índole técnica que afecten a los datos automatizados o a aplicaciones informáticas, se solicitará la ayuda de un servicio externo especializado en la materia, en caso de que las herramientas y medios humanos y materiales con los que cuenta internamente la entidad no sean capaces de poner llevar a cabo dichas erradicaciones.

Algunos procedimientos que se llevarán a cabo podrán ser:

- Definir el proceso de desinfección, basado en firmas, herramientas, nuevas versiones/revisiones de software, etc. y probarlo.
- Asegurar que el proceso de desinfección funciona adecuadamente sin dañar servicios.
- Comprobar la integridad de todos los datos almacenados en el sistema no han sido modificados.
- Revisar la correcta planificación y actualización de los motores y firmas de antivirus.
- Análisis con antivirus de todo el sistema, los discos duros y la memoria.
- Restaurar conexiones y privilegios paulatinamente. Especial acceso restringido paulatino de máquinas remotas o no gestionadas.

MEDIDAS DE RECUPERACIÓN

En la medida de recuperación se restablecerá el servicio en su totalidad, verificando su funcionamiento normal y evitando nuevos sucesos basados en la misma causa.

A parte de adoptar las medidas activas, también se incluirán controles periódicos y eficaces que permitan el seguimiento constante de los procesos de mayor riesgo.

Identificación y análisis de soluciones (corto, medio plazo): Se identificarán las diferentes medidas enfocadas a evitar nuevos incidentes de seguridad basados en la misma causa, así como intentar reducir el riesgo de los mismos. Se contrastarán con las medidas adoptadas para solventar el incidente en cuestión y garantizar un análisis detallado de soluciones.

Selección estrategia: Evaluando las necesidades, se seleccionará la estrategia a seguir para evitar nuevas incidencias.

Verificación de recuperación e implementación de medidas: Se garantizará no solo el restablecimiento a la situación previa al incidente, sino revisar el análisis de riesgos y recoger la implementación en la entidad de controles adicionales y periódicos para evitar futuros incidentes similares.

MEDIDAS DE RECOLECCIÓN Y CUSTODIA DE EVIDENCIAS

Se tomarán las medidas necesarias para contener y revertir el impacto que haya podido tener la brecha de seguridad sobre la entidad. Estas acciones pueden incurrir en la modificación de evidencias, lo que puede imposibilitar el uso de la información registrada por los sistemas involucrados de cara a la presentación de esta información frente a terceros, y en especial su uso como prueba en procedimientos judiciales y administrativos.

Para garantizar que la información generada por los sistemas involucrados en la brecha de seguridad cumpla los objetivos de cumplimiento de la organización, de cara a que dichos

registros puedan ser utilizados frente a terceros y/o en litigios, es necesario tener en consideración dos aspectos para cada brecha de seguridad:

- Definir la necesidad de uso de la información por parte de la organización en la propia fase de detección de la brecha de seguridad de cara a la recolección de evidencias.
- Establecer la cadena de custodia adecuada que satisfaga el uso de la información definido por la organización.

MEDIDAS DE COMUNICACIÓN E INFORME DE RESOLUCIÓN (INTERNA / EXTERNA)

Las conclusiones del proceso de comunicación del diagnóstico de la brecha de seguridad deben quedar debidamente registradas, incluyendo las valoraciones finales de los técnicos y responsables del equipo. Todas ellas deben quedar reflejadas en el informe de resolución.

Se debe dispondrá de la siguiente información para poder elaborar correctamente el informe:

- Descripción objetiva del incidente.
- Controles existentes en el momento del incidente.
- Enumeración de medidas efectivas de respuesta.
- Declaración de si a igual casuística el incidente se repetiría.
- Medidas de detección aplicadas para identificar nuevos casos.
- Registro de comunicaciones durante la respuesta.

Comunicación: dirección y partes interesadas.

La comunicación debe de ser activa durante todo el tiempo que dure el proceso de respuesta, y debe hacerse de una manera continuada de modo que la dirección y responsables de seguridad tengan una toda la información del incidente como de las acciones tomadas para resolverlo. Para poder informar correctamente a los afectados en caso de preguntar sobre todo si los datos se hacen públicos.

Elaboración del informe de resolución.

El objetivo del informe de resolución es el apoyo para no recaer en un futuro en los mismos errores. Con carácter interno, este informe facilitará a todos los equipos involucrados en la respuesta al incidente, el entendimiento de las acciones tomadas, así como las acciones marcadas para seguimiento en el corto, medio y largo plazo. Serán tenidos en cuenta los cambios necesarios que deberían ser incluidos en el análisis de riesgos de la organización.

El informe incluirá detalles técnicos sobre las diferentes acciones llevadas a cabo. Este informe constará en gran parte de la documentación elaborada durante el proceso de respuesta.

El informe de resolución se presentará de forma lineal, de modo que facilite el seguimiento de las diferentes acciones, e incluirá al menos información relativa a los siguientes apartados:

- 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.

9.- NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

El Reglamento General de protección de datos define las violaciones de seguridad de los datos o "quiebras de seguridad" como todo incidente 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. Si se produce una violación de la seguridad, el responsable debe notificarlo a la autoridad de control en un plazo máximo de 72 horas, a menos que sea improbable que constituya un riesgo para los derechos y libertades de las personas.

En caso de que no pueda realizarse la notificación en ese plazo, se realizará con posterioridad, o de forma escalonada, acompañada de una explicación de los motivos que han ocasionado el retraso.

Se considera que se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance. La mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

Si se considera que las características de la quiebra pudieran tener un gran impacto, sí se contactará con la Agencia Española de Protección de Datos tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

En el ANEXO VI: NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD se encuentra el formulario con el contenido mínimo a comunicar a la AGPD, pero las brechas de seguridad se comunicarán directamente a la Agencia Española de Protección de Datos a través de su sede electrónica:

https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

Se notificará al RESPONSABLE DEL TRATAMIENTO, sin dilación indebida, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia

Para entender mejor el procedimiento a seguir, a continuación, se indican varios puntos a tener en cuenta para la notificación de una manera correcta:

En primer lugar, cabe destacar que Según el Artículo 4, del 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 se entenderá por:

- «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

En segundo que lugar, que teniendo en cuenta todo lo relativo a la incidencia/violación de seguridad, el procedimiento concreto llevado a cabo será:

1. Detectada e identificada una brecha de seguridad por cualquier usuario de los sistemas de información, es necesario comunicarlo a la persona designada como Coordinador de Protección de Datos a efectos de su análisis, clasificación, elaboración de un plan de respuesta con el diseño de las medidas a adoptar para contener, reducir o eliminar posibles daños y, en su caso inicio del proceso de notificación.

   A tal efecto, ante cualquier detección de exposición de datos personales bien sean en lugares que incluyan soportes físicos o informáticos, el usuario que detecte la incidencia deberá cumplimentar el formulario del ANEXO V: REGISTRO DE INCIDENCIAS del Protocolo de Seguridad de la empresa (en caso de que la detección, dando el mayor número de detalles necesarios para su análisis y valoración, y enviarlo al Coordinador de Protección de Datos.

2. El Coordinador de Protección de Datos, con asesoramiento del Delegado de Protección de Datos, analizarán la comunicación para determinar si se está ante una brecha de seguridad relacionada con la protección de datos de carácter personal.

En caso de que lo sea, se determinarán las medidas correctoras a aplicar y los controles a implementar (indicadas en detalle en el apartado 8.1)

Para que esta notificación de información sea lo más veraz y correcta posible, se actuará de la siguiente manera:

El coordinador de Protección de datos recabará los datos necesarios para comunicar al Responsable de Tratamiento, una vez analizados todos factores influyentes y tras haber valorado y recopilado toda la información sobre la brecha o incidente ocasionado, procederá a comunicarlo a la Agencia de Protección de Datos en el plazo máximo de 72 horas desde su detección.

La/s persona/s que detecten la brecha o incidente de seguridad, deberán comunicar el máximo de información recabada al Coordinador de Protección de datos, como:

- La información temporal de la brecha: Fecha de la detección (si la misma es exacta o aproximada), si la misma está o no resuelta en el momento de la comunicación y medios de detección.

- Resumen del incidente, y tipo de brecha (brecha de confidencialidad (acceso no autorizado), de integridad (modificación no autorizada) o de disponibilidad (desaparición o pérdida)
- Medio por el que se ha materializado la brecha (hacking, malware, pishing, Dispositivos robados o perdidos, datos enviados por error…etc) y si la misma ha sido ejecutada de manera intencionada, tanto interna como externamente.
- Medidas preventivas aplicadas antes de la brecha.
- Información sobre que categoría de datos han sido afectados (datos básicos, económicos o financieros, credenciales de accesos, datos especialmente protegidos,…)
- Número aproximado de afectados.
- Tipología de datos afectados (empleados, clientes, proveedores…)

Además, cuando sea probable que la violación pueda comportar un alto riesgo para los derechos de los interesados, el responsable lo deberá comunicar a las personas afectadas sin dilaciones indebidas y en lenguaje claro y sencillo. En caso de que resulten afectados otros responsables de tratamiento, deberá comunicárseles también sin dilación indebida.

El objetivo de la comunicación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias Por ello el Reglamento General de Protección de Datos requiere que se realice sin dilación indebida, sin hacer referencia al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas.

Asimismo, en el caso de ser detectada una incidencia, y tener que notificar al Responsable de Tratamiento esta, se seguirán en todo momento las pautas acordadas en las obligaciones del Encargado de Tratamiento dispuestas en el Contrato formalizado entre Responsable y Encargado de tratamiento.

10. - PROCEDIMIENTOS DE REVISIÓN

Este protocolo de protección de datos deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en los datos personales tratados o como consecuencia de los controles periódicos realizados.
En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.
Además, deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
Se realizarán puntos de control anuales para analizar posibles cambios en la entidad que afecten a las medidas de seguridad de la información, y deban reflejarse en el presente manual.
El Coordinador de Protección de Datos será el encargado de aprobar las modificaciones del Protocolo de Protección de Datos, así como de comunicar las modificaciones al personal que pueda verse afectado.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.

Los informes de auditoría serán analizados por el Coordinador de Protección de Datos, que elevará las conclusiones al responsable de tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos.

11.- DISPOSICIÓN FINAL

El presente documento ha sido aprobado por ELECTRA DE ZAS, SL como responsable de tratamiento, aceptándolo en su totalidad y ordenando su ejecución y cumplimiento, en particular por todos aquellos a quienes afecta y, en general, por todo el personal de ELECTRA DE ZAS, SL.

En ZAS, 06 de marzo de 2025

ANEXO I: REGISTRO DE ACTIVIDADES

DATOS COMUNES A TODOS LOS TRATAMIENTOS	
DIRECCIÓN FISCAL	VILAR DO MATO Nº 27,15850- ZAS (A CORUÑA).
CENTROS DE TRABAJO	VILAR DO MATO Nº 27,15850- ZAS (A CORUÑA).
DEPENDENCIA EJERCICIO DERECHOS PROTECCIÓN DE DATOS	0; VILAR DO MATO Nº 27,15850 -ZAS (A CORUÑA).

A. REGISTRO DE ACTIVIDADES RESPONSABLE DE TRATAMIENTO

REGISTRO DE ACTIVIDAD - CLIENTES	
RESPONSABLE DE TRATAMIENTO	ELECTRA DE ZAS, SL
REPRESENTANTE DEL RESPONSABLE DE TRATAMIENTO	Dª. ARANZAZU POSSE FRAGA
LEGITIMACIÓN	- El consentimiento del interesado.
FINALIDADES DEL TRATAMIENTO	- Gestión de clientes fiscal, contable y administrativa - Prestar servicio contratado.
CATEGORÍAS DE INTERESADOS	- Clientes, solicitantes de servicio.
PROCEDENCIA DE LOS DATOS	Propio interesado o su representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nombre, apellidos, dirección, teléfono, firma, DNI, número de cuenta.
	ESPECIALMENTE SENSIBLES:
	OTROS DATOS TIPIFICADOS: Financieros económicos y de seguros, transacciones de bienes y servicios.
CESIONES PREVISTAS	- Administración tributaria. - Bancos, cajas de ahorros y cajas rurales. - Organizaciones o personas directamente relacionadas con el responsable: encargados de tratamiento (consultar ANEXO IV).
TRANSFERENCIAS INTERNACIONALES	
PLAZO DE CONSERVACIÓN	Se detalla en el punto 7.2 – PLAZOS DE CONSERVACIÓN DE INFORMACIÓN del presente protocolo de protección de datos.
SISTEMA DE TRATAMIENTO	Mixto.

REGISTRO DE ACTIVIDAD – AGENDA DE CONTACTOS Y PROVEEDORES	
RESPONSABLE DE TRATAMIENTO	ELECTRA DE ZAS, SL
REPRESENTANTE DEL RESPONSABLE DE TRATAMIENTO	Dª. ARANZAZU POSSE FRAGA
LEGITIMACIÓN	- La ejecución del contrato de prestación de servicios formalizado.
FINALIDADES DEL TRATAMIENTO	- Gestión de agenda de contactos, personas de contacto y proveedores. - Gestión fiscal, contable y administrativa.
CATEGORÍAS DE INTERESADOS	- Personas de contacto. - Proveedores.
PROCEDENCIA DE LOS DATOS	Propio interesado o su representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nombre, apellidos, dirección, teléfono, firma y DNI.
	ESPECIALMENTE SENSIBLES:
	OTROS DATOS TIPIFICADOS: Financieros económicos y de seguros, transacciones de bienes y servicios.
CESIONES PREVISTAS	- Administración tributaria. - Bancos, cajas de ahorros y cajas rurales. - Organizaciones o personas directamente relacionadas con el responsable: encargados de tratamiento (consultar ANEXO IV).
TRANSFERENCIAS INTERNACIONALES	-
PLAZO DE CONSERVACIÓN	Se detalla en el punto 7.2 – PLAZOS DE CONSERVACIÓN DE INFORMACIÓN del presente protocolo de protección de datos.
SISTEMA DE TRATAMIENTO	Mixto.

REGISTRO DE ACTIVIDAD – EMPLEADOS	
RESPONSABLE DE TRATAMIENTO	ELECTRA DE ZAS, SL
REPRESENTANTE DEL RESPONSABLE DE TRATAMIENTO	Dª. ARANZAZU POSSE FRAGA
LEGITIMACIÓN	- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
FINALIDADES DEL TRATAMIENTO	- Gestión de recursos humanos: control de vacaciones, horario laboral… - Gestión de nóminas, contratos laborales.
CATEGORÍAS DE INTERESADOS	- Empleados.
PROCEDENCIA DE LOS DATOS	Propio interesado o su representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nombre, apellidos, dirección, teléfono, firma, DNI y número seguridad social.
	ESPECIALMENTE SENSIBLES:
	OTROS DATOS TIPIFICADOS: Características personales, Académicos y Profesionales, Detalles del Empleo Financieros, económicos y de seguros.
CESIONES PREVISTAS	- Administración tributaria. - Bancos, cajas de ahorros y cajas rurales. - Organizaciones o personas directamente relacionadas con el responsable: encargados de tratamiento (consultar ANEXO IV). - Entidades aseguradoras. - Seguridad Social.
TRANSFERENCIAS INTERNACIONALES	-
PLAZO DE CONSERVACIÓN	Se detalla en el punto 7.2 – PLAZOS DE CONSERVACIÓN DE INFORMACIÓN del presente protocolo de protección de datos.
SISTEMA DE TRATAMIENTO	Mixto.

REGISTRO DE ACTIVIDAD - CURRÍCULUMS	
RESPONSABLE DE TRATAMIENTO	ELECTRA DE ZAS, SL
REPRESENTANTE DEL RESPONSABLE DE TRATAMIENTO	Dª. ARANZAZU POSSE FRAGA
LEGITIMACIÓN	- El consentimiento del interesado.
FINALIDADES DEL TRATAMIENTO	- Gestión de currículums y selección de personal.
CATEGORÍAS DE INTERESADOS	- Solicitantes de empleo y empleados.
PROCEDENCIA DE LOS DATOS	Propio interesado o su representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nombre, apellidos, dirección, teléfono, imagen, firma y DNI.
	ESPECIALMENTE SENSIBLES:
	OTROS DATOS TIPIFICADOS: Características personales, Académicos y Profesionales, Detalles del Empleo.
CESIONES PREVISTAS	-
TRANSFERENCIAS INTERNACIONALES	-
PLAZO DE CONSERVACIÓN	- Un año. - En caso de que el currículum pertenezca a un empleado de la empresa, se conservará según lo detallado en el punto 7.2 – PLAZOS DE CONSERVACIÓN DE INFORMACIÓN del presente protocolo de protección de datos.
SISTEMA DE TRATAMIENTO	Mixto.

REGISTRO DE ACTIVIDAD – USUARIOS WEB	
RESPONSABLE DE TRATAMIENTO	ELECTRA DE ZAS, SL
REPRESENTANTE DEL RESPONSABLE DE TRATAMIENTO	Dª. ARANZAZU POSSE FRAGA
LEGITIMACIÓN	- El consentimiento del interesado.
FINALIDADES DEL TRATAMIENTO	- Gestión de atención a consultas de usuarios de la página web.
CATEGORÍAS DE INTERESADOS	- Usuarios web/RRSS
PROCEDENCIA DE LOS DATOS	Propio interesado o su representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nombre, apellidos, dirección, teléfono.
	ESPECIALMENTE SENSIBLES:
	OTROS DATOS TIPIFICADOS:
CESIONES PREVISTAS	-
TRANSFERENCIAS INTERNACIONALES	-
PLAZO DE CONSERVACIÓN	Durante el tiempo necesario para atender y tramitar las consultas.
SISTEMA DE TRATAMIENTO	Automatizado.

ANEXO II: DESCRIPCIÓN DEL SISTEMA DE TRATAMIENTO – ANÁLISIS DEL CICLO DE LA VIDA

GESTIÓN DE CLIENTES

	ENTRADA	ALMACENAMIENTO	TRATAMIENTO	ACCESO - CESIÓN	DESTRUCCIÓN
ACTIVIDADES DEL PROCESO	Recogida de datos en: - Verbalmente.	Dar entrada a la información en sistemas de almacenamiento.	- Prestación del servicio. - Gestión administrativa derivada de la prestación del servicio.	Detalle de personal y Encargados de Tratamiento con acceso a datos en ANEXO IV.	- Mientras no se solicite la supresión de los mismos. - Incineración.
DATOS TRATADOS	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	- - Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	
INTERVINIENTES	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal y Encargados de Tratamiento con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.
TECNOLOGÍAS INTERVINIENTES	- Web. - Telefonía.	Detalle de sistemas informáticos de almacenamiento en ANEXO IV.	Detalle de sistemas informáticos de tratamiento en ANEXO IV	- Correo electrónico Detalle de sistemas informáticos en ANEXO IV.	- Borrado. - Formateo

GESTIÓN DE AGENDA DE CONTACTOS Y PROVEEDORES

	ENTRADA	ALMACENAMIENTO	TRATAMIENTO	ACCESO - CESIÓN	DESTRUCCIÓN
ACTIVIDADES DEL PROCESO	Recogida de datos en: - Fuentes accesibles al público. - Información facilitada directamente por el proveedor.	Dar entrada a la información en sistemas de almacenamiento.	- Prestación del servicio. - Gestión administrativa derivada de la prestación del servicio.	Detalle de personal y Encargados de Tratamiento con acceso a datos en ANEXO IV.	- Mientras no se solicite la supresión de los mismos - Incineración.
DATOS TRATADOS	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	- Datos Identificativos. - Económicos, Financieros y de Seguros. - Transacciones de Bienes y Servicios.	
INTERVINIENTES	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal y Encargados de Tratamiento con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.
TECNOLOGÍAS INTERVINIENTES	- Web. - Telefonía.	Detalle de sistemas informáticos de almacenamiento en ANEXO IV.	Detalle de sistemas informáticos de tratamiento en ANEXO IV.	- Correo electrónico. Detalle de sistemas informáticos en ANEXO IV.	- Borrado. - Formateo.

GESTIÓN DE EMPLEADOS

	ENTRADA	ALMACENAMIENTO	TRATAMIENTO	ACCESO - CESIÓN	DESTRUCCIÓN
ACTIVIDADES DEL PROCESO	Recogida de datos en: -Formulario en papel. -Contrato. -Verbalmente. -Correo electrónico.	Dar entrada a la información en sistemas de almacenamiento	Gestión de nóminas, personal y RRHH.	Detalle de personal y Encargados de Tratamiento con acceso a datos en ANEXO IV.	- Mientras dure el contrato laboral y hasta que no se solicite la supresión. - Incineración.
DATOS TRATADOS	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo. - Económicos, Financieros y de Seguros.	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo. - Económicos, Financieros y de Seguros.	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo. - Económicos, Financieros y de Seguros.	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo. - Económicos, Financieros y de Seguros.	
INTERVINIENTES	Detalle de personal con acceso a datos ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal y Encargados de Tratamiento con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.
TECNOLOGÍAS INTERVINIENTES	- Web - Telefonía	Detalle de sistemas informáticos de almacenamiento en ANEXO IV.	Detalle de sistemas informáticos de tratamiento en ANEXO IV.	- Correo electrónico Detalle de sistemas informáticos en ANEXO IV.	- Borrado. - Formateo.

CURRÍCULUMS

	ENTRADA	ALMACENAMIENTO	TRATAMIENTO	ACCESO - CESIÓN	DESTRUCCIÓN
ACTIVIDADES DEL PROCESO	Recogida de datos: -Currículum, aportado por el propio interesado, en formato papel o digital.	Dar entrada a la información en sistemas de almacenamiento.	Selección de personal.	Detalle de personal con acceso a datos en ANEXO IV.	- 1 año. - Incineración.
DATOS TRATADOS	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo.	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo.	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo.	- Datos Identificativos. - Características personales. - Académicos y profesionales. - Detalles del empleo.	
INTERVINIENTES	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.
TECNOLOGÍAS INTERVINIENTES	- Web.	Detalle de sistemas informáticos de almacenamiento en ANEXO IV.	Detalle de sistemas informáticos de tratamiento en ANEXO IV.	- Correo electrónico Detalle de sistemas informáticos en ANEXO IV.	- Borrado. - Formateo.

USUARIOS WEB

	ENTRADA	ALMACENAMIENTO	TRATAMIENTO	ACCESO - CESIÓN	DESTRUCCIÓN
ACTIVIDADES DEL PROCESO	Recogida de datos: - Correo electrónico -Formulario de contacto	Dar entrada a la información en sistemas de almacenamiento.	Dar respuesta a solicitudes de los usuarios de la página web.	Detalle de personal con acceso a datos y Encargados de Tratamiento en ANEXO IV.	- Mientras que no se solicite la supresión de los mismos. - Borrado. - Formateado.
DATOS TRATADOS	- Datos Identificativos.	- Datos Identificativos.	- Datos Identificativos. -	- Datos Identificativos.	
INTERVINIENTES		Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.	Detalle de personal con acceso a datos y Encargados de Tratamiento en ANEXO IV.	Detalle de personal con acceso a datos en ANEXO IV.
TECNOLOGÍAS INTERVINIENTES	- Web. - Redes sociales.	Detalle de sistemas informáticos de almacenamiento en ANEXO IV.	Detalle de sistemas informáticos de tratamiento en ANEXO IV.	Detalle de sistemas informáticos en ANEXO IV.	- Borrado. - Formateo.

ANEXO III: IDENTIFICACIÓN DE RIESGOS

GENERALES	
AMENAZA	**SOLUCIÓN**
Pérdidas económicas y daños reputacionales por incumplimiento de la legislación vigente.	- Contratación de los servicios externos de una consultora en protección de datos. - Información al personal con acceso a datos de los protocolos de protección de datos implantados.
Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas.	- Nombramiento de un coordinador de protección de datos encargado de implantar las medidas de seguridad detalladas en el protocolo de protección de datos. - Información al personal con acceso a datos de los protocolos y medidas de seguridad de protección de datos implantados.
Pérdida de competitividad de la entidad derivada de daños reputacionales causados por una deficiente gestión de la privacidad de las personas.	- Información al personal con acceso a datos de los protocolos y medidas de seguridad de protección de datos implantados. - Contratación de los servicios externos de una consultora en protección de datos.
Falta de conocimiento experto sobre protección de datos.	- Contratación de los servicios externos de una consultora en protección de datos.
LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE LOS DATOS PERSONALES	
Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	- Asegurarse de que no existen otras causas de legitimación más adecuadas. - Dado que el tratamiento de datos personales se legitima por una relación contractual, se ofrecerá siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para la prestación del servicio. - No se condicionará el disfrute de los servicios prestados al consentimiento para finalidades diferentes. - En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores.
Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un	- Evitar el uso de cookies y otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las

consentimiento válido tras una información adecuada.	menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies…). - Informar siguiendo un sistema de capas sobre el uso y finalidades de las cookies. - Respetar las preferencias de los afectados establecidas en sus navegadores sobre el rastreo de su navegación.
TRANSPARENCIA EN LOS TRATAMIENTOS	
Recoger datos personales sin proporcionar la debida información o de manera no autorizada (cookies, ubicación geográfica…).	- Informar con transparencia sobre el uso y finalidades de las cookies. - Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada.
En el entorno web, ubicar la información en materia de protección de datos en lugares de difícil localización o diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado.	- Verificar que la información se ofrece en todos los formularios. - Verificar que la información que se ofrece es coherente y sistemática. - Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión.
Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer ara que exista un tratamiento leal de sus datos personales.	- Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización.
CALIDAD DE LOS DATOS	
Solicitar datos innecesarios para las finalidades perseguidas.	- Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso.

Utilizar datos para finalidades no especificadas.	- Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en los formularios de recogida de datos, así como en cualquier documento dirigido a los clientes.
Carecer de procedimientos claros y herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez han dejado de ser necesarios para la finalidad perseguida.	- Definir plazos de cancelación de todos los datos personales de los sistemas de información. - Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de cancelación de la información. - Implantar mecanismos para llevar a cabo y gestionar dicha cancelación en el momento adecuado, incluyendo, si corresponde, el bloqueo temporal de los datos personales.
DEBER DE SECRETO	
Accesos no autorizados a datos personales.	- Se entregará al personal con acceso a datos un acuerdo de confidencialidad para concienciar sobre la obligación de guardar secreto profesional. - Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de seguridad en materia de protección de datos de la entidad. - Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales.
TRATAMIENTO POR ENCARGO	
Inexistencia de un contrato que refleje todos los apartados necesarios y las garantías adecuadas.	- Establecer procedimientos que garanticen que siempre que se recurre a un encargad de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.
Falta de diligencia o dificultad para mostrarla, en la elección de encargado de tratamiento.	- Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación.
No definición o deficiencias en los procedimientos para comunicar al	- Incluir en el contrato de encargo la obligación de comunicar al responsable las

responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento.	peticiones de ejercicio de los derechos de los interesados.
Dificultades para conseguir la portabilidad de los daos personales a otros entornos una vez finalizado el contrato.	- Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio. - Establecer medidas técnicas y organizativas que garanticen la portabilidad.
DERECHOS DE LOS INTERESADOS	
Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados.	- Se informará por escrito mediante cláusulas informativas del procedimiento a seguir por los interesados para facilitar ejercicio de sus derechos en materia de protección de datos. - Formar a todo el personal para que conozca que ha de hacer si recibe una petición de derecho de los interesados o ha de informar a los afectados sobre como ejercerla.
Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales.	- Definición de procedimientos de gestión en el contrato de encargado de tratamiento formalizado.
SEGURIDAD	
Carencia de medidas de seguridad o aplicación deficiente de las mismas. Indefinición de funciones de seguridad y de establecimiento de competencias.	- Nombramiento de un coordinador de protección de datos y establecimiento, por parte de la dirección, de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos. - Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del coordinador de protección de datos en las fases iniciales de los mismos.
Deficiencias organizativas en la gestión del control de accesos.	- Políticas estrictas de acceso a la información por necesidad de conocer para la concesión de accesos a la información y de escritorios limpios de documentación para minimizar las posibilidades de acceso no autorizado a los datos personales. - Establecer procedimientos que garanticen la revocación de permisos de acceso cuando ya no sean necesarios por

	abandono de la entidad, traslado, cambio de funciones, etc.
Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.	- Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales.
Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.	- Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes.

ANEXO IV: DETALLE DE MEDIDAS TÉCNICAS DE SEGURIDAD

1.- INTERVINIENTES CON ACCESO A DATOS - PERSONAL DE LA ENTIDAD

NOMBRE DEL USUARIO	PUESTO QUE DESEMPEÑA	ACTIVIDADES TRATAMIENTO	PERMISOS
Dª. ARANZAZU POSSE FRAGA	COORDINADOR PROTECCION DE DATOS / GERENTE	Clientes, agenda de contactos y proveedores, empleados, currículums y usuarios web.	Entrada, almacenamiento, tratamiento, cesión y destrucción.
D. JULIÁN BÉRTOA PORTEIRO	AUX. ADMINISTRATIVO	Clientes, agenda de contactos y proveedores, empleados, currículums y usuarios web.	Entrada, almacenamiento, tratamiento, cesión y destrucción.

2.- INTERVINIENTES CON ACCESO A DATOS - ENCARGADOS DE TRATAMIENTO

RAZÓN SOCIAL DEL ENCARGADO DE TRATAMIENTO	ACTIVIDAD DEL TRATAMIENTO	FINALIDAD DEL TRATAMIENTO DE DATOS	VERIFICADO CUMPLIMIENTO
ERREBE CONSULTORES EMPRESARIALES, SL	Agenda de contactos y proveedores y empleados.	Consultoría de Protección de Datos	SÍ
GABINETE XURÍDICO MONTEALÓN, SC	Clientes, agenda de contactos y proveedores.	Asesoramiento fiscal, contable y laboral	
DATA CENTER, SL	Clientes.	Consultoría de datos	

3.- REGISTRO DE SOLICITUDES DE ACCESOS EXTRAORDINARIOS

USUARIO	PROCEDIMIENTO DE ACCESO	ACTIVIDADES DE TRATAMIENTO	TIPO DE ACCESO AUTORIZADO

4.- INVENTARIADO DE APLICACIONES INFORMÁTICAS

NOMBRE DE LA APLICACIÓN	ACTIVIDAD DE TRATAMIENTO	FINALIDAD
PAQUETE OFIMÁTICO		GESTION GENERAL
CHC AGENTES		GESTION FACTURACION Y BASES DE DATOS
GESTION ELECTRICA		GESTION FACTURACION

5.- INVENTARIADO SOPORTES AUTOMATIZADOS

NOMBRE DEL EQUIPAMIENTO	NÚMERO	DESCRIPCIÓN
PC SOBREMESA	2	ASUS, PHILIPS
DISCOS DUROS EXTERNOS	1	GENERICO

ENTORNO DE SISTEMAS OPERATIVOS, COMUNICACIONES Y REDES	
Sistema de Redes	MIXTO
Archivos y recursos compartidos	NO
Conexiones remotas	NO
Control de acceso	SI, MEDIANTE SISTEMA DE USUARIOS Y CONTRASEÑAS
Control de acceso físico	SI, BAJO LLAVE
Antivirus	WINDOWS DEFENDER
Sistema operativo	WINDOWS

6.- INVENTARIADO DE LOS SOPORTES NO AUTOMATIZADOS

Relación de soportes físicos utilizados que contienen datos de carácter personal:

SOPORTE	NÚMERO/CÓDIGO	UBICACIÓN FÍSICA	DATOS ALMACENADOS	RESPONSABLE DEL SOPORTE

7.- AUTORIZACIÓN DEL TRATAMIENTO FUERA DEL CENTRO DE TRABAJO

ELECTRA DE ZAS, SL como responsable de tratamiento, autoriza expresamente mediante el presente documento a _____, para que pueda realizar el tratamiento de los datos de carácter personal relativos a la actividad de tratamiento _____ fuera del centro de trabajo habitual.

D./Dª. _____, se compromete a aplicar las medidas de seguridad detalladas en el PROTOCOLO DE PROTECCIÓN DE DATOS.

En ZAS, 06 de marzo de 2025

Fdo. Dª. ARANZAZU POSSE FRAGA

ANEXO V: REGISTRO DE INCIDENCIAS

FORMULARIO PARA REGISTRO DE INCIDENCIAS	
Número de incidencia	
Fecha y hora de incidencia	
Nombre del fichero	
Tipo de incidencia	
Descripción	
Efectos	
Persona que notifica la incidencia	Firma
Persona a la que se notifica la incidencia	Firma
Fecha de notificación	
Operaciones para solucionar notificación	

FORMULARIO DE RESOLUCION DE INCIDENCIAS
Código de incidencia
Descripción
Procedimiento de Recuperación
Pasos Realizados
Persona que realizó la recuperación

DETALLE DE LA RECUPERACIÓN DE DATOS
Registro de actividad
Nº de procedimiento
Persona que ejecuta el proceso Fdo._____
Datos restaurados
Datos grabados manualmente
Autorización del responsable de tratamiento Fdo. _____

MODELO DE AUTORIZACIÓN PARA LA RECUPERACIÓN DE LOS DATOS

ELECTRA DE ZAS, SL, como responsable de tratamiento, autoriza expresamente mediante el presente escrito a _____, para que pueda utilizar la copia de respaldo realizada el __ de _____ de 20__, con la finalidad de que se reconstruya la información y los datos al estado en el que se encontraban en el tiempo de producirse su pérdida/destrucción.

_____ se compromete a aplicar las medidas de seguridad detalladas en el PROTOCOLO DE PROTECCIÓN DE DATOS DE ELECTRA DE ZAS, SL.

En ZAS, 06 de marzo de 2025

Fdo. Dª. ARANZAZU POSSE FRAGA

ANEXO VI: NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

CONTENIDO MÍNIMO PARA NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

REGISTRO DE ACTIVIDADES AFECTADO:	
Categorías de datos afectados:	
Categorías de interesados afectados. ¿Se vulneran derechos o intereses de terceros con motivo de la quiebra?	
Operaciones realizadas para solventar la quiebra	
Fecha y método de comunicación a afectados – Medidas aplicadas para paliar efectos negativos sobre los interesados	
Detalle de recomendaciones notificadas a los afectados para hacer frente a las consecuencias de la quiebra	
Método de comunicado de brecha de seguridad a los interesados	
Comunicado a la Agencia Española de Protección de Datos del detalle de la Brecha de Seguridad	https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

PARA CUALQUIER ACLARACIÓN, MODIFICACIÓN O ACTUALIZACIÓN

POR FAVOR, PÓNGASE EN CONTACTO CON NOSOTROS EN:

empresas@rbsoluciones.com

www.rbsoluciones.com