"Año de la recuperación y consolidación de la economía peruana"

RESOLUCIÓN PRESIDENCIAL N° 027 -2025-UNTSJL-P

Lima, 11 de noviembre de 2025

VISTOS:

El Oficio N° 026-2025-UNTSJL-OTI de fecha 30 de octubre, Informe Legal N° 090-2025-UNTSJL/OAJ de fecha 05 de noviembre de 2025, el Informe N° 132-2025-UNTSJL/OPP, de fecha 10 de noviembre de 2025, Memorando N° 035-2025-UNTSJL/P, y Proveído del presidente de la Comisión Organizadora; y,

CONSIDERANDO:

Que, conforme a lo dispuesto por el Art. 18°, 4to párrafo de la Constitución Política del Estado, cada Universidad es autónoma en su régimen normativo de gobierno, académico, administrativo y económico. Las Universidades se rigen por sus propios estatutos en el marco de la constitución y las leyes;

Que, la Ley Universitaria Ley N° 30220, en su Art. 8°, establece que el Estado reconoce la autonomía Universitaria, la autonomía inherente a las Universidades se ejerce de conformidad con lo establecido en la Constitución, la presente Ley y demás normativa aplicable, esta autonomía se manifiesta en los siguientes regímenes: Normativo, de Gobierno, Académico, Administrativo y Económico;

Que, asimismo conforme al Art. 62°, Numeral 62.2, de la Ley Universitaria N° 30220, señala es atribución del Señor Presidente de la Comisión Organizadora Dirigir la actividad académica de la universidad y su gestión administrativa, económica y Financiera;

Que el Decreto Supremo Nº 157-2021-PCM, Decreto Supremo que reconoce al Oficial de Seguridad y Confianza Digital quien actúa de conformidad con lo establecido en el Decreto Nº1412, Decreto Legislativo que aprueba la Ley de gobierno Digital y su reglamento, así como el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y su reglamento

Que, el numeral 9.3 del Artículo 9° del Decreto de Urgencia Nº 007-2020, dispone que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), Designar un Oficial de Seguridad y Confianza Digital, un "Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT)" cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno y Transformación Digital (SEGDI), ente rector en materia de Confianza Digital liderada por el Oficial de confianza y seguridad digital.

Que, la Directiva Nº 001-223-PCM/SGTD, tiene como objetivo establecer criterios para la designación del Oficial de Seguridad y Confianza Digital, así como sus responsabilidades, de conformidad con lo dispuesto en el Artículo 111 ° del Reglamento del Decreto Legislativo Nº 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, aprobado mediante Decreto Supremo N° 029-2021-PCM;

"Año de la recuperación y consolidación de la economía peruana"

Que, el Equipo de Respuestas ante Incidentes de Seguridad Digital-CSIRT de la Universidad, es un equipo estratégico y técnico, conformado por gestores y especialistas en seguridad de las tecnologías de la información o informática, y es responsable de la gestión de incidentes de seguridad digital que afecten los activos de la Universidad o una red de confianza. Asimismo, es responsable de gestionar la respuesta y/o recuperación ante incidentes de seguridad digital que afecten a la Universidad Nacional del Centro del Perú y, coordinar y articular acciones con la Secretaría de Gobierno y Transformación Digital a través del Centro Nacional de Seguridad Digital, para atender los incidentes de seguridad digital.

Que, la jefatura de la Oficina de Tecnologías de la Información, considerando que el Oficial de Seguridad y Confianza Digital de la Universidad, permitirá la gestión y coordinación ante incidentes de Seguridad Digital, recomienda su designación; y

De conformidad al Dictamen Nº 01086-2025-R-UNCP, a las atribuciones conferidas por la normativa vigente

SE RESUELVE:

ARTICULO 1°.- DESIGNAR al **Ing. JESÚS OSWALDO CHECA AGUIRRE** con DNI N° 74171286, Jefe de la Oficina de Tecnología de la Información, como Oficial de Seguridad y Confianza Digital de la Universidad Nacional Tecnológica de San Juan de Lurigancho.

ARTÍCULO 2°.- ENCARGAR, el cumplimiento de la Resolución a la Dirección General de Administración, a través de las oficinas y unidades correspondientes.

REGÍSTRESE, COMUNÍQUESE Y EJECÚTESE

Dr. JULIO ALBERTO HENNINGS OTOYA
Presidente de la Comisión Organizadora
de la Universidad Nacional Tecnológica
de San Juan de Lurigancho

C.D. CESAR ANDRÉS BORJA VILLANUEVA
Secretario General de la Comisión Organizadora
de la Universidad Nacional Tecnológica
de San Juan de Lurigancho

2023

Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital

DIRECTIVA Nº 001-2023-PCM/SGTD

Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital

CONTROL DE VERSIONES

Versión	Fecha	Título	Elaborado por
1.0.0	2023/09	Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital	Secretaría de Gobierno y Transformación Digital

CONTENIDO

DIRECTIVA N° 001-2023-PCM/SGTD
DIRECTIVA QUE ESTABLECE EL PERFIL Y RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL

Artículo 1. Objeto

La presente Directiva tiene como objetivo establecer criterios para la designación del Oficial de Seguridad y Confianza Digital[1], así como sus responsabilidades, de conformidad con lo dispuesto en el artículo 111 del 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, aprobado mediante Decreto Supremo N° 029-2021-PCM.

Artículo 2. Marco legal

La presente Directiva toma como base legal las siguientes normas:

- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación 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, y modificatorias.
- Decreto Supremo N° 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto Supremo N° 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030.
- Resolución Ministerial N° 156-2021-PCM, que aprueba el Texto Integrado del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.

Artículo 3. Definiciones

Para los efectos de la presente Directiva, se consideran las siguientes definiciones:

a) **Ciberseguridad**: capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país[2].

b) **Confianza digital**: es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la

[1] Para todo efecto la mención referida al Oficial de Seguridad Digital debe entenderse como Oficial de Seguridad y Confianza Digital conforme a lo dispuesto en la Cuarta Disposición Complementaria Final del Decreto Supremo 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

[2] Literal h del artículo 3 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital[3].

c) **Dueño del proceso**: Es quien tiene la responsabilidad y autoridad para participar en el proceso de gestión de riesgos de seguridad de la información.
d) **Gestión de incidentes de seguridad digital**: proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares[4].
e) **Incidente de seguridad de la información**: un evento o una serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer los procesos, operaciones o la prestación de servicios de la entidad y de amenazar la seguridad de la información de la entidad pública.
f) **Incidente de seguridad digital**: evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales[5].
g) **Propietario del riesgo:** Es quien tiene la responsabilidad y autoridad para gestionar un riesgo de seguridad de la información.
h) **Riesgos de seguridad de la información**: Efecto de la incertidumbre sobre los objetivos de seguridad de la información de la entidad pública.
i) **Riesgo de seguridad digital**: efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan[6].
j) **Seguridad digital**: es 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 nacional y los objetivos nacionales en dicho entorno[7].
k) **Sistema de Gestión de Seguridad de la Información** (SGSI): comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación[8].

Artículo 4. Acrónimos

En la presente Directiva se utilizan los siguientes acrónimos:

a) **CNSD**: Centro Nacional de Seguridad Digital.
b) **CSCD**: Coordinador de Seguridad y Confianza Digital.

[3] Literal a del artículo 3 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
[4] Literal f) del artículo 3 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
[5] Literal e) del artículo 3 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
[6] Literal g del artículo 3 del Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
[7] Artículo 2 del Decreto Supremo N° 050-2018-PCM. Decreto que establece la definición de Seguridad Digital de ámbito nacional.
[8] Numeral 109.1 del artículo 109 del 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, aprobado mediante Decreto Supremo N° 029-2021-PCM.

c) **IEC**: International Electrotechnical Commission.
d) **ISO**: International Organization for Standardization.
e) **NIST:** National Institute of Standards and Technology.
f) **NTP**: Norma Técnica Peruana.
g) **OSCD**: Oficial de Seguridad y Confianza Digital.
h) **SGSI**: Sistema de Gestión de Seguridad de la Información

Artículo 5. Perfil del Oficial de Seguridad y Confianza Digital

5.1 El perfil del OSCD comprende tres (03) componentes: 1) conocimientos, 2) formación, y 3) experiencia profesional. Las entidades públicas para la designación del OSCD deben tomar en consideración lo siguiente:

5.1.1 Conocimientos

El OSCD designado cuenta con los siguientes conocimientos:

a) **Regulación nacional y estándares internacionales en seguridad y confianza digital**
   - Regulación en materia de seguridad digital, gobierno digital, transformación digital, confianza digital, seguridad de la información, interoperabilidad, computación en la nube, ciberseguridad, o protección de datos personales.
   - Estándares, marcos de referencia o metodologías para la gestión de riesgos de seguridad de la información, auditorías de seguridad de la información, ciberseguridad y protección de datos personales.

b) **Aplicación y uso de tecnologías digitales**
   - Metodologías, buenas prácticas y/o marcos de referencia para establecer procesos de desarrollo de software o sistemas de información seguros.
   - Sistemas y plataformas para:
     - Gestionar el acceso de usuarios a los sistemas de información o plataformas digitales.
     - Gestionar arquitecturas y/o sistemas de seguridad de red y perimetral.
     - Otros que sean de valor para la seguridad de la información de la entidad.

5.1.2 Formación

El OSCD debe contar con la siguiente formación:

a) **Grado o formación académica**
Bachiller o Titulado en ingeniería de sistemas o ingeniería de sistemas e informática, ingeniería informática o ingeniería de software o ingeniería electrónica o ingeniería de telecomunicaciones o ingeniería industrial o ciencias de la computación o ramas afines a la materia.

b) **Diplomaturas, programas y/o cursos**
   - Diplomatura, programa y/o curso en seguridad de la información, ciberseguridad o NTP-ISO/IEC 27001 o equivalente.
   - Diplomatura, programa y/o curso en gestión de riesgos o gestión de riesgos de seguridad de la información o NTP-ISO/IEC 27005 o NTP-ISO 31000 o equivalente.

Las condiciones sobre las diplomaturas, programas y cursos se sujetan a las disposiciones establecidas por la Autoridad Nacional del Servicio Civil (SERVIR).

5.1.3 Experiencia profesional

Para determinar la experiencia mínima del OSCD, la entidad pública puede tomar como referencia las siguientes alternativas:

a) Profesional con dos (02) años desempeñando roles o cargos como director o jefe de seguridad de la información, oficial de seguridad de la información u oficial de seguridad digital o afines en entidades públicas o privadas; o
b) Profesional con tres (03) años desempeñando roles o cargos como gestor, coordinador o líder implementando SGSI, auditor de seguridad de la información, en entidades públicas y/o privadas; o
c) Profesional con tres (03) años desempeñando roles o cargos como gestor, coordinador o líder gestionando riesgos de seguridad de la información, incidentes de seguridad de la información o ciberseguridad en entidades públicas y/o privadas; o
d) Profesional con cuatro (04) años desempeñando roles o cargos como especialista o analista en proyectos de implementación y/o operación y/o mantenimiento de SGSI o procesos para la gestión de riesgos de seguridad de la información, incidentes de seguridad de la información, ciberseguridad, y/o afines, en el sector público y/o privado.

5.2 La entidad pública, conforme a su contexto, estructura, necesidades y objetivos, puede establecer una experiencia profesional del OSCD superior a la señalada en el numeral 5.1.3 de la presente Directiva, ya sea en años, roles, cargos ejercidos y/o experiencia en la aplicación de estándares o marcos de referencia exigibles en el sector al que pertenece.

5.3 La formación y la experiencia profesional deben contar con la documentación sustentatoria correspondiente.

Artículo 6. Requisitos adicionales

6.1 La entidad pública, conforme a su contexto, estructura, necesidades y objetivos, puede establecer requisitos adicionales a los establecidos en los numerales 5.1.1 y 5.1.2 del artículo 5 de la presente Directiva para la designación del OSCD. Puede tomar como referencia los siguientes conocimientos y formación:

6.1.1 Conocimientos

La entidad pública puede requerir al OSCD, como requisitos adicionales, conocimientos en algunas de las siguientes normas técnicas reconocidas en seguridad y confianza digital que generen valor a la entidad pública o sean acordes con las establecidas en su sector o ámbito, entre ellas tenemos:

a) **Normas técnicas en seguridad y confianza digital vigentes**, tales como:
   - NTP-ISO/IEC 27002.
   - NTP-ISO/IEC 27003.
   - NTP-ISO/IEC 27004.
   - NTP-ISO/IEC 27017.
   - ISO/IEC 27018.
   - ISO/IEC 27021.

- ISO/IEC 27032.
- ISO/IEC 27701.
- ISO/IEC 27033.
- ISO/IEC 22301.
- ISO/IEC 29100.
- NIST Cybersecurity Framework.
- Otras normas técnicas[9] de valor para la entidad y/o exigibles en su sector.

b) Sistemas y plataformas de seguridad específicos

- Sistemas y plataformas de seguridad acorde a la misión y funciones de la entidad pública.

6.1.2 Formación

La entidad pública puede requerir al OSCD, como requisitos adicionales, certificaciones internacionales, cursos, programas y/o diplomaturas en:

a) Certificaciones internacionales relacionadas con la seguridad y confianza digital, tales como:

- Seguridad de sistemas de información.
- Seguridad para soluciones en nube.
- Gestión de seguridad de la información.
- Privacidad o gestión de soluciones de privacidad de datos.
- Protección de datos.
- Gestión de servicios de tecnologías de la información.
- Auditoría de sistemas de información.
- Gestión de riesgos.
- Gestión de proyectos.
- Otras certificaciones que generen valor a la entidad pública o sean acordes con las establecidas en su sector o ámbito.

b) Diplomaturas, programas y/o cursos:

- Diplomatura, programa y/o curso en auditoría de seguridad de la información.
- Diplomatura, programa y/o curso en protección de datos personales o privacidad.
- Diplomatura, programa y/o curso en gestión de proyectos.
- Diplomatura, programa y/o curso en transformación digital o gobierno digital.
- Diplomatura, programa y/o curso en gestión de incidentes de seguridad de la información.
- Diplomatura, programa y/o curso en la NTP-ISO/IEC 27002 o controles de seguridad de la información.
- Otras diplomaturas, programas y/o cursos afines a los especificados anteriormente.

6.2 Las diplomaturas, programas, cursos y certificaciones internacionales deben contar con la documentación sustentatoria correspondiente.

[9] Puede comprender a las normas técnicas peruanas emitidas por el INACAL, la SGTD, u otras emitidas por organismos de normalización internacional.

Artículo 7. Responsabilidades

El OSCD tiene las siguientes responsabilidades:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
b) Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
c) Formular y proponer políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.
d) Promover la conformación y adecuada operación del equipo de respuestas ante incidentes de seguridad de la información.
e) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.
f) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.
g) Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.
h) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.
i) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la entidad pública e informarlos a la máxima autoridad administrativa.
j) Informar a la máxima autoridad administrativa acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
k) Coordinar con el CNSD acciones de sensibilización y capacitación para los funcionarios y servidores civiles de la entidad sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
l) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.
m) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.
n) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización de la entidad su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.
o) Liderar a los CSCD designados en la entidad pública para la adecuada implementación del SGSI.

p) Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la unidad de organización de tecnologías de la información cuando ésta adquiera, tercerice o desarrolle software o implemente otro tipo de soluciones tecnológicas.
q) Coordinar con la unidad de organización responsable de las tecnologías de la información o la que haga sus veces en la entidad, cuando corresponda, en los temas relativos a sus responsabilidades.
r) Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

Artículo 8. Designación y comunicación del Oficial de Seguridad y Confianza Digital

8.1 El Titular de la entidad pública designa al OSCD mediante acto resolutivo en un plazo de quince (15) días hábiles posterior a la publicación de la presente norma.

8.2 En caso la entidad pública cuente con oficinas desconcentradas, órganos ejecutores, unidades de organización de servicios o procesos tecnológicos altamente especializados o críticos para el Estado, designa un Coordinador de Seguridad y Confianza Digital (CSCD) en cada una de ellas conforme con su criticidad y nivel de riesgo de seguridad de la información; la designación se realiza mediante acto de administración interna. El CSCD coordina y articula con el OSCD la implementación, operación, mantenimiento y mejora continua del SGSI de la entidad pública a la que pertenece, y apoya en el cumplimiento de las responsabilidades del OSCD. Las responsabilidades de los CSCD deben ser establecidas por el OSCD conforme sus necesidades.

8.3 En el caso de los Proyectos Especiales[10], su máxima autoridad ejecutiva o administrativa, previa evaluación de su contexto, estructura, necesidades y objetivos, puede designar un CSCD. Dicha evaluación debe mantenerse como información documentada.

8.4 Las entidades públicas que hayan designado a un Oficial de Seguridad de la Información, Oficial de Seguridad Digital u OSCD, a la fecha de publicación de la Resolución N° 001-2023-PCM/SGTD, evalúan, a través de sus Oficinas de Recursos Humanos o quien haga sus veces, si dicho rol cumple con lo establecido en la presente Directiva, de acuerdo con lo siguiente:

a) Si dicho rol cumple con el perfil señalado en el artículo 5 de la presente norma puede continuar ejerciendo como tal. No siendo necesario la realización de un acto resolutivo adicional.
b) En caso contrario, corresponde al OSCD fortalecer sus capacidades a fin de cumplir con el perfil establecido, para lo cual dispone de un plazo no mayor a seis (06) meses contados a partir del día siguiente de publicación de la presente norma. Para el fortalecimiento de conocimientos y capacidades el OSCD puede acceder a los contenidos disponibles en la Plataforma Nacional de Talento Digital.

Concluido dicho periodo, y siempre que el OSCD no logre cumplir con el perfil establecido, corresponde a la entidad realizar una nueva designación en un plazo no mayor a quince (15) días hábiles.

[10] La definición de proyectos especiales está establecida en el artículo 18 de los Lineamientos de Organización del Estado, aprobado mediante Decreto Supremo N° 054-2018-PCM y modificatorias. En el caso del Poder Ejecutivo se debe observar el Decreto Supremo N° 098-2021-PCM, Decreto Supremo que aprueba la calificación y relación de los Programas y Proyectos Especiales del Poder Ejecutivo, o norma vigente.

c) Los conocimientos son evaluados durante el proceso de selección (evaluación de conocimientos o entrevista). En el caso de los OSCD designados podrán acreditar los conocimientos mediante Declaración Jurada.

8.5 La designación del OSCD y, de ser el caso, del CSCD, se publica en la sede digital de la entidad en la Plataforma Digital Única para Orientación al Ciudadano (Plataforma GOB.PE). Asimismo, las entidades públicas informan a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros sobre las designaciones realizadas, así como cualquier cambio en estos, a través de la Plataforma Integral de Solicitudes Digitales del Estado Peruano (Plataforma Facilita Perú)[11].

Artículo 9. Aplicación de la Directiva por parte de los gobiernos locales

9.1 En el caso de los gobiernos locales tipo B, D, E, F y G, conforme a la clasificación realizada por el Ministerio de Economía y Finanzas, en el marco del Programa de Incentivos a la Mejora de la Gestión Municipal, designan a su OSCD de acuerdo con el siguiente perfil:

9.1.1 Formación

a) Titulados en carreras técnicas, tales como, computación e informática o administración de sistemas o tecnologías de la información o, seguridad de la información o administración de redes y comunicaciones o afines a lo especificado.

b) Diplomatura, programa y/o curso sobre la NTP ISO/IEC 27001 o norma equivalente.

9.1.2 Experiencia profesional

Mínimo un (01) año de experiencia en proyectos de implementación y/o mantenimiento de SGSI o en áreas de tecnologías de información o soporte informático, o afines a lo especificado

9.2 Los precitados gobiernos locales que, por razones de recursos y presupuesto, no cuentan con un profesional que cumpla con el perfil establecido en el numeral 9.1 del presente artículo, designan al responsable de la unidad de organización de tecnologías de la información o al que haga sus veces en la entidad.

9.3 En caso un gobierno local no cuente con una unidad de organización de tecnologías de la información, designa a la máxima autoridad administrativa como OSCD.

[11] Ver: https://facilita.gob.pe