POLITICA INTEGRADA DE LORGEN GENÉTICA Y PROTEÓMICA S.L.

LORGEN GENÉTICA Y PROTEÓMICA, S.L. es una empresa dedicada la investigación y la realización de análisis genéticos clínicos y forenses, así como al asesoramiento, evaluación, supervisión y peritación en materia genética molecular. La Dirección de Lorgen, considera que la calidad es un factor esencial para el éxito de la empresa y que cada persona de la organización es responsable de la función que realiza, por ello asume e impulsa la **POLITICA DEL SISTEMA INTEGRADA (ISO 9001, ISO 14001 e ISO 45001)** basada en los siguientes **principios**:

1. Implantar una cultura de calidad, protección del medio ambiente, seguridad laboral en todos los niveles de la organización, fomentando la implicación y motivación de los trabajadores, en todo lo relacionado con la **mejora continua** todos los aspectos del Sistema y la prevención de la contaminación para la mejora del desempeño ambiental, así como para proporcionar unas condiciones de trabajo seguras y saludables y eliminar los peligros derivados de nuestro trabajo.
2. Sea adecuada al contexto de la organización, a su naturaleza, apropiada a los impactos ambientales de nuestras actividades y magnitud de los riesgos laborales para la seguridad y salud en el trabajo.
3. Proporcione un marco adecuado sobre el que se puedan definir los objetivos y las metas de calidad, ambientales y prevención de riesgos laborales
4. Se comunique y entienda en toda la empresa a través de su publicación y explicación al personal, haciéndoles partícipe de sus obligaciones para su propia seguridad y salud en el trabajo y de las especificaciones ambientales para el desarrollo de las actividades con el mínimo impacto ambiental.
5. Se mantenga y revise para que sea siempre adecuada a la actividad y a los aspectos de seguridad y ambientales.
6. Se comprometa a que todos los recursos humanos estén entrenados y motivados para satisfacer el objetivo de esta Política, fomentando la participación de los trabajadores y sus representantes.
7. Compromiso de todos los profesionales que integramos Lorgen, motivados desde la Dirección, para lograr la satisfacción continuada de las necesidades de los clientes y cumplir con los requisitos legales y demás requisitos, ofreciendo un servicio con niveles óptimos de calidad.
8. Compromiso de la Dirección de adquirir recursos humanos y tecnológicos así como de la formación continúa del operario para garantizar la **calidad** en todos nuestros productos y servicios.
9. Garantizar una total **confidencialidad** sobre los resultados de los ensayos, mediante el cumplimiento de la legislación vigente en materia de Protección de Datos.
10. Dar a nuestros clientes una **amplia cobertura de ensayos**, cumpliendo tanto los requisitos especificados como los reglamentarios y garantizando los resultados.

Las **pautas** a seguir son:

I. Unificación de los criterios de trabajo en el **laboratorio**, con la realización de unas buenas prácticas profesionales, para obtener una mayor **calidad** de nuestros servicios prestados a nuestros clientes.
II. Que cada trabajador cumpla con sus funciones dentro del **laboratorio,** con el objeto de mantener la **calidad** de nuestros ensayos para conseguir la satisfacción continua de nuestros clientes y que el aprendizaje permanente sea la piedra angular de nuestro **laboratorio.**
III. Realizar los ensayos de acuerdo a los métodos establecidos, perfectamente definidos, documentados y actualizados.
IV. Que se piense en **prevenir futuros resultados erróneos**, tomando medidas como inspección en la recepción de muestras, suministros y servicios, formación y adiestramiento del personal, etc.
V. Que los servicios de calibración/verificación/mantenimiento se distingan por su elevada eficacia y así garanticen resultados fiables.
VI. Que todo el personal que participe en las actividades de ensayo y calibración del **laboratorio** se familiarice con la documentación sobre la **calidad** y ponga en práctica las políticas y procedimientos en su trabajo.
VII. Explicar a todo el mundo que todo es manifiestamente mejorable, y por tanto, todos se tienen que involucrar en la mejora continua.

Esta Política de Gestión Integrada se hace pública para el personal de la empresa, que debe entenderla y asumirla.

Jose Antonio Jiménez de la Cruz
Administrador Único
Granada a 7 de Enero 2020

POLITICA NORMA UNE-EN ISO 15189:2022 LABORATORIOS CLÍNICOS

La dirección de *LORGEN* conocedora de las tendencias en las exigencias de la normativa de aplicación y de la situación del mercado, en el ámbito del diagnóstico genético, se marca como objetivo la implantación, en su organización, de un Sistema de Calidad robusto para garantizar el cumplimiento de los criterios definidos en la norma internacional *UNE-EN ISO 15189:2022, Laboratorios Clínicos.* Requisitos particulares para la calidad y la competencia con el compromiso de mantenerlo y asegurar que sus análisis genéticos se realizan de acuerdo a las mejores técnicas disponibles en cada momento, ofreciendo a sus clientes los servicios que mejor se ajusten a sus necesidades y aseguren su satisfacción.

La Dirección de *LORGEN* garantiza que los servicios que ofrece a sus clientes se realizan conforme a su Sistema de Calidad, bajo criterios de Independencia, Imparcialidad, Integridad y Buenas Prácticas Profesionales, sin olvidar que en todo momento se dotará a la organización de los recursos materiales y humanos necesarios para:

- lograr una correcta prestación del servicio,
- cumplir los requisitos de la norma UNE-EN ISO 15189:2022, y
- mejorar continuamente la eficacia del sistema de gestión
- promover entre el equipo de profesionales las mejores prácticas en el ámbito de la genética y en la medida de lo posible utilizar tecnología punta dentro del sector.

Todo ello con el convencimiento de que el coste que implique no es otra cosa que una ventajosa inversión, estando atentos a las inquietudes del mercado y sus clientes, gestionando las quejas y reclamaciones, así como las posibles sugerencias de mejora.

La Dirección, además de realizar revisiones anuales de los objetivos de mejora establecidos, actualizando, en su caso, la política vigente, desarrollará, mantendrá actualizado y difundirá su Sistema de la calidad, asegurándose que es entendido, asumido y puesto en práctica por todo el personal que participe en actividades por él reguladas. Potenciará a su vez las acciones preventivas que consigan disminuir los trabajos No Conformes, cumpliendo en todo momento la legislación vigente y las normas complementarias.

Las actividades que se desarrollen gozarán de plena independencia frente a otras actividades llevadas a cabo por *LORGEN y* se realizarán en base a las previsiones del Sistema de Calidad, cuya implantación y seguimiento se encomiendan al Responsable de Calidad de la organización.

LA DIRECCIÓN

Fdo: Carmen Entrala Bernal
20/12/2023

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y

ESQUEMA NACIONAL DE SEGURIDAD

La dirección de **LORGEN**, consciente de la necesidad de promover, mantener y mejorar el enfoque hacia el cliente en todas sus actividades, ha implantado un Sistema de Gestión Integrado (SGI) conforme al estándar cuyo **objetivo** final es asegurar que entendemos y compartimos las necesidades y metas de nuestros clientes, intentando prestar servicios que cumplan sus expectativas, trabajando en la mejora continua. Manifiesta expresamente su compromiso de potenciar la **Seguridad y Ciberseguridad** de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, a mantener alta nuestra competitividad en los servicios y productos de **Recepción de Muestras para la realización de Análisis Genéticos de Identificación de Paternidad, Parentesco y Diagnóstico genético de enfermedades, emisión y envío de resultados, proyectos de Investigación, Desarrollo e Innovación en el campo de la medicina genómica.**

MISIÓN y OBJETIVOS:

- Fomentar la mejora continua de los servicios y soporte al cliente.
- Continuar el posicionamiento de **LORGEN** como referente en el sector.
- Proporcionar a los clientes el equipo más profesional y disponer de forma inmediata y durante el tiempo necesario de técnicos altamente cualificados, expertos en las disciplinas requeridas y acostumbrados a trabajar en equipo.
- Tener una prestación del servicio basada en nuestro compromiso con la mejora continua de nuestros sistemas, con la seguridad y ciberseguridad de la información como pilar central y por defecto.

Nuestra misión y los objetivos los conseguiremos a través de:

- Un sistema de objetivos, métricas e indicadores de mejora continua, seguimiento, medición de nuestros procesos internos, así como de la satisfacción de nuestros clientes. Estableciendo y supervisando el cumplimiento de los requisitos contractuales para asegurar un servicio eficaz y seguro.
- Formando y concienciando continuamente a nuestro equipo para tener el mayor grado de profesionalidad y especialización posible, además teniendo nuestras infraestructuras en un estado adecuado y en concordancia con los requerimientos de nuestros clientes.
- Con un procedimiento seguro de gestión de adquisición de productos.
- Cumpliendo las exigencias de la legislación vigente, especialmente con el GDPR y el cumplimiento de nuestra Documentación de Seguridad.
- Introduciendo los procesos de mejora continua que permitan un avance permanente en nuestra gestión de Seguridad de la Información.
- Gestionando y elaborando planes para la gestión y tratamiento de los riesgos con una metodología de análisis y gestión de riesgos utilizada, basada en estándares.
- Gestionando las comunicaciones internas y externas e información almacenada y en tránsito.
- Asegurando la interconexión con otros sistemas de información.
- Gestionando y monitorizando la actividad con la gestión de logs.
- Con especial atención a la gestión de incidentes de seguridad.
- Asegurando la continuidad y disponibilidad del negocio y de los servicios.
- Asegurando que nuestros Activos y Servicios cumplen con las medidas del ENS de Nivel ALTO para las dimensiones de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.

Además, estos principios se deberán contemplar en las siguientes **áreas de seguridad**:

- **Física**: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información, así como los accesos físicos.
- **Lógica**: Incluyendo los aspectos de protección de aplicaciones, redes, comunicación electrónica, sistemas informáticos y con los accesos lógicos.
- **Político-corporativa**: Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal.

El objetivo último de la seguridad de la información es asegurar que una organización pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Roles o funciones de seguridad:

Responsable de la Información: determinará los requisitos de la información tratada.

- Implantar y mantener el Sistema de Gestión Integrado (SGI) mejorando continuamente su eficacia.
- Implantar y mantener el ENS mejorando continuamente su eficacia.
- Supervisar los procedimientos y las instrucciones técnicas.
- Aplicar las medidas y seguimientos indicados por el DPO.
- Realizar el seguimiento y verificar la implantación y eficacia de todas las acciones correctoras y preventivas establecidas.
- Asegurar que el sistema implantado cumple con la norma establecida.
- Analizar los datos obtenidos en el Sistema de Gestión Integrado (SGI) y ENS y proponer mejoras.
- Elaborar el plan anual de auditorías internas.
- Participar en la toma de decisiones en la revisión por la dirección.
- Gestión de No Conformidades de seguridad.
- Participar en Auditoria Externas.
- Responsable de los datos privados de la empresa en cuanto a su pérdida, el robo y la desactualización.
- Cumplir con el manual de buenas prácticas de seguridad de la información.
- Imparte los programas de formación para que el personal sepa cómo actuar en el supuesto de que se produzca contingencias.
- Mantener actualizados los medios de contacto con las autoridades.
- Lleva el inventario de soportes que contienen datos de carácter personal.
- Analiza los informes de auditoría y elevan las conclusiones al responsable de los datos.
- Convoca las reuniones del CSI.
- Genera las actas de reunión del CSI.
- Gestiona las no conformidades, acciones correctivas y acciones preventivas de SI.
- Mantiene los documentos del SGI.

- Mantiene y despliega la política de seguridad de **LORGEN** así como el resto de las políticas al personal implicado en cada una de ellas.
- Responsable de la gestión de la auditoría de seguridad de protección de datos y RGPD.
- Supervisa las tareas de protección de datos del DPO.

- Confecciona los documentos de seguridad de **LORGEN**.
- Elabora los acuerdos para el tratamiento de datos por terceros.
- Atiende incidencias en materia de protección de datos.
- Se encarga de contactar con las autoridades en caso necesario.
- Aplicación y supervisión del cumplimiento de las políticas del SGI.
- Mantenimiento y aplicación del Documento de Aplicabilidad del SGI

Responsable de sistemas: Determina los requisitos de los servicios prestados.

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del RSI.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

Responsable de Seguridad de la Información: Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

- Responsable de la ciberseguridad.
- Supervisar el Manual de Seguridad, los procedimientos y las instrucciones técnicas.
- Responsabilidad general de administrar la implementación de las prácticas de seguridad.
- Asegurando que el sistema implantado cumple con la norma establecida.
- Analizar los datos obtenidos en el Sistema de Gestión de Seguridad de la Información y ENS y proponer mejoras.

- Participar en la toma de decisiones en la revisión por la dirección.
- Participar en Auditoria Externas.
- Responsable del riesgo de la intrusión física de los dispositivos de la empresa.
- Cumplir con el manual de buenas prácticas de seguridad de la información.

- Segregación de tareas y entornos.
- Comunicar cualquier emergencia de incendio, inundación o avería de los equipos de climatización que pueda activar el PCN.
- Revisa el Plan de Continuidad del negocio.
- Verifica el funcionamiento del Plan de Continuidad de Negocio.
- Controla el acceso de personas a los locales donde están instalados los sistemas.
- Supervisa las incidencias de seguridad producidas.
- Realiza y custodia las copias de seguridad.
- Genera los planes de tratamiento de gestión de riesgo y supervisa su implantación.
- Actualiza el análisis de riesgos.
- Supervisa la recogida de métricas.
- Realiza las revisiones de seguridad del SGI.
- Mantiene el Plan de Continuidad de Negocio.
- Incorpora en el registro de incidencias las medidas correctoras.
- Aplicación y supervisión del cumplimiento de las políticas de SGI.

Responsable del Servicio: Determina los niveles de seguridad de los servicios.

- Garantizar el cumplimiento de los objetivos y métricas establecidos para el servicio (SLAs).
- Organización diaria de los recursos.
- Responsable de la pérdida y robo de información de los servicios y soluciones informáticas para clientes y usuarios en general.
- Cumplir con el manual de buenas prácticas.
- Determina los requisitos de los servicios prestados.
- Programar, dirigir, coordinar, supervisar y controlar todas las actividades del servicio.
- Revisión y cumplimiento de los informes de los servicios.

El Comité de Seguridad de la Información (CSI) de **LORGEN** alcanza a toda la empresa, es el mecanismo de coordinación y resolución de conflictos, entre otras funciones:

- Designación y/o renovación de los cargos de seguridad, así como sus funciones y responsabilidades.
- Crear, planificar, implementar e integrar la dirección estratégica de la organización y alinearla con el SGSI.
- Conocimiento del mercado TIC y nuevas tecnologías y su aplicación en la compañía.
- Dirección y supervisión de los distintos proyectos de seguridad de la compañía.
- Participar y promover el cumplimiento de la política de seguridad de la información de la organización.
- Velar por el cumplimiento de disposiciones legales y normas de las administraciones públicas y de régimen interno relativas a seguridad de la información.
- Aprobación del SGSI, así como sus cambios y nuevas versiones.

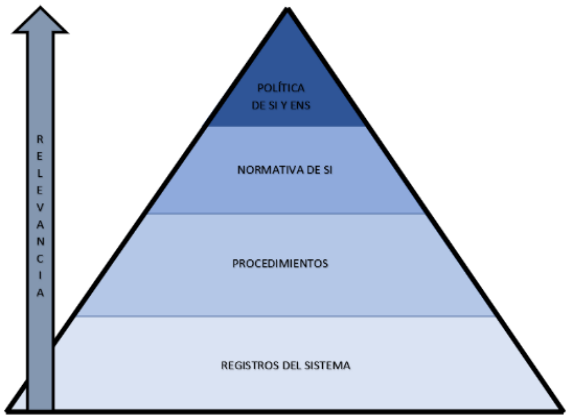
Componen el CSI:

- Responsable del Servicio.
- Responsable de Sistemas.
- Responsable de Seguridad de la información.
- Responsable de la Información

Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y tenida al día en todos los niveles de la organización.

Estructuración de la documentación de seguridad del sistema

La documentación del sistema sigue la siguiente estructura:



La clasificación de la información del sistema se clasifica en las siguientes categorías, tal y como se establece en los procedimientos PS.8 Gestión de Activos y PG.01 Control de documentos y registros:

- Uso Público
- Uso Interno
- Confidencial
- Secreta

Legislación aplicable en materia de tratamiento de datos de carácter personal

En materia de tratamiento de datos de carácter personal se tendrá en cuenta 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 y por el que se deroga la Directiva 95/46/CE y la legislación nacional correspondiente.

Los requisitos legales se encuentran recogidos en el documento Identificación-Evaluación de requisitos legales

Fdo:

José Antonio Jiménez de la Cruz

28/07/2022