POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

[RESUMEN PÚBLICO]

Sistema de Gestión de Seguridad de la Información · Esquema Nacional de Seguridad

1. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información entra en vigor en la fecha de su aprobación por la Gerencia de BIOARRAY y se mantiene vigente hasta que la sustituya una nueva versión. Este documento es un resumen público de la política aprobada.

2. Misión de la organización

BIOARRAY es un laboratorio de diagnóstico genético e investigación especializado en el análisis genético mediante tecnologías de vanguardia (NGS, arrays de CGH, citogenética molecular), al servicio del sector médico, investigador y biotecnológico.

Su actividad implica tratar datos genéticos y de salud, que son categorías especiales de datos personales. Por eso, la seguridad de la información forma parte de la calidad del servicio diagnóstico. La misión de BIOARRAY en materia de seguridad es proteger los datos clínicos y genéticos de los pacientes y todos los activos de información que soportan sus servicios de diagnóstico e investigación científica, garantizando:

Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Los usuarios autorizados acceden a la información cuando la necesitan.	La información y sus métodos de proceso son exactos y completos.	Solo las personas autorizadas pueden acceder a la información.	Quien accede a la información es quien dice ser.	Los accesos a la información pueden seguirse y verificarse.

Los sistemas de información deben administrarse con diligencia y protegerse frente a daños accidentales o deliberados. Para ello, BIOARRAY actúa de forma preventiva, supervisa la actividad diaria y reacciona con rapidez ante los incidentes. Lo hace de acuerdo con los principios básicos del Esquema Nacional de Seguridad: la seguridad como proceso integral, la gestión de la seguridad basada en los riesgos, la prevención, detección, respuesta y conservación, la existencia de líneas de defensa, la vigilancia continua y la reevaluación periódica, y la diferenciación de responsabilidades.

3. Alcance

La política se aplica a los sistemas de información que almacenan, procesan y transmiten datos clínicos y genéticos de pacientes y que dan soporte a los servicios de diagnóstico genético e investigación científica de BIOARRAY, así como a las personas y demás activos de información que intervienen en ellos.

Afecta a empleados, contratistas, proveedores, subcontratistas, colaboradores externos y a cualquier tercero que acceda a información de BIOARRAY o de sus pacientes, o que la procese, almacene, transmita o gestione, ya sea en las instalaciones del laboratorio, en remoto o mediante servicios tecnológicos. Los controles se aplican de forma proporcional al tipo de relación, las funciones desempeñadas, los activos accesibles y los riesgos asociados.

4. Objetivos

La Gerencia establece los siguientes objetivos de seguridad de la información:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos clínicos y genéticos de los pacientes.
- Asegurar la continuidad del servicio diagnóstico y la recuperación rápida y eficaz ante cualquier incidente o contingencia.
- Prevenir los incidentes de seguridad y reducir los riesgos derivados de la actividad del laboratorio.
- Cumplir la normativa aplicable, en especial la relativa a la protección de datos de salud y genéticos.
- Fomentar una cultura de ciberseguridad mediante la formación y la concienciación del personal.
- Mejorar de forma continua el Sistema de Gestión de Seguridad de la Información.

5. Marco normativo

BIOARRAY se compromete a cumplir los requisitos legales y regulatorios aplicables y los compromisos adquiridos con pacientes y clientes, y a mantenerse al día de sus cambios. El marco en el que desarrolla su actividad incluye, entre otras, las siguientes normas y referencias:

- Reglamento (UE) 2016/679 (RGPD), en especial el art. 9 sobre datos genéticos y de salud.
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Directiva (UE) 2022/2555 (NIS2), relativa a la ciberseguridad de las entidades esenciales e importantes.
- UNE-EN ISO 15189:2023, sobre requisitos de calidad y competencia de los laboratorios clínicos.
- Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza, y Reglamento (UE) 910/2014 (eIDAS).
- Real Decreto Legislativo 1/1996, Ley de Propiedad Intelectual, aplicable a los resultados de I+D+i.
- Guías del CCN-CERT (series CCN-STIC) y guías de la Agencia Española de Protección de Datos sobre brechas de seguridad.

6. Desarrollo y estructura documental

La política se desarrolla mediante un conjunto de documentos que ayudan a todas las personas a aplicarla en su trabajo:

- **Política de Seguridad:** el presente marco de principios y responsabilidades.
- **Normativa de seguridad:** reglas de uso de equipos, servicios e instalaciones, y responsabilidades del personal.
- **Procedimientos y guías de seguridad:** instrucciones sobre cómo operar los elementos del sistema de forma segura.
- **Registros y evidencias:** resultado de la aplicación de los anteriores.

La documentación se guarda en el repositorio corporativo de BIOARRAY y se clasifica según su nivel de confidencialidad (público, interno o confidencial). El acceso se concede según los perfiles autorizados. El Responsable de la Seguridad custodia y difunde la versión aprobada. Cada documento tiene un código, una versión y una fecha de aprobación. Los documentos obsoletos se retiran y se archivan. Los registros de seguridad se conservan durante un mínimo de cinco años, salvo que la normativa aplicable establezca un plazo mayor.

7. Organización de la seguridad

La responsabilidad última de la seguridad de la información recae en la Gerencia de BIOARRAY. La Gerencia organiza las funciones y responsabilidades, aprueba la política y facilita los recursos necesarios para alcanzar los objetivos. Los

directivos deben dar ejemplo cumpliendo las normas de seguridad establecidas. La Gerencia nombra formalmente a las personas que ocupan los siguientes roles:

Rol	Función principal
Responsable de la Información	Determina los requisitos de seguridad de la información tratada, su clasificación y su protección a lo largo de todo su ciclo de vida.
Responsable del Servicio	Determina los requisitos de seguridad de los servicios prestados y vela por su continuidad.
Responsable de la Seguridad (RSEG)	Lidera y coordina la seguridad de la información, supervisa el cumplimiento de la política, gestiona los incidentes e impulsa la formación y la concienciación.
Responsable del Sistema (RSIS)	Implanta y opera la seguridad en los sistemas de información, aplica los controles y gestiona las vulnerabilidades.
Delegado de Protección de Datos (DPD)	Supervisa la protección de los datos personales y el cumplimiento de la normativa de privacidad.

De acuerdo con el principio de diferenciación de responsabilidades, el Responsable de la Seguridad y el Responsable del Sistema son personas distintas, sin dependencia jerárquica entre ellas.

Resolución de conflictos

Los desacuerdos entre responsables se tratan en el Comité de Seguridad de la Información, que decide por mayoría y deja constancia en acta. Si no se alcanza un acuerdo, la Dirección resuelve de forma vinculante.

8. Comité de Seguridad de la Información y Comité de Crisis

El **Comité de Seguridad de la Información** es el órgano colegiado que gobierna la seguridad de la información en BIOARRAY. Lo preside la Gerencia, actúa como secretario el Responsable de la Seguridad y lo integran los demás responsables de seguridad y los responsables de los departamentos del laboratorio. Entre sus funciones están:

- Elaborar y revisar la Política de Seguridad.
- Coordinar todas las funciones de seguridad.
- Velar por el cumplimiento normativo.
- Coordinar los planes de continuidad.
- Seguir los riesgos residuales y la gestión de incidentes.
- Promover las auditorías.
- Aprobar los planes de mejora.

El **Comité de Crisis**, presidido por la Gerencia, es el máximo órgano de decisión ante una situación de crisis. Agiliza la toma de decisiones frente a incidentes que puedan afectar a la continuidad del servicio diagnóstico, a la confidencialidad de los datos de los pacientes o a la reputación del laboratorio.

9. Gestión de riesgos

Los sistemas incluidos en esta política se someten a un análisis de riesgos que identifica los activos críticos, las amenazas que les afectan y sus vulnerabilidades. El análisis sigue metodologías reconocidas como MAGERIT y abarca las cinco dimensiones de la seguridad. Se mantiene de forma continua y se revisa:

- al menos una vez al año;
- cuando hay cambios significativos en el entorno tecnológico;
- cuando cambia la normativa aplicable.

El Comité de Seguridad aprueba formalmente los análisis de riesgos. Los riesgos se clasifican según su probabilidad y su impacto, y se tratan evitándolos, reduciéndolos, transfiriéndolos o aceptándolos. La Dirección aprueba la aceptación del riesgo residual a propuesta del Comité, y ese riesgo se documenta y se revisa periódicamente.

10. Gestión de personal

Todos los miembros de BIOARRAY tienen la obligación de conocer y cumplir esta Política de Seguridad y la normativa de seguridad que la desarrolla. El Comité de Seguridad pone los medios necesarios para que esta información llegue a todas las personas afectadas.

Todo el personal recibe formación periódica en ciberseguridad adaptada a sus funciones. La formación incluye la identificación de amenazas, las buenas prácticas de autenticación, el tratamiento de datos confidenciales y la respuesta ante incidentes. Se organizan además campañas de concienciación y se evalúa la eficacia de la formación para mejorarla.

11. Profesionalidad

La seguridad de los sistemas está a cargo de personal cualificado, con la formación y la experiencia adecuadas a sus responsabilidades. Las funciones de seguridad se asignan de forma expresa a cada rol. Los terceros que prestan servicios a BIOARRAY quedan sujetos a las obligaciones de seguridad que les corresponden, en proporción a su acceso a la información y a los sistemas.

12. Autorización y control de los accesos

El acceso a los sistemas de información y a los datos de los pacientes está limitado a los usuarios, procesos y dispositivos debidamente autorizados. Cada acceso se identifica y se autentica, y se aplican los principios de necesidad de conocer y de mínimo privilegio. Los permisos se conceden según las funciones de cada persona y se revisan periódicamente.

13. Protección de las instalaciones

Las instalaciones donde se encuentran los sistemas de información y la información del laboratorio están protegidas frente a accesos no autorizados, daños e interferencias. Las medidas de protección física y ambiental son proporcionales a los riesgos identificados.

14. Adquisición de productos y contratación de servicios de seguridad

La seguridad se tiene en cuenta en la adquisición de productos y en la contratación de servicios tecnológicos. Siempre que es posible, se priorizan productos y servicios con una funcionalidad de seguridad certificada y adecuada al nivel de protección requerido. Los requisitos de seguridad se incluyen en la planificación y en las condiciones de contratación.

15. Mínimo privilegio y seguridad por defecto

Los sistemas se diseñan y configuran para ofrecer solo las funcionalidades imprescindibles para la actividad del laboratorio. La seguridad se integra en todo el ciclo de vida de los sistemas, desde su concepción hasta su retirada, incluidas las decisiones de desarrollo o adquisición y la explotación.

16. Integridad y actualización del sistema

Los cambios en los elementos físicos y lógicos de los sistemas se autorizan antes de su instalación y se controlan mediante un proceso de gestión de cambios. El estado de seguridad de los sistemas se evalúa de forma periódica frente a las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones disponibles. Ante cualquier riesgo detectado, se actúa con diligencia.

17. Protección de la información almacenada y en tránsito

BIOARRAY protege la información almacenada y la que circula por entornos no seguros, como los equipos portátiles, los soportes de información o las redes abiertas. Para ello aplica mecanismos criptográficos robustos y medidas proporcionales a la sensibilidad de los datos clínicos y genéticos.

18. Prevención ante otros sistemas de información interconectados

El perímetro de los sistemas está protegido, en especial en las conexiones con redes públicas. Se analizan los riesgos de cada interconexión con sistemas de terceros y se controla su punto de unión.

19. Registro de la actividad, detección de código dañino e incidentes

BIOARRAY registra la actividad de los usuarios en la medida necesaria para supervisar, analizar e investigar actuaciones indebidas o no autorizadas, de forma que siempre se pueda identificar a la persona que actúa. Lo hace respetando la normativa de protección de datos. Dispone también de mecanismos de detección y reacción frente a código dañino.

Los incidentes de seguridad se gestionan mediante procedimientos de detección, clasificación, análisis, resolución, comunicación a las partes interesadas y registro de las actuaciones. Las brechas de datos personales se notifican según establece la normativa. Las lecciones aprendidas se aprovechan para mejorar la seguridad.

20. Continuidad de la actividad

BIOARRAY dispone de copias de seguridad y de planes de continuidad y recuperación para que, ante un incidente, los servicios esenciales del laboratorio puedan seguir funcionando o restablecerse cuanto antes. Estos planes se ponen a prueba mediante simulacros periódicos y se revisan a partir de sus resultados.

21. Revisión y mejora continua

El Comité de Seguridad revisa esta política al menos una vez al año o cuando hay cambios significativos en la organización, la tecnología o la normativa. Antes de que la Gerencia la apruebe, la revisan el Responsable de la Seguridad y el Responsable del Sistema

Su cumplimiento se comprueba mediante auditorías internas y externas periódicas. Las desviaciones se corrigen con medidas correctivas y los resultados se comunican a la Dirección. La mejora continua aplica los criterios del Esquema Nacional de Seguridad y las guías CCN-STIC.

La Gerencia de BIOARRAY se compromete a dotar de los recursos necesarios a la seguridad de la información y a mejorarla de forma continua, como garantía de confianza para pacientes, profesionales sanitarios, clientes y colaboradores.

La Gerencia · BIOARRAY, S.L.