	DOCUMENTO ESPECÍFICO		
CÓDIGO: **PL-SGSI-001**		**VERSIÓN:** 01	**PÁGINA:** 01/14
		FEC. APROB: 24/01/2024	
RESOLUCIÓN DE SECRETARÍA GENERAL N° 004 –2024– ACFFAA/SG			

Firma Digital
ACFFAA
AGENCIA DE COMPRAS DE LAS F.F. A.A.
Firmado digitalmente por CASTILLO ARANSAENZ Ana Magdelyn FAU 20556939781 hard
Motivo: Doy V° B°
Fecha: 24.01.2024 17:34:11 -05:00

Firma Digital
ACFFAA
AGENCIA DE COMPRAS DE LAS F.F. A.A.
Firmado digitalmente por ALFARO CASTELLANOS Rene Ricardo FAU 20556939781 hard
Motivo: Doy V° B°
Fecha: 24.01.2024 17:21:53 -05:00

Firma Digital
ACFFAA
AGENCIA DE COMPRAS DE LAS F.F. A.A.
Firmado digitalmente por SALINAS ESPINOZA Hector FAU 20556939781 hard
Motivo: Doy V° B°
Fecha: 24.01.2024 16:28:09 -05:00

Firma Digital
ACFFAA
AGENCIA DE COMPRAS DE LAS F.F. A.A.
Firmado digitalmente por PEREZ BARRANTES Gary Lizardo FAU 20556939781 hard
Motivo: Doy V° B°
Fecha: 24.01.2024 16:54:45 -05:00

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS – ACFFAA

2024 - 2025

ÍNDICE

I. Introducción 3

II. Objetivo 4

III. Marco Legal 4

IV. Términos y definiciones 5

V. Contexto de la organización 7

VI. Mapa de procesos 7

VII. Alcance del SGSI 8

VIII. Proyecto de Implementación del Sistema de Gestión de Seguridad de la Información 8

IX. Cronograma de actividades 122

X. Recursos y presupuesto 122

XI. Monitoreo y evaluación 133

XII. Anexo 133

I. Introducción

El Instituto Nacional de Calidad (INACAL) desempeña un papel crucial en el fortalecimiento de estándares y prácticas de calidad en el ámbito nacional, promoviendo la excelencia en diversos sectores. En este contexto, la Resolución Directoral Nº 022-2022-INACAL/DN marca un hito significativo al oficializar la actualización de normativas clave en seguridad de la información. Con la aprobación del uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2022, que aborda la seguridad de la información, ciberseguridad y protección de la privacidad, el INACAL ha tomado medidas importantes para alinear las prácticas de gestión de seguridad de la información con los estándares internacionales más recientes.

Esta resolución, respaldada por la disposición establecida en el artículo 1 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD del 08 de setiembre de 2023, subraya la importancia de la Norma Técnica Peruana NTP ISO/IEC 27001:2022 como referencia esencial para todas las entidades del Estado. De acuerdo con la referida disposición, se establece la obligatoriedad de utilizar esta norma vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Este cambio refleja el compromiso del INACAL y del Estado peruano de fortalecer la seguridad de la información en consonancia con los avances más recientes en el ámbito internacional.

La Agencia de Compras de las Fuerzas Armadas (ACFFAA) es un organismo público ejecutor adscrito al Ministerio de Defensa que tiene a su cargo la contratación de servicios, consultorías, ejecuciones de obras y compras estratégicas de bienes esenciales para la Seguridad y Defensa Nacional. Su objetivo principal es optimizar los procesos del Sector Defensa, asegurando la eficiencia, transparencia y calidad en la adquisición de recursos y servicios. La ACFFAA opera conforme al Plan Estratégico de Compras del Sector Defensa, buscando economía de escala, homogeneización y estandarización en sus procesos para satisfacer las necesidades de los Órganos Bajo el Ámbito de su Competencia (OBAC). La misión de la entidad es llevar a cabo los procesos y procedimientos de contratación de los requerimientos estratégicos del Sector Defensa, mientras que su visión es ser reconocida como la institución líder en la gestión de compras, ofreciendo un servicio eficiente y de calidad para la Seguridad y Defensa Nacional. La ACFFAA tiene competencia para planificar, organizar y ejecutar procesos de contrataciones en el ámbito operativo requerido por diversas Unidades Ejecutoras y órganos del Sector Defensa.

La gestión de la seguridad de la información juega un rol muy importante en nuestra institución, manifestándose -entre otros- en la conformación de su Comité de Gobierno y Transformación Digital como estructura a cargo de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI; y que pone a disposición de sus partes interesadas el presente documento, el cual describe en forma detallada el Plan de Implementación del Sistema de Gestión de Seguridad de la Información de la entidad, precisando el alcance del programa así como las actividades y metas que se proyectan alcanzar durante los ejercicios 2024 y 2025, para cuya concreción se cuenta con la participación activa y

el compromiso de la Alta Dirección, Directores, Jefes, servidores públicos y terceros en lograr un nivel adecuado de cumplimiento de los lineamientos y requisitos previstos por la Norma Técnica Peruana NTP-ISO/IEC 27001:2022.

II. Objetivo

Implementar el SGSI en la Agencia de Compras de las Fuerzas Armadas, con el fin de preservar la confidencialidad, integridad y disponibilidad de sus activos de seguridad de la información, permitiendo identificar las vulnerabilidades y amenazas basado en la Norma Técnica Peruana NTP-ISO/IEC 27001:2022.

III. Marco Legal

- Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 29733, Ley de Protección de Datos Personales.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo Nº 030-2002-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado.
- Decreto Supremo N° 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.
- Decreto Supremo Nº 157-2021, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia Nº 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto Supremo Nº 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030.
- Resolución Ministerial Nº 087-2019-PCM, Resolución que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución Directoral N° 022-2022-INACAL/DN, Resolución que aprueba Normas Técnicas Peruanas sobre turismo, acuicultura y otros.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Resolución que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
- Resolución Jefatural N° 036-2019-ACFFAA, Resolución por la cual se reconforma el Comité de Gobierno Digital de la Agencia de Compras de las Fuerzas Armadas.

IV. Términos y definiciones

4.1. **Activo de Información:** Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa Información y tiene valor para la organización, como base de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la entidad, la Información como activo corporativo, puede existir de muchas formas (impresa, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en videos, suministrada en una conversación, conocimiento de las personas).

4.2. **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel de una organización.

4.3. **Amenazas:** Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

4.4. **Análisis de riesgo:** método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

4.5. **Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permite determinar la extensión en que se cumplen los criterios definidos para la auditoria interna.

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

4.7. **Comité de Gobierno y Transformación Digital:** Es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las entidades de la ad-ministración pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad.

4.8. **Compromiso:** Participación activa y en contribución a las actividades para lograr objetivos compartidos.

4.9. **Control:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de la organización.

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

4.11. **Confidencialidad:** Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados.

4.12. **Declaración de Aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el Sistema de Gestión de Seguridad de la Información de la entidad.

4.13. **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

4.14. **Eficacia:** Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

4.15. **Evaluación del riesgo:** Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado de riesgo.

4.16. **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar los aspectos asociados al riesgo dentro de una organización.

4.17. **Información:** Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

4.18. **Integridad:** En seguridad de la información, es salvaguardar la exactitud e integridad de la información y activos asociados.

4.19. **Norma Técnica:** Para los efectos del presente Plan, se refiere a la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 y demás estándares que conforman la familia ISO 27000.

4.20. **Oficial de Seguridad y Confianza Digital:** Para los efectos del presente Plan, se refiere al rol y responsabilidad que tiene el servidor designado como Oficial de Seguridad y Confianza Digital de la ACFFAA, para coordinar la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información – SGSI de la entidad.

4.21. **Proceso:** Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

4.22. **Responsabilidades:** Compromisos u obligaciones del personal o grupo de trabajo.

4.23. **Riesgo:** Consecuencias que pueden ser generadas por las amenazas asociadas a la Seguridad de la Información en los activos de la organización.

4.24. **Secretaría de Gobierno y Transformación Digital (SGTDI):** Unidad organizacional de la Presidencia del Consejo de Ministros que ejerce la rectoría del Sistema Nacional de Transformación Digital en el país y en las materias de Gobierno, Confianza y Transformación Digital, siendo la autoridad técnico-normativa a nivel nacional en dichas materias. Asimismo, es el Líder Nacional de Gobierno Digital responsable del proceso de transformación digital en el país y dirección estratégica del Gobierno Digital en el Estado Peruano.

4.25. **Seguridad de la Información (SI):** Es preservar la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.

4.26. **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 éstos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de Ciberseguridad, y acciones de colaboración y cooperación.

4.27. **Transformación Digital:** Es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intenso de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

4.28. **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.

4.29. **Vulnerabilidad:** Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

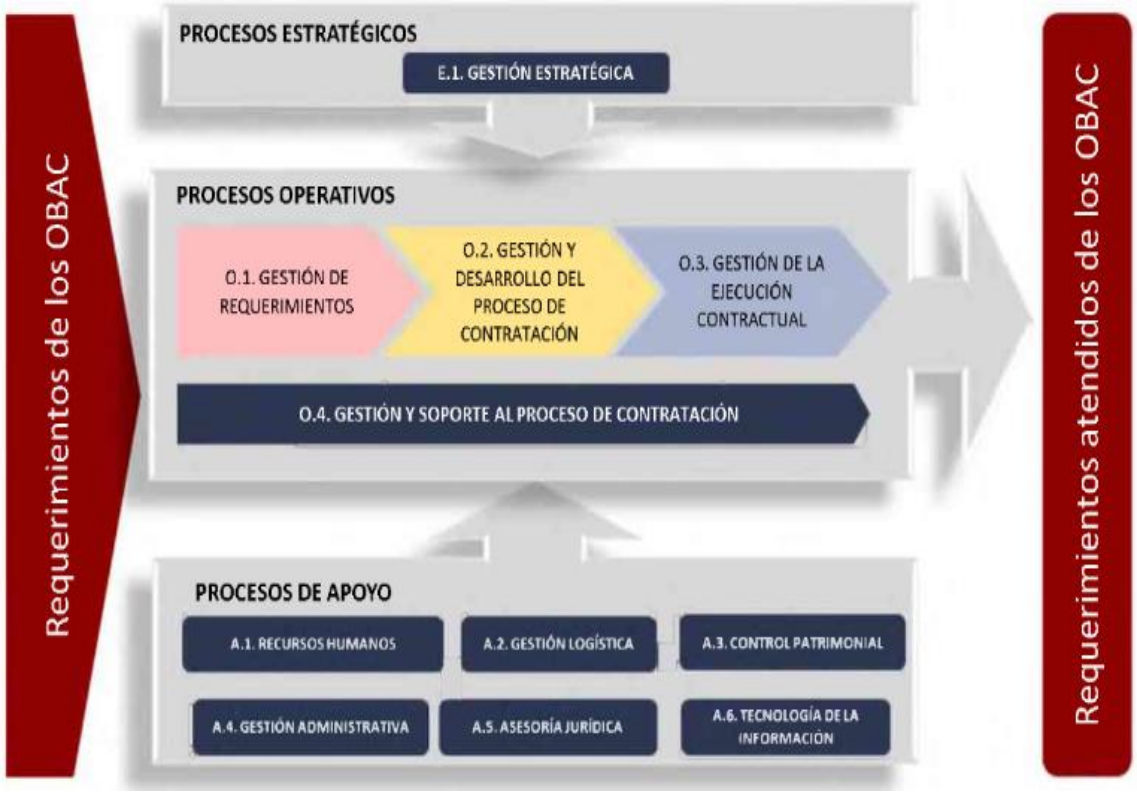
V. Contexto de la organización

En esta etapa, como requisito de su SGSI, la ACFFAA dispondrá de los documentos siguientes, lo que permitirá comprender la organización y su contexto interno y externo, así como conocer de las necesidades y expectativas de las partes interesadas, y establecer las políticas de liderazgo respectivas:

- Análisis de contexto externo.
- Análisis de contexto interno.
- Requerimiento de partes interesadas.
- Política de seguridad de la información.
- Roles y responsabilidades.

VI. Mapa de procesos

La ACFFAA ha determinado los procesos estratégicos, operativos y de apoyo sobre los que el SGSI interviene. Los procesos se visualizan en el Mapa de Procesos siguiente:



Fuente: *Resolución de Secretaría General N° 17-2019-ACFFAA/SG*

VII. Alcance del Sistema de Gestión de Seguridad de la Información

La ACFFAA determinara los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información, mediante la evaluación de la organización y su contexto, y la compresión de las necesidades y expectativas de las partes interesadas. Esta actividad se ejecutará de acuerdo al cronograma adjunto al presente Plan.

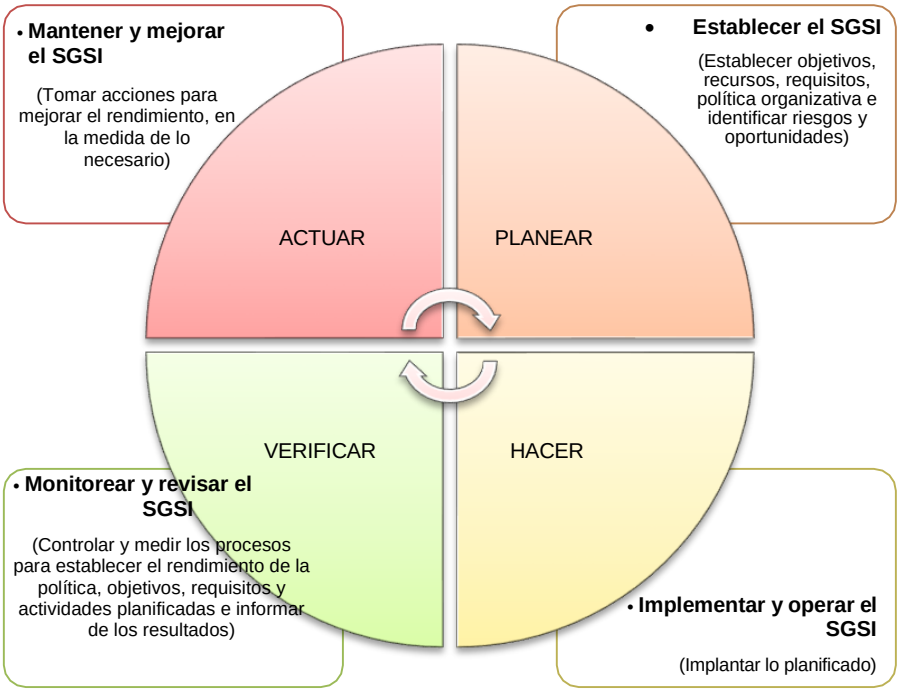
VIII. Proyecto de Implementación del Sistema de Gestión de Seguridad de la Información

8.1 Metodología

La metodología está basada en el ciclo PDCA o ciclo de Deming como enfoque a la mejora continua de los procesos, donde se establecen las fases de planificar, implementar, verificar y actuar del SGSI, las cuales están relacionadas a la Norma ISO 27001 que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información.

Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiéndose como tal al mejoramiento continuo del SGSI (disminución de incidentes, aumento de la eficacia, solución de problemas, previsión y disminución de riesgos potenciales, etc.).

Esta metodología describe:



8.2 Documentos del SGSI

Durante la implementación del SGSI, se elaborarán y/o actualizarán las propuestas de los siguientes documentos, en caso se requiera, sin perjuicio de otros que consideren pertinentes:

- **Alcance del Sistema de Gestión de Seguridad de la Información:** Lineamiento o documento que define el alcance del SGSI, en función a los procesos, funciones, activos, ubicaciones físicas, tecnología, partes interesadas y la determinación de los aspectos internos y externos a la organización.
- **Política de Seguridad de la Información:** Documento clave que define la forma en que la Institución controla la gestión de la seguridad de la información.
- **Metodología de evaluación y tratamiento de riesgos:** Documento que describe los métodos, procedimientos y parámetros que se deben emplear para la evaluación y tratamiento de riesgos de la información.

- **Informe sobre evaluación de riesgos y tratamiento del riesgo:** Documento que incluye toda la información generada en el proceso de evaluación y tratamiento de riesgos, incluido la matriz de riesgos y el plan de tratamiento de riesgos, donde se detallan los controles de seguridad a aplicar, los responsables, los plazos, entre otros temas relacionados.
- **Declaración de Aplicabilidad:** Documento que determina los objetivos y la necesidad u obligatoriedad de cada control establecido en el Anexo A de la norma ISO 27001.
- **Programa de Concientización y Entrenamiento en Seguridad de la Información:** Documento que determina la metodología de concientización, entrenamiento y educación a ser aplicado a todo el personal de la ACFFAA a fin de crear cultura en seguridad de la información.
- **Directiva de Control de Acceso al Data Center:** Documento que establece los lineamientos de seguridad para el control de acceso al ambiente del Data Center.
- **Procedimiento para control de Documentos y Registros:** Documento que establece las reglas básicas para la redacción, aprobación, distribución y actualización de documentos y registros.

8.3 Organización para la implementación del SGSI

Para la implementación de su SGSI, la ACFFAA se organizará de la siguiente manera:

- **Titular de la Entidad:** Es responsable de la implementación del SGSI, para lo cual, como mínimo, debe aprobar las políticas y objetivos para implementar, operar, mantener y mejorar el SGSI.
- **Máxima Autoridad Administrativa:** Es la encargada de informar semestralmente al Titular de la entidad los avances y dificultades en la implementación u operación del SGSI, así como el cumplimiento de la presente Resolución. Asimismo, es responsable de asegurar el cumplimiento de las políticas, objetivos, planes, procedimientos y marco normativo en materia de seguridad y confianza digital en la entidad pública.
- **Comité de Gobierno y Transformación Digital:** Es responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI. Asimismo, a solicitud del Titular de la entidad o la máxima autoridad administrativa emite opinión y recomendaciones sobre la gestión estratégica del SGSI. Sin perjuicio de lo indicado la entidad puede solicitar opinión a un órgano consultivo vinculado a la gestión de riesgos de la entidad.
- **Oficial de Seguridad y Confianza Digital:** Gestionará las acciones necesarias para la implementación del SGSI y realizará las

coordinaciones con el grupo de trabajo para la adopción de las medidas aprobadas.

- **Oficina de Informática:** Conformado por el Jefe, los especialistas y técnicos de los diferentes equipos internos de trabajo de dicha Oficina; quienes coordinarán con el Oficial de Seguridad y Confianza Digital a fin de implementar controles relacionados al control de acceso, criptografía, seguridad de las operaciones y comunicaciones, adquisición, desarrollo y mantenimiento de sistemas, entre otros temas propios de su función.
- **Grupo de Trabajo:** Equipo conformado por los representantes que designen los responsables de las unidades de organización de la ACFFAA, quienes coordinarán y apoyarán en los diversos aspectos de la implementación del SGSI en asistencia al Comité de Gobierno y Transformación Digital.

8.4 Riesgos del plan de implementación del SGSI

La implementación del SGSI implica un cambio de cultura organizacional, por ende, es relevante el compromiso integral de todo el personal y de las unidades de organización involucradas en el proyecto.

En ese sentido, los posibles riesgos que se puede enfrentar al momento de ejecutar las actividades enmarcadas son los siguientes:

- La Alta Dirección y el Comité de Gobierno y Transformación Digital podrían llegar a niveles no óptimos de apoyo y compromiso a la transformación digital.
- Los procesos de las unidades de organización podrían no interiorizar el alcance del SGSI.
- Limitación de presupuesto para la implementación del plan de tratamiento de riesgos resultante del proceso de análisis de riesgos.
- Los servidores y las unidades de organización de la entidad podrían no alcanzar niveles óptimos que demuestren estar comprometidos con la seguridad de la información.
- Los servidores que implementan los controles podrían no mantener niveles de capacitación y no se garantice la implementación de los controles de manera efectiva.

8.5 Acciones previas y permanentes

Para el inicio de la implementación del SGSI, se requieren efectuar las siguientes acciones:

- Seguimiento a las acciones de implementación por la Alta Dirección y el Comité de Gobierno y Transformación Digital.
- Sensibilización al personal de la ACFFAA sobre los alcances del SGSI.

- Análisis de brechas de seguridad de la información.
- Identificación de procesos y procedimientos.
- Fortalecimiento de las capacidades del Oficial de Seguridad y Confianza Digital en los temas de ISO 27001, ISO 27002, ISO 27032, ISO 31000, entre otras.

Durante la implementación del SGSI, se deben realizar las siguientes acciones:

- Fortalecimiento de las capacidades de los responsables de la implementación del SGSI, en los temas relativos a los “Fundamentos de Seguridad de la Información” y la “Protección de Datos Personales”.
- Realización de *Ethical Hacking*, en intervalos de mínimo de tres (03) meses para determinar vulnerabilidades o intrusión a los sistemas informáticos.
- Realización de Auditoría Informática especializada que permita establecer indicadores de cumplimiento y de gestión.

8.6 Herramientas de apoyo al SGSI

Todos los documentos se crearán empleando herramientas ofimáticas, dado que no se cuenta con una aplicación que automatice el Sistema de Gestión de Seguridad de la Información; sin embargo, se requiere la continuidad de la plataforma de análisis de vulnerabilidad.

Se creará una carpeta compartida en la red local donde se almacenarán las actas y los documentos generados durante la implementación del SGSI.

Todos los miembros del equipo a cargo de la implementación tendrán acceso a esos documentos en modo lectura. Únicamente el Oficial de Seguridad y Confianza Digital se encuentra autorizado a editar los datos.

Se empleará el sistema de gestión documental SGD como plataforma de comunicaciones para uso interno así como el correo institucional, para desplegar las acciones de concientización de seguridad de la información.

IX. Cronograma de actividades

Las actividades son detalladas en el Anexo del presente Plan.

X. Recursos y presupuesto

Las actividades consideradas en el presente Plan no requieren financiamiento, son de costo cero.

XI. Monitoreo y evaluación

El proceso de monitoreo y evaluación del Plan de Implementación de Seguridad de la Información de la ACFFAA se realizará en el marco de la Norma Técnica Peruana NTP-ISO/IEC 27001:2022.

Semestralmente, deberá emitirse un Informe conteniendo los avances en la ejecución de las actividades previstas en el presente Plan.

XII. Anexo

Anexo “Cronograma de actividades del Plan de Implementación del SGSI – ACFFAA 2024-2025”.

CUADRO DE CONTROL DE CAMBIOS DE LOS DOCUMENTOS

DETALLE	VERSIÓN	FECHA
Versión inicial del documento	01	24/01/2024