1. OBJETIVO

La presente Política de Seguridad de la Información (en adelante, “la Política”) tiene por finalidad establecer los lineamientos generales para la implementación, mantenimiento y mejora constante del Sistema de Gestión de la Seguridad de la Información (SGSI) en ELYTRON BIOTECH (en adelante, “ELYTRON” o “la Organización”). Su meta es salvaguardar los activos de información críticos, atenuar los riesgos asociados y cumplir con los requisitos legales y contractuales vigentes, en especial aquellos propios de la República Argentina, como la Ley 25.326 de Protección de Datos Personales, la Ley 11.723 de Propiedad Intelectual y las normas aplicables en materia de ciberdelitos.

---

2. ALCANCE

Esta Política se aplica a todos los procesos de negocio de ELYTRON, así como a las personas que gestionen información de la Organización o empleen sus recursos tecnológicos (empleados, contratistas, proveedores, socios comerciales, entre otros). Cuando determinadas áreas o procesos entren dentro del alcance de una certificación ISO 27001, se podrán definir controles específicos o adicionales para tales unidades.

Los requerimientos descritos a lo largo de este documento abarcan cualquier formato de información (físico, digital, portátiles, entre otros) y cualquier ubicación reconocida por ELYTRON (instalaciones propias o espacios autorizados de terceros).

---

3. OBJETIVOS Y PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

ELYTRON adopta los siguientes principios y objetivos para su Sistema de Gestión de la Seguridad de la Información:

1. **Confidencialidad**
   Asegurar que la información sea accesible únicamente para quienes cuenten con la debida autorización.
2. **Integridad**
   Garantizar que la información se mantenga exacta, completa y veraz, previniendo cualquier alteración no autorizada.
3. **Disponibilidad**
   Promover el acceso oportuno a la información y a los sistemas de apoyo cuando se requiera, contribuyendo a la continuidad de las operaciones.

Para materializar estos objetivos, se implementarán medidas técnicas, organizativas y legales en línea con las mejores prácticas internacionales, especialmente ISO 27001:2022 bajo las recomendaciones de implementación ISO 27002, y las normas locales que resulten aplicables. Las definiciones específicas de procedimientos y controles se establecen en el resto de los instrumentos que conforman el SGSI, siempre en coherencia con la presente Política.

---

4. ALINEACIÓN CON ESTÁNDARES Y REQUISITOS

La referencia principal para los criterios de seguridad en ELYTRON es la Norma ISO 27001:2022, complementada por las guías y buenas prácticas de la ISO 27002. Asimismo, se atenderán los requisitos legales y contractuales que pudieran surgir de la actividad de la Organización, tanto a nivel nacional como internacional, con la debida asesoría profesional.

Esta Política se integra con documentos internos —procedimientos, directrices, normas internas y manuales— que:

- Definen controles y metodologías para cumplir los objetivos de seguridad.
- Se actualizan regularmente para reflejar cambios normativos, tecnológicos o del entorno de riesgos.
- Se comunican y se ponen a disposición de las partes interesadas en la Organización, en función de su pertinencia y nivel de acceso.

---

5. CONTROLES PRIORITARIOS

Sin perjuicio de otros aspectos que puedan regularse en el SGSI, se resaltan como prioritarios los dominios principales recogidos en la ISO 27001:2022 (Anexo A):

- Normas y procedimientos de seguridad de la información (A.5)
  Deben existir lineamientos claros sobre la creación, revisión y aprobación de documentos que protejan la información de ELYTRON.

- Organización de la gestión de la seguridad (A.6)
  Se definirá una estructura de roles y responsabilidades que garantice la eficacia y continuidad del SGSI, abarcando modalidades de trabajo remoto y el uso de dispositivos móviles.

- Recursos humanos (A.7)
  La incorporación, permanencia y desvinculación de personal deben contemplar controles de concientización y la suscripción de compromisos de confidencialidad adecuados.

- Gestión de activos (A.8)
  Procedimientos para la identificación, clasificación, etiquetado y protección de activos, a fin de asegurar la confidencialidad, integridad y disponibilidad de la información.

- Control de accesos (A.9)
  Es necesario regular el acceso lógico y físico, otorgando privilegios solo según el rol y las funciones de cada persona.

- Criptografía (A.10)
  Deberán definirse directrices para el cifrado de información que requiera mayor protección, con algoritmos y protocolos apropiados.

- Seguridad física y del entorno (A.11)
  Se establecerán controles que eviten accesos no autorizados, robos, daños o pérdida de información en las instalaciones y equipos de ELYTRON.

- Seguridad de las operaciones (A.12)
  Incluye controles sobre la operación diaria, protección contra malware, respaldos, registro de incidentes, integridad de software, gestión de vulnerabilidades y auditorías periódicas.

- Comunicaciones (A.13)
  Protección de la información en tránsito (digital, física o verbal), enfocada en asegurar la confidencialidad e integridad de los datos.

- Mantenimiento de sistemas (A.14)
  Procedimientos para garantizar la eficiencia y disponibilidad de sistemas mediante actualizaciones, soporte continuo y monitoreo.

- Gestión de proveedores (A.15)
  Cláusulas y requisitos de seguridad en contratos con terceros, de modo que la cadena de suministro cumpla los mismos estándares de protección.

- Incidentes de seguridad (A.16)
  Mecanismos formales para notificar, analizar y responder a incidentes con el fin de prevenir su repetición y reducir su impacto.

- Continuidad del negocio (A.17)
  Establecer planes y medidas orientados a la recuperación de servicios ante eventos críticos que interrumpan las actividades esenciales.

- Cumplimiento (A.18)
  Incluye el cumplimiento de normativas, leyes y reglamentaciones vigentes, apoyado en auditorías internas y externas para evaluar la eficacia del SGSI.

---

6. CUMPLIMIENTO Y MEJORA CONTINUA

Los instrumentos que conforman el SGSI deben alinearse con los objetivos de seguridad y garantizar que ELYTRON cumpla los requisitos legales, regulatorios y contractuales.

Cuando sea viable, se establecerán métricas e indicadores con el fin de evaluar objetivamente la eficacia de los controles implementados. De igual modo, la Organización revisará y actualizará periódicamente (al menos una vez al año) la totalidad de estos instrumentos para adaptarlos a cambios tecnológicos, regulatorios y de riesgo, promoviendo la mejora permanente del SGSI.

---

7. RESPONSABILIDADES

- **Dirección**
  Aprueba la Política, asigna los recursos necesarios para su adecuada implementación y fomenta la mejora continua del SGSI.

- **Responsable del SGSI**
  Lidera, ejecuta, supervisa y verifica el cumplimiento de la Política y de los documentos del SGSI. Propone ajustes cuando advierta cambios relevantes en la Organización o en el entorno externo.

- **Propietarios de la información**
  Cuando la normativa interna así lo establezca, clasifican y definen las necesidades de seguridad de los datos bajo su custodia, cumpliendo todos los requisitos establecidos.

- **Colaboradores, empleados, contratistas y proveedores**
  Cumplen esta Política y las normas asociadas al SGSI, reportan incidentes conforme a los procedimientos vigentes y actúan con diligencia en la gestión de la confidencialidad, integridad y disponibilidad de la información de ELYTRON.

---

8. SANCIONES

El incumplimiento —doloso o por negligencia— de la presente Política o de cualquier otro documento integrado en el SGSI podrá implicar la aplicación de medidas disciplinarias, de acuerdo con la normativa laboral y los procedimientos internos de ELYTRON.

Además, en caso de que la infracción afecte leyes argentinas (por ejemplo, Ley 25.326, Ley 11.723 o disposiciones en materia penal), la Organización podrá, de corresponder y dentro de lo establecido por la legislación, dar intervención a las autoridades competentes.

En relación con proveedores, contratistas y terceros, cualquier quebrantamiento de las obligaciones de seguridad podrá originar medidas contractuales que incluyan la suspensión o la finalización del vínculo, así como la posibilidad de iniciar acciones legales por daños y perjuicios.

---

1. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción del cambio	Elabora
07/02/2024	00	Creación de Documento	RSGSI