POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, DEL PROGRAMA NACIONAL “A COMER PESCADO”

Política y Objetivo de Seguridad de la Información

PROGRAMA NACIONAL “A COMER PESCADO”

Junio 2023

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 21:19:49-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:55:48-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:30:07-0500

Firmado digitalmente por: PUENTE DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:23:17-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:18:49-0500

Ciclo de Aprobación

Rol	Nombre	Firma	Fecha
Creado por:	Sub Unidad de Abastecimiento		2023
Revisado por:	Comité de Gobierno Digital		2023
Aprobado por:	Coordinación Ejecutiva		2023

Historia de Cambios

Versión (Estado)	Autor	Descripción del Cambio	Fecha

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 21:22:45-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:30:42-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:56:16-0500

Firmado digitalmente por: GUERRE DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:23:29-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:19:03-0500

TABLA DE CONTENIDO

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 21:30:24-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:31:09-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:56:56-0500

Firmado digitalmente por: GUERRA DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:23:48-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:19:12-0500

1 OBJETIVO

Mediante la presente Política de Seguridad de la Información, se establece el marco general de gestión para proteger adecuadamente la información institucional, asegurar el compromiso de la Coordinación Ejecutiva, llevar a cabo un tratamiento adecuado de los riesgos y promover una cultura en seguridad de la información.

2 ALCANCE

La presente políticas y las disposiciones que se inmersa en el marco de esta, son obligatorias para todo el personal del Programa Nacional "A Comer Pescado", independientemente del régimen laboral o vínculo contractual al que se encuentren sujetos, así como para el personal de terceros contratados por el Programa Nacional "A Comer Pescado", en tanto realicen tareas o tengan acceso información, mientras que se desempeñen sus labores en el Programa Nacional "A Comer Pescado".

Las elaboraciones de las Políticas de Seguridad de la Información están fundamentadas bajo la norma Técnica Peruana "NTP ISO/IEC 27001:2014, han sido planteadas, analizadas y revisadas con el fin de no contravenir con las garantías básicas de los usuarios, y pretende ser una forma de operar los sistemas con seguridad, respetando en todo momento estatutos y reglamentos internos de Programa Nacional "A Comer Pescado".

3 BASE LEGAL

- Ley del Marco de Modernización de la Gestión del Estado – Ley N°27658, que establece el cumplimiento de funciones y evaluación de resultados en el marco del proceso de modernización de la gestión del Estado y sus modificatorias.
- Decreto de Urgencia Nº 007-2020, que aprueba el marco de confianza digital.
- Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Resolución Ministerial N° 246-2007-PCM, Aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Códigos de buenas prácticas para la gestión de la seguridad de la información. 2do Edición".
- Resolución Ministerial N° 004-2016-PCM, Aprueba 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 Información". Requisitos. 2da Edición, en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial Nº 041-2017-PCM, aprueban 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.

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 21:47:29-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:31:36-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:57:28-0500

Firmado digitalmente por: GUERRA DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:23:59-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:19:21-0500

- Resolución de Coordinación Ejecutiva Nº009-2022-PNACP, creación del Comité de Gobierno y Transformación Digital del Programa Nacional "A Comer Pescado".

4 DEFINICIONES Y SIGLAS

A continuación, se describe algunas de las definiciones y siglas que es utilizado en el contexto del Plan de Trabajo de Sistemas de Gestión de la Seguridad de la Información.

- **PNACP**: Programa Nacional "A Comer Pescado"
- **SGSI:** Sistema de Gestión de Seguridad de la Información, en ingles el acrónimo usado es ISMS.
- **IEC:** Comisión Electrotécnica Internacional.
- **ISO:** Organización de Estándares Internacionales.
- **NTP:** Norma Técnica Peruana.
- **PNACP:** Programa Nacional A Comer Pescado.
- **Activo de Información:** Bien o servicio tangible o intangible, que genera, procesa, almacena información, transmite y/o sirve de soporte de la información, necesaria para la operación y el cumplimiento de los objetivos de la organización.
- **Propietario de Activo de Información:** Individuo de forma responsable, que cuenta con la aprobación de la Coordinación Ejecutiva, para el control del desarrollo, mantenimiento, utilización y seguridad de los activos. El término propietario no significa que la persona disponga de los derechos de propiedad reales del activo.

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 21:35:37-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:32:00-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:57:57-0500

Firmado digitalmente por: GUERRA DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:24:09-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:19:30-0500

5 PRINCIPIOS

Los siguientes principios constituyen los fundamentos de base para cualquier acción, en materia de seguridad de la información, sobre los activos de información.

- **Integridad:** para protegerlos de cambios indebidos o no autorizados.
- **Confidencialidad:** para mantenerlos protegidos y asegurar su correcta accesibilidad y privacidad.
- **Disponibilidad:** para que estén disponibles para su uso por parte de los usuarios autorizados toda vez que lo requieran, garantizados el acceso oportuno a la información.

6 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

a) <u>De la naturaleza y gestión de la seguridad de la información</u>
-El PNACP es un programa adscrito al Ministerio de la Producción, que considera a la información como un activo valioso para el cumplimiento de sus funciones y alcance de sus objetivos estratégicos. Por tanto, resulta necesario gestionar la seguridad de la información estableciendo mecanismos para proteger con confidencialidad, disponibilidad e integridad ante amenazas internas o externas, deliberadas o accidentales; y se compromete a cumplir con los requisitos aplicables en seguridad de la información y mejorar continuamente su SGSI.

-El PNACP establece los mecanismos para respaldar la difusión y actualización, tanto de la presente política como de los demás componentes de la Seguridad de la Información.

b) <u>De la cultura y difusión de la seguridad de la información</u>
Establecer estrategia de comunicación de seguridad de la información, para luego difundir a todo el personal del PNACP, con el fin concientizar y sensibilizar la seguridad de la información a todo el personal PNACP, que se va a difundir por medio electrónicos y/o digitales.

c) <u>De la protección y acceso a los activos de información</u>
-Resguardar los activos de información mediante controles de seguridad aplicables a partir del análisis, evaluación y tratamiento de los riesgos que afecten su confidencialidad, integridad y disponibilidad.
-Proteger la información, sus medios de procesamiento, conversación y transmisión, del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje y otras acciones que pudieran perjudicar o poner en riesgo.
-Asegurar que los propietarios de los activos de información son responsables de definir las reglas de accesos y restricciones que son requeridas; así como la revisión periódica de los derechos de acceso a los mismos.

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 21:39:59-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:32:32-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:58:42-0500

Firmado digitalmente por: GUERRA DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:24:24-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:19:40-0500

-La información confidencial contenida en documentos físicos no debe ser transferida fuera de las instalaciones del PNACP y debe ser almacenada en lugares seguros y/o gabinetes con llave evitando accesos no autorizados.

-Toda Información del PNACP debe contar con controles que eviten una alteración y/o eliminación no autorizada.

d) <u>De los sistemas de información y servicios del PNACP</u>
-Establecer control de mecanismos de seguridad de la información en el desarrollo y/o mantenimiento de la página institucional de la web y el Sistema PNACP, como el acceso al personal autorizado,

-La Sub Unidad de Abastecimiento es responsable de la seguridad de los recursos y servicios informáticos, realiza tareas de actualización periódica sobre el software de los servidores, equipos de cómputo, comunicaciones y seguridad perimetral.

-El Personal de PNACP que detecten vulnerabilidades o debilidades que puedan poner en peligro la información, recursos o servicios de TI, debe comunicar a la Sub Unidad de Abastecimiento.

e) <u>De las acciones correctivas de la seguridad de la información</u>
-Establecer medidas que permitan asegurar que las vulnerabilidades e incidentes de seguridad detectados o reportados, se gestionen de manera oportuna y se adopten las acciones correctivas para evitar su recurrencia.
-Definir los tipos de información que es manejada por las personas autorizadas dentro de la organización.

f) <u>De la continuidad y cumplimiento de la seguridad de la información</u>
-Asegurar la continuidad operacional a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.
-Dar cumplimiento a la Resolución Ministerial N° 004-2016-PCM, la cual ha aprobado el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información.
-Establecer el acceso a las copias de respaldo, que está permitido a la Sub Unidad de Abastecimiento.
-Mantener la configuración de copias de respaldo de archivos y base de datos.
-Mantener activados los logs de auditorías.

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 22:08:36-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:33:00-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:59:14-0500

Firmado digitalmente por: GUERRA DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:24:37-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:19:50-0500

7 SANCIONES

El Personal del PNACP que incumplan las disposiciones contenidas en la presente Política, incurren en falta disciplinaria que se sanciona de acuerdo a lo dispuesto en la Ley N° 27815, Ley del Código de Ética de la Función Pública; la Ley N° 30057, Ley del Servicio Civil, y su Reglamento General, aprobado mediante el Decreto Supremo N° 040-2014-PCM; y la normatividad vigente que sanciona las transgresiones a la seguridad de la información en las entidades del Estado peruano.

8 REVISIONES

La presente política se revisa por lo menos una vez al año, cuando ocurran cambios significativos que afecten al Sistema de Gestión de Seguridad de la Información, o cuando el Comité de Gobierno y Transformación Digital lo vea pertinente para asegurar su conveniencia, adecuación y eficacia continua.

9 DIFUSIÓN

La comunicación de los documentos que componen la seguridad de la información se efectúa de manera que el contenido de la documentación sea accesible y compresible para todo el personal indicado en el alcance de esta Política.

Visado por LUCAS VELARDE Elizabeth Noemi FAU 20504794637 hard
Fecha: 2023/06/28 22:11:06-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20504794637 hard
Fecha: 2023/06/28 20:33:28-0500

Visado por CHUMPITAZ VILLALOBOS Percy Gaston FAU 20504794637 hard
Fecha: 2023/06/28 19:59:44-0500

Firmado digitalmente por: GUERRE DE LA VEGA CHUMBE Felix Fabian FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:24:48-0500

Firmado digitalmente por: TORREBLANCA GARCIA Miluska Erika FAU 20504794637 hard
Motivo: Doy V° B°
Fecha: 28/06/2023 20:20:01-0500