APENDICE III-MEDIDAS DE SEGURIDAD

El Encargado aplicará las medidas de seguridad que se indican a continuación que le sean aplicables por la naturaleza, alcance, contexto del tratamiento, teniendo en cuenta el estado de la técnica y el nivel de riesgo del tratamiento, debiendo actualizarse este listado en función de las características del tratamiento:

Apartado	**Medida Implementada**
Política de Seguridad	La dirección aprueba y publica una política de seguridad de la información. Esta se comunica a todos los empleados o terceros relevantes.
Revisión Política de Seguridad	Es revisada periódicamente o cuando se producen cambios significativos y es adecuada, eficaz y suficiente.
Roles y responsabilidades	En ella se definen y asignan los deberes y responsabilidades en función de los distintos roles y funciones que existen dentro de la organización.
Procedimientos de seguridad	Se han establecido procedimientos para el uso correcto de equipos, sistemas, servicios e instalaciones o que les afecten, así como lo que se considera uso indebido y las consecuencias del mismo.
Procedimientos detallados de seguridad	Se han establecido procedimientos que detallan de manera clara y precisa como se deben llevar a cabo las tareas habituales.
Proceso de autorización	Se han establecido procesos formales de autorizaciones respecto de todos los elementos que forman parte de los sistemas de información.
Análisis de riesgos	Se ha realizado un análisis de riesgos sobre los activos de los sistemas de información e implementado las salvaguardas necesarias para protegerlos de las amenazas más probables.
Arquitectura de seguridad	La seguridad de los sistemas ha sido objeto de un planeamiento integral.
Identificación	La identificación de los usuarios del sistema se realiza mediante identificadores únicos que garantizan el acceso de acuerdo con los derechos y/o permisos otorgados por las personas autorizadas.
Proceso de gestión de derechos de acceso	El proceso de gestión de derechos de acceso se realizará en base al cumplimiento de los principios de “mínimo privilegio”, “necesidad de conocer” y “capacidad de autorizar”.
Mecanismo de autenticación	Se ha implementado un mecanismo de autenticación sustentado en contraseñas complejas que expiran automáticamente dentro de intervalos previamente definidos (nunca superior a 12 meses) y cuenta con un sistema de bloqueo ante intentos fallidos de acceso.
Acceso Local	Se han implementado medidas de forma que el acceso a los puestos de trabajo no permite identificar la información del sistema, se bloquea tras un cierto número de intentos fallidos y se registran todos los intentos de acceso.
Acceso remoto	Se ha establecido un procedimiento de acceso remoto mediante red privada virtual
Inventario de activos	Se mantiene un inventario actualizado de todos los elementos del sistema.

Configuración de Seguridad	Los activos del sistema han sido configurados previamente con las medidas de seguridad adecuadas según el riesgo.
Mantenimiento	Complementa al anterior: Son mantenidos de acuerdo con las indicaciones de los fabricantes y se ha establecido un procedimiento de actualización y mejora.
Protección frente a código dañino	Se han implementado mecanismos de prevención y reacción frente a código dañino.
Registro de actividad de los usuarios	Se ha implementado un registro de actividad en los sistemas que permite controlar las actividades realizadas por los usuarios. El nivel de detalle depende del nivel de riesgo establecido.
Protección de claves criptográficas	Las claves criptográficas son protegidas durante todo su ciclo de vida
Contratación de servicios con acceso a datos	Se han establecido contractualmente las obligaciones y responsabilidades de las partes en relación con el acceso a datos personales, cumpliendo los requisitos mínimos exigidos por el art. 28 RGPD.
Sistema de métricas	Se han establecido un sistema de métricas que permite conocer el grado de cumplimiento de las medidas de seguridad implementadas.
Áreas separadas y control de acceso	Se han establecido áreas separadas y con acceso controlado a las zonas de trabajo y equipos.
Identificación de personas	Los locales donde hay equipamiento que forma parte del sistema de información cuentan con mecanismos para controlar el acceso Y disponen de elementos adecuados para garantizar un eficaz funcionamiento y protegerlo de amenazas e incidentes.
Acondicionamiento de los locales	
Energía eléctrica	
Protección frente a incendios	
Registro de entrada y salida de equipamiento	Se ha establecido un registro de entrada y salida de equipamientos
Deberes y obligaciones	Se ha informado a cada empleado y/o personal empleado por terceros con acceso a los sistemas de sus deberes y responsabilidades en materia de seguridad y protección de datos.
Concienciación	Se realizan acciones formativas regularmente en materia de seguridad y protección de datos.
Política de mesas limpias	Se han implantado políticas de mesas limpias.
Protección de portátiles	Los equipos portátiles cuentan con medidas de seguridad que garantizan la misma seguridad que los equipos locales.
Perímetro seguro	Se ha implementado un sistema de cortafuegos que separa la red interna del exterior.
Protección de autenticidad e integridad	Se han implementado redes privadas virtuales para su uso cuando las comunicaciones discurran por fuera del dominio de seguridad.

Etiquetado	Se han implementado sistemas de etiquetado de los soportes que no revelan su contenido.
Custodia	Se han establecido medidas de físicas y lógicas de custodia que permitan el control de los soportes de información.
Borrado y destrucción	Se han establecido procedimientos de borrado seguro y/o de destrucción segura.
Aceptación y puesta en servicio	Se han implementado medidas de forma que el desarrollo de aplicaciones se realiza en entornos diferentes al de producción. Estos cuentan con elementos de seguridad similares a los sistemas habituales en relación con la identificación, autenticación y restantes medidas de protección de la información. En el caso de pruebas, estas no se realizan con datos reales.
Datos de carácter personal	Se han implantado las medidas de seguridad aplicables a los sistemas que contienen datos de carácter personal, en función del análisis de riesgos realizado.
Calificación de la información	Se ha clasificado y categorizado la información atendiendo a su valor, requisitos legales, sensibilidad, nivel de confidencialidad y criticidad para la organización.
Limpieza de documentos	Los documentos publicados o van a ser difundidos ampliamente son sometidos a un proceso de limpieza que garantiza la confidencialidad, fuentes y orígenes de la información, así como la reputación de la organización.
Copias de Seguridad	Se realizan copias de seguridad que permiten recuperar la información de manera adecuada. Se comprueban regularmente y abarcan todos los sistemas de información digitales.
Protección del correo electrónico	Se ha protegido el correo electrónico corporativos frente amenazas que le son propias (como spam, códigos dañinos, etc.) y se ha regulado el uso del mismo mediante un procedimiento de uso aceptable.
Protección de servicios y aplicaciones Web	Se han implementado medidas de seguridad en los servicios o aplicaciones web que garantizan el control de acceso a la documentación, los ataques vía URL, vía cookies, inyección de código, intentos de escalado de privilegios, Cross site scripting o manipulación de "proxies" y "caches". Así mismo, se emplean certificados de autenticación en todos los sitios web.