LINEAMIENTOS PARA LA IMPLEMENTACIÓN, OPERACIÓN Y MEJORA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL CONGRESO DE LA REPÚBLICA

Directiva - DI	17-2024-DTI-DGA-CR
Versión:	PRIMERA VERSIÓN
Nº páginas:	19
Órgano responsable:	Departamento de Tecnologías de la Información

DESCRIPCIÓN	CARGO O PUESTO	FIRMA
EN SEÑAL DE CONFORMIDAD	OFICIAL MAYOR	Firmado digitalmente por: FORNO FLOREZ Giovanni Carlo Antonio FAU 20161749126 soft Motivo: En señal de conformidad Fecha: 10/09/2024 15:48:03-0500
	DIRECTOR GENERAL PARLAMENTARIO	Firmado digitalmente por: ABENSUR PINASCO Jaime Americo FAU 20161749126 soft Motivo: En señal de conformidad Fecha: 03/09/2024 09:27:04-0500
	DIRECTOR GENERAL DE ADMINISTRACIÓN	Firmado digitalmente por: PAIS VERA Carlos Luis FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 02/09/2024 15:33:29-0500
	JEFE DE LA OFICINA LEGAL Y CONSTITUCIONAL DEL CONGRESO	Firmado digitalmente por: TORRES SARAVIA Jorge Luis FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 28/08/2024 15:49:16-0500
	JEFE DEL DEPARTAMENTO DE GESTIÓN DOCUMENTAL	Firmado digitalmente por: RAMOS PAULETT Julian Saul FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 27/08/2024 12:59:35-0500
	JEFA DE LA OFICINA DE PARTICIPACIÓN CIUDADANA	Firmado digitalmente por: BETETA RUBIN Karina Juliza FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 27/08/2024 10:56:40-0500

DESCRIPCIÓN	CARGO O PUESTO	FIRMA
EN SEÑAL DE CONFORMIDAD	JEFA DEL DEPARTAMENTO DE RECURSOS HUMANOS	Firmado digitalmente por: FIGUEROA VALDEZ Haidy Janette FAU 20161749126 soft Motivo: En señal de conformidad Fecha: 27/08/2024 11:30:13-0500
	JEFE DEL DEPARTAMENTO DE TECNOLOGIAS DE LA INFORMACIÓN	Firmado digitalmente por: MARTINEZ ASENJO Richard Jackson FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 26/08/2024 14:10:16-0500
	JEFE DE LA OFICINA DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN	Firmado digitalmente por: ALCANTARA INFANTES William Federico FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 26/08/2024 14:14:50-0500
VISTO BUENO	JEFA DEL ÁREA DE MODERNIZACIÓN	Firmado digitalmente por: SARAVIA BONIFACIO Celia Antonia FAU 20161749126 hard Motivo: Doy V° B° Fecha: 26/08/2024 11:18:44-0500

1. OBJETIVO

Establecer y definir los lineamientos para la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en el Congreso de la República, así como la identificación y mitigación de los riesgos, la protección de datos e información crítica y la garantía de la integridad, confidencialidad y disponibilidad de la información manejada en el Congreso de la República.

2. FINALIDAD

Lograr que el Congreso de la República gestione la información de manera segura y eficiente cumpliendo con las normativas nacionales e internacionales de seguridad de la información, con un enfoque de mejora continua de los procesos de gestión de la información que brinde a los ciudadanos datos precisos, actualizados y seguros.

3. ALCANCE

Las disposiciones establecidas en la presente directiva son de aplicación y cumplimiento obligatorio de la Oficialía Mayor, del Departamento de Tecnologías de la Información, de la Oficina de Planeamiento, Presupuesto y Modernización, del Comité de Gobierno y Transformación Digital, del Oficial de Seguridad de Confianza Digital, del Comité de Gestión de Seguridad de la Información, del Equipo de Respuesta ante Incidentes de Seguridad Digital; así como de los dueños de los procesos y responsables de los órganos y unidades orgánicas.

4. BASE LEGAL

4.1 Reglamento del Congreso de la República.
4.2 Acuerdo de Mesa Directiva No 055-2023-2024/MESA-CR, de fecha de 17 de noviembre de 2023.
4.3 Resolución No 080-2022-2023-OM-CR, por el cual se aprueba la Política General de Seguridad de la Información del Congreso de la República.
4.4 Resolución No 002-2024-2025-OM-CR, que aprueba la Directiva 10-2024-AM-OPPM-OM-CR, "Elaboración de documentos normativos del Servicio Parlamentario del Congreso de la República – Segunda Versión.
4.5 Decreto de Urgencia No 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
4.6 Decreto de Urgencia No 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
4.7 Decreto Legislativo No 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
4.8 Decreto Supremo No 050-2018-PCM, que aprueba la definición de Seguridad Digital en el ámbito nacional.
4.9 Decreto Supremo No 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo No 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
4.10 Decreto Supremo No 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia No 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

4.11 Resolución Ministerial No 166-2017-PCM, que modifica el artículo 5 de la R.M. No 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
4.12 Resolución Ministerial No 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, las mismas que modifica los artículos 1 y 2 de la Resolución Ministerial No 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
4.13 Resolución Ministerial No 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
4.14 Resolución Directoral No 022-2022-INACAL/DN, que aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros, entre los que se encuentra la 'NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición.
4.15 Resolución de Secretaría de Gobierno y Transformación Digital No 003-2023-PCM/SGTD, por el cual se establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
4.16 Resolución de Secretaría de Gobierno y Transformación Digital No 002-2023-PCM/SGTD, que aprueba la Directiva N.001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
4.17 Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital.
4.18 Guía para el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.

5. RESPONSABILIDADES

5.1 El Oficial Mayor (en adelante OM) es responsable de la implementación del SGSI. Debe aprobar y asegurar el cumplimiento de las políticas, objetivos y planes para implementar, operar, mantener y mejorar el SGSI.

5.2 El Comité de Gobierno y Transformación Digital (en adelante CGTD) es responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI. Asimismo, emite opinión y recomendaciones sobre la gestión estratégica del SGSI.

5.3 El Oficial de Seguridad y Confianza Digital (en adelante OSCD) es responsable de coordinar, de manera transversal, la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) en el Congreso de la República; asimismo, de emitir informes a la Oficialía Mayor, quien a su vez informa a la Mesa Directiva de los avances y dificultades en la implementación u operación del SGSI. El rol del OSCD recae en un servidor del Congreso de la República designado por el titular de la Institución, con conocimiento, experiencia profesional y formación según el Anexo 01. El perfil profesional es evaluado por el Departamento de Recursos Humanos.

5.4 El Auditor Líder del Sistema de Gestión de Seguridad de la Información es responsable de liderar el equipo de auditores. Tiene como misión principal llevar a cabo el proceso de auditoría interna dentro de la organización. Entre sus principales funciones está la planificación y dirección de todas las actividades de auditoría. Esto incluye la elaboración del programa anual de auditorías del Sistema de Gestión de Seguridad de la Información (SGSI). Además, es el encargado de convocar y llevar a cabo las reuniones de apertura y cierre de las auditorías internas, durante las cuales se acuerdan los plazos para resolver las no conformidades que se hayan detectado.

5.5 El Comité de Gestión de Seguridad de la Información (en adelante CGSI) está encargado de realizar la implementación y mantenimiento del SGSI en el Congreso de la República, apoyar en la gestión de riesgos y proponer las mejoras al SGSI. El CGSI es un equipo de trabajo técnico y multidisciplinario, conformado por representantes del Departamento de Tecnologías de la Información, Oficina de Planeamiento, Presupuesto y Modernización, Oficina Legal y Constitucional del Congreso y Departamento de Recursos Humanos, que cumplen con los requisitos del Anexo 02 y formalizado por Resolución de OM. Asimismo, es liderado por el OSCD.

5.6 El Equipo de Respuestas ante Incidentes de Seguridad Digital (en adelante ERISD) es un equipo técnico conformado por especialistas en seguridad de las tecnologías de la información que cumplen con los requisitos del Anexo 03, con roles específicos y especiales, que son propuestos por el Departamento de Tecnologías de la Información y formalizado por la OM. Este equipo es liderado por el responsable de gestionar los incidentes de seguridad digital. De ser necesario, coopera con equipos reguladores y fuerzas del orden.

5.7 El jefe del Departamento de Tecnologías de la Información es responsable de informar al OSCD sobre todo incidente de seguridad digital crítico de forma inmediata. Asimismo, articula con el OSCD la implementación de controles de seguridad de la información y coordina con el ERISD la gestión de incidentes de seguridad digital.

5.8 La Oficina de Planeamiento, Presupuesto y Modernización apoya al OSCD con el asesoramiento técnico en la elaboración de los documentos normativos relacionados, así como en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y presupuestal.

5.9 Los órganos o unidades orgánicas del Servicio Parlamentario del Congreso de la República, así como los dueños de los procesos, son responsables de apoyar en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así también coadyuvan en la gestión de incidentes según corresponda. Dicha gestión se realizará en coordinación con el OSCD.

6. DISPOSICIONES GENERALES

6.1. Implementación del Sistema de Gestión de Seguridad de la Información

El Congreso de la República hace uso de la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del SGSI y establece los alcances necesarios para los procesos misionales y aquellos relevantes para la operación y funcionamiento de la Institución.

6.2. Articulación de la seguridad de la información

6.2.1. El Comité de Gobierno y Transformación Digital es responsable de vigilar la implementación, mantenimiento y documentación del Sistema de Gestión de Seguridad de la Información, para lo cual debe gestionar la asignación de personal y recursos necesarios.

6.2.2. Los riesgos e incidentes de seguridad de la información incluyen los riesgos e incidentes de seguridad digital. Su gestión es responsabilidad de la Alta Dirección, el Departamento de Tecnologías de la Información, el Oficial de Seguridad y Confianza Digital, el Oficial de Datos Personales, el Coordinador del Equipo de Respuesta ante Incidentes de Seguridad Digital (ERISD), los dueños de los procesos y los propietarios de los riesgos.

6.3. Funciones adicionales en el cumplimiento de los roles en materia de seguridad de la información

6.3.1. Oficial de Seguridad y Confianza Digital

6.3.1.1. Coordina la implementación, operación, mantenimiento y mejora continua del SGSI de la Institución, en el marco de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

6.3.1.2. Coordina con los órganos y unidades orgánicas de la Institución las acciones orientadas a implementar y mantener el SGSI.

6.3.1.3. Formula y propone políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.

6.3.1.4. Propone medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.

6.3.1.5. Informa a la Oficialía Mayor acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las

auditorías de seguridad de la información internas o externas realizadas anualmente a la Institución.

6.3.1.6. Planifica y coordina la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales.

6.3.1.7. Coordina con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en temas relativos a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la Institución.

6.3.1.8. Coordina con los dueños de los procesos, propietarios de riesgos y responsables de los órganos y unidades orgánicas su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.

6.3.1.9. Asegura y supervisa la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos.

6.3.2. Líder del Equipo de Respuestas ante Incidentes de Seguridad Digital

6.3.2.1. Comunica al Comité de Gobierno y Transformación Digital, al Oficial de Seguridad y Confianza Digital y al Departamento de Tecnologías de la Información todo incidente de seguridad digital.

6.3.2.2. Implementa la gestión de incidentes en la Institución.

6.3.2.3. Adopta medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos.

6.3.2.4. Coordina la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la Institución.

6.3.2.5. Difunde alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital.

6.3.2.6. Monitorea el estado y los accesos de la infraestructura tecnológica y mantiene la disponibilidad de sus recursos dentro de las restricciones y excepciones fijadas.

6.3.2.7. Asegura acciones de investigación e inteligencia de amenazas, respecto a nuevas vulnerabilidades que puedan afectar a la Institución.

6.3.2.8. Gestiona los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.

6.3.2.9. Solicita a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.

6.3.2.10. Coordina y colabora con redes de confianza establecidas con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital.

7. DISPOSICIONES ESPECÍFICAS

7.1. Planificación Anual del SGSI

El Plan Anual del Sistema de Gestión de Seguridad de la Información (SGSI) es el documento clave que establece los lineamientos para la administración anual del SGSI en el Congreso de la República; Este plan, propuesto por el Oficial de Seguridad y Confianza Digital, es aprobado por el Comité de Gobierno y Transformación Digital. Dicho plan debe incluir:

7.1.1. Objetivos anuales del SGSI: definidos para ser alcanzados dentro del año, alineados con los objetivos estratégicos del PEI del Congreso de la República y los requisitos de la norma NTP-ISO/IEC 27001:2022.

7.1.2. Detalle de actividades a desarrollar: descripción detallada de las acciones que se realizan durante el año para la mejora y mantenimiento del SGSI.

7.1.3. Asignación de recursos: definir los recursos humanos, materiales y financieros a ser asignados para cada actividad propuesta en el plan.

7.1.4. Cronograma: establecer un calendario detallado con fechas límite para la ejecución de las actividades.

7.2. Gestión de Riesgos del SGSI

La gestión de riesgos en el ámbito de la seguridad de la información es un proceso, integral y estructurado para la protección eficaz de los activos de información y la continuidad de las operaciones a cargo del Comité de Gestión de Seguridad de la Información; entre otros aspectos incluye:

7.2.1. Establecimiento del contexto del riesgo: comprensión del entorno del Congreso, tanto interno como externo, y definir el alcance del proceso de gestión de riesgos. Se debe identificar los activos de información clave, entender los requisitos legales y técnicos, y reconocer el entorno de amenazas y vulnerabilidades específicas.

7.2.2. Identificación de riesgos: realización de un análisis para identificar posibles riesgos que afecten la seguridad de la información en el

Congreso. Esto incluye amenazas como ataques cibernéticos, errores humanos, fallos técnicos y brechas de seguridad.

7.2.3. Análisis y evaluación de riesgos: se hace uso de enfoques cualitativos y cuantitativos para entender el impacto potencial y la probabilidad de ocurrencia de cada riesgo, lo que ayuda a priorizarlos y a tomar decisiones informadas para su tratamiento.

7.2.4. Tratamiento de riesgos: se seleccionan y aplican medidas para mitigar, transferir, aceptar o evitar los riesgos. Esto puede incluir la implementación de controles de seguridad adicionales, la revisión de políticas y procedimientos, y la educación y capacitación del personal. En esta etapa es necesaria la participación de los dueños de los procesos involucrados en el SGSI.

7.2.5. Monitoreo y revisión continuos: los riesgos y las estrategias de tratamiento se monitorean y revisan regularmente para asegurar su eficacia y para adaptarse a cambios en el entorno y en la organización. Esto incluye la revisión regular de los sistemas de seguridad y la evaluación continua de la eficacia de las políticas y procedimientos.

7.2.6. Comunicación y consulta: se debe mantener una comunicación efectiva y una consulta continua con todas las partes interesadas, incluyendo la Alta Dirección y los empleados.

7.3. Implementación y Operación del SGSI

Durante la implementación y operación del SGSI, el Oficial de Seguridad y Confianza Digital asegura que se ejecutan los objetivos de seguridad de la información, con las siguientes acciones:

7.3.1. Implementación de controles y medidas de mitigación

7.3.1.1. Supervisar la implementación de los controles seleccionados por parte de los órganos y unidades orgánicas responsables de los procesos que estén dentro del alcance del SGSI; se basa en los resultados del análisis de riesgos. Esto incluye la aplicación de sistemas de cifrado, procedimientos de autenticación, políticas de acceso a la información y otros controles necesarios.

7.3.1.2. Verificar la efectividad y adecuación de los controles implementados en relación con los riesgos identificados; los ajusta cuando es necesario para garantizar su eficiencia.

7.3.2. Capacitación y concientización del personal

7.3.2.1. Organizar sesiones de capacitación y concientización para todo el personal involucrado en el SGSI del Congreso, cubriendo las políticas y procedimientos de seguridad de la información.

7.3.2.2. Enfatizar la importancia de la seguridad de la información y el papel de cada individuo en la protección de los activos de información, fomentando una cultura de seguridad.

7.3.3. Integración de la seguridad en los procesos operativos

7.3.3.1. Integrar las prácticas y procedimientos de seguridad de la información en las actividades diarias y los procesos operativos del Congreso.

7.3.3.2. Verificar que la seguridad de la información sea una consideración prioritaria en la adquisición de nuevos sistemas informáticos, en el desarrollo de políticas de teletrabajo y en la gestión de relaciones con terceros.

7.3.4. Evaluación y ajuste continuo

7.3.4.1. Monitorear y evaluar continuamente la efectividad de los controles de seguridad implementados y la conciencia de seguridad en el personal.

7.3.4.2. Realizar actualización y mejoras, según sea necesario, para mantener la seguridad de la información alineada con los objetivos del SGSI y las cambiantes condiciones y amenazas.

7.4. Supervisión y Revisión del SGSI

Para medir y evaluar el éxito de las actividades llevadas a cabo durante la implementación y operación del SGSI que proporcione una comprensión clara y detallada de su eficacia y eficiencia, el Oficial de Seguridad y Confianza Digital debe llevar a cabo las siguientes acciones:

7.4.1. Auditorías internas y externas

7.4.1.1. Coordinar con el auditor líder e interno del Congreso, el inicio del ciclo de auditorías internas; establecer el calendario anual que identifique los ámbitos y procesos del SGSI a auditar. Esto debe basarse en una evaluación de riesgos y en la importancia estratégica de los diferentes elementos del SGSI.

7.4.1.2. El auditor interno debe encontrarse capacitado y ser objetivamente independiente del área auditada para llevar a cabo las auditorías; esto garantiza la imparcialidad y la eficacia del proceso de revisión. Asimismo, debe documentar hallazgos, evidencias y cualquier desviación o incumplimiento detectado durante la auditoría, facilitando así la trazabilidad y la rendición de cuentas.

7.4.1.3. El Oficial de Seguridad y Confianza Digital debe programar auditorías externas para ser realizadas por instituciones independientes y acreditadas, al menos una vez al año, con el fin de proporcionar una perspectiva objetiva sobre la efectividad y el cumplimiento del SGSI.

7.4.2. Revisión y supervisión de incidentes de seguridad

7.4.2.1. Implementar un proceso para la recopilación y análisis sistemático de los incidentes de seguridad, incluyendo la identificación de causas raíz y el impacto de los incidentes.

7.4.2.2. Utilizar los resultados del análisis para identificar oportunidades de mejora en los controles y procedimientos de seguridad, y ejecutar las acciones correctivas pertinentes.

7.4.2.3. Supervisar los reportes que realiza el Líder del ERISD, a efectos de coadyuvar a la mejora de los procesos de mitigación de incidentes.

7.4.3. Monitoreo y medición del rendimiento del SGSI

7.4.3.1. Establecer indicadores clave de rendimiento (KPIs) y métricas específicas para evaluar la eficacia del SGSI, incluyendo el análisis del número y la gravedad de los incidentes de seguridad, el tiempo de respuesta a los incidentes y el grado de cumplimiento con las políticas de seguridad.

7.4.3.2. Efectuar el seguimiento continuo de los indicadores, proporcionando informes periódicos al Comité de Gobierno y Transformación Digital y a la Alta Dirección para su revisión.

7.5. Mejora continua del SGSI

Esta etapa garantiza que el SGSI permanezca efectivo y relevante frente a las amenazas y desafíos en seguridad de la información; En tal sentido, el Oficial de Seguridad y Confianza Digital debe realizar las siguientes acciones:

7.5.1. Implementación de mejoras

Revisar y actualizar las políticas y procedimientos existentes, la introducción de nuevos controles de seguridad, y la optimización de los controles ya existentes, asegurando su gestión de forma estructurada y orientada a la optimización del SGSI.

7.5.2. Actualización de la evaluación de riesgos y la declaración de aplicabilidad

7.5.2.1. Revisar y actualizar regularmente la evaluación de riesgos y la Declaración de Aplicabilidad[1] para reflejar el dinamismo del entorno de seguridad de la información.

7.5.2.2. Asegurar que el SGSI se mantenga alineado con el panorama actual de riesgos y que los controles aplicados continúen siendo pertinentes y eficaces.

[1] Documento formado por la relación completa de los controles de seguridad de la información evaluables, que se indican en el anexo A de la NTP ISO/IEC 27001:2022. En ella se indica si cada uno de estos controles es de aplicación o no, y se detallan los motivos y su estado de implantación.

7.5.3. Formación y sensibilización continua

Mantener la formación y sensibilización sobre seguridad de la información como procesos continuos en toda la organización, adaptándose a nuevos riesgos y cambios en el SGSI.

7.5.4. Revisión y ajuste del plan anual del SGSI

Revisar y, de ser necesario, actualiza el Plan Anual del SGSI, a efectos de asegurar que el plan mantenga su relevancia y efectividad para orientar las actividades de seguridad de la información durante el año.

7.5.5. Acciones correctivas y preventivas

Planificar y ejecutar acciones correctivas y preventivas en base a los resultados obtenidos de la evaluación de mejoras, auditorías y revisiones de incidentes.

7.6. Revisión por el Comité de Gobierno y Transformación Digital

La revisión del SGSI por el CGTD es esencial para garantizar que el sistema cumpla con sus objetivos iniciales y se mantenga alineado con las metas estratégicas y operativas del Congreso de la República. El OSCD debe informar semestralmente el estado del SGSI, teniendo en cuenta lo siguiente:

7.6.1. Evaluación del desempeño del SGSI

7.6.1.1. El CGTD ejecuta evaluaciones periódicas del desempeño del SGSI.

7.6.1.2. Revisa informes de auditoría, resultados de las mediciones de rendimiento y reportes de incidentes de seguridad para obtener una visión integral de la eficacia del SGSI.

7.6.1.3. Analiza si los objetivos del SGSI están siendo alcanzados y su contribución a los objetivos generales del Congreso de la Republica.

7.6.2. Aseguramiento de la alineación estratégica

7.6.2.1. Verifica que el SGSI esté alineado con las metas y objetivos estratégicos del Congreso.

7.6.2.2. Actualiza el SGSI para responder a cambios en la dirección estratégica o en el entorno operativo, asegurando su apoyo a la misión y visión del Congreso de la Republica.

7.6.3. Identificación de oportunidades de mejora

7.6.3.1. Identifica oportunidades de mejora tanto en la seguridad de la información como en la eficiencia y eficacia de su gestión.

7.6.3.2. Evalúa la inversión en nuevas tecnologías, cambios en procesos o políticas y mejoras en la capacitación y sensibilización del personal.

7.6.4. Provisión de recursos

Asegura que el SGSI disponga de los recursos necesarios para su operación efectiva y mejora continua, incluyendo el personal y recursos necesarios.

7.6.5. Fomento de una cultura de seguridad de la información

Promueve una cultura de seguridad de la información en todo el Congreso de la República mediante campañas de sensibilización con el apoyo de la Alta Dirección.

7.7. Registro y Documentación

El registro y la documentación son fundamentales para el mantenimiento y mejora del SGSI, lo que proporciona una base sólida para la transparencia, la rendición de cuentas y la eficacia en la gestión de la seguridad de la información. El Oficial de Seguridad y Confianza Digital debe considerar lo siguiente:

7.7.1. Incluir registros de evaluación de los riesgos, decisiones sobre la implementación de controles, incidentes de seguridad, acciones tomadas en respuesta y resultados de auditorías y revisiones.

7.7.2. Asegurar que las políticas de seguridad, procedimientos operativos, la Declaración de Aplicabilidad y manuales de capacitación estén organizados y sean fáciles de consultar para todos los involucrados.

7.7.3. Revisar y actualizar constantemente la documentación del SGSI, con el objetivo de contar con los cambios en los entornos de amenazas, tecnología y procesos mediante revisiones regulares.

7.7.4. Implementar el control de versiones de la documentación del SGSI para garantizar que todos los usuarios tengan acceso a la última versión de los documentos.

8. DISPOSICIONES FINALES

Los aspectos que no se encuentren previstos en la presente directiva, serán analizados y resueltos por el Departamento de Tecnologías de la Información y el Oficial de Seguridad y Confianza Digital.

9. VIGENCIA

La presente Directiva entra en vigencia a partir del día siguiente de su publicación.

10. ANEXOS

N.º DE ANEXO	DETALLE
ANEXO 01	PERFIL DEL OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL
ANEXO 02	COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
ANEXO 03	EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DIGITAL

ANEXO 01

PERFIL DEL OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL

I. Conocimientos

a) Regulación nacional y estándares internacionales en seguridad y confianza digital

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

b) Aplicación y uso de tecnologías digitales

- Metodologías, buenas prácticas y marcos de referencia para establecer procesos de desarrollo de software o sistemas de información seguros.
- Sistemas y plataformas para gestionar el acceso de usuarios a los sistemas de información o plataformas digitales, así como de arquitecturas y sistemas de seguridad de red y perimetral.

II. Formación

a) Grado o formación académica

Titulado en ingeniería de sistemas o ingeniería de sistemas e informática, ingeniería informática o ingeniería de software o ingeniería electrónica o ingeniería de redes y comunicaciones o ingeniería de telecomunicaciones o ingeniería industrial o ciencias de la computación o ramas afines a la materia.

Estudios de maestría en seguridad de la información o seguridad informática o derecho digital o auditoría de seguridad de la información o protección de datos personales.

b) Diplomatura

- Diplomatura en auditoría de seguridad de la información.
- Diplomatura en seguridad de la información.
- Diplomatura en protección de datos personales o privacidad.
- Diplomatura en gestión de proyectos.
- Diplomatura en transformación digital o gobierno digital.
- Diplomatura en gestión de incidentes de seguridad de la información.
- Diplomatura en seguridad en redes, sistemas y aplicaciones.
- Otras diplomaturas afines a los especificados anteriormente.

c) Certificaciones

- Certificado en "ISO/IEC 27001 Lead Implementer" o "Certified Information Security Manager (CISM)".

- Contar con al menos dos (2) de las siguientes certificaciones vigentes:
  - Certified Information Systems Auditor (CISA).
  - Certified Data Privacy Solutions Engineer (CDPSE).
  - Certified Information System Security Professional (CISSP).
  - Certified Penetration Testing Engineer (CPTE).
  - Certified Professional Ethical Hacker (CPEH).
  - Certified in Cybersecurity Certification (CC).
  - ISO/IEC 27001 Lead Auditor.
  - ISO/IEC 27005 o ISO/IEC 31000 Lead Risk Manager.
  - ISO/IEC 27032 Lead CyberSecurity Manager.
  - ISO/IEC 27035 Lead Implementer.
  - ISO/IEC 22301 Lead Implementer.

d) Experiencia profesional

Profesional con dos (02) años desempeñando roles o cargos como director o jefe de Seguridad de la Información, oficial de Seguridad de la Información u oficial de Seguridad Digital o afines en instituciones públicas o privadas.

ANEXO 02

COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La conformación de un equipo de trabajo técnico multidisciplinario es esencial para alcanzar los objetivos de esta normativa de manera efectiva por las siguientes razones:

- Diversidad de habilidades y conocimientos: un equipo multidisciplinario aporta una amplia gama de habilidades y conocimientos cruciales para abordar los diversos aspectos de la seguridad de la información que abarca la NTP-ISO/IEC 27001:2022.
- Gestión de riesgos efectiva: la identificación, evaluación y tratamiento de riesgos requieren de perspectivas variadas que solo un equipo multidisciplinario puede ofrecer.
- Cumplimiento normativo: para cumplir con todos los requisitos de la NTP-ISO/IEC 27001:2022, es necesario contar con expertos en diferentes áreas como legal, TI, seguridad y gestión de procesos.
- Mejora continua: un equipo diverso favorece la innovación y la mejora continua en el SGSI, elementos fundamentales de la NTP-ISO/IEC 27001:2022.

La propuesta de conformación de dicho equipo debe ser elevada al Comité de Gobierno y Transformación Digital para su evaluación y, de ser aprobado, se formaliza con resolución de OM; el comité estaría conformado por:

- Oficial de Seguridad y Confianza Digital.
- Coordinador y Gestor de Incidentes en Seguridad Digital.
- Auditor en Seguridad de la Información.
- Representante de la Oficina Legal y Constitucional del Congreso.
- Representante de la Oficina de Planeamiento, Presupuesto y Modernización.
- Representante del Departamento de Recursos Humanos.
- Representantes del Departamento de Tecnologías de la Información y sus áreas dependientes.

ANEXO 03

EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL

Un equipo de respuestas ante incidentes de seguridad digital es un equipo técnico conformado principalmente por especialistas en seguridad de las tecnologías de la información o informática. En tal sentido, es responsabilidad de esta área o la que haga sus veces, la determinación de las responsabilidades del ERISD mediante la designación de los roles relevantes. La responsabilidad se define en función del perfil del equipo y su autoridad; de esta manera, puede cooperar incluso con equipos reguladores y fuerzas del orden.

Los roles básicos son:

a. Líder del ERISD: es responsable de efectuar las coordinaciones necesarias para el fortalecimiento de las capacidades de respuesta a incidentes en el Congreso de la República, para lo cual realiza todas las actividades de gestión del ERISD y de la gestión de los incidentes de seguridad digital, así como también de la comunicación del incidente al Comité de Gobierno y Transformación Digital.

b. Gestor de Redes y Comunicaciones: es responsable de la seguridad de redes de comunicación de la Institución. Implementa medidas de cifrado para la protección de la confidencialidad de las comunicaciones y determina el modelo de monitorización de estas.

c. Gestor de Infraestructuras Digitales: es responsable de la seguridad de los servidores e infraestructuras de nube; determina las reglas de seguridad a nivel del sistema operativo y aplicaciones.

d. Oficial de Seguridad y Confianza Digital: participa como miembro del ERISD para realizar las funciones de apoyo en la gestión de incidentes y articulador de los ámbitos de seguridad y confianza digital que sean relevantes al incidente.

e. Otros roles que se determinen.

11. ÍNDICE

página

Congreso de la República
Oficialía Mayor

RESOLUCIÓN N° 020 -2024-2025-OM-CR

Lima, 12 de setiembre de 2024

VISTOS:

El Acta 009-2024-CR/CGTD, Acta de la Novena Sesión del Comité de Gobierno y Transformación Digital del Congreso de la República, los Memorando N° 460-2024-DTI-DGA-CR y N° 593-2024-DTI-DGA-CR del jefe del Departamento de Tecnologías de la Información, el Informe N° 196-2024-AM-OPPM-OM-CR de la jefa del Área de Modernización, el Memorando N° 1274-2024-OPPM-OM-CR del jefe de la Oficina de Planeamiento, Presupuesto y Modernización y el Informe N° 159-2024-AAJ-OLCC-OM-CR, del jefe del Área de Asesoría Jurídica de la Oficina Legal y Constitucional del Congreso.

CONSIDERANDO:

Que, mediante el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece el 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;

Que, en virtud del artículo 94 de la Constitución Política del Perú y los artículos 3 y 33 del Reglamento del Congreso, el Congreso de la República se encuentra facultado para autorregularse en materia de Gobierno Digital manteniendo una relación de coordinación con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros;

Que, en el marco de la autonomía administrativa que ostenta el Congreso de la República, resulta necesario aprobar, actualizar y/o modificar los instrumentos normativos internos que permitan establecer un orden administrativo en la gestión institucional;

Que, mediante el Acuerdo 055-2023-2024/MESA-CR, la Mesa Directiva del Congreso de la República, en su sesión de fecha 17 de noviembre de 2023, acordó, entre otros, disponer que la Dirección General de Administración desarrolle e implemente sus propias políticas internas de Gobierno y Transformación Digital pudiendo adoptar como marco referencial las disposiciones en materia de gobierno digital dictadas por la Secretaría de Gobierno y Transformación Digital;

Que, el Comité de Gobierno y Transformación Digital del Congreso de la República, mediante Acta N° 009-2024-CR/CGTD correspondiente a su novena sesión realizada el 31 de mayo de 2024, acordó aprobar la Directiva "Lineamientos para la implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información del Congreso de la República";

CONGRESO DE LA REPÚBLICA V°B° J. TORRES S. JEFE Oficina Legal y Constitucional

CONGRESO DE LA REPÚBLICA V°B° H. PUENTE JEFE Área de Asesoría Jurídica

Que, mediante los Memorandos N° 460-2024-DTI-DGA-CR y N° 593-2024-DTI-DGA-CR emitidos por el Departamento de Tecnologías de la Información y el Informe N° 196-2024-AM-OPPM-OM-CR, emitido por el Área de Modernización, proponen la Directiva Nº 17-2024-DTI-DGA-CR "Lineamientos para la implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información del Congreso de la República";

Que, mediante el Memorando N° 1274-2024-OPPM-OM-CR, la Oficina de Planeamiento, Presupuesto y Modernización, remite a la Oficina Legal y Constitucional del Congreso; y esta a su vez al Área de Asesoría Jurídica, la versión final del proyecto de directiva "Lineamientos para la implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información del Congreso de la República", y solicita la elaboración de la resolución respectiva para su aprobación, previa verificación de los requisitos exigidos para tal efecto;

Que, en ese sentido el Área de Asesoría Jurídica de la Oficina Legal y Constitucional del Congreso, a través del informe de vistos, señala que la versión final del proyecto de directiva cumple con los procedimientos y requisitos establecidos en la Directiva 10-2024-AM-OPPM-OM-CR "Elaboración de Documentos Normativos del Servicio Parlamentario del Congreso de la República" – Segunda Versión;

Que, es competencia del Oficial Mayor la aprobación, actualización y/o modificación de los documentos normativos internos de gestión;

CONGRESO DE LA REPÚBLICA V°B° J. TORRES S. JEFE Oficina Legal y Constitucional

De conformidad con lo establecido en el artículo 40 del Reglamento del Congreso y en el numeral 7.2.5.5 de la Directiva 10-2024-AM-OPPM-OM-CR – Segunda Versión, con las opiniones favorables de la Oficina de Planeamiento Presupuesto y Modernización, y de la Oficina Legal y Constitucional del Congreso; y

Con cargo a dar cuenta a la Mesa Directiva.

SE RESUELVE:

CONGRESO DE LA REPÚBLICA V°B° H. PUENTE JEFE Área de Asesoría Jurídica

<u>Artículo Único</u>.- APROBAR la Directiva Nº 17-2024-DTI-DGA-CR "Lineamientos para la implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información del Congreso de la República".

Regístrese, comuníquese, cúmplase y archívese.

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA