



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

A : **CESAR OCTAVIO RAMOS HIDALGO**
PRESIDENTE DEL COMITE DE GOBIERNO Y
TRANSFORMACION DIGITAL

De : **PEDRO ARTURO PACHAS SUAREZ**
JEFE DE LA OFICINA DE TECNOLOGIAS DE LA
INFORMACION

Asunto : Informe anual de implementación del Plan de Gobierno Digital,
evaluación del desempeño del Modelo de Gestión Documental
(MGD), Modelo de Datos Abiertos Gubernamentales y Sistema
de Gestión de Seguridad de la Información (SGSI) – Periodo
2025

Referencia : PROVEIDO D000069-2026-SENACE-GG/OTI (30ENE2026)

Tengo el agrado de dirigirme a usted, con relación al asunto de la referencia, a fin de informarle lo siguiente:

I. ANTECEDENTES

- 1.1. Mediante el Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública al 2021.
- 1.2. Mediante Decreto Supremo N° 016-2017-PCM, que aprueba la “Estrategia Nacional de Datos Abiertos Gubernamentales del Perú 2017 - 2021” y el “Modelo de Datos Abiertos Gubernamentales del Perú”.
- 1.3. Decreto Legislativo N° 1412-2018, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- 1.4. Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, modificada por la Resolución Ministerial N° 087-2019-PCM.
- 1.5. Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI, que aprueba los lineamientos para la formulación del Plan de Gobierno Digital.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

- 1.6. Resolución de Presidencia Ejecutiva N.º 00003-2023-SENACE-PE que aprobó el Plan de Gobierno Digital 2023–2026 del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles– Senace.
- 1.7. Mediante Resolución de Presidencia Ejecutiva N° 00080-2020-SENACE/PE, de fecha 23-12-2020, la Presidencia Ejecutiva aprueba con eficacia anticipada al 02 de enero de 2020, el Plan de Gobierno Digital 2020 – 2023 del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace, en adelante PGD.
- 1.8. Mediante Resolución de Presidencia Ejecutiva N° 00003-2023-SENACE-PE, de fecha 17-01-2023, la Presidencia Ejecutiva aprueba el Plan de Gobierno Digital 2023 – 2026 del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace.
- 1.9. Mediante Memorando Múltiple N° D000001-2026-SENACE-CGTD de fecha 30-01-2026, la Presidencia de Comité de Gobierno Digital solicita a la OTI informar sobre la implementación del Plan de Gobierno Digital, evaluación del desempeño del Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) durante el año 2025, en el marco de su competencia.

II. ANÁLISIS

2.1. Objetivo

El presente documento tiene por objetivo informar la implementación del Plan de Gobierno Digital y el Sistema de Gestión de Seguridad de la Información (SGSI) – Periodo 2025 del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace, en el marco de la competencia de la OTI.

2.2. Análisis técnico

El actual Comité de Gobierno y Transformación Digital del Senace fue reconstituido mediante la Resolución de Presidencia Ejecutiva N° 00027-2025-SENACE/PE, de fecha 08 de abril de 2025 y está conformado por¹:

- Cesar Octavio Ramos Hidalgo, Asesor de Presidencia Ejecutiva, en representación de la Presidenta Ejecutiva del Senace, quien lo preside;
- El Jefe de la Oficina de Tecnologías de la Información.

¹ Se encuentra en trámite la designación del nuevo Líder de Gobierno y Transformación Digital, tras la culminación de las funciones de la señora Jessica Bravo, quien precedió en el cargo.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

- El Jefe de la Unidad de Recursos Humanos;
- El Jefe de la Oficina de Atención a la Ciudadanía y Gestión Documentaria;
- El Oficial de Seguridad de la Información;
- El Jefe de la Oficina de Asesoría Jurídica; y,
- La Jefa de la Oficina de Planeamiento y Presupuesto.

A finales del periodo 2025, el Comité de Gobierno y Transformación Digital ha iniciado las gestiones para la aprobación cuando se del nuevo Plan de Gobierno Digital del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace. El PGD vigente aprobado consta de un total de ocho (08) proyectos a ser desarrollados entre febrero de 2023 y diciembre de 2026.

2.3. Estado de avance e implementación del PGD en el periodo 2025

Respecto a la cartera de proyectos del PGD 2023-2026, ésta consideró un total de ocho (08) proyectos, de los cuales un (01) proyecto fue implementado y siete (07) proyectos fueron planificados para iniciar a partir del 2024.

En este sentido, hasta el 31-12-2025 se ha logrado un avance de implementación del PGD del 11.24%.

A continuación, se muestra la situación de cada proyecto:

No	Denominación del Proyecto	Estado	Avance
PGD01	Implementación de un centro de datos alterno.	Planificado	0%
PGD02	Implementación del portal de datos georreferenciados - Geosenace 2.0	Implementado	100%
PGD03	Certificación de la ISO 27001:2013 Sistema de gestión de seguridad de la información.	Planificado	0%
PGD04	Implementación del sistema de gestión de proyectos y portafolios del Senace.	Planificado	0%
PGD05	Implementación de soluciones de ciberseguridad	Planificado	0%
PGD06	Implementación del tablero de control - BSC del Senace.	Planificado	0%
PGD07	Implementación de la NTP ISO/IEC 12207 - Ingeniería de software y sistemas, procesos del ciclo de vida del software en el Senace.	Planificado	0%
PGD08	Mejoramiento y ampliación del sistema de información del Senace (PIP).	Planificado	0%

En este sentido, se informa que los indicadores del Plan de Gobierno Digital para el periodo 2025 se han mantenido sin cambios respecto al periodo anterior debido a las limitaciones presupuestales de la entidad para los

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

proyectos contemplados en este plan. Sin embargo, se indica que el Senace ha culminado la etapa de elaboración del Documento Equivalente del Proyecto de Inversión del Senace, del cual se han completado cuatro componentes definidos en su alcance.

El Documento Equivalente constituye una etapa previa necesaria para la implementación del proyecto "PGD08 – Mejoramiento y ampliación del sistema de información del Senace", contemplado en el Plan de Gobierno Digital. En ese sentido, tal como se informa, se han registrado avances significativos en el desarrollo del referido proyecto, los cuales deben ser incorporados en el PGD para reflejar adecuadamente su grado de ejecución. Por lo expuesto, resulta necesario modificar el alcance del proyecto con la finalidad de incluir formalmente esta etapa previa dentro de su estructura y cronograma, garantizando la coherencia técnica y la alineación con los lineamientos de gestión del portafolio de proyectos digitales.

2.4. Estado de avance e implementación del PGD en el periodo 2025

2.4.1. La Norma Técnica Peruana NTP ISO/IEC 27001:2022, respecto al SGSI – precisa la preservación de la confidencialidad, la integridad y la disponibilidad de la información, así como de los sistemas implicados en su tratamiento dentro de una organización. El Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital, en su artículo 30°, define a la seguridad digital como "el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno".

2.4.2. Durante el año 2025, se organizaron 4 capacitaciones en Seguridad de la Información bajo la modalidad de curso virtual, a través de la Plataforma Educativa Digital del Senace. Estas se desarrollaron en las siguientes fechas:

- Grupo 01 - 11 abril 2025 (Inducción nuevo personal en modalidad presencial para 39 personas)
- Grupo 02 - 30 junio 2025 al 11 julio 2025 (Inducción nuevo personal en modalidad virtual para 16 personas)
- Grupo 03 - 29 setiembre al 03 octubre (Inducción nuevo personal en modalidad virtual para 16 personas)
- Grupo 04 - 17 de noviembre al 30 de diciembre 2025 (Capacitación personal CAS en modalidad virtual para 32 personas)

2.4.3. A la fecha, se encuentran vigentes documentos de seguridad de información, los cuales son: Política de Seguridad de la Información (2024), Documento de Alcance (2017), Metodología de Gestión de Riesgos de Seguridad de la Información (2017) y Política de Áreas Seguras (2017).

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

- 2.4.4. Todos los documentos vigentes requieren actualizarse considerando las nuevas necesidades de la entidad y el actual entorno de trabajo. Asimismo, el modelo requiere mantenimiento y mejoras continuas de forma urgente considerando la inversión de horas /hombre de un puesto a tiempo completo como vendría a ser el Oficial de Seguridad y Confianza Digital.
- 2.4.5. Por otro lado, en el marco de la seguridad digital según el Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, la seguridad informática es un conjunto de actividades destinadas a gestionar los riesgos inherentes a la seguridad de la plataforma tecnológica, servicios informáticos, servicios de red para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información en el Senace. En este contexto, se ha implementado y mantienen en óptimas condiciones diversos mecanismos de seguridad. De forma permanente, se llevan a cabo las siguientes acciones:
1. Protección contra ataques web: Implementación de un Firewall de Aplicación Web (WAF) basado en la nube, que mitiga ataques como inyección SQL, cross-site scripting (XSS) y otras amenazas dirigidas a aplicaciones web.
 2. Prevención de intrusiones (IPS): Uso de un Sistema de Prevención de Intrusos (IPS) que analiza el tráfico de red en tiempo real para detectar y bloquear intentos de explotación, malware o actividades anómalas.
 3. Seguridad perimetral mediante SASE: Implementación de una arquitectura de Seguridad de Borde (SASE), que integra funcionalidades como Zero Trust Network Access (ZTNA), firewall en la nube y filtrado seguro del tráfico para usuarios remotos, asegurando acceso con doble autenticación (MFA) a los recursos institucionales.
 4. Modelo Zero Trust: Aplicación de políticas de acceso basadas en el principio de "nunca confiar, siempre verificar", limitando el acceso a recursos según la identidad del usuario, su dispositivo y el contexto de conexión.
 5. Protección de dispositivos finales (EPP): Uso de plataformas avanzadas de protección de endpoints, que incluyen defensa contra malware, ransomware y técnicas evasivas.
 6. Respaldo de información: Ejecución de copias de seguridad periódicas en soportes externos (como cintas magnéticas), garantizando la recuperación ante incidentes o pérdida de datos.
 7. Antivirus institucional: Empleo de soluciones antivirus de clase empresarial (como Kaspersky), con protección en tiempo real, análisis heurístico y actualización automática de firmas.
 8. Certificados de seguridad web (SSL/TLS): Uso de certificados digitales para asegurar la transmisión cifrada de datos en las plataformas web del SENACE, garantizando la autenticidad y la integridad de la comunicación.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

2.4.6. Asimismo, durante el año 2025, se ejecutaron las acciones correctivas derivadas del informe técnico del servicio especializado de Ethical Hacking contratado en 2023. Como resultado, a la fecha se ha alcanzado un avance del 81 % en la subsanación de las vulnerabilidades identificadas, encontrándose en proceso de remediación los hallazgos pendientes.

Estas acciones contribuyen significativamente a la reducción y control del riesgo asociado a amenazas cibernéticas, vulnerabilidades críticas y posibles interrupciones operativas, fortaleciendo la confidencialidad, integridad y continuidad de los servicios digitales institucionales.

2.4.7. Se precisa que, a partir de mayo de 2018, la OTI dejó de contar con el puesto CAS denominado Especialista en Seguridad de la Información que cumplía el rol de "Oficial de Seguridad de la Información" a tiempo completo, quien logró realizar en su gestión acciones para la implementación de un modelo de seguridad de la información. Al dejar de contar en este puesto, la gran mayoría de acciones sufrieron un impacto en la inversión de horas/hombre, ya que se tuvo que nombrar a un Oficial de Seguridad de la Información encargado en adición de sus funciones al Especialista I en Procesos en Tecnologías de la Información y del mismo modo trasladando funciones de seguridad informática del Coordinador de Infraestructura y Soporte de Tecnologías de la Información puesto que también la OTI dejó de contar, lo cual comprometió, seriamente la sostenibilidad del modelo de seguridad de información. Actualmente el rol de Oficial de Seguridad de la Información se encargó al Coordinador de Proyectos de Sistemas de Información en adición de sus funciones lo que genera una sobrecarga en sus labores, una atención básica a las funciones del rol y un riesgo de incompatibilidad entre las actividades del puesto y rol ejercido por la misma persona.

2.4.8. Por lo expuesto en el numeral anterior, se reitera que es de vital importancia contar con un "Especialista en Seguridad y Confianza Digital" (actual denominación del Oficial de Seguridad de la Información) CAS a tiempo completo, para actualizar y mantener vigente el modelo de gestión de la seguridad de la información en la entidad, al mismo tiempo asumir funciones relacionadas a la seguridad informática, ciberseguridad, riesgos digitales para fortalecer la seguridad digital en los servicios informáticos que ofrece el Senace para sus usuarios internos y externos.

2.4.9. Mediante Resolución de Gerencia General N.º D000015-2025-SENACE-GG, de fecha 30 de septiembre de 2025, se designó formalmente el Equipo de Trabajo Técnico y Multidisciplinario responsable de la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI) del Senace.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

III. CONCLUSIONES

Conforme a las consideraciones expuestas es posible concluir lo siguiente:

- 3.1. El Plan de Gobierno Digital 2023-2026 del Senace incluye una cartera de ocho (8) proyectos de tecnología digital, de los cuales un (1) proyecto está implementado y siete (7) proyectos estaban planificados para iniciar. En este sentido, el porcentaje de avance del PGD alcanzado al 31-12-2025 es del 11.24%, cifra que se ha mantenido sin cambios respecto al periodo anterior debido a las limitaciones presupuestales de la entidad.
- 3.2. Se ha cumplido con informar el proceso de la implementación del Plan de Gobierno Digital y Sistema de Gestión de Seguridad de la Información (SGSI) del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace al 31-12-2025.
- 3.3. Finalmente, el modelo del Sistema de Gestión de Seguridad de la Información requiere urgente mantenimiento y la implementación de mejoras, así como seguir actualizando toda la documentación vigente para que pueda tener sostenibilidad, requiriéndose para ello contar con personal CAS a dedicación exclusiva.

IV. RECOMENDACIONES

- 4.1. Informar a la instancia correspondiente la implementación del Plan de Gobierno Digital y Sistema de Gestión de Seguridad de la Información (SGSI) – Periodo 2025 del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles – Senace.
- 4.2. Formular un nuevo Plan de Gobierno Digital del Senace alineado con los lineamientos SGTD-PCM (2018) e incorporando las necesidades institucionales actuales.
- 4.3. Gestionar la incorporación de un personal especialista para que cumpla el rol de Oficial de Seguridad y Confianza Digital a tiempo completo con la finalidad de realice las actividades en mantenimiento, sostenibilidad y mejora continua del SGSI.
- 4.4. Realizar campañas de sensibilización en seguridad de información.

Atentamente,

Documento firmado digitalmente

PEDRO ARTURO PACHAS SUAREZ
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

PAPS/laci