POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ROL	NOMBRE	CARGO
Elaborado por:	Jaime Alfredo Enero Antonio	Oficial de Seguridad y Confianza Digital
Revisado por:	Jaime Adhemir Gallegos Rondón	Presidente del Comité de Gobierno y Transformación Digital
Aprobado por:	Silvia Cuba Castillo	Presidenta Ejecutiva

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace declara que los activos de información son de vital importancia para la prestación de sus procesos y servicios. En tal sentido, se compromete a preservar su confidencialidad, integridad y disponibilidad, con la finalidad de ofrecer información oportuna y confiable a los usuarios de la entidad.

El Senace asume el compromiso de implementar un conjunto de medidas proactivas y reactivas, mantener una gestión y aplicación de seguridad de la información, una adecuada gestión de riesgos, la aplicación de medidas de control y una cultura de seguridad de la información; así como desarrollar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), en cumplimiento del marco normativo vigente, aplicando las buenas prácticas en materia de seguridad digital del Estado Peruano.

1. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Proteger los activos de información del Senace para la correcta operatividad de sus procesos y ejecución de sus funciones frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la preservación de la confidencialidad, integridad y disponibilidad de los activos de información relevantes.
- Proporcionar los recursos necesarios para asegurar la aplicación de las medidas de control comprendidas en el SGSI, para una gestión eficiente de los riesgos relacionados a la seguridad de la información.
- Mejorar continuamente el modelo del sistema de gestión de seguridad de la información, a fin de lograr una adecuada gestión de los riesgos relacionados a la seguridad de la información.
- Establecer una cultura de seguridad de la información.
- Cumplir con los requisitos legales, regulatorios y otros requerimientos relacionados a la seguridad de la información.
- Concientizar y sensibilizar al personal del Senace respecto a la gestión de la seguridad de la información.

2. ALCANCE

La presente política y las disposiciones emanadas en el marco de la misma son de cumplimiento obligatorio por parte de los colaboradores del Senace, independientemente del régimen laboral o vínculo contractual al que se encuentren sujetos, así como de las personas naturales o jurídicas vinculadas a la entidad que tengan acceso a información del Senace.

3. BASE LEGAL

- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba la “NTP-ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición Reemplaza a la NTP-ISO/IEC 27001:2014.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad.** Los activos de información deben mantenerse protegidos para asegurar que sólo los usuarios autorizados puedan acceder a los mismos.
- **Disponibilidad.** Los activos de información deben estar disponibles para su uso, por parte de los usuarios autorizados cuando lo requieran, garantizando el acceso oportuno.
- **Integridad.** Los activos de información deben estar protegidos para asegurar su integridad; es decir, que la información y sus métodos de proceso son exactos y completos.

5. REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información y el SGSI se establece de conformidad con los requisitos legales y reglamentarios vigentes en materia de seguridad de la información.

6. GESTIÓN ESTRATÉGICA DE RIESGO

La gestión de riesgos de la seguridad de la información forma parte de la gestión de riesgo institucional, encontrándose alineada con el plan estratégico institucional.

7. CRITERIOS DE EVALUACIÓN DEL RIESGO

Los criterios de evaluación de riesgos de seguridad de la información se describen en la Norma Técnica Peruana NTP-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.

8. CONTINUIDAD DE OPERACIONES

La gestión de la continuidad de las operaciones de la entidad se desarrolla en el Plan de Continuidad Operativa del Senace.

9. RESPONSABILIDADES

Las responsabilidades respecto del SGSI son las siguientes:

- La Alta Dirección asegura la implementación del SGSI de acuerdo con la Política de Seguridad de la Información.
- El Oficial de Seguridad y Confianza Digital es responsable de la coordinación operativa de SGSI y su mantenimiento.
- El Comité de Gobierno y Transformación Digital revisa el SGSI al menos una vez al año o cada vez que se produzca un cambio normativo, con el propósito de establecer su idoneidad, adecuación y eficacia; dejando constancia de dicha acción en las actas correspondientes.
- El Jefe de la Oficina de Administración, en coordinación con el Oficial de Seguridad y Confianza Digital, gestionan la capacitación en seguridad de la información para el personal del Senace.
- El responsable de un activo brinda la protección de la confidencialidad, integridad y disponibilidad del mismo.
- Todos los incidentes de seguridad de la información deben ser reportados al Oficial de Seguridad y Confianza Digital y éste a su vez al Consejo Nacional de Seguridad Digital, tal como se define en la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital emitida por la PCM[1].

10. DEFINICIONES

- **Acceso:** Permiso otorgado a una cuenta de usuario, que lo faculta para usar determinada información, sistemas, servicios u otros recursos informáticos.
- **Activo de información:** Es un recurso que tiene valor para una organización, que abarca datos, información, hardware, software, procedimientos u otros elementos esenciales para el funcionamiento y seguridad de la entidad.
- **Ciberseguridad:** Es un conjunto de prácticas, tecnologías y procesos destinados a proteger sistemas, redes, programas y datos contra ataques, daños o accesos no autorizados en el entorno digital. Su objetivo es asegurar la confidencialidad, integridad y disponibilidad de la información y los sistemas en entornos cibernéticos.
- **Comité de Gobierno y Transformación Digital:** Es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las

[1] Decreto de Urgencia Nº 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento

entidades de la Administración Pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad[2].

- **Confidencialidad:** Es el principio que garantiza que solo los usuarios autorizados puedan acceder a la información clasificada como confidencial.
- **Disponibilidad:** Consiste en asegurar que los recursos y servicios críticos estén siempre accesibles y operativos para los usuarios autorizados.
- **Integridad:** Consiste en garantizar que la información se mantenga sin alteraciones.
- **Incidentes de seguridad de la información:** Es la ocurrencia de uno o más eventos que comprometen la confidencialidad, integridad o disponibilidad de la información.
- **Oficial de seguridad y confianza digital:** Es el rol responsable de coordinar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad pública[3].
- **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas implementadas por las organizaciones y sistemas tecnológicos para resguardar y proteger la información, con el objetivo de mantener la confidencialidad, disponibilidad e integridad de los datos.
- **Seguridad digital:** Es el nivel de confianza en el entorno digital que se logra mediante la gestión y aplicación de medidas para mitigar los riesgos que afectan la seguridad de los usuarios.
- **Usuario:** Es cualquier persona o entidad con acceso autorizado a los sistemas, redes o recursos de información de una organización.

.

[2] El DS N.º 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

[3] Directiva Nº 001-2023-PCM/ SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, aprobada con la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.