DIRECTIVA DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA NACIONAL DE EDUCACIÓN SUPERIOR UNIVERSITARIA - SUNEDU

ROL	NOMBRE	CARGO	FIRMA
Elaborado por:	Guillermo Pérez Silva	Jefe de la Oficina de Tecnologías de la Información	Documento firmado digitalmente **GUILLERMO PÉREZ SILVA** Jefe de la Oficina de Tecnologías de la Información Superintendencia Nacional de Educación Superior Universitaria
Revisado por:	Luis Rafael Hoyle Ganoza	Jefe de la Oficina de Planeamiento y Presupuesto	Documento firmado digitalmente **LUIS RAFAEL HOYLE GANOZA** Jefe de la Oficina de Planeamiento y Presupuesto Superintendencia Nacional de Educación Superior Universitaria
	Carlos Fernando Mesía Ramírez	Jefe de la Oficina de Asesoría Jurídica	Documento firmado digitalmente **CARLOS FERNANDO MESÍA RAMÍREZ** Jefe de la Oficina de Asesoría Jurídica Superintendencia Nacional de Educación Superior Universitaria

CONTROL DE CAMBIOS

N°	Ítem	Descripción del cambio
-	1.0	Versión Inicial del documento

1. OBJETIVO

Establecer las disposiciones que regulen la gobernanza de la seguridad de la información y el resguardo de los activos de información, recursos informáticos o plataformas tecnológicas donde se procesa y almacena información en la Sunedu frente a amenazas, internas o externas, deliberadas o accidentales con el fin de mitigar los riesgos.

2. FINALIDAD

Gestionar adecuadamente la seguridad de la información que permita asegurar la confidencialidad, integridad y disponibilidad de la información institucional ante amenazas internas y externas, minimizando los riesgos de daño a la información digital o física y que puedan afectar la continuidad operativa y servicios que brinda la entidad, mediante el cumplimiento y/o implementación de los lineamientos establecidos en la presenta Directiva, contribuyendo al cumplimiento de los objetivos institucionales.

3. BASE LEGAL[1]

3.1. Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
3.2. Ley N° 29733, Ley de Protección de datos personales.
3.3. Ley N° 30220, Ley Universitaria.
3.4. Decreto Legislativo N° 1412, aprueba la Ley de Gobierno Digital.
3.5. Decreto de Urgencia Nº 006-2020, crea el Sistema Nacional de Transformación Digital
3.6. Decreto de Urgencia N° 007-2020, Marco de Confianza Digital y dispone medidas para su Fortalecimiento.
3.7. Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la información Pública.
3.8. Decreto Supremo Nº 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de protección de Datos Personales.
3.9. Decreto Supremo N° 012-2014-MINEDU, que aprueba el Reglamento de Organización y Funciones - ROF de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU.
3.10. Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 - Ley del Procedimiento Administrativo General.
3.11. Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información.
3.12. Decreto Supremo 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo 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.
3.13. Decreto Supremo Nº 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia Nº 006-2020, Decreto Supremo que crea el Sistema Nacional de Transformación Digital

[1] Cuando se hace mención a las referidas normas, se incluyen sus respectivas disposiciones ampliatorias y modificatorias, de ser el caso.

3.14. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2° Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
3.15. Resolución Ministerial N° 119-2018-PCM, mediante la cual se dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
3.16. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/ SGTD que aprueba la Directiva Nº 001-2023-PCM/SGTD, directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
3.17. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas
3.18. Resolución de Secretaría General N° 0008 -2023-SUNEDU, que aprueba la actualización del "Manual de Procedimientos de los procesos PS.4.1 Planificación de TIC, PS.4.2 Soluciones de TIC y PS.4.3 Operaciones de TIC".
3.19. Resolución de Secretaría General N° 0059-2022-SUNEDU, que aprueba la Directiva para la elaboración, aprobación, modificación y derogación de los documentos de Gestión interna de la Superintendencia Nacional de Educación Superior Universitaria - Sunedu.
3.20. ISO/IEC 27000:2018 "Tecnología de la información. Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Visión general y vocabulario".
3.21. ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos".
3.22. ISO/IEC 27002:2022 "Tecnologías de la Información - Técnicas de Seguridad - Código de prácticas para los Controles de Seguridad de la Información".

4. ALCANCE

Los lineamientos de la presente directiva son de cumplimiento obligatorio para todo el personal que preste servicios a la institución, indistintamente de su régimen laboral o modalidad contractual.

5. DEFINICIONES

5.1 **Activo de Información:** Cualquier información que tiene valor para la entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.

Los activos son los recursos necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección

5.2 **Confidencialidad:** Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados, conforme a las normas de la materia.

5.3 **Comité de Gobierno y Transformación Digital:** Es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las entidades de la Administración Pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad

Para todo efecto la mención al Comité de Gobierno Digital que se efectúe en cualquier disposición, norma o documento de gestión de la entidad, debe entenderse al Comité de Gobierno y Transformación Digital.

5.4 **Disponibilidad:** Propiedad de ser accesible y utilizable cuando lo requiera una entidad autorizada.

5.5 **Dispositivo Móvil**: Es un equipo tecnológico con capacidades de procesamiento y memoria, con conexión a Internet de fácil trasladado tanto dentro como fuera de la red informática de la entidad, y que se utiliza para almacenar, procesar y transportar información institucional, y permiten al personal y proveedor desempeñar su trabajo, accediendo al correo, Teams, sistemas de información y demás aplicaciones de la entidad. Este tipo de dispositivo puede incluir teléfonos móviles, tabletas, computadoras portátiles y cualquier otro dispositivo que permita la manipulación y transporte de información de la entidad.

5.6 **Estación de Trabajo:** Equipo de cómputo asignado por la entidad que están en las oficinas y conectados dentro de la red interna de la Sunedu o mediante conexión remota por VPN y es usada por el/la usuario/a como herramienta de trabajo para conectarse a sistemas de información, u otros servicios, tales como, correo electrónico, internet, etc.

5.7 **Entidades externas**: Son todas las instituciones públicas del Estado Peruano y organizaciones extrajeras que por algún motivo requieren compartir, transferir información entre ellas, conforme las leyes vigentes y convenios celebrados entre ellas.

5.8 **Equipo de Respuestas ante Incidentes de Seguridad Digital de la Sunedu:** Es el Equipo de Respuestas ante Incidentes de Seguridad Digital responsable de la gestión de incidentes de seguridad digital que afectan los activos de la entidad.

5.9 **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.

5.10 **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.

5.11 **Información:** Conjunto de datos contenidos en documentos físicos (Papel, Microfichas, Libros, etc.), medios magnéticos, medios ópticos y/o medios electrónicos.

5.12 **Integridad:** Propiedad de salvaguardar la exactitud y completitud de los activos.

5.13 **Propietario del Activo de Información:** Es el funcionario encargado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.

5.14 **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

5.15 **Sistema de Información:** Conjunto interdependiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, presentación, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

5.16 **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.

5.17 **Usuario/a:** Persona registrada y autorizada a utilizar un sistema de información determinado, bajo un nivel de acceso pre-establecido.

5.18 **Oficial de Gobierno de Datos:** Es el responsable de asegurar el uso ético de las tecnologías digitales y datos en la entidad pública, proponer iniciativas de innovación basadas en datos, fomentar una cultura basada en datos, articular y gestionar el uso de datos gubernamentales, y asegurar la calidad e integridad de datos que contribuya a la creación de valor público. Asimismo, es responsable impulsar y coordinar el modelamiento, procesamiento, análisis y desarrollo de servicios de información de datos gubernamentales y datos abiertos con los responsables de los procesos correspondientes, así como de coordinar la implementación del Modelo de Referencia de Datos de la entidad. Reporta al Comité de Gobierno y Transformación Digital institucional y, a la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros la implementación y aplicación de las normas en materia de gobernanza y gestión de datos.

5.19 **Oficial de Datos Personales:** Es el responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en la Sunedu.

5.20 **Oficial de Seguridad y Confianza Digital:** Es el Servidor/a de Sunedu que se le asigna el rol responsable de coordinar la implementación y mantenimiento del Sistema de Gestión de Seguridad de información (SGSI) en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital, transformación digital y gobierno digital.

Para todo efecto la mención al Oficial de Seguridad de la Información y Oficial de Seguridad Digital que se efectúe en cualquier disposición, norma o documento de gestión de la entidad, debe entenderse al Oficial de Seguridad y Confianza Digital.

5.21 **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.

5.22 **Teletrabajo:** Modalidad especial de prestación de labores, de condición regular o habitual. Se caracteriza por el desempeño subordinado de dichas labores sin presencia física del servidor civil en el centro de trabajo. Se realiza a través de la utilización de plataformas y tecnologías digitales.

5.23 **Trabajo remoto:** Prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita. Este no se limita al trabajo que puede ser realizado mediante medios informáticos, de telecomunicaciones u análogos, sino que se extiende a cualquier tipo de trabajo que no requiera la presencia física del trabajador en el centro de labores.

5.24 **SIGLAS**

- CGTD: Comité de Gobierno y Trasformación Digital.
- CNSD: Centro Nacional de Seguridad Digital
- NTP: Norma Técnica Peruana.
- MGD: Modelo de Gestión Documental.
- SGSI: Sistemas de Gestión de la Seguridad de la Información.
- TI: Tecnologías de la Información.
- VPN: "Virtual Private Network" (Red privada virtual).

- OTI: Oficina de Tecnologías de la Información.
- ORH: Oficina de Recursos Humanos
- OA: Oficina de Administración.
- UAB: Unidad de Abastecimiento

6. RESPONSABILIDAD

6.1. El CGTD es responsable de:

a) Formular el Plan de Gobierno Digital en coordinación con los órganos o unidades orgánicas de la entidad.
b) Liderar y dirigir el proceso de transformación digital en la entidad.
c) Evaluar que el uso actual y futuro de las tecnologías digitales sea acorde con los cambios tecnológicos, regulatorios, necesidades de la entidad, objetivos institucionales, entre otros, con miras a implementar el Gobierno Digital.
d) Gestionar la asignación de personal y recursos necesarios para la implementación del Plan de Gobierno Digital, MGD, Modelo de Datos Abiertos Gubernamentales y SGSI en los Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.
e) Promover y gestionar la implementación de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, identidad digital y datos en la entidad.
f) Elaborar informes anuales que midan el progreso de la implementación del Plan de Gobierno Digital y evalúen el desempeño del MGD, Modelo de Datos Abiertos Gubernamentales y SGSI.
g) Vigilar el cumplimiento de la normatividad relacionada con la implementación del gobierno digital, interoperabilidad, seguridad de la información y datos abiertos en las entidades públicas.
h) Promover el intercambio de datos, información, software público, así como la colaboración en el desarrollo de proyectos de digitalización entre entidades.
i) Gestionar, mantener y documentar el MGD, Modelo de Datos Abiertos Gubernamentales y SGSI de la entidad.
j) Promover la conformación de equipos multidisciplinarios ágiles para la implementación de proyectos e iniciativas de digitalización de manera coordinada con los responsables de órganos y unidades orgánicas de la entidad.
k) Promover y dar seguimiento a la implementación de los presentes lineamentos que garanticen la seguridad de la información y los activos que la soportan; así como la actualización de los mismos.
l) Tener autoridad y responsabilidad sobre la gestión del Sistema de Gestión de Seguridad de la Información de la Sunedu.

6.2. Los/las directores/as y jefes/as de órganos y unidades orgánicas son responsables de:

a) Cumplir y hacer cumplir en el ámbito de su competencia, los lineamientos de la presente Directiva y el cumplimiento de las normativas de seguridad de la información y confianza digital.
b) Hacer cumplir las cláusulas incluidas dentro de los contratos, órdenes de Servicio y/o declaraciones juradas de acuerdos de confidencialidad, que están referidas a salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Sunedu.

6.3. El personal de cualquier modalidad laboral (Contrato Administrativo de Servicios – CAS/ Ley N° 30057, Ley del Servicio Civil) que brinde servicios a la Sunedu es responsable de:

a) Cumplir los lineamientos de la presente Directiva.
b) Utilizar la información a la cual accede de una manera adecuada y segura.
c) Velar por el uso y resguardo de la información y activos de información de lo cual es responsable, así como de la información que se use y trate en los servicios con proveedores y entidades externas.

6.4. El Oficial de Seguridad y Confianza Digital es responsable de:

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 de la Sunedu.
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 e informarlos a la máxima autoridad administrativa de la Sunedu.
j) Informar a la máxima autoridad administrativa de la Sunedu 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 los órganos y unidades orgánicas de la Sunedu 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) 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 Oficina de Tecnologías de la información cuando ésta adquiera, tercerice o desarrolle software o implemente otro tipo de soluciones tecnológicas.
q) Coordinar con Oficina de Tecnologías de la información, cuando corresponda, en los temas relativos a sus responsabilidades.

7. DISPOSICIONES GENERALES

7.1. La Sunedu gestiona, mantiene, monitorea, documenta y efectúa el mejoramiento continuo del SGSI mediante su CGTD y la OTI, así como promueve el cumplimiento de normas técnicas, estándares internacionales y de las mejores prácticas de seguridad de la información, a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

7.2. Todo lo contenido en este documento es de aplicación obligatoria por parte de todo el personal bajo los distintos regímenes laborales de la Sunedu, y ante su incumplimiento, se reportará al CGTD para su conocimiento y disponga las acciones correspondientes de considerarlo necesario, de esa forma, la autoridad competente de la institución, aplicará las medidas disciplinarias de acuerdo a las normas vigentes de la institución.

En el caso de los/las proveedores/as que prestan servicios a la Sunedu, los responsables de las direcciones, órganos o unidades orgánicas usuarias deben comunicar al CGTD si tienen conocimiento de actos que impliquen la contravención a la seguridad y/o confidencialidad de la información de la entidad a la que tienen acceso para el cumplimiento de los servicios contratados, a fin de que se evalúe la aplicación de las acciones que correspondan.

7.3. Toda información interna (generada por la Sunedu) o externa (de propiedad de entidades externas, administrados, proveedores y/o empresas) contenida en equipos informáticos, en medios físicos o digitales y/o en sistemas de información de la Sunedu, están bajo custodia de la Entidad y por lo tanto deberán ajustarse a la presente Directiva de seguridad de la información.

7.4. Toda información que se intercambie con otras Instituciones públicas o privadas, deberá ser tratada conforme a los acuerdos de confidencialidad que se encuentren establecidos en la Entidad.

7.5. Todo responsable de la dirección del órgano o unidad orgánica deberá asegurar que el personal a su cargo conozca los niveles de confidencialidad y criticidad de la información que se maneja en su dirección, órgano o unidad.

7.6. Todo el personal bajo los distintos regímenes laborales de la Sunedu debe:

a) Aplicar los presentes lineamientos para el desempeño de sus funciones y actividades en la institución.
b) Utilizar los recursos informáticos y/o sistemas de información puestos a su disposición, de manera legal, profesional y ética.
c) Aplicar las disposiciones de seguridad física; es decir prevenir accesos no autorizados, daños en las instalaciones y resguardar los equipos ubicándolos en áreas protegidas con controles de acceso adecuados.
d) Comunicar o reportar al Oficial de Seguridad y Confianza Digital, cualquier evento, debilidad o amenaza que atente o podría atentar contra la información o activo de información requeridos para la función de la institución.
e) Proporcionar la información requerida por el Oficial de Seguridad y Confianza Digital ante la detección de un incidente de seguridad digital, o por procedimientos de revisión sobre activos de información de la Sunedu.
f) Respetar los lineamientos de acceso físico a los ambientes y zonas restringidas de la Sunedu, en donde se cuente con bienes e información restringida y/o confidencial.
g) Respetar los lineamientos de seguridad de la información de acuerdo con la legislación vigente en materia de protección de datos personales.
h) Respetar los lineamientos de seguridad de la información de acuerdo con la legislación vigente en materia de la transparencia y acceso a la información.
i) Respetar los lineamientos de seguridad de la información alineados a la seguridad digital y confianza digital de acuerdo con la legislación vigente.

8. DISPOSICIONES ESPECÍFICAS

8.1 De la organización de la seguridad de la información

8.1.1. Segregación de funciones

Los órganos o unidades orgánicas deben segregar funciones asignando roles y/o responsabilidades a su personal para reducir oportunidades de modificación no autorizada o no intencional e intencionales o mal uso de los activos de información de la organización, así como para garantizar la protección de los activos de información y la gestión de riesgos de Seguridad digital.

Es responsabilidad de los propietarios de los activos de información autorizar los accesos a la información de acuerdo a la definición y segregación de funciones y definido en los perfiles de usuarios/as para el acceso a cada servicio informático y sistema de información.

8.1.2. Gestión de servicios y proyectos de TI

La OTI debe integrar la seguridad de la información en sus procesos de gestión de servicios y proyectos de TI, para garantizar que los riesgos de seguridad digital sean identificados y tratados pertinentemente.

8.1.3. Contacto con autoridades y grupos de interés especial

El CGTD y la OTI deben establecer y mantener canales de comunicación con el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital para el apoyo y asesoría, legales y reguladoras en materia de seguridad de la información. Asimismo, se debe mantener contacto con grupos de interés como foros especializados, organismos y/ o empresas expertas en seguridad de la información y seguridad digital.

8.1.4. Dispositivos móviles

La Sunedu permite el uso de dispositivos móviles dentro y fuera de la infraestructura de comunicaciones de la entidad, ya sean estos bienes asignados por la Sunedu o bienes en posesión del personal que no son asignados por la Sunedu, debidamente autorizados para el acceso a la red de la entidad o el ingreso físico a los ambientes de la entidad, en los que se almacena, transfiere o procesa información de propiedad de la Sunedu. La entidad mantiene el derecho a controlar dicha información, aunque no haya asignado el dispositivo móvil, previas coordinaciones y autorizaciones correspondientes, de acuerdo con las normas vigentes en materia de Protección de Datos Personales.

Obligaciones:

a) La OTI es responsable de coordinar y gestionar la instalación de controles de seguridad en los dispositivos móviles.
b) Todo usuario/a de dispositivos móviles que contengan información confidencial o de uso interno de la Sunedu debe usar la última o la más segura versión de los productos de software. Los parches o actualizaciones serán los obtenidos de manera formal, provenientes del fabricante.
c) La OTI debe mantener actualizado el software antivirus de los dispositivos móviles de la entidad. A su vez, el personal es responsable de mantener actualizado el software antivirus del dispositivo móvil que se conecte a la red de la entidad y/o utilice los sistemas de ésta, previa autorización de la Sunedu.
d) Todo/a usuario/a poseedor/a de un dispositivo móvil personal que no es asignado por la Sunedu, en coordinación con el Oficial de Seguridad y Confianza Digital deben precisar el tipo de información que se puede mantener en las computadoras personales que son utilizados fuera de la Sunedu. El acceso a estos dispositivos debe estar protegido mediante controles como contraseña y nunca debe quedar el computador desatendido sin ningún bloqueo de acceso.
e) La OTI debe configurar los dispositivos móviles asignados por Sunedu destinados a ser utilizados fuera de las instalaciones de Sunedu con mecanismos de control de acceso seguro que impidan su utilización en caso de pérdida o robo.
f) Todo/a usuario/a de un dispositivo móvil debe obtener las aplicaciones instaladas en el dispositivo de canales oficiales y con el licenciamiento debido.
g) La OTI debe implementar, para los dispositivos asignados por Sunedu que lo soporten, instrumentos y herramientas técnicas (hardware/software) que permitan bloquear y/o borrar la información de forma remota.
h) La OTI debe contar con procedimientos para la reutilización y/o eliminación de dispositivos asignados por Sunedu (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible anteriormente almacenada.

8.1.5. Teletrabajo y trabajo remoto

En el caso que las labores se realicen mediante la modalidad del teletrabajo o trabajo remoto, ya sea con equipos informáticos asignados por Sunedu o bienes en posesión del personal que no son propiedad de la Sunedu, debidamente autorizados; la información que se almacena, transfiere o procesa para el desempeño de las labores es de propiedad de la Sunedu por lo que la entidad mantiene el derecho a controlar esos datos, previas coordinaciones y autorizaciones correspondientes, de acuerdo con las normas vigentes en materia de Protección de Datos Personales.

Obligaciones:

a) La OTI debe asegurar que sólo los equipos de cómputo debidamente autorizados por la Sunedu; tendrán acceso remoto vía VPN para acceder a los recursos informáticos. En tal sentido, tales equipos serán previamente

identificados a efectos de su autorización.

b) La OTI debe contar con un inventario de accesos remotos otorgados, identificando a la persona que cuenta con el acceso, el motivo por el cual se le otorgó y el plazo por el cual está autorizado.
c) La OTI debe monitorear y analizar el tráfico de datos de acceso remoto para identificar posibles anomalías de seguridad.
d) La OTI debe configurar los equipos utilizados por el/la usuario/a para el trabajo en acceso remoto, los cuales deben contar con protección ante software malicioso y conexiones seguras a través de una red privada virtual o VPN.
e) La OTI debe definir dónde se debe guardar la información que generen los/las usuarios/as mediante acceso remoto.
f) Todo/a usuario/a debe asegurar que los dispositivos desde los cuales se establezcan conexiones remotas deben cumplir con la configuración de seguridad de la institución como: antivirus actualizado, parches del sistema operativo correctamente instalados, etc.
g) Todo/a usuario/a debe de asegurar que dispone de un entorno de trabajo adecuado y seguro para proteger el equipo y/o las credenciales de acceso a los sistemas e información de los que es responsable.
h) Todo/a usuario/a debe autorizar el acceso remoto por parte del personal de soporte técnico y/o informático de la entidad a los equipos de los/las usuarios/as para realizar actividades de mantenimiento o configuración.

8.2 Seguridad de los recursos humanos

La Sunedu debe promover una cultura de seguridad de la información, de tal manera que las acciones de su personal no pongan en riesgo la confidencialidad, integridad y disponibilidad de la información de la entidad.

8.2.1 Previo al vínculo laboral

Obligaciones:

a) La ORH debe verificar los antecedentes laborales de la persona seleccionada para laborar en la entidad y las competencias requeridas para el puesto.
b) La ORH debe establecer en el Contrato de Trabajo y/o en una declaración Jurada cláusulas de confidencialidad de la información, así como las responsabilidades del cumplimiento de las políticas de seguridad de la información que rigen a la entidad, de derecho de autor y de protección de datos personales, según corresponda.
c) La ORH debe informar a la persona seleccionada de las responsabilidades administrativas y judiciales por el no cumplimiento de las disposiciones de la Seguridad de la Información.

8.2.2 Durante el vínculo laboral

Obligaciones:

a) La ORH debe fortalecer el compromiso del personal con la Seguridad de la Información a través de programas de inducción para el personal que se vincule a Sunedu, así como actualizaciones regulares de corresponder.
b) La ORH debe coordinar con el Oficial de Seguridad y Confianza Digital, los contenidos de inducción y capacitación sobre seguridad de la información, incluyendo políticas, normas y directivas sobre la materia.
c) La ORH debe comunicar al personal sus responsabilidades con respecto a la Seguridad de la Información según las funciones o actividades que realicen.
d) La ORH debe comunicar a la OTI, el inicio del vínculo laboral o rotación interna del personal para el otorgamiento de los correspondientes accesos a los sistemas de información, con una anticipación no menor a dos (2) días hábiles a la fecha prevista para el inicio de las labores.
e) La OTI y Los propietarios responsables de administrar los sistemas de información deben ejecutar la "alta" efectiva de los accesos con un (1) día hábil de anticipación a la fecha prevista para el inicio de las labores del personal.
f) La ORH comunica a la Secretaría Técnica de los Procedimientos Administrativos Disciplinarios, los actos que suponen el incumplimiento de las disposiciones de seguridad de la información establecidos en el presente instrumento, a fin de que se lleve a cabo la precalificación de la supuesta conducta infractora y de ser el caso se disponga el inicio del Procedimiento Administrativo Disciplinario.
g) La ORH debe desarrollar programas de formación y concientización especializados para ciertos perfiles de empleados en ciberseguridad y seguridad de la información.
h) Todos/as los/as directores/as y jefes/as o encargados/as de los órganos y unidades orgánicas deben asegurar el cumplimiento por parte del personal y terceros, de las políticas, directivas y procedimientos de seguridad de información establecidos.
i) Todos/as los/as directores/as y jefes/as o encargados/as de los órganos y unidades orgánicas, que requieran de servicios de terceros, debe asegurar que se defina las responsabilidades de éstos y que se les informe respecto a las políticas, directivas y procedimientos de seguridad de información vigentes.
j) Todo el personal de la Sunedu, debe asistir a las capacitaciones en temas de seguridad de la información y ciberseguridad cuando se les convoque.

8.2.3 Al término del vínculo laboral

Obligaciones:

a) La ORH debe comunicar a la OTI, la finalización del vínculo laboral del personal para la baja de accesos correspondiente, con una anticipación no menor a un (1) día hábil a la fecha prevista para la extinción del vínculo laboral.

b) En los casos en los cuales los órganos y/o unidades orgánicas informen a la ORH sobre ceses o renuncias, la ORH debe comunicarlo a la OTI en el mismo día de haber tomado conocimiento.
c) La OTI o el órgano o unidad orgánica responsable del sistema de información debe ejecutar la baja efectiva de los accesos a los sistemas de información el último día del periodo del vínculo laboral del personal.
d) En el caso de prestación de servicios de terceros, en que, por la necesidad del servicio, se les hubiere autorizado el acceso a los sistemas de información, las directores/a o jefes/as de los órganos y unidad orgánicas usuarias deben informar oportunamente a OTI sobre el fin del contrato de los terceros, a fin de que la OTI ejecute la "baja" efectiva de los accesos que se hubiesen autorizado.
e) Los/las directores/a o jefes/as de los órganos y unidad orgánicas, cuando se produzca ausencia temporal o vacaciones del personal a su cargo, podrán notificar a la OTI la necesidad de bloquear provisionalmente los accesos a cargo de el/la usuario/a durante de la ausencia de éste.

8.3 Seguridad relativa a los activos de información

8.3.1 Inventarios de activos de información

Obligaciones:

a) La OTI debe mantener un inventario de activos de sistemas de información actualizado semestralmente. Para el inventario de activos informáticos de toda la entidad (hardware, software, licencias, programas, sistemas de información), la OTI debe considerar las normativas vigentes de inventarios y registros contables en el sector público.
b) La OA, mediante la UAB, debe mantener un inventario de equipos informáticos actualizado y revisado semestralmente.

8.3.2 Propiedad de los activos

Obligaciones:

a) El/la propietario/a del activo de información es responsable de asegurar la apropiada clasificación y protección del mismo; para lo cual, debe definir y revisar periódicamente las restricciones de acceso y las clasificaciones, realizar el monitoreo continuo sobre la manipulación, traslado y almacenamiento de la información o activos de información.
b) El/la propietario/a del activo de información, en coordinación con el Oficinal de Seguridad de la Información, debe identificar y registrar el activo en el Inventario de Activos de Información, según lo detallado en el documento Metodología de Gestión de Riesgos de Seguridad de la Información.
c) La Sunedu es el propietario de los activos de información de la organización, y delega su custodia a los/as directores/as y jefes/as de los órganos y unidades

orgánicas con la finalidad de descentralizar y mejorar la eficiencia en la administración de la seguridad de información.

d) Los/as directores/as y jefes/as de los órganos y unidades orgánicas también deberán delegar la custodia de los activos de información de manera jerárquica a los/las usuarios/as finales, pero ellos siguen manteniendo la responsabilidad ya asignada sobre los activos.
e) Todo el personal que utilice, traslade o almacene toda información o activo de información como parte del desempeño de sus funciones y/o actividades y que estas guarden relación con la función de la Sunedu, debe considerarla propiedad de la entidad.

8.3.3 Uso de activos de información

Obligaciones:

a) Todo el personal debe usar los activos de información para los fines y objetivos de la Sunedu, bajo el criterio de buen uso y de acuerdo con las normas, políticas y procedimientos que se definan en la Entidad.
b) Todos los órganos y unidades orgánicas deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo la presente Directiva.
c) La OA a través de la UAB debe de consignar cláusulas o disposiciones referidas a la confidencialidad de la información en las relaciones que la Sunedu establezca con los proveedores o con entidades externas, mediante órdenes de servicio, convenios y/o contratos.
d) Todo el personal solo podrá desempeñar sus funciones y actividades laborales utilizando los equipos informáticos administrados por la Sunedu, ya sean estos asignados por la entidad o equipos en posesión del personal que no son asignados por la Sunedu, previamente autorizados.

8.3.4 Retorno de activos de información

Obligaciones:

a) La OA, a través de la UAB, debe supervisar el retorno de los equipos informáticos de la Entidad, asignados a los/las servidores/as que se desvinculan laboralmente de la Sunedu.
b) La OA, a través de la UAB, debe notificar a la OTI respecto a cada equipo de cómputo retornado para las acciones de preparación previa a una nueva asignación.
c) La OTI debe verificar el estado de los activos tecnológicos en la devolución, así como procederá a la eliminación de la información contenida en los mismos.

8.3.5 Clasificación de la información

Obligaciones:

a) Todo el personal debe considerar que toda información que posea la Sunedu es de acceso público, salvo las excepciones previstas en las normas de la materia. El acceso a información pública está sujeta a los procedimientos establecidos en las normas de la materia.
b) Los/las propietarios/as de activos de información, en coordinación con el Oficial de Seguridad y Confianza Digital, deben de clasificar y etiquetar la información que generan en cada proceso y/o proyecto, en caso se trate de información confidencial, de acuerdo a los criterios establecidos en las normas de la materia. El Oficial de Seguridad y Confianza Digital debe proceder a registrarlo en los inventarios correspondientes.
c) Todo el personal debe velar por la conservación y custodia de toda información.
d) Todo el personal que tenga acceso a información confidencial debe ser consciente de la sensibilidad de la información que maneja y comprender a detalle las responsabilidades relacionadas con la protección de la información.
e) Todo el personal de la entidad debe conocer la clasificación de la información.

8.3.6 Manejo de activos

Obligaciones

a) Todo activo de información de la Sunedu deberá tener un “propietario” quien será el encargado de establecer los niveles de protección que le aplique.
b) Toda información documentada deberá ser de uso exclusivo dentro de la Sunedu.
c) El/la propietario/a de la información o el activo de información debe:
   - Proporcionar al Oficial de Seguridad y Confianza Digital los riesgos de seguridad digital a los cuales se encuentra expuesta la información o activo de información.
   - Asegurar que el plan de tratamiento de riesgos de seguridad digital acordado sea debidamente implementado sobre los activos de información que le pertenezcan.

8.3.7 Manejo de los medios extraíbles (Usb, discos externos)

Obligaciones

a) La OTI debe asegurar que toda la información almacenada en medios extraíbles de la Sunedu esté debidamente controlada en cuanto a su uso, transporte y almacenamiento.
b) Todo/a usuario/a debe utilizar los medios extraíbles de forma segura y protegida (información confidencial).

c) Todo/a usuario/a debe utilizar los dispositivos de medios extraíbles solo con fines laborales.
d) Todo/a usuario/a debe limitar la copia de archivos mediante medios extraíbles, a menos que sea necesario o haya sido autorizado. Se recomienda tener un sistema DLP (prevención de pérdida de datos).
e) Todo/a usuario/a debe escanear los medios extraíbles en busca de malware antes de transferir información.
f) Todo/a usuario/a debe aplicar protección con contraseña al medio extraíble de almacenamiento.
g) Todo/a usuario/a debe cifrar información confidencial en caso esté contenida en un dispositivo de almacenamiento extraíble.
h) Todo/a usuario/a que traslade información desde la Sunedu a un sitio externo debe transportarla en forma segura. La OTI debe trasportar la información en forma segura para el almacenamiento de las copias de respaldo en sitios externos a la institución.

8.4 Seguridad relativa al control de accesos

8.4.1. Gestión de acceso a recursos de información y estaciones de trabajo

Obligaciones:

a) La OTI debe establecer los procedimientos formales para asignar los derechos de acceso a los recursos de información relacionados con los servicios de TI y sistemas de información.
b) La OTI debe implementar los controles necesarios para garantizar la autenticación y el acceso a los recursos de información relacionados con los servicios de TI y sistemas de información.
c) La OTI debe gestionar el acceso a las estaciones de trabajo a fin de evitar accesos no autorizados a recursos o activos de información.
d) El/la propietario/a del activo de información debe autorizar el acceso a la información o activo de información, así como definir los niveles de acceso adecuados a quien corresponda.
e) El/la directora/a o jefe/a del órgano o unidad orgánica debe solicitar a la OTI la alta y baja de accesos a los servicios de TI, sistemas de información para el personal a su cargo, indicando los niveles de acceso o privilegios. En el caso que, por la necesidad de los servicios contratados, se requiera que los proveedores accedan a los sistemas de información de la entidad, el/la directora/a o jefe/a del órgano o unidad orgánica del área usuaria debe solicitar a la OTI la alta y baja de accesos a dichos servicios.
f) La OTI debe establecer las pautas para la asignación y cambio de contraseñas.
g) La OTI debe generar, a la comunicación del inicio de vínculo laboral de los/las servidores/as por parte de la ORH o los órganos y unidades orgánicas, las credenciales de acceso que identifique única y exclusivamente al personal para el uso de los siguientes servicios de TI y sistemas de información:

- Acceso al Dominio y VPN
- Acceso a al Sistema de gestión documental
- Acceso al Correo electrónico institucional y herramientas colaborativas

h) La OTI debe garantizar la aplicación de buenas prácticas de seguridad en cuanto a la elección y uso de contraseñas considerando que todo personal:
   - Debe utilizar contraseñas con una secuencia de caracteres con al menos ocho caracteres de longitud, considerando contener como mínimo, un carácter numérico, un carácter alfabético en mayúscula y uno en minúscula.
   - Debe cambiar su contraseña si existe un indicio de que haya sido vulnerado o estar en riesgo un activo de información (en ese caso, se debe reportar el incidente de seguridad digital).
   - Debe cambiar las contraseñas generadas por defecto en el primer ingreso a un sistema de información.
   - No debe considerar información relacionada directamente con el/la usuario/a (nombre, fecha de nacimiento, DNI, etc.)
   - No debe revelar las contraseñas a otras personas, incluyendo al personal de asistencia técnica de la OTI y a los administradores de los sistemas de información.
   - No debe transferir o distribuir su contraseña por ningún medio (oral, escrito, electrónico, etc.) por ser estrictamente personal y de su responsabilidad.
   - No debe llevar un registro de las contraseñas, a menos que se realice en un documento o archivo digital debidamente cifrado o encriptado mediante una contraseña que cumpla los niveles de complejidad descritos en el presente documento.
   - No debe almacenar contraseñas en un sistema de registro automatizado (por ej., macros o explorador), sin tener las configuraciones de seguridad necesarios.

i) Todo el personal que preste sus servicios a Sunedu debe contar con un nombre de usuario y una contraseña que corresponde a la identidad de la persona y sea único dentro de la red para el acceso a los sistemas de información autorizados, de acuerdo al perfil asignado.

8.4.2. Control de acceso a las redes de comunicaciones

Obligaciones:

a) La OTI debe gestionar el acceso a las redes de comunicaciones y recursos de red internos y externos de manera que el personal no comprometa la seguridad de los activos de información.
b) La OTI debe tomar acciones apropiadas y controles necesarios para monitorear el uso de los medios de procesamiento, redes y servicios de red, detectar posibles fallas y analizarlas para las soluciones respectivas.

c) La OTI debe gestionar los perfiles de acceso y directivas de acceso lógico considerando los servicios de red y conexiones a las redes a los que un/a usuario/a puede tener acceso.
d) La OTI debe considerar la verificación de los medios usados para el acceso a los servicios de red.
e) La OTI debe implementar mecanismos de identificación de un/a usuario/a que se conecta remotamente a la red de la entidad, así como la identificación del punto de conexión remota.
f) La OTI debe identificar a qué redes o segmentos de red se pueden conectar los equipos remotos.
g) La OTI debe implementar control de ruteo de redes para asegurar que las conexiones y los flujos de información entre computadores no violen las políticas de control de acceso de los sistemas de información.

8.4.3. Control de acceso en los sistemas de información

Obligaciones:

a) La OTI debe establecer e implementar las pautas de control de acceso a los sistemas de información que garanticen la restricción efectiva para uso exclusivo del personal debidamente autorizado.
b) La OTI debe informar a los/las usuarios/as sobre las responsabilidades a la que conlleva los accesos provistos y la obligatoriedad de la confidencialidad y cambio de contraseña de acuerdo a la disposición establecida.
c) La OTI y los órganos o unidades orgánicas responsables de los sistemas de información deben generar los perfiles de los/las usuarios/as según el derecho de acceso a la información y al nivel de clasificación de dicha información.
d) Todo personal que preste sus servicios a Sunedu deben aplicar todos los controles de seguridad para garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades o que por otras situaciones esté bajo su custodia.
e) Todo personal que brinde sus servicios a Sunedu debe tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas.
f) El órgano o unidad orgánica responsable de la información debe autorizar formalmente el acceso a la información a su cargo. Para la autorización de acceso a la información debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con dicho acceso.
g) La OTI debe implementar controles de acceso a la información que estén sujetos a garantizar la trazabilidad de las acciones realizadas sobre la misma, considerando la identificación de el/la usuario/a que realicen el acceso, acciones realizadas, instante de tiempo en que se realizan las acciones y ubicación desde la cual se realiza el acceso a la misma.

8.4.4. Gestión de derecho de acceso remoto

Obligaciones:

a) La OTI debe establecer e implementar los mecanismos para permitir el acceso remoto mediante el uso de tecnología de acceso seguro como la VPN y mecanismos de autenticación con credenciales de accesos únicos.
b) La OTI debe establecer los procedimientos para la asignación, uso y revocación del derecho de acceso remoto, el cual debe considerar la autorización del jefe inmediato y justificación de la necesidad.
c) La OTI debe gestionar y controlar otros mecanismos de acceso o conexión remota no autorizados o institucionales, incluyendo el uso de herramientas y software de escritorio o terminal remoto (Anydesk, TeamViewer, etc.).

8.4.5. Gestión de derechos de acceso privilegiado

Obligaciones:

a) La OTI debe establecer los procedimientos para la asignación, uso y revocación de los derechos de accesos privilegiados, el cual debe considerar la autorización del jefe inmediato y justificación de la necesidad.
b) La OTI debe gestionar el control de acceso privilegiado.
c) Los derechos de acceso privilegiado sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones.
d) La OTI debe asegurar que los accesos realizados con credenciales de acceso privilegiados deben ser registrados y controlados periódicamente.
e) La OTI debe asegurar que una credencial de acceso privilegiado sólo debe ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios.
f) La OTI debe definir los procedimientos necesarios para evitar el uso no autorizado de cuentas con derechos de acceso privilegiados.
g) La OTI debe asegurar que las actividades regulares de un/a usuario/a no deben ser realizadas desde cuentas privilegiadas.
h) Todo personal que utilice una credencial de acceso privilegiado no debe usarla en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.
i) La OTI debe asegurar que las credenciales de acceso privilegiadas tales como “administrador”, “root” o similares que son definidas por defecto en los sistemas y componentes, no deben ser utilizadas siempre que sea posible generar cuentas de acceso privilegiados.
j) La OTI debe asegurar el contar con un mecanismo de recuperación de acceso privilegiado
k) La OTI debe asegurar que el acceso privilegiado se realice desde dispositivos debidamente fortalecidos para tal fin.

8.5 Seguridad relativa a la criptografía

Obligaciones:

a) La OTI debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión interna o externa de información, cuente con mecanismos de cifrado de datos, si fuera necesario.
b) La OTI debe configurar el uso del protocolo https para todas las páginas internas y externas de la entidad.
c) La OTI debe configurar en las aplicaciones web con conexiones cifradas con un certificado firmado Secure Socket Layer (SSL) aprobado.
d) Todo/a usuario/a que realice el cifrado de información, deben mantener copia de las claves de cifrado en lugar seguro de tal forma que la recuperación de la información cifrada sea factible en caso de ausencia temporal o permanente del custodio de la información cifrada.

8.6 Seguridad relativa a las instalaciones y el entorno físico

La seguridad en las instalaciones y el entorno físico se alcanza mediante la adopción de medidas destinadas a prevenir, detectar, neutralizar y/o disminuir los riesgos que la amenazan, las mismas que se basan en el convencimiento de que no hay ningún peligro que temer al haberse adoptado las medidas necesarias para evitar todo riesgo.

8.6.1. Áreas físicas

Obligaciones:

a) Cada órgano o unidad orgánica, que sea responsable de un área física clasificado como restringida, debe implementar los controles necesarios para garantizar un acceso autorizado a dichos espacios físicos y las medidas de protección contra amenazas externas y ambientales considerando los siguientes, de corresponder:
   - Control de acceso
   - Video vigilancia y seguridad física
   - Control de humedad
   - Detectores de incendio o humo
   - Extintores o sistema de extinción de fuego
   - Sistema de puesta o pozo a tierra
   - Sensores de aniegos
   - Sistema de alimentación ininterrumpida (UPS)
   - Grupo electrógeno
   - Pararrayos
b) Cada órgano o unidad orgánica debe asegura que el acceso a un área física clasificada como restringida está permitido para personas externas a la Sunedu, siempre que sea para un motivo específico, que se cuente con la autorización respectiva del jefe/a inmediato responsable del área en cuestión y debe estar

siempre acompañado por un personal de la Sunedu.

c) Cada órgano o unidad orgánica debe asegurar que las áreas restringidas deben de contar con un circuito cerrado de video, sistema de video vigilancia o equivalente.
d) la OTI debe gestionar la protección del Centro de Datos, el suministro de energía eléctrica, un sistema automático de protección contra incendios, teniendo un control de fácil acceso, un sistema de monitoreo automático y/o manual de las condiciones ambientales de temperatura y humedad y cualquier otro sistema que sea considerada como crítica y que pudiera afectar el funcionamiento de los sistemas de información.
e) La OTI debe proteger el Centro de Datos de fallas por falta de suministro de energía y otras anomalías eléctricas.
f) La OTI debe monitorear las condiciones ambientales como temperatura y humedad, que puedan afectar negativamente la operatividad de los equipos en el Centro de Datos.
g) La OA debe asegurar que los accesos a la entidad cuenten con controles que aseguren el acceso físico sólo a usuarios/as debidamente autorizados. En caso de locadores y demás proveedores se deberá contar con autorización expresa de responsable del órgano o unidad orgánica que gestionará las actividades, así como las responsabilidades de estos.
h) La OTI debe asegurar que los sistemas críticos que manejen información de la Sunedu estén en un Centro de Datos aislado de los/las usuarios/as comunes y deberá tener controles de acceso físico y lógico seguros.

8.6.2. Equipos de cómputo

Obligaciones:

a) La OA, a través de la UAB, debe autorizar las solicitudes de traslados de bienes y/o activos a otra ubicación.
b) La OA, a través de la UAB y la OTI deben garantizar la protección de los equipos informáticos de fallas por falta de suministro de energía y otras anomalías eléctricas.
c) La OTI debe garantizar la protección del cableado de la red de datos y los equipos de comunicaciones de fallas por falta de energía o protección física.
d) La OTI debe mantener un plan de mantenimiento preventivo de la infraestructura tecnológica incluyendo los equipos de cómputo, escaneo, impresión y servidores del Centro de Datos a fin de garantizar la continuación de los servicios.
f) La OA, a través de la UAB y la OTI deben mantener un plan de mantenimiento preventivo de los equipos de acondicionamiento de temperatura, humedad, sistemas de energía ininterrumpida (UPS) y detección o extinción de fuego a fin de garantizar su operatividad.
g) La OTI y su personal de asistencia técnica son los únicos autorizados para realizar instalaciones y configuraciones de los equipos de cómputo, escaneo e

impresión.

8.6.3. Equipos de usuarios/as desatendidos

Obligaciones:

a) Los/las usuarios/as de red deben bloquear el acceso a su PC/laptop y/o servidores al dejar un equipo desatendido temporalmente, independientemente del tiempo que permanezca alejado.
b) Los/las usuarios/as de red deben apagar el equipo al terminar la jornada de trabajo, siempre y cuando no se encuentren ejecutándose procesos programados fuera de horario de oficina o actividades adicionales y respondan a labores propias del cargo del colaborador o se requiera acceso remoto al equipo por VPN. En caso de ausentarse de la oficina por un periodo prolongado de tiempo, se debe cancelar las sesiones de usuario dentro de las aplicaciones, además de bloquear la pantalla.
c) La OTI debe promover y orientar a los usuarios respecto al procedimiento de bloqueo de sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin que la sesión del usuario no quede activa para evitar el uso inadecuado por terceras personas.

8.6.4. Pantalla y escritorio limpio

Obligaciones:

a) Todo el personal, al momento de retirarse momentáneamente del sitio de trabajo o al finalizar la jornada, debe dejar los escritorios y áreas de trabajo libres de documentos que contengan información de uso interno de la entidad. Deben dejarlos bajo llave en archivadores, cajones, cajas fuertes u otros medios seguros.
b) La OTI debe orientar al personal respecto a mantener el escritorio del equipo de cómputo libre de información de uso interno propia de la institución, que pueda ser alcanzada, copiada o utilizada por personal que no tenga autorización para su uso o conocimiento.
c) La OTI debe garantizar el bloqueo de la pantalla de un computador administrado por la Sunedu para forzar un nuevo inicio de sesión, si la persona se ausenta del computador.
d) La OTI debe garantizar el cierre de toda sesión activa de un usuario en los sistemas de información institucionales para obligar un nuevo inicio de sesión, indistintamente si se encuentra en un computador administrado por Sunedu o no, siempre que la persona no tiene actividad en el sistema de información por un período de 5 minutos.
e) Toda la información clasificada como confidencial, ya sean documentos impresos o soportes de almacenamiento digital, es considerada sensible y no deben estar expuestos en el escritorio del puesto de trabajo u otras zonas de

trabajo (incluyendo impresoras y fotocopiadoras) para evitar el acceso no autorizado a los mismos.

f) Los/las usuarios/as deben resguardar sus contraseñas y no ser expuestas a otras personas, dejándolas en notas adhesivas publicadas en sus estaciones de trabajo o escritas en un lugar accesible.
g) Los/las usuarios/as deben borrar información restringida y/o confidencial contenidas en pizarras.

8.6.5. Disposición o reutilización seguro de equipos

Obligaciones:

a) La OTI debe asegurar que todo equipo de cómputo que contenga medios de almacenamiento sea revisado para que todos los datos sensibles y software licenciado se hayan eliminado de forma segura antes de su eliminación o reutilización.
b) La OTI debe realizar y verificar la destrucción de la información de los equipos informáticos que vayan a ser reutilizados o eliminados, mediante mecanismos que aseguren que esta información no pueda ser recuperada por procesos técnicos

8.7 Seguridad relativa a las operaciones

La Sunedu debe contar con mecanismos para asegurar que sus operaciones e instalaciones de procesamiento de la información sean correctas y seguras, mitigando los riesgos de seguridad digital como las intrusiones no autorizadas y ejecución de código malicioso dentro de la infraestructura tecnológica de la entidad.

8.7.1. Procedimientos operativos documentados

Obligaciones:

a. La OTI debe mantener actualizados los procedimientos relacionados con la operación y administración de seguridad de la infraestructura tecnológica que soporta los sistemas de información, estableciendo responsabilidades y los recursos utilizados para su ejecución eficiente, asimismo, estos deben estar a disposición del personal autorizado.
b. La OTI debe mantener actualizada la documentación relacionada con los manuales de configuración, operación y uso de los sistemas de información de la Entidad.

8.7.2. Gestión de cambios

Obligaciones:

a) La OTI debe mantener un registro de control de cambios de los sistemas de

información, equipos de comunicaciones, bases de datos, equipos de cómputo y perfiles de acceso a través de la implementación de acciones y procedimientos necesarios para asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.

b) La OTI debe recibir todas las solicitudes de cambios por el propietario de la información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado se revertirá al estado anterior al cambio.
c) La OTI debe asegurar de no poner en peligro la integridad de la información debido a la falta de revisión de los cambios.

8.7.3. Gestión de la capacidad

Obligaciones:

a) La OTI debe garantizar la capacidad de los recursos a fin de asegurar el óptimo desempeño y la continuidad de los sistemas de información y la infraestructura tecnológica que la soporta.
b) La OTI debe realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la infraestructura tecnológica.
c) La OTI debe realizar un monitoreo continuo del uso de sus capacidades para advertir eventos e incidencias relacionadas.

8.7.4. Separación de entornos de desarrollo de software

Obligaciones:

a) La OTI debe separar los entornos de desarrollo, calidad y producción a fin de garantizar el mejor desempeño requerido por los sistemas de información durante todo su ciclo de vida.
b) La OTI debe contar con entornos separados de desarrollo, pruebas y producción, para que no se realicen pruebas, instalaciones o desarrollos sobre el entorno de producción. Debe efectuar el desarrollo y mantenimiento de los sistemas de información utilizando sistemas de autenticación y autorización independientes para los diferentes ambientes, con el fin de evitar errores de integridad de la información utilizada en la entidad.
c) La OTI debe asegurar que el ambiente de desarrollo y pruebas simule la configuración del ambiente de producción lo más posible, pero no debe contener los mismos datos, salvo autorización de los propietarios.

8.7.5. Protección contra software y código malicioso:

La Sunedu proporciona los mecanismos necesarios para garantizar la protección de la información y el equipamiento informático donde se procesa y almacena la información contra el hurto, modificación o daño ocasionados por el contagio de software malicioso.

Obligaciones:

a) La OTI debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo, el cual debe estar actualizado. Asimismo, el sistema operativo y los aplicativos de oficina deben contar con las últimas actualizaciones de seguridad (parches).
b) La OTI debe revisar los equipos portátiles (laptops) que no sean asignados por la Sunedu y que por motivos de prestación de servicios sean autorizados a ingresar en la red interna de la Sunedu, para verificar que tengan instalado software antivirus actualizado, sistema operativo actualizado y que no exista algún software instalado que implique un potencial riesgo a la seguridad de la red interna.
c) La OTI, debe ejecutar el proceso de desinfección como medida de prevención, al detectar que algún servidor de red, estación de trabajo o computadora portátil esté infectada con algún tipo de malware. En caso no se pueda desinfectar el equipo, se procederá a aislarlo de la red inmediatamente.

8.7.6. Respaldo de información

Obligaciones:

a) La OTI debe realizar el respaldo de la información de la entidad, priorizando la información crítica.
b) La OTI debe elaborar y aplicar los procedimientos de copia y restauración de la información de la entidad.
c) La OTI debe comprobar que las copias estén bien realizadas y que pueden restaurarse, esto se debe evidenciar con pruebas de restauración de copias de respaldo que deberán estar documentadas
d) La OTI debe clasificar y etiquetar las copias de respaldo que le permita la fácil identificación de los medios de almacenamiento, la información contenida y la ubicación física para su posterior ubicación y acceso a los medios que contienen la información resguardada del centro de datos.
e) La OTI debe evaluar periódicamente la vigencia tecnológica de la infraestructura de hardware y software utilizados para el respaldo y recuperación de la información.

8.7.7. Registro y Monitoreo

Obligaciones:

a) La OTI debe generar los registros de eventos de los sistemas de información tal como la activación de registros de auditoría, registros de uso de recursos y de conexiones.
b) La OTI debe realizar un monitoreo de los registros para seguimiento e investigación de incidencias presentadas.
c) La OTI debe gestionar los accesos a los repositorios de registros.
d) La OTI debe monitorear todos los servicios de TI y sistemas de información.

8.7.8. Sincronización de reloj

Obligaciones:

La OTI debe asegurar que todos los sistemas de información dentro de la organización deben sincronizar sus relojes implementando Network Protocolo de tiempo (NTP) o una capacidad similar. Todos los sistemas de información deben sincronizarse con el mismo sistema primario fuente de tiempo.

8.7.9. Gestión de vulnerabilidades técnicas

Obligaciones:

a) El Oficial de Seguridad y Confianza Digital debe gestionar la ejecución de un hackeo ético y Análisis de Vulnerabilidades en los sistemas de información y en la infraestructura de Tecnologías de Información de la entidad.
b) La OTI debe implementar las recomendaciones resultantes posteriormente a la identificación de vulnerabilidades de seguridad y debe de determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas de información críticos y en alto riesgos deben ser priorizados.
c) La OTI debe probar los parches de seguridad y evaluarlos antes de que sean instalados a fin de asegurar que sean efectivos y no causen efectos secundarios contraproducentes.

8.7.10. Control de software operacional

Obligaciones:

a) La OTI debe instalar únicamente el software libre autorizado o el que cuente con licencia autorizada para todos los equipos de cómputo de propiedad de la Sunedu o asignados por la entidad. El software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley sobre el Derecho de Autor.

b) La OTI, en caso deba habilitar a un usuario/a la conexión de un equipo de cómputo que no es asignado por la Sunedu, debe revisar que no tenga instalado software que pudiera afectar la seguridad de la red e información de la entidad, y como mínimo que tenga actualizado los parches de seguridad del sistema operativo e instalado un antivirus actualizado; de lo contrario no procederá con dicha conexión a la red.
c) La OTI debe restringir y limitar el otorgamiento de privilegios para la instalación de software en los equipos de cómputo del Sunedu.

8.8 Seguridad relativa a las comunicaciones

La Sunedu debe contar con mecanismos para asegurar las redes de comunicaciones y la infraestructura que la soporta, mitigando los riesgos de seguridad digital como las intrusiones no autorizadas e interceptaciones de información tanto dentro como fuera de la Entidad

8.8.1. Acceso al dominio Sunedu

Obligaciones:

a. La OTI debe establecer los procedimientos para la asignación, uso y revocación de las cuentas de dominio.
b. La OTI debe asegurar que los equipos de cómputo cuenten con adherencia al dominio Sunedu a fin de garantizar el uso de cuentas de dominio como mecanismo de autenticación y control de acceso.
c. La OTI debe asignar una cuenta de dominio individual al personal de la Sunedu, la cual debe permitir el inicio de sesión en un equipo de cómputo.
d. La OTI debe gestionar la asignación de cuentas de dominio para terceros cuando, por la naturaleza del servicio, se requiera el acceso de personal externo a los equipos informáticos y servicios de TI de la Sunedu. Una cuenta de dominio para terceros debe ser autorizado por los/las directores/a o jefes/as de los órganos y unidad orgánicas quienes se responsabilizan de la custodia y uso del mismo.
e. El uso del dominio y las redes de comunicación interna debe estar restringido para realizarse mediante el uso de equipos de cómputo bajo la gestión de la Sunedu. El uso de equipos de cómputo y dispositivos móviles personales será posible únicamente previa autorización.

8.8.2. Acceso a internet

Obligaciones:

a. La OTI debe garantizar la protección del servicio de internet contra ataques de intrusiones o denegación de servicio, así como el acceso a páginas no autorizadas.
b. La OTI debe promover la concientización a los/las usuarios/as respecto a las

consideraciones de seguridad que deben adoptar para el adecuado uso del internet.

c. La OTI debe realizar el monitoreo de los servicios prestados por los proveedores o por convenios con entidades externas a fin de asegurarse la adecuada provisión y operatividad de los servicios acordados.
d. La OTI debe supervisar las medidas de seguridad implementadas por parte de los proveedores de servicio y entidades externas.
e. La OTI debe asegura que el acceso a Internet sea un servicio de TI disponible para todo el personal del Sunedu para uso estricto de actividades laborales relacionadas con las funciones que desempeñan y no para uso con propósitos de índole personal o comercial.
f. La OTI debe habilitar accesos a internet con navegación especial previa autorización de los/las directores/a o jefes/as de los órganos y unidad orgánicas en caso de que se requiera el acceso a portales de redes sociales, video a demanda o a ambos, u otros portales. Los accesos habilitados estarán sujetos a controles y auditorias con la finalidad de garantizar el buen uso del servicio.

8.8.3. Seguridad de servicios de red

Obligaciones:

a) La OTI debe asegurar que todos los sistemas y servicios de red estén actualizados con los parches y recomendaciones de los fabricantes para asegurar los niveles óptimos de control y seguridad.
b) Cada director/a o jefe/a del órgano o unidad orgánica debe determinar el acceso del personal a su cargo a los servicios de red, según amerite las funciones y actividades de cada colaborador.
c) La OTI debe implementar controles y medidas especiales para salvaguardar la confidencialidad, integridad y disponibilidad de los datos que pasen a través de redes públicas, así como para proteger los aplicativos y servicios web conectados utilizando hardware tales como firewall, UTM (gestiones unificadas de amenazas), IPS/IDS, filtro de contenidos, WAF, Anti DoS/ DDoS, Antispam, entre otros.
d) La OTI debe asegurar que los cambios en los servicios de proveedores deben ser planificados y autorizados considerando los riesgos que podrían generar.
e) La OTI debe asegurar que los servicios webs a ser integrados con los sistemas de entidades externas estén implementados por canales seguros como es un VPN, acceso HTTPS, SSH, encriptación de datos, con autenticación, entre otros y configurar el acceso solo desde la entidad externa.

8.8.3. Correos electrónicos

Obligaciones:

a) Todo/a usuario/a que usa el correo electrónico debe cumplir con la normatividad interna del correo institucional.

b) Todo/a usuario/a debe usar el correo institucional para fines laborales en la entidad
c) Todo/a usuario/a debe proteger los datos contenidos en un mensaje de correo electrónico o un archivo adjunto, de acuerdo a las normas de la materia.
d) La OTI debe garantizar la protección de las cuentas de correo electrónicos de accesos no autorizados, denegación de servicios o suplantación de identidad.

8.8.4. Segmentación de las redes

Obligaciones:

a) La OTI debe mantener una red de datos segmentada por redes virtuales, grupos de servicios, grupos de usuarios/as, ubicación física o cualquier otra tipificación que se considere conveniente en la Sunedu, debiendo estar documentada en la arquitectura correspondiente.
b) La OTI debe de segmentar la red de datos, sea esta cableada o inalámbrica, para aislar los accesos de visitantes de la red de datos del personal administrativo, de los servicios de TI y de los sistemas de información.
c) La OTI debe implementar controles para minimizar los riesgos contra accesos no autorizados a la infraestructura de redes de comunicaciones interna y para salvaguardar la información de las estaciones de trabajo y los sistemas de información.

8.8.5. Transferencia de información

Obligaciones:

La OTI debe establecer los controles a las transferencias e intercambios de información externas por medios físicos (medios removibles) y electrónicos (correos electrónicos, archivos compartidos o FTP) de tal manera que solo sea emitida y recibida íntegramente por las personas apropiadas y autorizadas en el momento y lugar oportuno.

8.8.6. Acuerdos de confidencialidad o de no divulgación

Obligaciones:

a) Los Órganos y unidades orgánicas que transmitan información en formato impreso o digital con entidades externas, deben hacerlo bajo acuerdos de confidencialidad mutua y transferencia segura de información entre la Sunedu y dichas instituciones, donde quedarán especificadas las responsabilidades para cada una de las partes.
b) La OTI debe implementar controles necesarios para el intercambio de información, para proteger la información transmitida de intercepción, copiado, modificación, cambio de ruta y destrucción y debe promover el uso de mecanismos seguros en tecnologías de la información y redes de

telecomunicaciones.

8.9 Seguridad relativa a la adquisición, desarrollo y mantenimiento de sistemas

La Sunedu debe asegurar que los sistemas de información cumplan con los requisitos de seguridad para evitar pérdidas, modificación o mal uso de la información que se procese en ellas, así como proteger la confidencialidad, autenticidad e integridad de la información.

8.9.1. Procesos y documentación de los Sistemas de Información

Obligaciones:

a. La OTI debe establecer un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas de información.
b. La OTI debe mantener la documentación de los sistemas de información desarrollados con la finalidad de garantizar la ejecución de sus actividades y la realización de mantenimiento posterior.

8.9.2. Requisitos de seguridad de los Sistemas de Información

Obligaciones:

a) La OTI debe establecer en su metodología de desarrollo de software, los requerimientos de seguridad y buenas prácticas de desarrollo de software seguro.
b) La OTI debe proporcionar a todo desarrollador de software las consideraciones elementales de seguridad de la información, controles, estándares y metodologías.
c) La OTI debe realizar evaluaciones de riesgos y seleccionar los controles adecuados para proteger la información involucrada en las aplicaciones web que pasan a través de redes públicas.
d) La OTI debe asegurar que las aplicaciones web en redes públicas deben seguir los lineamientos especificados en los documentos vigentes de la Guía OWASP Top 10 y la guía de pruebas OWASP.
e) Todo sistema de información desarrollado por el personal del Sunedu es de propiedad de la Entidad.
f) La OTI debe verificar que los acuerdos con proveedores en materia de adquisición o desarrollo de sistemas, incluyan clausulas relativas a la cesión de derechos a favor de la Sunedu y confidencialidad de la información para el resguardo de la propiedad intelectual de la Sunedu.
g) La OTI debe asegurarse de que todo sistema de información, ya sea este adquirido o desarrollado, implemente los requisitos de seguridad establecidos y utilice los componentes de software debidamente licenciados.
h) La OTI debe asegurar que el desarrollo de software por proveedores debe

cumplir con las directivas relacionadas al desarrollo y mantenimiento de sistemas de información y todos los controles asociados.

i) La OTI debe asegurar que al recibir el sistema terminado se realicen todas las pruebas, bajo los mismos procedimientos establecidos para el desarrollo interno, a fin de certificar la calidad, seguridad y exactitud del trabajo realizado.
j) La OTI debe considerar, en el contrato con proveedores, acuerdos de licenciamiento, propiedad del código, derechos de propiedad intelectual y servicio de soporte y mantenimiento.

8.9.3. Procesamiento correcto de los Sistemas de Información

Obligaciones:

a) La OTI debe asegurarse de validar los datos de entrada, el procesamiento interno y los datos de salida mediante controles de seguridad.
b) La OTI debe identificar los requerimientos para garantizar la autenticidad y la integridad de los datos en los sistemas de información.
c) La OTI debe establecer tiempo de duración de las sesiones activas en los sistemas de información, terminándolas cuando se cumpla el tiempo de inactividad.
d) La OTI debe implementar el uso de la encriptación y otros controles criptográficos que permitan proteger la confidencialidad, autenticidad e integridad de la información de acuerdo a su clasificación y nivel de exposición al riesgo.

8.9.4. Control de acceso al Código Fuente de los Sistemas de Información

Obligaciones:

a) La OTI debe implementar controles para restringir y controlar el acceso al código fuente de los sistemas de información.
b) La OTI debe gestionar el acceso a los repositorios de código fuente o de software desarrollado manteniendo un registro de uso.

8.9.5. Control de cambios de los Sistemas de Información

Obligaciones:

a) La OTI debe asegurar que todo sistema y aplicaciones utilizados para el procesamiento de la información de la Sunedu deberá ser instalado y actualizado a través de procedimientos formales de control de cambios los cuales deben asegurar que sólo los cambios autorizados sean implantados. Deberán existir procedimientos que obliguen a una aprobación formal por parte de los órganos y unidades orgánicas propietarias de la información (funcionalidad) y Seguridad de la Información (riesgos), para que los sistemas

sean implantados en los entornos de producción. Deberá mantener un registro de todas las implantaciones realizadas en el ambiente de producción.

b) La OTI debe establecer controles para asegurar que los cambios o actualizaciones de los sistemas informáticos no provoquen errores de procesamiento de información y evitar la pérdida de integridad de los datos.

8.9.6. Datos de prueba para los Sistemas de Información

Obligaciones:

a) La OTI debe seleccionar, proteger y controlar los datos de pruebas de manera cuidadosa previos al uso de los sistemas de información.
b) La OTI debe asegurar que los datos personales utilizados en los ambientes de desarrollo y de prueba sólo sean utilizados por el personal de desarrollo del aplicativo correspondiente, previa autorización del dueño (responsable) del banco de datos.
c) La OTI debe asegurar que los datos de producción no deben ser accedidos desde el ambiente de pruebas para la ejecución de las mismas.
d) La OTI debe asegurar que toda prueba de software que deba realizarse con datos de producción, no deberá contener detalles específicos de los mismos que puedan ser críticos o sensibles. Se deben definir los procedimientos para el uso de la información requerida
e) La OTI debe asegurar de tomarse muestras (porción de los datos) de acuerdo a las metodologías de extracción de datos para las pruebas correspondientes por el área de desarrollo de software, así como las señaladas en la NTP ISO/IEC 12207.

8.9.7. Seguridad en los procesos de desarrollo y pase a producción

Obligaciones:

a) La OTI debe establecer una política o procedimiento de desarrollo seguro para el software desarrollado por personal propio de la entidad o adquirido a proveedores.

8.9.8. Gestión de vulnerabilidades de seguridad

Obligaciones:

a) La OTI debe realizar semestralmente pruebas de comprobación técnica para verificar que se cuenta con los controles de seguridad debidamente implementados.
b) La OTI debe asegurarse de implementar las recomendaciones resultantes posteriormente a la identificación de vulnerabilidades de seguridad y debe de determinar los riesgos asociados e implementar los controles necesarios

para mitigarlos. Los sistemas de información críticos y en alto riesgos deben ser priorizados.

c) La OTI debe validar la efectividad de toda actualización propuesta en el entorno de control de calidad y debe cumplir con los controles establecidos para la gestión de cambios.

8.10 Sobre las relaciones con los proveedores

La Sunedu debe garantizar la protección de sus activos de información accesibles por los proveedores.

8.10.1. Seguridad con relación a los proveedores

Obligaciones:

a) La OA, a través de la UAB, debe asegurar que todo proveedor de bienes y servicios suscriba un acuerdo de confidencialidad y no divulgación entre la Sunedu y el proveedor, el mismo que deberá ser parte del contrato o los términos de referencia. Dicho acuerdo deberá especificar los responsables, la información que se requiera entregar al proveedor producto de la prestación del servicio, las medidas mínimas de seguridad aplicadas, la forma de proceder frente a incidentes, la extensión del acuerdo a terceros subcontratados, la propiedad de los productos desarrollados, el tiempo de vigencia del acuerdo, las sanciones frente a su incumplimiento y su aceptación formal.

b) La OA, a través de la UAB, y los órganos y unidades orgánicas, deben velar porque el proveedor y su personal cumpla con las consideraciones de seguridad de la información aplicables de la presente Directiva.

c) La Sunedu puede suministrar al proveedor información confidencial, relacionada con sus actividades, productos, servicios y/o su estrategia operativa únicamente si cuenta con una autorización expresa previa por parte del propietario de dicha información.

d) En el caso en que un proveedor requiera información de la institución, adicional a aquella establecida en los acuerdos contractuales, o que no sea inherente a la naturaleza del mismo, el propietario de la información analizará los motivos de dicho requerimiento y procederá a aprobar o rechazar de modo expreso la entrega de la misma con previo consentimiento expreso del Oficial de seguridad y Confianza Digital.

e) En todo intercambio de información entre la Sunedu y los proveedores, se deberá implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar razonablemente la seguridad en el acceso y la transferencia de datos, considerando la aplicación de cifrado en las comunicaciones y la validación de identidad.

f) La OA debe asegurar que los proveedores que presten sus servicios a la Sunedu, al finalizar sus contratos, efectúen la devolución de información o activos de información propiedad de la entidad que le fueron dados y

procurar la destrucción o borrado seguro de información conocida en razón de su actividad.

g) La OA y los órganos y unidades orgánicas debe velar que los proveedores que presten sus servicios a la Sunedu deben cumplir con la reglamentación en materia de derechos de autor y propiedad intelectual, incluido, pero no limitado al uso de información y software.
h) La OA y los órganos y unidades orgánicas deben velar que los proveedores que, por la necesidad de la prestación de sus servicios, reciban información de la Sunedu apliquen todas las medidas de seguridad razonables a su alcance, para evitar divulgación, fuga o uso no autorizado de información y protejan la información suministrada aplicando los controles que se especifiquen al momento de la entrega de la información.

8.11 Seguridad relativa a la gestión de incidentes de seguridad digital.

La Sunedu debe asegurar que los incidentes de seguridad digital sean comunicados oportunamente a las instancias correspondientes con finalidad de adoptar acciones preventivas y correctivas que correspondan.
Obligaciones:

a) El Equipo de Respuestas ante Incidentes de Seguridad Digital de la Sunedu debe adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
b) La OTI debe establecer un conjunto de procedimientos y responsabilidades para el manejo de eventos e incidentes de seguridad digital con el fin de asegurar una respuesta efectiva, restablecer la operación de los servicios y analizar las causas con fines de auditoría.
c) Todo personal debe notificar los incidentes de seguridad digital que afecten a la integridad o la disponibilidad mediante correo electrónico o llamada telefónica a Mesa de Ayuda de OTI.
d) El Equipo de Respuestas ante Incidentes de Seguridad Digital de la Sunedu debe asignar responsables para el tratamiento de los incidentes de seguridad digital, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
e) La OTI debe asegurar que los sistemas de información deben contar con registros de eventos de seguridad, y en lo posible generar alertas.

8.12 Seguridad relativa a la continuidad de servicios de TI

8.12.1. Continuidad de la seguridad de la información

Obligaciones:

a) La OTI y en coordinación con el Comité de Continuidad Operativa de la entidad,

deben asegurar la continuidad de las operaciones en caso surja una contingencia no prevista con el fin de reducir el impacto en el negocio. Para ello deberá existir un plan de contingencia de Tecnologías de Información (TI) debidamente documentado y administrado para el desarrollo, puesta en marcha los servicios y aplicaciones informáticos de la Sunedu.

b) La OTI debe realizar la continuidad de seguridad de la información según los lineamientos definidos en el Plan de Contingencias de TI.
c) La OTI debe verificar, revisar y evaluar el Plan de Contingencias de TI.

8.12.2. Redundancias

Obligaciones:

a) La OTI debe implementar con redundancia suficiente las instalaciones de procesamiento de información para cumplir con el requisito de disponibilidad.
b) La OTI debe probar los sistemas de información redundantes para garantizar que la conmutación funcione adecuadamente.
c) La OTI debe asegurar la disponibilidad de copias de respaldo de información de servidores y la efectividad de su restauración en casos de recuperación de información.

8.13 Sobre el cumplimiento

La Sunedu busca prevenir el incumplimiento de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información y así garantizar una gestión de la seguridad de la información en concordancia con la presente Directiva de Lineamientos de Seguridad de la Información de la Sunedu.

8.13.1. Cumplimiento de los requisitos legales y contractuales

Obligaciones:

a) la OTI debe identificar, documentar, mantener y cumplir todos los requisitos regulatorios y contractuales para los sistemas de información de la Sunedu
b) La OTI debe tener un control respecto de la cantidad y vigencia de las licencias de software base (sistemas operativos), base de datos y aplicaciones comerciales utilizadas por Sunedu.
c) La Sunedu tiene los derechos de propiedad intelectual sobre todos los sistemas, aplicativos, manuales, y documentos físicos como digitalizados, desarrollados tanto por su personal (de cualquier régimen laboral) como por proveedores de servicios y/o entidades externas que se encuentra en el dominio de la entidad.
d) El Oficial de Datos Personales es designado por la máxima autoridad administrativa de la entidad y actúa como enlace con la Autoridad Nacional de Protección de Datos Personales. Coopera y sigue los lineamientos y

directivas que emita dicha Autoridad en los ámbitos de su competencia, así como aquellos establecidos en las normas de la materia.

8.13.2. Revisión independiente de la seguridad de la información

Obligaciones:

a) La OTI debe realizar la supervisión del cumplimiento de procedimientos y políticas relacionadas con la Seguridad de la Información que se implemente o estén implementados.
b) La OTI debe planificar la pertinencia de auditorías periódicas internas y externas de seguridad de la información y con auditores independiente al proceso a auditar.

8.13.4. Cumplimiento de las políticas y normas de seguridad

Obligaciones:

a) El Oficial de Seguridad y Confianza Digital en conjunto con el CGTD deben asegurar que todas las políticas, procedimientos y estándares definidos en materia de seguridad de la información sean cumplidas por el personal de Sunedu.
b) Los/las directores/as o jefes/as o encargados de los órganos o unidades orgánicas deben asegurarse que se cumplan correctamente todas las directivas, políticas y procedimientos de seguridad de información, siendo los gestores en su dependencia e informar oportunamente al Oficial de Seguridad y Confianza Digital en caso de no cumplimiento.

9. DISPOSICIONES COMPLEMENTARIAS

Los controles técnicos de seguridad de la información que se requieren para cumplir con la política y requieran tecnología se implementarán conforme se adquiera en los planes anuales de la entidad.

10. ANEXOS

No aplica