TIPO DE DOCUMENTO: PLAN

NOMBRE DEL DOCUMENTO: PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

NOMBRE DE LA ORGANIZACIÓN: UNIDAD EJECUTORA “IMPLEMENTACIÓN DEL MODELO DE LA INFRAESTRUCTURA Y FUNCIONAMIENTO DE LA BICAMERALIDAD DEL PODER LEGISLATIVO”

San Luis, agosto 2025

Versión. 1.0

CONTROL DE VERSIONES

Código	Nombre
SGSI-PLAN-001	Plan de Implementación del Sistema de Gestión de Seguridad de la Información
Versión	1.0
Fecha	11.08.2025

DESCRIPCIÓN	CARGO	FIRMA
Elaborado por:	Unidad de Tecnologías de la Información	FIRMA DIGITAL Firmado digitalmente por: RENGIFO TAM William David FAU 20613768484 hard Motivo: Soy el autor del documento Fecha: 11/08/2025 18:16:46-0500
Revisado por:	Oficina de Administración	FIRMA DIGITAL Firmado digitalmente por: GONZALES CLEMENTE Jose Antonio FAU 20613768484 hard Motivo: Doy V° B° Fecha: 11/08/2025 18:30:57-0500
Aprobado por:	Dirección Ejecutiva	FIRMA DIGITAL Firmado digitalmente por: FERNANDEZ PANIAGUA Enrique FAU 20613768484 hard Motivo: En señal de conformidad Fecha: 11/08/2025 20:19:20-0500

Contenido

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. INTRODUCCIÓN

Mediante Decreto Legislativo Nº 1412 y sus modificatorias, que aprueba la Ley de Gobierno Digital, se establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

Según lo dispuesto en el artículo 30 del Decreto Legislativo N° 1412: *"la 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; se sustenta en la articulación con actores de los sectores público y privado y otros quienes apoyan en la implementación de controles, acciones y medidas".*

El artículo 96 del Reglamento del Decreto Legislativo N° 1412, aprobado con Decreto Supremo N° 029-2021-PCM, señala que: *"el Modelo de Seguridad Digital es la representación holística y sistémica de los componentes que comprende el Marco de Seguridad Digital del Estado Peruano"*, atendiendo a los principios establecidos en la normatividad de la materia y de Seguridad de la Información en el Estado Peruano, así como el Modelo de Seguridad Digital, que contiene al Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) como uno de sus componentes.

Las entidades de la administración pública deben implementar un SGSI teniendo como alcance mínimo sus procesos o actividades misionales, las cuales son relevantes para su operación.

El presente documento establece el marco y los lineamientos para la implementación y gestión efectiva del SGSI a nivel institucional de la Unidad Ejecutora "Implementación del Modelo de la Infraestructura y Funcionamiento de la Bicameralidad del Poder Legislativo" (en adelante, UEB), quien reconoce la información como un activo vital para la UEB.

En ese sentido, este Plan incorpora todos los aportes las unidades de la organización de la UEB y deberá ser aprobado por el Comité de Gobierno y Transformación Digital (CGTD). Su implementación en la Entidad requerirá el liderazgo y compromiso de la Dirección Ejecutiva de la UEB, con el objetivo de adoptar e incorporar la seguridad de la información como un componente fundamental de la cultura organizacional.

Con el fin de garantizar una implementación coherente y sólida del SGSI, este plan está elaborado conforme a la NTP-ISO/IEC 27001:2022 para ser aplicable a los activos de información relevantes de la organización, independientemente de su ubicación o formato.

2. OBJETIVOS DEL PLAN SGSI

2.1. OBJETIVO GENERAL

Implementar de manera efectiva el SGSI siguiendo las normas y mejores prácticas reconocidas internacionalmente, así como la Norma Técnica Peruana NTP ISO/IEC 27001:2022 vigente, para mejorar la gestión institucional de la UEB.

2.2. OBJETIVOS ESPECÍFICOS

a) Aplicar controles de seguridad que permitan preservar la confidencialidad, integridad y disponibilidad de al menos el 80 % de los activos de información críticos identificados en la UEB, durante el periodo de implementación del SGSI, priorizando aquellos con mayor exposición a amenazas.
b) Realizar una campaña de concientización en seguridad de la información para los servidores parlamentarios de la UEB, durante el periodo de implementación del SGSI, buscando alcanzar una participación efectiva del 60 % del personal convocado.
c) Lograr la implementación del 30% de los controles aplicados y definidos en la Declaración de Aplicabilidad de la Norma Técnica Peruana - NTP ISO/IEC 27001:2022, durante el periodo de implementación del SGSI, y verificar su conformidad mediante auditoría interna.
d) Identificar y evaluar los riesgos de seguridad de la información asociados a los principales activos de información en la primera fase del Plan, y aplicar medidas de tratamiento a por lo menos el 70 % de los riesgos clasificados como alto o muy alto.

3. FINALIDAD

El presente Plan tiene como finalidad establecer un marco estratégico y operativo que permita la implementación eficaz y progresiva del Sistema de Gestión de Seguridad de la Información (SGSI) en la UEB, garantizando la protección de los activos de información críticos para el cumplimiento de sus funciones.

Asimismo, este documento busca:

- ✓ Definir una estructura ordenada de fases, actividades, hitos y responsables, que oriente la implementación del SGSI conforme a la Norma Técnica Peruana NTP ISO/IEC 27001:2022.
- ✓ Proteger la confidencialidad, integridad y disponibilidad de los activos de información relevantes de la UEB frente a amenazas internas y externas.
- ✓ Asegurar el cumplimiento normativo en materia de seguridad de la información, transformación digital y confianza digital, conforme a lo establecido en el Decreto Supremo N.º 029-2021-PCM y demás disposiciones aplicables.
- ✓ Determinar roles, funciones y responsabilidades claras para el equipo multidisciplinario encargado de la implementación, seguimiento y mejora del SGSI.
- ✓ Establecer un enfoque de mejora continua que permita la revisión y ajuste permanente del SGSI frente a los cambios en el entorno, riesgos emergentes y evolución tecnológica.

4. MARCO LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27269, Ley de Firmas y Certificados Digitales y su reglamento y su modificatoria.
- Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
- Ley N° 29733, Ley de Protección de Datos Personales y modificatoria.
- Ley N° 30096, Ley de Delitos Informáticos y su modificatoria.
- Ley N° 31572, Ley del Teletrabajo y su modificatoria.
- Decreto Legislativo Nº 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses y su modificatoria.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital.

- Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 050-2018-PCM, que establece la definición de Seguridad Digital de ámbito nacional.
- Decreto Supremo N° 021-2019-JUS, que aprueba la Ley de Transparencia y Acceso de la Información Pública y su Reglamento.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412 -Ley de Gobierno Digital.
- Decreto Supremo Nº 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional de Transformación Digital.
- Decreto Supremo N° 002-2023-TR, Reglamento de la Ley N° 31572 – Ley del Teletrabajo.
- Decreto Supremo N° 016–2024-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y modificatoria.
- Resolución Ministerial Nº 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016- Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la administración Pública.
- Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución Ministerial N° 320-2021-PCM, que aprueba los lineamientos para la gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de gobierno.
- Resolución Secretarial N° 001-2018-PCM/SEGDI, que aprueba los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano.
- Resolución Directoral N° 022-2022-INACAL/DN que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.
- Directiva N° 001-2022-PCM/SGTD Directiva que establece el Perfil y Responsabilidades del Oficial de Gobierno de Datos.
- Directiva Nº 001-2023-PCM/SGTD Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD que aprueban la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
- Política General de Seguridad de la Información, SGSI-POLI-01 del Congreso de la República, aprobada con Resolución N° 080-2022-2023-OM-CR.
- Resolución de Contraloría General N° 320-2006-CG – Normas de Control Interno.
- Resolución Directoral N° 012-2025-DE-UEB/CR, que conforma el Comité de Gobierno y Transformación Digital de la UEB; y designa al Líder de Gobierno y Transformación Digital, así como al Oficial de Seguridad y Confianza Digital.
- Resolución Directoral N° 015-2025-DE-UEB/CR, que aprueba la Política de Seguridad de la Información de la UEB.
- Resolución Directoral N° 018-2025-DE-UEB/CR, mediante el cual designa al Oficial de Datos Personales, así como al Oficial de Gobierno de Datos.
- Las normas mencionadas incluyen sus respectivas normas modificatorias, reglamentarias, complementarias y conexas, de ser el caso.

5. DEFINICIONES Y ACRÓNIMOS

5.1. DEFINICIONES

- **Activo de información:** Es cualquier elemento que tenga valor para una organización y requiera protección, como datos, sistemas, aplicaciones, infraestructura tecnológica, equipos, instalaciones, recursos humanos, entre otros.
- **Análisis de riesgo:** Es un proceso sistemático que busca identificar, evaluar y mitigar los riesgos a los que están expuestos los activos de información de una organización. Involucra la identificación de amenazas, la determinación de vulnerabilidades y el cálculo de la probabilidad e impacto asociados.
- **Amenazas:** Son eventos, circunstancias o acciones que tienen el potencial de causar daño, comprometer la seguridad de la información o interrumpir las operaciones de la UEB.
- **Auditoría:** Es el proceso sistemático de evaluación y verificación de la implementación y efectividad de los controles de seguridad de la información, así como el cumplimiento de requisitos y normativas.
- **Confidencialidad**: Es la propiedad o atributo de la información o de un sistema de información que garantiza que solo las personas autorizadas puedan acceder a la información y que se mantenga protegida contra divulgación no autorizada.
- **Conformidad:** Es el estado de cumplimiento de los requisitos, normas, políticas y estándares establecidos en relación con la seguridad de la información.
- **Control:** Son medidas, políticas, procedimientos o prácticas que se implementan para mitigar los riesgos y proteger la seguridad de la información.
- **Disponibilidad:** Es la propiedad o atributo de la información o de un sistema de información que garantiza que sea accesible, en el lugar y momento oportuno, cuando sea necesario para los usuarios autorizados.
- **Eficacia:** Es la medida en la que se alcanzan los objetivos establecidos en relación con la seguridad de la información. Se refiere a la capacidad de los controles y medidas implementadas para cumplir con sus propósitos y mitigar los riesgos identificados.
- **Efectividad:** Es la medida en la que los controles y las medidas implementados logran su objetivo de proteger los activos de información como el manejo de los recursos utilizados y disponibles
- **Gestión de riesgo:** Es el proceso sistemático que permite identificar, analizar, evaluar, responder, monitorear y controlar los riesgos de seguridad de la información que puedan afectar el logro de los objetivos de la UEB. Establece controles de forma preventiva contra las amenazas que se puedan encontrar y consigue reducirlas.
- **Impacto:** Es el resultado o consecuencia de que una amenaza se materialice. Puede referirse a la magnitud del daño, la pérdida de información, la interrupción de servicios, el costo financiero u otros efectos negativos.
- **Incidente de seguridad de la información:** Es cualquier evento o suceso que indica una posible violación de la seguridad de la información. Puede involucrar acceso no autorizado, divulgación, alteración, destrucción o pérdida de información.
- **Integridad:** Es la propiedad o atributo de la información o de un sistema de información que garantiza que los datos sean precisos, completos y no hayan sido modificados de manera no autorizada.
- **ISO/IEC 27001:** Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 y la última versión fue publicada en octubre de 2022**.** Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.
- **Oficial de seguridad y confianza digital (OSCD):** Es el rol responsable de coordinar la implementación, operación, mantenimiento y mejora continua del SGSI en la entidad pública, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital.

- **Propietario de información:** Es la persona o entidad que tiene la responsabilidad de asegurar la integridad, confidencialidad y disponibilidad de un activo de información específico, así como tomar decisiones sobre su uso y acceso.
- **Probabilidad**: Es la posibilidad, en este caso, que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Proceso:** Es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en productos o servicios que satisfacen la necesidad de su cliente, luego de la asignación de recursos.
- **Reducción de riesgo:** Es el proceso de mitigación para aplicar medidas o controles para disminuir la probabilidad o el impacto de un riesgo.
- **Responsable de riesgo:** Es la persona o entidad que tiene la responsabilidad de identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información en una organización.
- **Riesgo:** Es la probabilidad de que una amenaza se materialice y cause un impacto negativo en un activo de información. Se calcula considerando la probabilidad de ocurrencia de una amenaza y el impacto potencial asociado.
- **Seguridad de la información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **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.
- **Tratamiento de riesgo:** Es el proceso de seleccionar e implementar medidas para modificar el riesgo, ya sea reduciendo su probabilidad de ocurrencia, disminuyendo su impacto o transfiriendo el riesgo a otra parte.

5.2. ACRÓNIMOS

- **CGTD**: Comité de Gobierno y Transformación Digital
- **CNSD:** Centro Nacional de Seguridad Digital
- **GR:** Gestor de Riesgos
- **NTP**: Norma Técnica Peruana
- **OA:** Oficina de Administración
- **OGP:** Oficina de Gestión de Proyectos
- **OI:** Oficina de Infraestructura
- **OSCD**: Oficial de Seguridad y Confianza Digital
- **PI**: Propietario de la Información
- **UAF**: Unidad de Asuntos Financieros
- **UL**: Unidad de Logística
- **URH:** Unidad de Recursos Humanos
- **UTI:** Unidad de Tecnologías de la Información

6. CONTEXTO DE LA ENTIDAD

6.1. DE LA ORGANIZACIÓN Y SU CONTEXTO

Se identifican los asuntos externos e internos pertinentes, en coherencia con el propósito y la dirección estratégica de la UEB, que pueden afectar en su capacidad para alcanzar los resultados esperados de acuerdo al alcance del SGSI. Para este análisis se emplearán herramientas como el PESTEL (externo) y el FODA (externo e interno).

6.1.1. ANÁLISIS DE CONTEXTO EXTERNO (PESTEL)

Se realiza el análisis PESTEL (Político, Económico, Social, Tecnológico, Ambiental y Legal) de la UEB, el cual se desarrolla en los siguientes puntos:

POLÍTICO (P)

- ✓ Dependencia del Congreso de la República: La UEB es una entidad creada por Ley N° 32172 y sujeta al presupuesto institucional del Pliego 028: Congreso de la República. Esta dependencia estructural puede impactar en las decisiones políticas y la asignación de recursos.
- ✓ Coyuntura Política: Al ser un organismo del Poder Legislativo, la UEB debe tomar en cuenta los cambios que se produzcan en el entorno relacionados con el ámbito político, que puedan impactar las decisiones sobre el SGSI y los procesos definidos en su alcance. Los cambios en las decisiones políticas de la mesa directiva del Congreso que afecten a la UEB podrían impactar en el liderazgo del SGSI.
- ✓ Temporalidad: La UEB ha sido constituida con un carácter temporal y específico, lo que condiciona la planificación a corto plazo. Cualquier cambio político o legislativo o de funcionarios, puede impactar directamente su continuidad, funciones y recursos.
- ✓ Riesgo de Hacktivismo por Asociación: Como la UEB depende del Congreso, existe una amenaza significativa de ser un blanco para hacktivistas ("Activista ideológico") que no aprueban las acciones del Congreso y, por ende, arrastran a la UEB como objetivo de ciberataques. Estos grupos buscan la desestabilización y destrucción, la explotación de vulnerabilidades en sitios de Internet y la desfiguración de plataformas digitales para difundir mensajes o dañar la imagen institucional.
- ✓ Mandatos Gubernamentales para SGSI: La UEB, como entidad pública, está obligada a implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), según el Decreto Supremo N° 029-2021-PCM y la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, con un alcance mínimo en sus procesos misionales y relevantes para su operación. La política de seguridad de la información de la UEB se elabora tomando como referencia la NTP ISO/IEC 27001:2022.
- ✓ Autonomía y Adaptación Normativa: La UEB cuenta con autonomía normativa, técnica, económica, financiera y administrativa, lo que le permite flexibilidad y la capacidad de aplicar disposiciones (a nivel de seguridad de la información y administrativa) aprobadas por otras instancias del Congreso para optimizar sus funciones.

ECONÓMICO (E)

- ✓ Coyuntura Económica: Las fluctuaciones en la economía y en la industria peruana, como consecuencia del crecimiento o de la criticidad de los sectores económicos, la Bolsa de Valores, las entidades bancarias, la negociación o la entrada en vigor de tratados internacionales, entre otros. Eventualmente, estos cambios económicos podrían tener un impacto en el SGSI.
- ✓ Recorte y ajuste de recursos presupuestales: La implementación de controles requiere el uso de recursos, entre ellos, presupuestales. En ese sentido, un posible recorte en el presupuesto institucional debido a las prioridades establecidas por la UEB, podría generar limitaciones en la capacidad de la UEB para cumplir con la adecuada implementación del SGSI.
- ✓ Situación de Personal Técnico: El equipo de la Unidad de Tecnologías de la Información de la UEB cuenta con tres personas, las mismas que se encargarán de la implementación de controles en adición a las actividades de soporte y gestión de servicios, lo que podría generar recarga de trabajo e impactar en la demora de la implementación de los controles.
- ✓ Continuidad de Recursos Financieros: La UEB debe destinar los recursos económicos para la implementación de los controles de seguridad conforme a las prioridades establecidas, las cuales deben mantenerse ante cualquier

cambio de los funcionarios; así también cada unidad de organización debe destinar recursos humanos para dicha implementación.
- ✓ Impacto de Incidentes en Costo y Cronograma: La materialización de riesgos puede generar impactos económicos y de tiempo significativos, ya que muchos riesgos identificados tienen un impacto en costo aún no definido, pero con severidad Alta o Muy Alta.

SOCIAL (S):

- ✓ Cultura de Seguridad y Concientización: Es fundamental fortalecer la cultura en seguridad de la información de los funcionarios, servidores y colaboradores de la UEB mediante capacitaciones y difusión de comunicados.
- ✓ Impacto en la Imagen Institucional: Los ataques, especialmente de hacktivistas, pueden resultar en desfiguración y una grave afectación de la imagen institucional de la UEB. La Política de Seguridad de la Información busca mejorar la confianza de las partes interesadas sobre la adecuada gestión de sus riesgos.
- ✓ Gestión del Comportamiento del Usuario: Se requiere concientización sobre el uso responsable de la información, el cuidado de credenciales, el manejo de documentos físicos y el uso seguro de internet para mitigar riesgos derivados de errores humanos o negligencia.

TECNOLÓGICO (T)

- ✓ El SGSI de la Entidad: La UEB es una unidad ejecutora nueva, lo que implica que está desarrollando su primer plan SGSI, el cual se encuentra en fase de implementación, con controles esenciales aún "En implementación".
- ✓ Cambios Tecnológicos: El SGSI se verá afectado por los cambios tecnológicos que puedan producirse en el futuro. Por tanto, es necesario realizar un seguimiento de dichos cambios y evaluar su impacto en el SGSI.
- ✓ Dependencia de Servicios en la Nube y On-Premise: Utiliza una combinación de servicios en la nube (SharePoint Online, OneDrive, M365) y recursos locales (proveídos por el Congreso de la República). Esto requiere asegurar la protección de datos en ambos entornos.
- ✓ Infraestructura del Congreso: Algunos sistemas críticos de la UEB dependen de la infraestructura tecnológica del Congreso (SIGA, SIAF, Sistema de Trámite Documentario), lo que puede generar riesgos de disponibilidad si la infraestructura del Congreso se ve afectada.
- ✓ Activos Críticos y Privilegiados: Los activos como SharePoint Online (Sites), información en SISPER (Remuneraciones), Información de Proyectos en SyPro, Cartas Fianzas y las Cuentas privilegiadas de Administradores TI son de criticidad "Muy alto" o "Alto" y son particularmente sensibles a ataques.

AMBIENTAL (E)

- ✓ Amenazas Físicas y Naturales: La infraestructura de la UEB está expuesta a amenazas físicas (incendio, agua, contaminación, explosión) y fenómenos naturales (climáticos, sísmicos, volcánicos, meteorológicos, inundaciones, pandemias/epidemias).
- ✓ Protección de Instalaciones y Activos Físicos: Se requiere la implementación de controles para asegurar oficinas, salas e instalaciones, incluyendo perímetros de seguridad física, gestión de medios de almacenamiento físicos, y protección de registros físicos contra pérdida o destrucción.

LEGAL (L)
- ✓ Marco Normativo Amplio: La UEB opera bajo un marco legal y regulatorio que incluye leyes de firmas y certificados digitales, delitos informáticos, protección de datos personales, gobierno digital, seguridad digital, y acceso a la información

pública. Del mismo modo, todo lo correspondiente a normatividad en materia de transformación digital, gobierno digital y seguridad de la información que es de obligatorio cumplimiento por parte de la UEB

- ✓ Obligación de Cumplimiento: La Política de Seguridad de la Información de la UEB aprobada por Resolución Directoral (previa exposición ante el CGTD), es de aplicación obligatoria para todo el personal y terceros, y su incumplimiento puede acarrear medidas disciplinarias según la normativa aplicable.
- ✓ Derechos de Propiedad Intelectual: Se deben implementar controles para evitar infracciones relacionadas con los derechos de propiedad intelectual, como licencias de software y el registro de software desarrollado por la UEB o terceros.
- ✓ Privacidad y Protección de Datos Personales: Existe un requisito legal específico para identificar y proteger los bancos de datos personales, obtener consentimiento informado e implementar medidas de seguridad conforme a las directivas de la Autoridad Nacional de Protección de Datos Personales.
- ✓ Gestión de Contratos con Proveedores: Los acuerdos con proveedores deben incluir cláusulas de seguridad de la información, confidencialidad, cumplimiento de políticas y, si aplica, auditorías y gestión de la cadena de suministro de TIC.
- ✓ Auditorías y Revisiones: La UEB debe realizar auditorías internas o externas al SGSI anualmente, lideradas por el Oficial de Seguridad y Confianza Digital, para verificar el cumplimiento de las políticas y normas de seguridad.

6.1.2. ANÁLISIS INTERNO Y EXTERNO (FODA)

Se realiza el análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas), el cual se desarrolla en los siguientes puntos:

FORTALEZAS (FACTORES INTERNOS POSITIVOS)

- ✓ Compromiso de la Dirección Ejecutiva: ha aprobado la Política de Seguridad de la Información, promoviendo activamente la implementación del SGSI. Dicho compromiso se extiende en la conformación oficial del Comité de Gobierno y Transformación Digital, la designación del Líder de Gobierno Digital, el Oficial de Seguridad y Confianza Digital, el Oficial de Datos Personales y el Oficial de Gobierno de Datos.
- ✓ Marco Normativo Sólido y Actualizado: La UEB cuenta con una Política de Seguridad de la Información basada en la NTP ISO/IEC 27001:2022 y un enfoque de Riesgos de la Seguridad de la Información de acuerdo a la NTP ISO/IEC 27005:2022, en concordancia con las normativas vigentes sobre seguridad digital y protección de datos personales. Además, la UEB cuenta con un Plan Maestro que establece un enfoque estratégico y técnico sólido para la intervención integral de cinco activos clave, este instrumento no solo orienta la planificación y ejecución de proyectos, sino que fortalece la alineación institucional y la priorización de recursos.
- ✓ Principios de Seguridad Definidos: La Política de Seguridad de la Información se sustenta en principios clave como la confidencialidad, integridad y disponibilidad de la información, además de no repudio, auditabilidad, legalidad, calidad, seguridad, concientización, responsabilidad y mejora continua.
- ✓ Enfoque Proactivo en la Gestión de Riesgos: La UEB reconoce la necesidad de contar con un SGSI para minimizar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información de toda la Entidad, incluyendo los que impacten en la Implementación del Plan Maestro, y ha realizado el análisis de riesgos de los activos de información basado en la NTP ISO/IEC 27005:2022 para identificar vulnerabilidades y criticidad de los activos de información relevantes.
- ✓ Declaración de Aplicabilidad definida: Se cuenta con el inventario de activos de información relevantes, los cuales han sido clasificados por formato, criticidad,

confidencialidad y propietario; sobre los cuales se han identificado los controles de la NTP ISO/IEC 27001:2022 que se aplicarán de manera justificada.
- ✓ Planificación de Monitoreo y Evaluación: Se ha establecido un monitoreo de los controles de seguridad y la medición del cumplimiento de los objetivos del SGSI mediante indicadores y metas claras.

OPORTUNIDADES (FACTORES EXTERNOS/INTERNOS POSITIVOS)

- ✓ Alineación con Requerimientos Legales y Regulatorios: La implementación del SGSI es una oportunidad para asegurar el cumplimiento de los requisitos legales y regulatorios en materia de seguridad y confianza digital, incluyendo leyes de protección de datos personales. El marco normativo nacional impulsa la implementación del SGSI en entidades públicas (DS N.º 029-2021-PCM) y la normativa vigente con respecto a Seguridad Digital, lo que permite que los esfuerzos de la UEB tengan un enfoque de cumplimiento.
- ✓ Continuidad en la Implementación de Controles: Una gran cantidad de controles de seguridad de la información (Anexo A de NTP-ISO/IEC 27001:2022) están actualmente "En Implementación", lo que representa una hoja de ruta clara para mejorar la postura de seguridad de la UEB.
- ✓ Fortalecimiento de la Cultura Organizacional: Existen objetivos y acciones específicas para fortalecer la cultura en seguridad de la información de todo el personal a través de capacitaciones (concientización) y comunicados internos.
- ✓ Mejora en la Gestión de Incidentes: La implementación del SGSI busca gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información, lo que permitirá una respuesta preventiva (controles), más rápida y efectiva ante posibles amenazas.
- ✓ Énfasis en la Mejora Continua: El principio y el objetivo de la mejora continua del SGSI aseguran que el sistema se adapte y evolucione frente a los cambios tecnológicos y las nuevas amenazas.

DEBILIDADES (Factores Internos Negativos)

- ✓ Falta de Experiencia Histórica y de Datos: Al ser el primer plan SGSI de la Entidad, la UEB no cuenta con datos históricos sobre incidentes de seguridad o la efectividad de controles, lo que dificulta la evaluación precisa de la probabilidad y las consecuencias de los riesgos.
- ✓ Alta dependencia de la infraestructura tecnológica del Congreso: Debido a que actualmente se alojan los principales sistemas de información utilizados por la UEB (Sistema de Trámite Documentario, SIGA, SIAF). Esta infraestructura se encuentra en obsolescencia tecnológica, lo que podría generar riesgos de disponibilidad y continuidad operativa, al no contar con autonomía plena sobre los entornos tecnológicos críticos.
- ✓ Demora en la implementación de controles: Existe la posibilidad de que algunos controles no se implementen en el tiempo adecuado debido a que el personal de UTI realizará estas actividades de forma compartida con tareas de soporte y gestión de los servicios.

AMENAZAS (Factores Externos Negativos)

- ✓ Ataques de Hacktivistas por el vínculo con el Congreso: dada la naturaleza de la UEB como una entidad que depende del Congreso de la República, existe una amenaza significativa de ser un blanco atractivo para ataques de hacktivistas a través de la destrucción de la imagen institucional (reputación) de la UEB, revelación de información confidencial, o hasta la "Obstaculización del funcionamiento" mediante operaciones de sabotaje o ataques de denegación de servicio distribuidos (DDoS).

- ✓ Exposición a Ciberataques por Retrasos en la Implementación: Los retrasos en la implementación de controles críticos están de acuerdo a la capacidad de recursos. Esta situación deja a la UEB en una posición vulnerable frente a posibles ataques informáticos, lo que podría comprometer la confidencialidad, integridad y disponibilidad de la información.
- ✓ Ciberataques y Acceso No Autorizado: Amenazas persistentes como "Ciberataque / Acceso no autorizado / Exposición a contenido malicioso" debido a "Credenciales débiles o phishing", que pueden resultar en Pérdida, Divulgación o Fuga de Información.
- ✓ Errores Humanos o Ataques de Ransomware: Estos son identificados como causas de pérdida de Integridad para diversos activos digitales como SharePoint Online, One Drive, Licencias de Software y sistemas como SISPER y Software de Asistencia.
- ✓ Interrupción de Servicios o Fallas Técnicas: La indisponibilidad de información y servicios debido a "Falla técnica o ciberataque" o "Afectación en la infraestructura tecnológica del Congreso", que puede generar retrasos en las actividades del personal.
- ✓ Riesgos Asociados a Proveedores de Servicios en la Nube: El posible "incumplimiento con controles de seguridad de la información del servicio en nube" por parte de proveedores representa una amenaza para la disponibilidad de activos críticos como "Información de Proyectos en SyPro", "Sharepoint Online" y "Sistema Procura Digital".
- ✓ Divulgación No Autorizada de Información Sensible: La exposición visual o el inadecuado resguardo de documentos físicos y credenciales compartidas constituyen amenazas directas de acceso no autorizado y fuga de información para activos confidenciales.

6.2. COMPRENSIÓN DE NECESIDADES Y EXPECTATIVAS

La UEB ha identificado las siguientes partes interesadas, junto con sus necesidades y expectativas, cuya atención es relevante para el SGSI, y serán abordadas adecuadamente.

Partes interesadas	Necesidades y Expectativas	Abordable mediante SGSI
Dirección Ejecutiva	a. Cumplimiento de la normatividad vigente. b. Protección de la confidencialidad, integridad y disponibilidad de los activos de información de la organización. c. Plataforma informática confiable y segura. d. Eficiente gestión de recursos informáticos.	a), b), c) y d)
Servidor parlamentario	a. Tratamiento seguro y protección de sus datos personales. b. Conocer la política y procedimientos de seguridad que debe cumplir en la entidad.	a) y b)
Organismos u Órganos Reguladores y de Control	a. Cumplimiento de la normativa aplicable en materia de seguridad de la información. b. Reportes de avances de cumplimiento de funciones y objetivos.	a)
Proveedores y Prestadores de Servicios	a. Relación comercial segura y confiable. b. Almacenamiento seguro de sus datos.	b)

Fuente: Elaboración Propia

7. INVENTARIO DE PROCESOS DE LA ENTIDAD

La UEB tiene como principales procesos los siguientes:

Código	Proceso Nivel 1
E01.01	Gestión del Planeamiento Institucional
E01.02	Gestión del Presupuesto Institucional
E01.03	Gestión de Modernización
E01.04	Asesoría Jurídica
S01.01	Organización del Trabajo
S01.02	Gestión del Empleo
S01.03	Gestión de las Compensaciones
S01.04	Gestión del Rendimiento
S01.05	Gestión de la Capacitación y Desarrollo
S01.06	Gestión de Relaciones Humanas y Sociales
S02.01	Programación
S02.02	Procedimientos de Selección
S02.03	Ejecución Contractual
S03.01	Devengado
S03.02	Giros
S03.03	Gestión Contable
S03.04	Conciliación
S03.05	Administración del Módulo de Instrumentos Financieros
S03.06	Administración de Cartas Fianzas
S04.01	Administración del Portal de Transparencia
S04.02	Administración de la operatividad informática
O01.01	Gestión de Proyectos
O01.02	Gestión de la Infraestructura Parlamentaria

8. ALCANCE DEL SGSI

Para determinar el Alcance del SGSI, se han utilizado documentos de gestión internos vigentes:

- Manual de Operaciones de la UEB.
- Plan Maestro

- Plan para la "Implementación del Modelo de la Infraestructura y Funcionamiento de la Bicameralidad del Poder Legislativo"
- Política de Seguridad de la Información.
- Inventario de Procesos.

El alcance del Plan está delimitado a los procesos mencionados, el cual se ejecuta en las unidades orgánicas de la UEB, considerados dentro del alcance del SGSI.

El Sistema de Gestión de Seguridad de la Información (SGSI) de la UEB abarca los principales procesos, servicios, activos de información, recursos tecnológicos y personas responsables del tratamiento, almacenamiento, administración, transmisión o acceso a información institucional, sin importar su forma, medio o soporte, y con independencia del modelo de provisión tecnológica (local o en la nube).

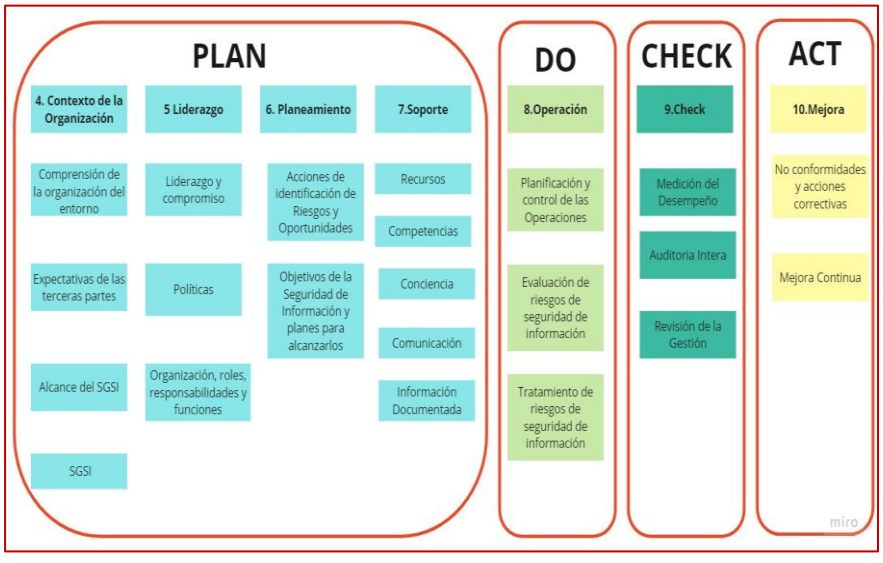
Este alcance incluye el tratamiento seguro de la información institucional, tales como datos personales, documentos normativos, archivos administrativos, recursos digitales compartidos y toda la infraestructura tecnológica utilizada por la UEB, ya sea de forma interna o mediante servicios contratados. La aplicación del SGSI es obligatoria para todo el personal de la UEB, independientemente de su modalidad de contratación, y constituye el marco rector para la implementación, operación, mantenimiento y mejora continua del SGSI.

9. METODOLOGÍA

Para realizar la implementación del SGSI en la UEB, en base a la NTP ISO/IEC 27001:2022 (Norma Técnica Peruana vigente), se plantea usar la Metodología de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar, por sus siglas en inglés: *Plan, Do, Check, Act*), también conocida como Ciclo de Deming, que impulsa la mejora continua del SGSI y se desarrolla en las siguientes etapas:

- Plan (Planificar)
- Do (Hacer)
- Check (Verificar)
- Act (Actuar)

Metodología de la Mejora Continua - PDCA



9.1. ROLES Y RESPONSABILIDADES EN LA IMPLEMENTACIÓN DEL SGSI

9.1.1. COMITÉ DE GOBIERNO Y TRANSFORMACIÓN DIGITAL

Tiene las siguientes funciones:

- Informar semestralmente al/a la titular de la UEB los avances y dificultades en la implementación u operación del SGSI.
- Asegurar el cumplimiento de las políticas, objetivos, planes, procedimientos y marco normativo en materia de seguridad y confianza digital en la entidad pública.
- Apoyar al Oficial de Seguridad y Confianza Digital en las actividades relacionadas al SGSI, como la concienciación a los usuarios, dentro del alcance del Órgano y/o Unidad Orgánica al que pertenece.
- Otras relacionadas con el Gobierno y Transformación Digital de la entidad.

9.1.2. EQUIPO DE TRABAJO MULTIDISCIPLINARIO PARA EL SGSI

El Equipo de Trabajo Multidisciplinario está encargado de realizar la implementación y mantenimiento del SGSI en la entidad, sus responsabilidades son:

- Identificar y documentar los activos de información críticos de la unidad orgánica a su cargo, lo cual incluye datos, sistemas, procesos y cualquier otra forma de información que sea valiosa y requiera protección.
- Mantener actualizada la clasificación de su inventario de activos.
- Incorporarse al grupo de trabajo multidisciplinario del SGSI para implementar los controles del Plan en coordinación con el OSCD.
- Establecer niveles de acceso y criticidad de los activos de información, y realizar una revisión periódica con la finalidad de protegerlos de un acceso no autorizado.
- Validar la implementación de los controles y proponer mejoras como parte de la mejora continua del Plan.
- Participar en las validaciones de auditoría, generando evidencia de la implementación de los controles.

La organización del Equipo debe considerar el contexto, tamaño, complejidad y estructura de la UEB. Las responsabilidades de los miembros del Equipo de Trabajo, son las siguientes:

OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL

Es el coordinador del Plan de Implementación del SGSI en la UEB. Tiene como responsabilidades:

- Liderar el equipo de trabajo multidisciplinario.
- Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI en la UEB
- Coordinar con los integrantes del grupo de trabajo multidisciplinario la implementación de controles del Plan SGSI.
- Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

GESTOR DE RIESGOS

Es el rol responsable de:

- Identificar los riesgos.
- Realizar la matriz de evaluación de riesgos para los procesos principales y activos de Información
- Realizar el tratamiento de riesgos
- Realizar el seguimiento del estado de los riesgos
- Otras responsabilidades asignadas por el Oficial de Seguridad y Confianza Digital.

PROPIETARIOS DE LA INFORMACIÓN

Son los directivos/servidores responsables de la gestión, protección y control de la información generada, procesada, almacenada o transmitida en el marco de las funciones de su unidad de organización. Su rol es fundamental para la aplicación de controles que permitan garantizar la seguridad, disponibilidad, integridad y confidencialidad de los activos de información. Los propietarios de la información que formarán parte del equipo de trabajo multidisciplinario son designados por el CGTD.

10. CRONOGRAMA DE ACTIVIDADES

La implementación del SGSI comprende cuatro (04) fases, las cuales se desarrollarán de acuerdo al siguiente cronograma.

FASES	ACTIVIDADES	RESPONSABLES	ENTREGABLES	2025 - 2026											
				JUN	JUL	AGO	SET	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY
FASE I Planificación**	Comprender la Organización y su contexto	OSCD	Análisis PESTEL, FODA	X											
	Comprender las necesidades y expectativas de las partes interesadas.	OSCD CGTD													
	Determinar el alcance del SGSI	OSCD CGTD	Alcance del SGSI	X											
	Elaborar el Plan de Implementación del SGSI	OSCD CGTD	Plan de Implementación del SGSI	X	X										
	Identificar Riesgos de Seguridad de la Información	GR	Reporte de Riesgos de Seguridad de la Información	X											
	Elaborar la Política de Seguridad de la información	OSCD	Política de Seguridad de la Información	X											
	Asignar Roles y responsabilidad para la gestión del SGSI	OSCD CGTD	Roles y Responsabilidades del SGSI		X										
	Realizar un inventario de activos de información	OSCD PI	Inventario de activos de información.	X	X										
	Analizar y evaluar los riesgos y elaborar el tratamiento de Riesgos	OSCD GR	Reporte de Riesgos de Seguridad de la Información	X											
	Elaborar el documento de Aplicabilidad	OSCD CGTD	Declaración de Aplicabilidad (SoA)	X	X										
	Elaborar en Plan de concientización y comunicación en Seguridad de la Información.	OSCD URH	Plan de concientización y comunicación en Seguridad de la Información		X	X									
FASE II Implementación	Ejecutar el Tratamiento de Riesgos	UTI, URH, UL, OA, UAF, OI, OGP*	Seguimiento al Tratamiento de Riesgo			X	X	X	X	X					
	Ejecutar el Plan de concientización y comunicación en Seguridad de la Información	OSCD URH	Informe de implementación del Plan de concientización, capacitación y comunicación en Seguridad de la Información				X	X	X	X	X				
	Ejecutar la implementación de controles de seguridad de la información[1]	UTI, URH, UL, OA, UAF, OI, OGP*	Reporte de seguimiento de implementación de controles de Seguridad de la Información			X	X	X	X	X	X	X	X		
FASE III Monitoreo y Revisión	Realizar el seguimiento al Tratamiento de Riesgos	OSCD GR	Informe de monitoreo de la evaluación y tratamiento de riesgos periódicos.				X		X		X	X			
	Verificar la revisión de controles de seguridad de la información	OSCD GR	Informe de controles implementados en el SGSI.					X			X		X	X	
	Realizar auditoría interna del SGSI	Auditor Interno	Informe de auditoría interna										X	X	
FASE IV Mantener y Mejorar	Implementar las acciones correctivas	UTI, URH, UL, OA, UAF, OI, OGP*	Informe sobre la atención de las acciones correctivas											X	X
	Realizar auditoría externa del SGSI	Auditor Externo	Informe de auditoría externa											X	X
	Realizar informe de cierre de la implementación del SGSI	OSCD CGTD	Informe final de cierre de implementación											X	X

[1] Anexo A de la NTP ISO/IEC 27001:2022
* En caso impacten en la Implementación del Plan Maestro
** Esta fase se ha venido ejecutando desde junio 2025 a la fecha

11. RIESGOS DEL PLAN DE IMPLEMENTACIÓN DEL SGSI

11.1. LISTA DE RIESGOS IDENTIFICADOS

La implementación del SGSI implicará una transformación en la cultura organizacional. En ese sentido, se muestra una lista de riesgos identificados que podrían alterar o retrasar los objetivos planteados en el presente Plan:

- **Recorte presupuestal o falta del mismo:** Disponer de un presupuesto limitado o la falta del mismo por motivos de recorte presupuestal desde el Congreso de la República, son causas que obstaculizan o retrasan la implementación del SGSI.

- **Ampliación de plazos en la presentación y aprobación de documentos oficiales (evidencia):** La falta de documentos oficiales aprobados puede generar incertidumbre y dudas en la toma de decisiones relacionadas con la implementación del SGSI. Sin la evidencia legal adecuada, es posible que los responsables de la implementación del SGSI no cuenten con la información necesaria para definir y ejecutar acciones de seguridad de manera efectiva.

- **Retrasos en la aplicación o implementación de controles definidos en el Plan SGSI:** debido a que el personal realiza actividades operativas diarias de soporte y gestión de servicios, lo que limita la disponibilidad para dedicar tiempo exclusivo a la aplicación de los controles definidos en el marco de la implementación del SGSI.

- **Resistencia al cambio**: por parte de los servidores parlamentarios con respecto a la aplicación y aceptación de las políticas de seguridad y directivas que se conformen como parte de los lineamientos del uso de los recursos informáticos.

En la siguiente tabla se muestra la matriz de probabilidad e impacto sobre la cual se realizará el análisis de riesgos que afectarían positiva o negativamente a la implementación del SGSI.

Matriz de Análisis de Riesgos de Implementación del SGSI	**Probabilidad**	5 Muy Alta	MODERADO	MODERADO	IMPORTANTE	INACEPTABLE	INACEPTABLE
		4 Alta	MODERADO	MODERADO	IMPORTANTE	IMPORTANTE	INACEPTABLE
		3 Media	TOLERABLE	MODERADO	MODERADO	IMPORTANTE	IMPORTANTE
		2 Baja	ACEPTABLE	TOLERABLE	MODERADO	MODERADO	MODERADO
		1 Muy Baja	ACEPTABLE	ACEPTABLE	TOLERABLE	MODERADO	MODERADO
			1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
			Impacto				

Probabilidad de Ocurrencia	
PROBABILIDAD	**VALOR**
MUY ALTA	5
ALTA	4
MEDIA	3
BAJA	2
MUY BAJA	1

Impacto del Riesgo	
IMPACTO	**VALOR**
CATASTRÓFICO	5
MAYOR	4
MODERADO	3
MENOR	2
INSIGNIFICANTE	1

11.2. EVALUACIÓN DE RIESGOS

Conforme a los riesgos identificados que podrán afectar la implementación del SGSI, se ha elaborado en la siguiente tabla el nivel de riesgo.

Código	Riesgo	Probabilidad	Impacto	Nivel de riesgo
R001	Recorte presupuestal o falta del mismo durante la vigencia del Plan, para brindar continuidad a la implementación del SGSI conforme al cronograma propuesto.	3	4	12
R002	Ampliación de plazos en la presentación y aprobación de documentos oficiales (evidencia).	4	3	12
R003	Retrasos en la aplicación o implementación de controles definidos en el Plan SGSI.	4	4	16
R004	Resistencia al cambio por parte de los servidores parlamentarios.	4	4	16

11.3. MEDIDAS DE CONTINGENCIA O MITIGACIÓN

Para mitigar los riesgos identificados, se ha elaborado en la siguiente tabla las medidas de mitigación, las cuales están enfocadas en las acciones que debe realizar la UEB para asegurar en la mejor medida la implementación del SGSI.

Código	Riesgo	Acciones de Contingencia
R001	Recorte presupuestal o falta del mismo	• Realizar una evaluación de los recursos necesarios para la implementación del SGSI y asegurarse de que estén disponibles y asignados adecuadamente. Esto puede incluir la contratación de servicios especializados para la implementación de los controles y/o auditoría interna / externa para la evaluación del SGSI. • Realizar indagaciones de mercado eficientes con el fin de obtener cotizaciones a precios favorables sin comprometer la calidad y resultados esperados. • Priorizar implementación de controles de mayor impacto. • Ejecutar el presupuesto del primer semestre eficientemente. • Solicitar refuerzos presupuestales argumentando el cumplimiento normativo obligatorio.
R002	Ampliación de plazos en la presentación y aprobación de documentos oficiales (evidencia legal).	• Establecer plazos realistas para la presentación y aprobación de documentos oficiales, así como contar con una comunicación clara y continua con las partes interesadas relevantes.

Código	Riesgo	Acciones de Contingencia
		• Establecer mecanismos para seguir avanzando en el plan de trabajo, incluso si existen retrasos en la obtención de los documentos oficiales, garantizando la adopción de medidas provisionales que aseguren la protección de la información en tanto se resuelven los trámites pendientes. • Programar reuniones con el Comité de Gobierno y Transformación Digital, las mismas que deben ser programadas con anticipación y comunicadas de manera clara a todos los miembros del Comité
R003	Retrasos en la aplicación o implementación de controles definidos en el Plan SGSI.	• Priorizar implementación de controles de mayor impacto • Gestión temprana de dependencias con terceros o el Congreso. • Delegar tareas específicas a personal especializado y formalizar responsables por control. • Contratación o soporte técnico especializado temporal.
R004	Resistencia al cambio por parte de los servidores parlamentarios.	• Obtener el compromiso de la Dirección Ejecutiva y los jefes de las unidades de organización para sensibilizar y predisponer a los servidores parlamentarios bajo su cargo, sobre la importancia de cumplir con las políticas de seguridad de la información. • Los responsables de las unidades de la organización deben fomentar a sus colaboradores la predisposición sobre la implementación del SGSI y sus controles. • Programar charlas informativas sobre seguridad de la información, haciendo énfasis en los riesgos a los que la Entidad se encuentra expuesta.

12. RECURSOS Y PRESUPUESTO

Los recursos y presupuesto para la implementación del SGSI en la UEB será efectuada a través de la contratación de servicios especializados y el esfuerzo del personal propio de la UEB, los cuales estarán considerados en el presupuesto institucional asignado a las unidades de la organización en coordinación con la Oficina de Administración.

N°	Actividad / Componente	Descripción resumida	Costo estimado (S/)
1	**Suscripción de herramientas en la nube**	Licencias 365 E1, E3, E5 con seguridad avanzada (MFA, AD en la nube, etc.)	120,000
2	**Alquiler de Infraestructura Tecnológica**	Gabinete, Switch L3, UPS para seguridad de red y segmentación	20,000
3	**Servicio de custodia de cartas fianza – BN**	Servicio físico de custodia de documentos en el Banco de la Nación	264
4	**Servicio de Backup as a Service (BaaS) – 5TB**	Almacenamiento seguro cifrado y gestionado para respaldos críticos	5,000
5	**Auditoría interna SGSI**	Auditoría de cumplimiento ISO 27001, previo a auditoría externa	0
6	**Simulaciones de ataques y campañas de phishing**	Uso de plataforma Microsoft Defender Attack Simulation + diseño de campañas	0
7	**Comunicación institucional y difusión**	Materiales visuales, gráficas de concientización	0

N°	Actividad / Componente	Descripción resumida	Costo estimado (S/)
8	**Inducción sobre Concientización SGSI**	Sesiones de concientización al personal	0
9	**Auditoría externa SGSI**	Auditoría de cumplimiento ISO 27001	35,000
10	**Contingencias e imprevistos**	Reservado para adecuación de ambientes, licencias temporales, capacitaciones extra	5,000
		TOTAL ESTIMADO	**185,264**

13. MONITOREO Y EVALUACIÓN

La UTI como gestor principal de los riesgos relacionados a la infraestructura tecnológica de la UEB, en coordinación con el Equipo de Trabajo Multidisciplinario, evalúa el desempeño de la seguridad de la información y la efectividad del SGSI, manteniendo y protegiendo los registros respectivos. Cuando se identifican incumplimientos en los objetivos de seguridad y en las acciones programadas para el tratamiento de riesgos, se realizará el análisis respectivo para generar las acciones correctivas correspondientes, siempre retroalimentando al Comité de Gobierno y Transformación Digital sobre los avances.

14. VIGENCIA

El Plan de implementación del SGSI tiene vigencia de un año, la cual inicia a partir del día siguiente de su aprobación formal por parte de la Dirección Ejecutiva; deberá ser revisado y actualizado en caso corresponda o en el caso de producirse modificaciones a las normas legales o cambios significativos en la organización o en los procesos que afecten la seguridad de la información.

15. ANEXOS

- Anexo 1 - Inventario de Procesos
- Anexo 2 - Inventario de Activos de Información
- Anexo 3 - Reporte de Riesgos
- Anexo 4 - Declaración de Aplicabilidad (SoA)

Anexo 1 - INVENTARIO DE PROCESOS

Tipo	Código	Macro Proceso Nivel 0	Código	Proceso Nivel 1
Estrategico	E01	Gestión del Planeamiento y Presupuesto	E01.01	Gestión del Planeamiento Institucional
			E01.02	Gestión del Presupuesto Institucional
			E01.03	Gestión de Modernización
	E02	Gestión Legal	E01.04	Asesoría Jurídica
Soporte	S01	Gestión de Recursos Humanos	S01.01	Organización del Trabajo
			S01.02	Gestión del Empleo
			S01.03	Gestión de las Compensaciones
			S01.04	Gestión del Rendimiento
			S01.05	Gestión de la Capacitación y Desarrollo
			S01.06	Gestión de Relaciones Humanas y Sociales
	S02	Gestión Logística	S02.01	Programación
			S02.02	Procedimientos de Selección
			S02.03	Ejecución Contractual
	S03	Gestion Contable y Financiera	S03.01	Devengado
			S03.02	Giros
			S03.03	Gestión Contable
			S03.04	Conciliación
			S03.05	Administación del Módulo de Instrumentos Financieros
			S03.06	Administración de Cartas Fianzas
	S04	Gestión de Tecnologías de la Información	S04.01	Administración del Portal de Transparencia
			S04.02	Administración de la operatividad informatica
Operativo	O01	Gestión de Proyectos	O01.01	Gestión de Proyectos
	O02	Gestión de Infraestructura	O01.02	Gestion de la Infraestructura Parlamentaria

Anexo 2 - Inventario de Activos de Información (SGSI)

Código de Activo	Activo de Información	Formato (Físico / Digital)	Nivel de Criticidad (Muy Alto, Alto, Medio, Bajo, Muy Bajo)	Ubicación (Congreso, Nube, OnPremise, Oficina, PC Usuario)	Clasificación de la Información (Pública, Interna, Confidencial)	Propietario
A001	SharePoint Online - UEB_Institucional	Digital	Muy alto	Nube	Interna	UEB
A002	SharePoint Online - UEB_Externos	Digital	Alto	Nube	Confidencial	UEB
A003	SharePoint Online - UEB_Institucional_Restringido	Digital	Muy alto	Nube	Confidencial	UEB
A004	SharePoint Online - UEB_Procesos	Digital	Alto	Nube	Confidencial	UEB
A005	SharePoint Online - UEB_Seguimiento	Digital	Medio	Nube	Interna	UEB
A006	One Drive - UE1767@ueb.gob.pe	Digital	Alto	Nube	Interna	UTI
A007	One Drive - PC@ueb.gob.pe	Digital	Alto	Nube	Interna	UL
A008	Cartas Fianzas	Físico	Muy alto	Oficina	Confidencial	UAF
A009	Documentos físicos OGP	Físico	Alto	Oficina	Interna	OGP
A010	Información de Proyectos en SyPro	Digital	Muy alto	Nube	Interna	OI
A011	Expedientes de Contratación	Físico	Alto	Oficina	Interna	UL
A012	Expedientes de Contratación NEC	Físico	Alto	Oficina	Interna	UL
A013	Documentos físicos UL	Físico	Medio	Oficina	Interna	UL
A014	Política de Seguridad de la Información	Digital	Alto	Nube	Interna	UEB
A015	Manual de Operaciones	Digital	Alto	Nube	Interna	UEB
A016	Información del SIGA	Digital	Alto	Congreso	Interna	UL
A017	Información del SIAF	Digital	Alto	Congreso	Interna	UAF
A018	Información en AutoCAD	Digital	Medio	PC Usuario	Interna	OI
A019	Información en Revit	Digital	Medio	PC Usuario	Interna	OI
A020	Información en Primavera	Digital	Medio	PC Usuario	Interna	OI
A021	Información en S10	Digital	Medio	PC Usuario	Interna	OI
A022	Legajo de Personal	Físico	Muy alto	Oficina	Confidencial	URH
A023	Información en SISPER (Remuneraciones)	Digital	Muy alto	PC Usuario	Confidencial	URH
A024	Correo Institucional Outlook/M365	Digital	Alto	Nube	Interna	UTI
A025	Red compartida y recursos locales	Digital	Medio	OnPremise	Interna	UTI
A026	Cuenta O365 - Mesa de Partes	Digital	Medio	Nube	Interna	OA
A027	Credenciales Institucionales (usuarios y contraseñas)	Digital	Alto	Nube	Interna	UEB
A028	Página web UEB	Digital	Medio	Congreso	Pública	UTI
A029	Licencias de software	Digital	Medio	Nube	Interna	UTI
A030	Respaldo de información	Digital	Muy alto	OnPremise	Confidencial	UTI
A031	Cuentas privilegiadas (Administradores TI)	Digital	Muy alto	Nube	Confidencial	UTI
A032	Información en Sistema de Trámite Documentario	Digital	Alto	Congreso	Interna	OA
A033	Información Software de Asistencia	Digital	Alto	PC Usuario	Interna	URH
A034	Información del Sistema Procura Digital	Digital	Alto	Nube	Interna	UL

Anexo 3 - Reporte de Riesgos - Plan de Implementacion del SGSI

	IDENTIFICACIÓN DEL RIESGO													ANÁLISIS DEL RIESGO								PLANIFICACIÓN E IMPLEMENTACIÓN DE RESPUESTA AL RIESGO									MONITOREO DEL RIESGO					
N°	Riesgo ID	Fecha de Identificación del Riesgo	Activo de Información	Código Activo de Información	Nivel Activo de Riesgo	Fuente	Riesgo Identificado por	Ciclo de Inversión	Nivel de Riesgo	Categoría	SubCategoría	Tipo de Riesgo	Descripción del Riesgo	Causa del Riesgo	Consecuencia del Riesgo	Propietario del Riesgo (R)	Probabilidad (%)	Impacto	Severidad	Prioridad n	Impacto no	Evaluación de Impacto no Cuantificable Clave	Estimación no Cuantificable Costo	Estrategia de Respuesta	Descripción Detallada de Respuesta al Riesgo	Propietario de la Acción de Respuesta	Tipo de Acción	Fecha Inicio	Fecha Fin	Estado de la implementación de la Respuesta	Fecha Actualización del Estado de la Respuesta de la Respuesta	Riesgo activado	Estado	Seguimiento (Comentarios)	Fecha de Actualización del Estado del Riesgo	Resultado/s	Fecha de Resultado/s	Lecciones Aprendidas
0001	RSE_0001	20/08/2025	BluePoint Online - USB_Institucional	A001	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Acceso No Autorizado	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Credenciales débiles o phishing	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la	Alta	Muy alto	Alta	9	Alarce	No definido	No definido	Mitigar	Implementar SIEM y realizar concientización sobre seguridad de la información	Unidad de Tecnología de la información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0002	RSE_0002	20/08/2025	BluePoint Online - USB_Gobierno	A002	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Acceso No Autorizado	Amenaza	Acceso no autorizado / Fuga de información	Eliminación accidental de información	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la	Alta	Alta	Alta	6	Alarce	No definido	No definido	Mitigar	Establecer una disposición para el control de cambios de los accesos	Unidad de Tecnología de la información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0003	RSE_0003	20/08/2025	BluePoint Online - USB_Institucional_Rodriguito	A002	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Confidencialidad	Amenaza	Acceso no autorizado / Fuga de información	Permisos inadecuados	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Revisar y restringir permisos de acceso. Establecer una disposición para el control de cambios de los accesos	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0004	RSE_0004	20/08/2025	BluePoint Online - USB_Procesos	A003	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Pérdida de Integridad	Errores humanos o ataques de ransomware	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la	Alta	Muy alto	Alta	9	Alarce	No definido	No definido	Mitigar	Realizar copias de seguridad de forma semanal	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0005	RSE_0005	20/08/2025	BluePoint Online - USB_Seguridad	A005	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Interrupción de servicio	Falla técnica o climatológica	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la	Medio	Alta	Media	9	Alarce	No definido	No definido	Mitigar	Establecer una disposición para el control de cambios de los accesos	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0006	RSE_0006	20/08/2025	One Drive - LSI7557@usb.gob.pe	A006	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Pérdida de Integridad	Errores humanos o ataques de ransomware	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la	Alta	Muy alto	Alta	9	Alarce	No definido	No definido	Mitigar	Realizar copias de seguridad de forma semanal	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0007	RSE_0007	20/08/2025	One Drive - PCC@usb.gob.pe	A007	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Confidencialidad	Amenaza	Acceso no autorizado / Fuga de información / Acceso compartido por el usuario	Credenciales compartidas	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad Logística	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Implementar SIEM y realizar concientización sobre seguridad de la información	Unidad Logística	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0008	RSE_0008	20/08/2025	Cartas Fianzas	A008	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Confidencialidad	Amenaza	Exposición visual de documentos confidenciales	Inadecuado resguardo de documentos físicos de acceso confidencial	Acceso No Autorizado, Fuga de Información	Unidad de Asuntos Financieros	Alta	Muy alto	Alta	9	Alarce	No definido	No definido	Mitigar	Implementar un espacio físico de acceso restringido al personal. Destinar un servicio de alquiler de casillero de seguridad	Unidad de Asuntos Financieros	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0009	RSE_0009	20/08/2025	Documentos Notas OSP	A009	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Exposición a daños del documento físico	Inadecuado resguardo de documentos físicos	Deterioro de documentos físicos	Oficina de Gestión de Proyectos	Medio	Medio	Media	9	Alarce	No definido	No definido	Mitigar	Implementar un espacio físico de acceso restringido al personal.	Oficina de Gestión de Proyectos	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0010	RSE_0010	20/08/2025	Información de Proyectos en SyPo	A010	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Interrupción de servicio	Posible incumplimiento con controles de seguridad de la información del servicio en nube	Retrasos en las actividades del personal por indisponibilidad del servicio	Oficina de Infraestructura	Medio	Muy alto	Media	9	Alarce	No definido	No definido	Mitigar	Asegurar que el proveedor en nube cumpla con la ISO 27001	Oficina de Infraestructura	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0011	RSE_0011	20/08/2025	Expedientes de Contabilidad	A011	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Confidencialidad	Amenaza	Exposición visual de documentos confidenciales	Inadecuado resguardo de documentos físicos de acceso confidencial	Acceso No Autorizado, Fuga de Información	Unidad Logística	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Implementar un espacio físico de acceso restringido al personal.	Unidad Logística	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0012	RSE_0012	20/08/2025	Expedientes de Contabilidad OCC	A012	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Confidencialidad	Amenaza	Exposición visual de documentos confidenciales	Inadecuado resguardo de documentos físicos de acceso confidencial	Acceso No Autorizado, Fuga de Información	Unidad Logística	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Implementar un espacio físico de acceso restringido al personal.	Unidad Logística	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0013	RSE_0013	20/08/2025	Documentos Notas UL	A013	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Exposición a daños del documento físico	Inadecuado resguardo de documentos físicos	Deterioro de documentos físicos	Unidad Logística	Medio	Muy alto	Media	9	Alarce	No definido	No definido	Mitigar	Implementar un espacio físico de acceso restringido al personal.	Unidad Logística	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0014	RSE_0014	20/08/2025	Política de Seguridad de la Información	A014	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Pérdida de Integridad	Eliminación accidental de información	Pérdida de Información	Dirección Ejecutiva	Baja	Baja	Baja	3	Alarce	No definido	No definido	Mitigar	Realizar copias de seguridad de forma semanal	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0015	RSE_0015	20/08/2025	Manual de Operaciones	A015	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Pérdida de Integridad	Eliminación accidental de información	Pérdida de Información	Dirección Ejecutiva	Baja	Baja	Baja	3	Alarce	No definido	No definido	Mitigar	Realizar copias de seguridad de forma semanal	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0016	RSE_0016	20/08/2025	Información del SIGA	A016	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Interrupción de servicio	Afectación en la infraestructura tecnológica del Congreso	Retrasos en las actividades del personal por indisponibilidad del servicio	Unidad Logística	Medio	Alta	Media	4	Alarce	No definido	No definido	Mitigar	Realizar copias de seguridad de forma semanal	Unidad Logística	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0017	RSE_0017	20/08/2025	Información del SSP	A017	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Interrupción de servicio	Afectación en la infraestructura tecnológica del Congreso	Retrasos en las actividades del personal por indisponibilidad del servicio	Unidad de Asuntos Financieros	Medio	Alta	Media	4	Alarce	No definido	No definido	Mitigar	Realizar copias de seguridad de forma semanal	Unidad de Asuntos Financieros	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0018	RSE_0018	20/08/2025	Información en AutoCAD	A018	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Pérdida de Información de la Aplicación	Eliminación accidental de información	Pérdida de Información	Oficina de Infraestructura	Medio	Alta	Media	4	Alarce	No definido	No definido	Mitigar	El usuario debe mantener actualizada la copia de seguridad y alojarlo en Sharepoint	Oficina de Infraestructura	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0019	RSE_0019	20/08/2025	Información en Revit	A019	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Pérdida de Información de la Aplicación	Eliminación accidental de información	Pérdida de Información	Oficina de Infraestructura	Medio	Alta	Media	4	Alarce	No definido	No definido	Mitigar	El usuario debe mantener actualizada la copia de seguridad y alojarlo en Sharepoint	Oficina de Infraestructura	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0020	RSE_0020	20/08/2025	Información en Primavera	A020	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Pérdida de Información de la Aplicación	Eliminación accidental de información	Pérdida de Información	Oficina de Infraestructura	Medio	Alta	Media	4	Alarce	No definido	No definido	Mitigar	El usuario debe mantener actualizada la copia de seguridad y alojarlo en Sharepoint	Oficina de Infraestructura	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0021	RSE_0021	20/08/2025	Información en STI	A021	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Pérdida de Información de la Aplicación	Eliminación accidental de información	Pérdida de Información	Oficina de Infraestructura	Medio	Alta	Media	4	Alarce	No definido	No definido	Mitigar	El usuario debe mantener actualizada la copia de seguridad y alojarlo en Sharepoint	Oficina de Infraestructura	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0022	RSE_0022	20/08/2025	Legajo de Personal	A022	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Confidencialidad	Amenaza	Exposición visual de documentos confidenciales	Inadecuado resguardo de documentos físicos de acceso confidencial	Acceso No Autorizado, Fuga de Información	Unidad de Recursos Humanos	Alta	Alta	Alta	9	Alarce	No definido	No definido	Mitigar	Implementar un espacio físico de acceso restringido al personal	Unidad de Recursos Humanos	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0023	RSE_0023	20/08/2025	Información en ESPER (Remuneraciones)	A023	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Errores humanos o ataques de ransomware	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Recursos Humanos	Alta	Alta	Alta	9	Alarce	No definido	No definido	Mitigar	El usuario debe mantener actualizada la copia de seguridad y alojarlo en Sharepoint	Unidad de Recursos Humanos	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0024	RSE_0024	20/08/2025	Correo Institucional Outlook/M365	A024	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Ingeniería Social	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Credenciales débiles o phishing	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la Información	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Implementar SIEM y realizar concientización sobre seguridad de la información	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0025	RSE_0025	20/08/2025	Red compartida y recursos locales	A025	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Continuidad del Negocio	Amenaza	Pérdida de Disponibilidad	Falla de una fuente de energía servidor NAS	Pérdida de Información	Unidad de Tecnología de la Información	Alta	Alta	Alta	6	Alarce	No definido	No definido	Mitigar	Implementar fuente redundante en el servidor NAS	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0026	RSE_0026	20/08/2025	Cuenta CSSI - Sitios de Partes	A026	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Ingeniería Social	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Credenciales débiles o phishing	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Oficina Administrativa	Muy Alta	Muy alto	Muy Alta	6	Alarce	No definido	No definido	Mitigar	Implementar SIEM y realizar concientización sobre seguridad de la información	Oficina Administrativa	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0027	RSE_0027	20/08/2025	Credenciales Institucionales (usuarios y contraseñas)	A027	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Ingeniería Social	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Credenciales débiles o phishing	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la Información	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Implementar SIEM y realizar concientización sobre seguridad de la información	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0028	RSE_0028	20/08/2025	Página web USB	A028	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Errores humanos o ataques de ransomware	Deliberado, alteración de la imagen institucional	Unidad de Tecnología de la Información	Alta	Alta	Alta	6	Alarce	No definido	No definido	Mitigar	Proteger equipo de usuario administrador: sonita software nativos	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0029	RSE_0029	20/08/2025	Licencias de software	A029	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Acceso No Autorizado	Amenaza	Pérdida de Integridad	Errores humanos o ataques de ransomware	Acceso No Autorizado, Fuga de Información	Unidad de Tecnología de la Información	Media	Alta	Media	3	Alarce	No definido	No definido	Mitigar	Proteger equipo de usuario administrador: sonita software nativos	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0030	RSE_0030	20/08/2025	Respaldo de información	A030	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Pérdida de Integridad	Errores humanos o ataques de ransomware	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la Información	Alta	Muy alto	Alta	9	Alarce	No definido	No definido	Mitigar	Activar la accesibilidad de inmutabilidad en el servidor NAS	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0031	RSE_0031	20/08/2025	Cuentas privilegiadas (Administradores TI)	A031	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Ingeniería Social	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Credenciales débiles o phishing	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Tecnología de la Información	Muy Alta	Muy alto	Muy Alta	9	Alarce	No definido	No definido	Mitigar	Implementar SIEM y realizar concientización sobre seguridad de la información	Unidad de Tecnología de la Información	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0032	RSE_0032	20/08/2025	Información en Sistema de Trámite Documentario	A032	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Interrupción de servicio	Afectación en la infraestructura tecnológica del Congreso	Retrasos en las actividades del personal por indisponibilidad del servicio	Oficina Administrativa	Alta	Alta	Alta	6	Alarce	No definido	No definido	Mitigar	Realizar descargas de la documentación remitida y almacenarla como respaldo de información	Oficina Administrativa	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0033	RSE_0033	20/08/2025	Información Software de Asistencia	A033	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Integridad	Amenaza	Ciberataque / Acceso no autorizado / Exposición a entornos nativos	Errores humanos o ataques de ransomware	Pérdida de información, Divulgación de información, Fuga de información, Acceso No Autorizado	Unidad de Recursos Humanos	Alta	Alta	Alta	6	Alarce	No definido	No definido	Mitigar	El usuario debe mantener actualizada la copia de seguridad y alojarlo en Sharepoint	Unidad de Recursos Humanos	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		
0034	RSE_0034	20/08/2025	Información del Sistema Presura Digital	A034	Riesgo	No aplica	Unidad de Tecnología de la Información	Ejecución - ET	Riesgo Operacional	Riesgo_Seguridad_de_la_Información	Disponibilidad	Amenaza	Interrupción de servicio	Posible incumplimiento con controles de seguridad de la información del servicio en nube	Retrasos en las actividades del personal por indisponibilidad del servicio	Unidad Logística	Alta	Alta	Alta	6	Alarce	No definido	No definido	Mitigar	Asegurar que el proveedor en nube cumpla con la ISO 27001	Unidad Logística	Control	1/09/2025	31/07/2026	En progreso		9	Verificado			Para información		

Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI

Fecha de Elaboración	1/08/2025		Autor	Omar Manuel Huarcaya Lima	

	Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
Control	5.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal como por las partes interesadas pertinentes, además revisadas en intervalos planificados y cuando ocurran cambios significativos	Si	DE	Implementado	Requisito Legal	Requisito normativo del SGSI, Alineamiento estratégico institucional, Base para la concienciación y cumplimiento. Se elaboró la política de seguridad de la información basada en la NTP 27001:2022, la misma que fue aprobada por el CGTD y por Resolución Directoral N°015-2025-DE-UEB-CR.	A014
	5.2	Roles y responsabilidades en la Seguridad de la Información	Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización	Si	DE	En implementación	Buena Práctica	Claridad en funciones de seguridad, Prevención de conflictos de interés, Mejora en la rendición de cuentas. Las Unidades de la Organización realizarán una matriz RACI del SGSI.	A033
	5.3	Segregación de funciones	Funciones en conflicto y áreas de responsabilidad en conflicto deben ser segregadas	Si	DE	Implementado	Requisito Legal	Requisito normativo del SGSI, Alineamiento estratégico institucional. Las funciones están correctamente segregadas conforme al MOPE vigente.	A015
	5.4	Responsabilidades de la dirección	La Dirección debe requerir a todo el personal que aplique la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización	Si	DE	Implementado	Requisito Legal	Liderazgo visible en seguridad, Impulso a la cultura organizacional, Cumplimiento de NTP 27001:2022. La Política de seguridad de la información fue comunicada mediante MEMORANDO MULTIPLE N°006-2025-DE-UEB/CR.	A014
	5.5	Contacto con autoridades	La organización debe establecer y mantener contacto con las autoridades pertinentes	No	No Aplica	Excluido	No Aplica	No se requiere contacto directo con autoridades externas en el contexto actual de la UEB. Las coordinaciones institucionales se canalizarán a través del Congreso. No se han presentado incidentes que requieran esta relación.	No Aplica
	5.6	Contacto con grupos especiales de interés	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en seguridad	No	No Aplica	Excluido	No Aplica	Se prioriza la implementación interna del SGSI. No se cuenta con personal con disponibilidad para representación externa. No se ha definido una política de relacionamiento externo. Se puede realizar el contacto con grupos externos (SEGDI, PCM, otros) mediante el Congreso.	No Aplica
	5.7	Inteligencia de amenazas	La información relacionada con las amenazas a la seguridad de la información debe ser recopilada y analizada para producir inteligencia sobre las amenazas	No	No Aplica	Excluido	No Aplica	No se cuenta con herramientas de threat intelligence. No se dispone de personal especializado. No se ha identificado una necesidad crítica. Se prioriza la implementación de controles preventivos básicos. En esta etapa no se tratarán las amenazas, se coordina con PCM para la inteligencia de amenazas.	No Aplica
	5.8	Seguridad de la Información en la gestión de proyectos	La seguridad de la información debe estar integrada en la gestión de proyectos	Si	OGP, OI	En implementación	Buena Práctica	Integración temprana de controles, Reducción de costos por reprocesos, Protección de información crítica. Se elaborará el Plan de riesgos para los proyectos.	A010, A020, A034
	5.9	Inventario de información y otros activos asociados	Un inventario de la información y otros activos asociados, incluidos los propietarios, debe ser desarrollado y mantenido	Si	UEB	En implementación	Buena Práctica	Identificación de activos críticos, Base para análisis de riesgos. Se elaborará inventario de activos de información, inventario de equipamiento asignado.	A008, A009, A011, A012, A013, A014, A015, A022
	5.10	Uso aceptable de la información y otros activos asociados	Reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debe ser identificada, documentada e implementada	No	No Aplica	Excluido	No Aplica	No se ha definido una política formal, es decir, que no se dispone de un marco normativo interno aprobado. No se ha identificado un incidente que lo justifique. Se prioriza la concienciación general antes de normar el uso.	No Aplica
	5.11	Devolución de activos	El personal y otras partes interesadas, según sea apropiado, deben devolver todos los activos de la organización en su posesión cuando cambien o terminen su empleo, contrato o acuerdo	No	No Aplica	Excluido	No Aplica	No existe un procedimiento formalizado. La gestión de activos se realiza de forma operativa. Se prioriza la implementación de controles de acceso.	No Aplica
	5.12	Clasificación de la información	La información debe ser clasificada de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos de las partes interesadas pertinentes	Si	UEB	En implementación	Buena Práctica	Protección según sensibilidad, Cumplimiento de requisitos legales, Priorización de controles de seguridad. Se elaborará identificación de información confidencial.	A008, A009, A011, A012, A013, A014, A015, A022
	5.13	Etiquetado de la información	Un conjunto de procedimientos apropiado para el etiquetado de información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización	Si	UEB	En implementación	Buena Práctica	Apoyo a la clasificación, Facilita el manejo adecuado, Transferencia de información. Se etiquetará la información enfocado en la liquidación de la UE y la transferencia de información.	A008, A009, A011, A012, A013, A014, A015, A022
	5.14	Transferencia de información	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones para transferencia, dentro de la organización y entre la organización y otras partes	No	No Aplica	Excluido	No Aplica	No se han definido reglas formales. No se cuenta con herramientas de cifrado. Se prioriza la clasificación de la información antes de normar su transferencia.	No Aplica
	5.15	Control de acceso	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos del negocio y de seguridad de la información	Si	UL, UTI	En implementación	Tratamiento Riesgo	Prevención de accesos no autorizados, Protección de la confidencialidad, Cumplimiento de principio de mínimo privilegio. Se implementarán permisos acotados en Sharepoint.	A001–A007, A010, A014–A017, A020–A028, A030–A034
	5.16	Gestión de identidades	El ciclo de vida completo de las identidades debe ser gestionado	Si	UTI	En implementación	Tratamiento Riesgo	Control del ciclo de vida de usuarios, Prevención de cuentas huérfanas, Integridad de los accesos. Se implementará una disposición para la baja de cuentas de usuarios.	A001–A007, A016, A017, A024, A027, A028, A031, A032
	5.17	Información de autenticación	La asignación y gestión de la información de autenticación debe ser controlada por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación	Si	UTI	En implementación	Tratamiento Riesgo	Protección de credenciales, Reducción de suplantación de identidad, Prevención de accesos no autorizados. Se implementará MFA en los activos de información que sean factibles de acuerdo a la tecnología aplicada.	A001–A007, A016–A021, A024, A026–A028, A032

Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI

	Fecha de Elaboración	1/08/2025		Autor	Omar Manuel Huarcaya Lima

	Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
Organizacionales	5.18	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben ser aprovisionados, revisados, modificados y removidos en concordancia con la política específica de la organización y las reglas para el control de acceso	Si	UTI	En implementación	Tratamiento Riesgo	Asignación basada en roles, Revisión periódica de accesos, Prevención de accesos no autorizados. Se realizará la revisión de niveles de acceso. Se implementará una disposición para baja de cuentas de usuarios.	A027
	5.19	Seguridad de la información en las relaciones con proveedores	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de productos o servicios del proveedor	No	No Aplica	Excluido	No Aplica	No se han definido procesos de evaluación de proveedores. Se prioriza la contratación con proveedores en nube certificados en la 27001:2022. No se dispone de un procedimiento de homologación de proveedores.	No Aplica
	5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor	No	No Aplica	Excluido	No Aplica	No se ha definido un modelo contractual estándar. No se ha identificado un incidente contractual. Se prioriza la contratación con proveedores en nube que cuenten con Certificación 27001:2022.	No Aplica
	5.21	Gestión de seguridad de la información en la cadena de suministro de las tecnologías de la información y las telecomunicación (TIC)	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de las TIC	No	No Aplica	Excluido	No Aplica	No se gestiona directamente la cadena de suministro TIC. Se depende de infraestructura del Congreso. Se prioriza la contratación con proveedores en nube que cuenten con Certificación 27001:2022.	No Aplica
	5.22	Seguimiento, revisión y gestión del cambio en servicios de proveedores	La organización debe hacer seguimiento, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios	No	No Aplica	Excluido	No Aplica	No se han definido responsables de esta función. No se dispone de herramientas de monitoreo. Se prioriza la implementación de controles internos.	No Aplica
	5.23	Seguridad de la información en el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización	Si	UTI	En implementación	Buena Práctica	Protección de datos en entornos externos, Priorización de controles de seguridad, Cumplimiento de contratos y SLA. Se priorizará la contratación de servicios en la nube que cuenten con la certificación 27001	A001–A007, A024, A034
	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y preparar la gestión de los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, las funciones y las responsabilidades de gestión de incidentes de seguridad de la información	No	No Aplica	Excluido	No Aplica	No se cuenta con un equipo de respuesta a incidentes. No se ha definido un proceso formal de gestión de incidentes. La atención es reactiva y no estructurada. Se prioriza la implementación de controles preventivos.	No Aplica
	5.25	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y decidir si se categorizan como incidentes de seguridad de la información	No	No Aplica	Excluido	No Aplica	Se considera en una fase posterior del SGSI. No se ha establecido un procedimiento para categorizar eventos. No se han registrado incidentes que requieran esta evaluación.	No Aplica
	5.26	Respuesta a incidentes de seguridad de la información	Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados	No	No Aplica	Excluido	No Aplica	Se prioriza la prevención antes que la reacción. La respuesta es ad-hoc y depende del personal disponible. No se cuenta con un equipo designado para respuesta.	No Aplica
	5.27	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información	No	No Aplica	Excluido	No Aplica	Se considera en la etapa de madurez del SGSI. No se realiza análisis post-incidente. No se cuenta con historial de incidentes formales.	No Aplica
	5.28	Recolección de evidencia	La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información	No	No Aplica	Excluido	No Aplica	No se han definido procedimientos forenses. No se cuenta con herramientas de recolección de evidencia. Se considera en una fase avanzada del SGSI.	No Aplica
	5.29	Seguridad de la información durante una interrupción	La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción	No	No Aplica	Excluido	No Aplica	Se considera en el desarrollo del plan de continuidad. Se considera en un fase avanzada del SGSI. No se cuenta con un plan de continuidad aprobado.	No Aplica
	5.30	Preparación de las TIC para la continuidad del negocio	La preparación para las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC	Si	UTI	En implementación	Buena Práctica	Garantizar disponibilidad de servicios, Reducción de impacto ante incidentes. Se elaborará procedimiento de restauración de información.	A030
	5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Los requisitos legales, estatutarios, regulatorios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados	No	No Aplica	Excluido	No Aplica	Se cuenta con la Política de Seguridad de la Información aprobada. No se ha identificado normativa específica adicional. Se considera en la fase de auditoría legal del SGSI.	No Aplica
	5.32	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual	No	No Aplica	Excluido	No Aplica	No se gestionan activos con propiedad intelectual propia. No se han identificado riesgos asociados. No se cuenta con contratos que lo regulen.	No Aplica
	5.33	Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada	Si	UEB	En implementación	Tratamiento Riesgo	Protección según sensibilidad, Cumplimiento legal y auditoría, Prevención de pérdida o alteración. Se custodiarán los activos de información físicos en un ambiente de acceso restringido.	A008, A009, A011, A012, A013, A014, A015, A022
	5.34	Privacidad y protección de la información de identificación personal (IIP)	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales	Si	UAF, UL, URH	En implementación	Requisito Legal	Cumplimiento de leyes de protección de datos personales, Protección de la confidencialidad, Protección de información sensible. Se elaborará un procedimiento para la notificación de incidencias en que se hayan vulnerado información relacionada a los datos personales.	A008, A011, A012, A022

Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI

	Fecha de Elaboración	1/08/2025		Autor	Omar Manuel Huarcaya Lima

	Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
	5.35	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluídas las personas, procesos y tecnologías, debe revisarse de forma independiente en intervalos planificados o cuando se produzcan cambios significativos	No	No Aplica	Excluido	No Aplica	No se cuenta con recursos internos o externos para auditoría. No se ha planificado una revisión formal. No se dispone de presupuesto para auditorías externas. No se han definido criterios de revisión. Se considera en la fase de madurez del SGSI.	No Aplica
	5.36	Cumplimiento con políticas, reglas y normas de seguridad de la información	Se debe revisar periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas específicas, las reglas y las normas	No	No Aplica	Excluido	No Aplica	Se considera en la fase de implementación de controles. No se ha definido un mecanismo de revisión periódica. No se han realizado auditorías internas.	No Aplica
	5.37	Procedimientos operativos documentados	Los procedimientos operativos de las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite	No	No Aplica	Excluido	No Aplica	Las actividades de TI se ejecutan actualmente de forma operativa y no estandarizada, sin contar con procedimientos formales aprobados. La UEB se encuentra en una etapa inicial de implementación del SGSI, por lo que se ha priorizado la atención de controles críticos y de mayor impacto. Se prevé abordar este control en una fase posterior del SGSI, cuando se haya alcanzado un mayor nivel de madurez institucional y operativa.	No Aplica
Controles de Personal	6.1	Selección	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continúa, teniendo en cuenta las leyes, regulaciones y ética aplicables, y ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos percibidos	No	No Aplica	Excluido	No Aplica	El proceso de contratación no está regulado por normas del Congreso. No se han identificado incidentes relacionados con personal contratado. Se realiza este procedimiento a modo de buenas practicas mediante la plataforma "Debida Diligencia del Sector Público".	No Aplica
	6.2	Términos y condiciones del empleo	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización con respecto a la seguridad de la información	No	No Aplica	Excluido	No Aplica	Los contratos no incluyen cláusulas específicas de seguridad de la información. No se han identificado incumplimientos contractuales en esta materia. Se considera en futuras actualizaciones de RRHH.	No Aplica
	6.3	Toma de conciencia, educación y entrenamiento sobre la seguridad de la información	El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada concientización, educación y capacitación en seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos, según sea pertinente para su función laboral	Si	DE, URH, UTI	En implementación	Buena Práctica	Reducción de errores humanos, Fomento de cultura de seguridad, Alineamiento estratégico institucional. Se elaborará Plan de concientización en seguridad de la información dirigido a todo el personal.	A001–A007, A024, A027, A031
	6.4	Proceso disciplinario	Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información	No	No Aplica	Excluido	No Aplica	No se ha definido un proceso específico para violaciones de seguridad. No se han presentado casos que requieran sanción formal. La URH no cuenta con un comité disciplinario interno. Se considera en la fase de madurez del SGSI.	No Aplica
	6.5	Responsabilidades después del cese o cambio de empleo	Las responsabilidades y obligaciones en materia de seguridad de la información que siguen siendo válidos después del cese o cambio de empleo deben definirse, aplicarse y comunicarse al personal pertinente y otras partes interesadas	No	No Aplica	Excluido	No Aplica	Se prioriza la gestión de accesos durante la relación labora. No se han definido responsabilidades específicas tras el cese. No se han identificado incidentes tras desvinculaciones. No se cuenta con un procedimiento de baja formalizado.	No Aplica
	6.6	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes	Si	URH, UL	En implementación	Buena Práctica	Protección de información sensible, Formalización de compromisos, Reducción de fugas de información. Se elaborará un documento a modo de Acta de Confidencialidad o no divulgación, la cual deberá ser suscrita por todo el personal.	A001–A007, A024, A027, A031
	6.7	Trabajo remoto	Se debe implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización	No	No Aplica	Excluido	No Aplica	No se dispone de infraestructura segura para acceso remoto. Actualmente no se permite el trabajo remoto en la UEB. No se han identificado necesidades operativas que lo justifiquen. Se considera en caso de cambios normativos o de contexto.	No Aplica
	6.8	Reporte de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o bajo sospecha a través de los canales apropiados de manera oportuna	No	No Aplica	Excluido	No Aplica	Se considera en el plan de concienciación de seguridad de la información. La comunicación de incidentes se realiza por correo electrónico. No se cuenta con un sistema de tickets o alertas.	No Aplica
	7.1	Perímetros de seguridad física	Los perímetros de seguridad deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados	Si	UL	En implementación	Buena Práctica	Protección contra accesos no autorizados, Control de zonas críticas, Prevención de sabotajes o robos. Se solicitarán los Planos e identificarán las zonas seguras. Se realizarán los registros de acceso físico al micro centro de datos.	A008, A009, A011, A012, A013, A022
	7.2	Ingreso físico	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados	Si	UL	En implementación	Buena Práctica	Registro de accesos, Control de visitantes, Prevención de sabotajes o robos. Se realizarán los registros de acceso físico al micro centro de datos. Se realizará el registro de visitas en la Plataforma oficial del estado.	A008, A009, A011, A012, A013, A022
	7.3	Asegurar oficinas, salas e instalaciones	Se debe diseñar e implementar la seguridad física para las oficinas, salas e instalaciones	Si	UL	En implementación	Requisito Legal	Protección de equipos e información, Reducción de exposición a amenazas físicas, Cumplimiento de estándares de seguridad. Se realizarán las gestiones para obtener el CITSE (Certificado de Inspección Técnica de Seguridad en Edificaciones).	A008, A009, A011, A012, A013, A022
	7.4	Supervisión de la seguridad física	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados	No	No Aplica	Excluido	No Aplica	No se cuenta con sistemas de videovigilancia instalados. La supervisión física se encuentra a cargo del coworking. Se considera en el plan de mejora de infraestructura futura.	No Aplica

	CONGRESO REPÚBLICA / UEB	**Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI**

	Fecha de Elaboración	1/08/2025		**Autor**	Omar Manuel Huarcaya Lima

	Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
Controles Físicos	**7.5**	**Protección contra amenazas físicas y ambientales**	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura	No	No Aplica	Excluido	No Aplica	La infraestructura física es parte del servicio de coworking y cualquier adecuación es coordinada con el proveedor. No se han implementado medidas específicas contra desastres naturales.	No Aplica
	7.6	**Trabajo en áreas seguras**	Deben diseñarse e implementarse medidas de seguridad para trabajar en áreas seguras	No	No Aplica	Excluido	No Aplica	No se han identificado procesos que requieran aislamiento físico. No se dispone de controles de acceso físico diferenciados. Se considera en la fase de madurez del SGSI.	No Aplica
	7.7	**Escritorio y pantalla limpios**	Deben definirse y aplicarse adecuadamente reglas, de papeles y medios de almacenamiento extraíbles y reglas de pantalla limpia en las instalaciones de procesamiento de información	Si	UEB	En implementación	Buena Práctica	Prevención de exposición visual, Reducción de fugas de información, Mejora del orden y control. Se fomentará como parte de la concientización de seguridad de la información, la práctica de escritorios limpios después de utilizar el documento físico, al igual que la limpieza de pantallas de usuario limpias.	A008, A009, A011, A012, A013, A022
	7.8	**Ubicación y protección de los equipos**	Los equipos deben estar ubicados de forma segura y protegidos	No	No Aplica	Excluido	No Aplica	No se han definido controles específicos para la ubicación de equipos. No se cuenta con mobiliario especializado (racks, gabinetes). No se han identificado incidentes por ubicación inadecuada.	No Aplica
	7.9	**Seguridad de los activos fuera de las instalaciones**	Los activos fuera del sitio deben protegerse	No	No Aplica	Excluido	No Aplica	No se dispone de políticas de uso remoto. Se considera en caso de habilitar trabajo remoto en el futuro.	No Aplica
	7.10	**Medios de almacenamiento**	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación	Si	UAF, UL, URH, UTI	En implementación	Buena Práctica	Protección de datos en tránsito y reposo, Prevención de exposición visual, Prevención de pérdida o alteración. Aplicar inmutabilidad a la información almacenada en el NAS. Se aplicará la característica de inmutabilidad en el servidor de almacenamiento NAS. Se resguardarán los activos de información físicos relevantes en un ambiente de acceso restringido. Se encriptará el disco de almacenamiento externo.	A008, A009, A011, A012, A022, A030
	7.11	**Servicios de suministro de apoyo**	Las instalaciones de procesamiento de información deben protegerse de cortes de energía y otras interrupciones causadas por fallas en los servicios de suministro de apoyo	No	No Aplica	Excluido	No Aplica	La infraestructura eléctrica depende del Coworking. No se han implementado medidas contra cortes de energía. No se han identificado interrupciones críticas recientes.	No Aplica
	7.12	**Seguridad del cableado**	Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra interceptaciones, interferencias o daños	No	No Aplica	Excluido	No Aplica	La red principal es wireless por lo que los cables de datos son mínimos. La infraestructura eléctrica depende del Coworking. No se han identificado incidentes por manipulación de cables.	No Aplica
	7.13	**Mantenimiento de equipos**	El equipo debe mantenerse correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información	No	No Aplica	Excluido	No Aplica	Los equipos de usuarios son laptops alquiladas, las cuales cuentan con SLA y tiempos de respuesta ante cualquier incidencia como parte del contrato. El mantenimiento se realiza de forma correctiva y reactiva. No se han identificado fallas recurrentes.	No Aplica
	7.14	**Eliminación segura o reutilización de equipos**	Los elementos del equipo que contienen medios de almacenamiento deben verificarse para asegurar de que los datos sensibles y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización	No	No Aplica	Excluido	No Aplica	Como parte del servicio de alquiler de laptops, se realiza un procedimiento de eliminación de datos al momento de realizar la devolución de cualquier equipo. La eliminación se realiza de forma manual.	No Aplica
	8.1	**Dispositivos terminales del usuario**	La información almacenada, procesada o accesible a través de los dispositivos terminales de usuario debe protegerse	Si	UEB	En implementación	Tratamiento Riesgo	Protección de endpoints, Control de acceso físico y lógico, Prevención de malware y pérdida de datos. Se instalará un software antimalware XDR en los equipos de usuario. Se implementará mejoras en el acceso a equipos de usuario mediante la configuración de credenciales complejas.	A018–A021, A033
	8.2	**Derechos de acceso privilegiados**	La asignación y el uso de derechos de acceso privilegiado deben restringirse y administrarse	Si	UTI	En implementación	Tratamiento Riesgo	Control de cuentas críticas, Prevención de abusos de privilegios, Reducción de errores humanos. Se aplicará el doble factor de autenticación a las credenciales de administradores de Microsoft 365. Se revisarán los privilegios de "Propietario" en Sharepoint Online.	A001–A007, A024, A027, A028, A031, A032
	8.3	**Restricción de acceso a la información**	El acceso a la información y a otros activos asociados debe restringirse de acuerdo con la política específica establecida sobre el control de acceso	Si	UTI	En implementación	Tratamiento Riesgo	Aplicación del principio de mínimo privilegio, Reducción de superficie de ataque, Reducción de errores humanos. Se aplicará el mínimo privilegio a las cuentas de usuario conforme a las aplicaciones que requiera utilizar. Se aplicará el doble factor de autenticación a las credenciales de administradores de Microsoft 365.	A027, A031
	8.4	**Acceso al código fuente**	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las librerías de software debe administrarse adecuadamente	No	No Aplica	Excluido	No Aplica	No se realiza desarrollo de software propio. No se han identificado riesgos asociados a esta actividad. No se cuenta con personal de desarrollo. No aplica al contexto operativo de la UEB.	No Aplica
	8.5	**Autenticación segura**	Se deben implementar tecnologías y procedimientos de autenticación seguros en función de las restricciones de acceso a la información y la política específica sobre control de acceso	Si	UTI	En implementación	Tratamiento Riesgo	Fortalecimiento de mecanismos de acceso, Prevención de accesos no autorizados, Reducción de superficie de ataque. Se aplicará las configuraciones para la autenticación segura mediante el doble factor de autenticación a las credenciales de usuarios de Microsoft 365. Se aplicará las configuraciones para la autenticación segura mediante el doble factor de autenticación en Procura Digital y SyPro.	A001–A007, A016–A021, A024–A026, A028, A030, A032, A034

Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI

	Fecha de Elaboración	1/08/2025		Autor	Omar Manuel Huarcaya Lima

	Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
Controles	8.6	Gestión de capacidad	El uso de recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados	Si	UTI	En implementación	Buena Práctica	Prevención de interrupciones por disponibilidad de recursos, Planificación de recursos, Garantizar disponibilidad de servicios. Se realizará monitoreo del uso y/o consumos de los recursos disponibles en Microsoft 365 y Sharepoint Online. Se realizará monitoreo del uso y/o consumo de recursos del servidor NAS.	A001–A007, A025
	8.7	Protección contra programas maliciosos (malware)	La protección contra programas maliciosos (malware) debe implementarse y respaldarse mediante la toma de conciencia adecuada del usuario	Si	UTI	En implementación	Tratamiento Riesgo	Prevención de infecciones, Reducción de impacto operativo, Protección de endpoints. Se instalará un software de protección contra programas maliciosos, antimalware que opere como unr XDR en los equipos. Se incorporará este tema en el Plan de concientización en seguridad de la información dirigido a todo el personal.	A001–A007, A016, A017, A023, A024, A033
	8.8	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas	No	No Aplica	Excluido	No Aplica	Los sistemas utilizados son provistos por terceros (Congreso, Microsoft). No se realiza desarrollo de software propio. No se han identificado riesgos asociados a esta actividad. No se cuenta con personal de desarrollo. No aplica al contexto operativo de la UEB.	No Aplica
	8.9	Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse	Si	UTI, URH	En implementación	Buena Práctica	Control de cambios no autorizados, Reducción de errores de configuración, Prevención de recuperación no autorizada. Se revisará con la URH las configuraciones del SISPER y Software de Asistencia. Se monitoreará que la URH realice los respaldos de configuración en repositorios seguros.	A023, A033
	8.10	Eliminación de información	La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria	Si	UTI	En implementación	Buena Práctica	Protección de datos sensibles, Reducción de fugas de información, Prevención de recuperación no autorizada. Se gestionará con los proveedores que en el momento de realizar la devolución de equipos alquilados, estos pasen por un procedimiento de eliminación de información a nivel lógico, incluyendo credenciales.	A027, A030, A031
	8.11	Enmascaramiento de datos	El enmascaramiento de datos debe utilizarse de acuerdo con la política específica de la organización sobre control de acceso, otras políticas específicas relacionadas y los requisitos del negocio, teniendo en cuenta la legislación aplicable	No	No Aplica	Excluido	No Aplica	Los sistemas utilizados son provistos por terceros (Congreso, Microsoft). No se realiza desarrollo de software propio. No se han identificado riesgos asociados a esta actividad. No se cuenta con personal de desarrollo. No aplica al contexto operativo de la UEB. No se gestionan bases de datos propias con información sensible. No se cuenta con herramientas de enmascaramiento.	No Aplica
	8.12	Prevención de fuga de datos	Las medidas de prevención de fuga de datos deben implementarse a los sistemas, redes y otros dispositivos que procesan, almacenan o transmitan información sensible	No	No Aplica	Excluido	No Aplica	No se han implementado herramientas DLP. No se han identificado incidentes de fuga de información. Se considera en la fase de madurez del SGSI.	No Aplica
	8.13	Copia de seguridad de la información	Las copias de respaldo de la información, el software y los sistemas deben mantenerse y probarse regularmente de acuerdo con la política específica sobre copias de seguridad	Si	UTI, OI	En implementación	Tratamiento Riesgo	Recuperación ante pérdida de datos, Cumplimiento de continuidad operativa, Protección ante ransomware. Se realizarán copias de seguridad a los 5 sites de Sharepoint Online (nube) mediante el uso de herramientas disponibles. Se monitoreará que la OI y OGP realicen los respaldos de información de las aplicaciones que tienen instalados en sus equipos (Revit, S10, Primavera, Autocad, Ms Project).	A001–A007, A010, A014–A017, A023–A026, A029, A030, A032, A033, A034
	8.14	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir los requisitos de disponibilidad	Si	UTI	En implementación	Buena Práctica	Asegurar disponibilidad de servicios de respaldo, Protección ante ransomware, Mejora de resiliencia operativa. Se implementará el servidor NAS con redundancia a nivel de paridad de discos de almacenamiento para realizar de manera óptima el respaldo de información, así también la implementación debe contemplar redundancia a nivel de fuente de alimentación.	A025, A030
	8.15	Registro	Se deben producir, almacenar, proteger y analizar los registros que guarden actividades, excepciones, fallas y otros eventos relevantes	No	No Aplica	Excluido	No Aplica	No se cuenta con herramientas de logging centralizado. No se han identificado incidentes que requieran trazabilidad. No se dispone de infraestructura para almacenamiento local de logs. Se considera en la implementación de herramientas de monitoreo.	No Aplica
	8.16	Actividades de monitoreo	Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y tomar acciones para evaluar posibles incidentes de seguridad de la información	Si	UTI	En implementación	Buena Práctica	Detección temprana de incidentes, Registro de eventos críticos, Mejora de la capacidad de respuesta. Se monitoreará el servicio de Internet incluyendo el firewall, con énfasis en el sistema de asistencia. Se monitoreará la consola de administración del XDR, con énfasis en SISPER. Se monitoreará la Plataforma de Administración de Microsoft 365, con énfasis en el módulo Defender.	A023, A033

	CONGRESO REPÚBLICA / UEB	**Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI**

	Fecha de Elaboración	1/08/2025	**Autor**	Omar Manuel Huarcaya Lima	

	Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
Tecnológicos	**8.17**	**Sincronización de reloj**	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse para fuentes de tiempo aprobadas	No	No Aplica	Excluido	No Aplica	La infraestructura tecnológica de la UEB depende de servicios provistos por el Congreso de la República, incluyendo la configuración de red y servidores, por lo que no se tiene control directo sobre la sincronización horaria. La criticidad de los activos de información gestionados por la UEB no requiere, en esta etapa, una precisión horaria estricta para efectos de trazabilidad o auditoría. Se prioriza la implementación de controles de mayor impacto en la confidencialidad, integridad y disponibilidad de la información, considerando los recursos técnicos y humanos limitados.	No Aplica
	8.18	**Uso de programas de utilidad privilegiados**	Se debe restringir y controlar estrictamente el uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones	No	No Aplica	Excluido	No Aplica	No se han identificado programas de utilidad privilegiados en uso dentro de la infraestructura tecnológica de la UEB. Las actividades administrativas y técnicas se realizan mediante herramientas estándar provistas por el Congreso de la República o por proveedores certificados, sin requerir herramientas que puedan anular controles de seguridad. La infraestructura tecnológica aún se encuentra en fase de consolidación, por lo que se prioriza la implementación de controles básicos y preventivos. Este control será reevaluado en futuras etapas del SGSI conforme se amplíe el alcance operativo y tecnológico de la entidad.	No Aplica
	8.19	**Instalación de software en sistemas operativos**	Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos	No	No Aplica	Excluido	No Aplica	No se han definido procedimientos formales para la instalación segura de software en los sistemas operativos utilizados por la UEB. Las instalaciones se realizan de forma manual y bajo demanda, sin un proceso estandarizado ni herramientas de gestión centralizada. Además, la infraestructura tecnológica es limitada y no se cuenta con un entorno de pruebas o validación previo a la instalación. Este control será considerado en una etapa posterior del SGSI, cuando se disponga de mayor madurez operativa y recursos técnicos adecuados.	No Aplica
	8.20	**Seguridad de redes**	Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en sistemas y aplicaciones	Si	UTI	En implementación	Buena Práctica	Protección del perímetro, Segmentación de tráfico, Prevención de accesos no autorizados. Se gestionará para que en la configuración del Firewall se activen el IPS e IDS. Se controlará mediante la Seguridad Gestionada las posibles intrusiones o ataques. Se implementarán las redes internas con distintos niveles de acceso.	A001–A007, A010, A016, A017, A024, A030, A032, A034
	8.21	**Seguridad de servicios de red**	Deben identificarse, implementarse y monitorearse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red	Si	UTI	En implementación	Buena Práctica	Aseguramiento de comunicaciones, Protección de integridad y confidencialidad, Prevención de accesos no autorizados. Se implementará una red privada virtual (VPN) para que el acceso remoto de usuarios se realice de manera segura. Se monitoreará la seguridad gestionada a nivel de intrusiones o ataques bloqueados en la red perimetral.	A001–A007, A024
	8.22	**Segregación de redes**	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización	Si	UTI	En implementación	Buena Práctica	Aislamiento de entornos críticos, Reducción de propagación de amenazas, Mejora de control de tráfico. Se implementarán redes segregadas con distintos niveles de acceso para usuarios, servicios, administradores de los servicios y visitantes.	A025, A027, A031
	8.23	**Filtrado de la web**	El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso	Si	UTI	En implementación	Buena Práctica	Prevención de acceso a sitios maliciosos, Control de navegación del usuario, Reducción de errores humanos. Se implementará el filtrado web en la red con políticas de navegación para los usuarios para reducir la exposición a contenido malicioso.	A024–A026, A030
	8.24	**Uso de criptografía**	Debe definirse e implementarse reglas para el uso eficaz de la criptografía, incluída la gestión de claves criptográficas	No	No Aplica	Excluido	No Aplica	No se cuenta con infraestructura de clave pública (PKI). No se han definido políticas de uso de criptografía.	No Aplica
	8.25	**Ciclo de vida de desarrollo seguro**	Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas	No	No Aplica	Excluido	No Aplica	No se realiza desarrollo de software propio. No se cuenta con entornos de desarrollo internos. No se dispone de personal de desarrollo. No aplica al contexto operativo de la UEB.	No Aplica
	8.26	**Requisitos de seguridad de la aplicación**	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones	No	No Aplica	Excluido	No Aplica	La infraestructura tecnológica de la UEB depende de servicios provistos por el Congreso de la República, incluyendo la seguridad de las aplicaciones, por lo que no se tiene control directo sobre las mismas. No se desarrollan aplicaciones propias. Las aplicaciones utilizadas son adquiridas a terceros.	No Aplica
	8.27	**Arquitectura de sistemas seguros y principios de ingeniería**	Los principios de ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistema de información	No	No Aplica	Excluido	No Aplica	La infraestructura tecnológica de la UEB depende de servicios provistos por el Congreso de la República, incluyendo la arquitectur de los sistemas, red y servidores, por lo que no se tiene control directo sobre la misma. No se realiza diseño de sistemas internos. No se cuenta con personal de arquitectura de sistemas. No se han identificado proyectos que lo requieran.	No Aplica
	8.28	**Codificación segura**	Los principios de codificación segura deben aplicarse al desarrollo de software	No	No Aplica	Excluido	No Aplica	No se realiza desarrollo de software. No se cuenta con programadores como parte del staff. No se dispone de entornos de desarrollo. No aplica al contexto actual de la UEB.	No Aplica

Anexo 4 - DECLARACIÓN DE APLICABILIDAD DEL SGSI

Fecha de Elaboración	1/08/2025		**Autor**	Omar Manuel Huarcaya Lima	

Código NTP ISO/IEC 27001:2022	Nombre del control de seguridad NTP ISO/IEC 27001:2022	Descripción del Control o del Objetivo de control	Control Seleccionado (Si/No)	Responsable(s) del Control	Estado del control: Implementado, En Implementación, Excluido	Justificación: Buena práctica, Requisito Legal, Tratamiento de Riesgo, No Aplica	Detalle de la Justificación / Actividad de Aplicación del Control	Activos de Información
8.29	**Pruebas de seguridad en desarrollo y aceptación**	Los procesos de pruebas de seguridad deben definirse y implementarse en el ciclo de vida del desarrollo	No	No Aplica	Excluido	No Aplica	No se desarrollan aplicaciones internamente. No se cuenta con entornos de prueba.	No Aplica
8.30	**Desarrollo subcontratado**	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados	No	No Aplica	Excluido	No Aplica	No se realiza desarrollo de software. No se ha contratado desarrollo de software a terceros.	No Aplica
8.31	**Separación de los entornos de desarrollo, prueba y producción**	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos}	No	No Aplica	Excluido	No Aplica	No se realiza desarrollo de software. No se realiza desarrollo ni pruebas internas. No se dispone de infraestructura para ambientes separados. No aplica al modelo operativo actual de la UEB.	No Aplica
8.32	**Gestión de cambios**	Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios. Se implementarán disposiciones para la solicitud de cambios en los accesos, privilegios, permisos en Sharepoint Online	Si	UTI	En implementación	Buena Práctica	Control de modificaciones en los servicios, Reducción de errores operativos, Control de modificaciones en los accesos.	A029
8.33	**Información de las pruebas**	La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente	No	No Aplica	Excluido	No Aplica	No se realiza desarrollo de software. No se cuenta con entornos de prueba. No aplica al entorno actual de la UEB.	No Aplica
8.34	**Protección de los sistemas de información durante las pruebas de auditoría**	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente	No	No Aplica	Excluido	No Aplica	La infraestructura tecnológica de la UEB depende de servicios provistos por el Congreso de la República, incluyendo los sistemas de información, red y servidores, por lo que no se tiene control directo sobre la protección de los sistemas ante pruebas de auditoria o análisis de vulnerabilidades. No aplica al entorno actual de la UEB.	No Aplica