Firma Digital
PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA

Firmado digitalmente por HINOJOSA ANGULO Fredy Hernan FAU 20550154065 hard
Cargo: Director Ejecutivo
Motivo: Soy el autor del documento
Fecha: 28.09.2022 15:48:20 -05:00

Santiago De Surco, 28 de Septiembre del 2022

RESOLUCION DIRECCION EJECUTIVA N° D000390-2022-MIDIS/PNAEQW-DE

REPÚBLICA DEL PERÚ

Resolución de Dirección Ejecutiva

VISTOS:

El Memorando Nº D000396-2022-MIDIS/PNAEQW-UTI de la Unidad de Tecnologías de la Información; el Memorando N° D002655-2022-MIDIS/PNAEQW-UPPM, de la Unidad de Planeamiento, Presupuesto y Modernización; y el Informe N° D000585-2022-MIDIS/PNAEQW-UAJ de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 008-2012-MIDIS y normas modificatorias, se crea el Programa Nacional de Alimentación Escolar Qali Warma (PNAEQW), como Programa Social del Ministerio de Desarrollo e Inclusión Social, con el propósito de brindar un servicio alimentario de calidad, adecuado a los hábitos de consumo locales, cogestionado con la comunidad, sostenible y saludable para las/los escolares de las instituciones educativas públicas bajo su cobertura;

Que, mediante Resolución de Dirección Ejecutiva N° D000289-2019-MIDIS/PNAEQW-DE, se aprueba la "Directiva para la Formulación, Modificación y Aprobación de Documentos Normativos del Programa Nacional de Alimentación Escolar Qali Warma", la cual establece disposiciones para la formulación, modificación, y aprobación de los documentos técnicos normativos que requieren los órganos del Programa Nacional de Alimentación Escolar Qali Warma para garantizar el desarrollo de sus procesos;

Firmado digitalmente por VERA DIAZ Edgar Alejandro FAU 20550154065 soft
Motivo: Doy V° B°
Fecha: 28.09.2022 15:06:12 -05:00

Que, de acuerdo a lo establecido en el literal e) del artículo 25° del Manual de Operaciones del PNAEQW aprobado por Resolución Ministerial N° 283-2017-MIDIS, la Unidad de Tecnologías de la Información es responsable de "*proponer y/o actualizar documentos normativos orientados a la gestión, planeamiento, desarrollo y seguridad de las tecnologías de información y comunicaciones del Programa, en el marco de lo dispuesto por el MIDIS y PCM. Promover y dirigir la innovación tecnológica de las infraestructuras, plataformas y sistemas informáticos*";

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 14:31:33 -05:00

Que, mediante Memorando N° D000129-2022-MIDIS/PNAEQW-UTI de fecha 31 de marzo de 2022, sustentado en el Informe N° D000067-2022-MIDIS/PNAEQW-UTI-DER, la Unidad de Tecnologías de la Información remite a la Unidad de Planeamiento, Presupuesto y Modernización el proyecto de "Lineamientos de seguridad de la información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo LIN-015-PNAEQW-UTI, Versión N° 01, elaborado en cumplimiento de lo previsto en la Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC-27001:2014 Tecnología de la

Firmado digitalmente por RAMIREZ GARRO Jose Aurelio FAU 20550154065 soft
Motivo: Doy V° B°
Fecha: 28.09.2022 14:31:11 -05:00

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;

Que, se indica en el Informe N° D000067-2022-MIDIS/PNAEQW-UTI-DER que la propuesta del referido documento normativo tendrá los siguientes beneficios: continuar con las actividades que permitan cumplir con la Resolución Ministerial N° 004-2016-PCM; proporcionar a los usuarios un instrumento normativo que oriente hacia una adecuada gestión de la seguridad de la información en el PNAEQW; cumplir con parte de los requisitos exigidos por la NTP ISO/IEC 27001:2014 Sistema de Gestión de Seguridad de la Información – SGSI a fin de certificar al Programa en la norma internacional ISO 27001:2013; y cumplir con los dispuesto en la Resolución Ministerial N° 002-2021-MIDIS que aprueba los lineamientos de seguridad de la información del MIDIS, en cuyo artículo 3 resuelve que los programas nacionales adscritos al Ministerio de Desarrollo e Inclusión Social, deben adecuar sus protocolos o lineamientos internos, a las disposiciones previstas en los lineamientos de seguridad de la información del MIDIS;

Que, con Proveído N° D004378-2022-MIDIS/PNAEQW-UPPM de fecha 19 de agosto de 2022, la Unidad de Planeamiento, Presupuesto y Modernización remite a la Unidad de Tecnologías de la Información el proyecto de documento normativo para su actualización, en el marco de la revisión efectuada al "Manual del Sistema de Gestión de la Seguridad de la Información del PNAEQW";

Que, mediante Memorando N° D000396-2022-MIDIS/PNAEQW-UTI, de fecha 08 de setiembre de 2022, la Unidad de Tecnologías de la Información remite a la Unidad de Planeamiento, Presupuesto y Modernización el Informe N° D000192-2022-MIDIS/PNAEQW-UTI-DER, indicando que se ha cumplido con la actualización del documento normativo denominado "Lineamientos de seguridad de la información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo LIN-015-PNAEQW-UTI, Versión N° 01, según lo indicado en el Proveído N° D004378-2022-MIDIS/PNAEQW-UPPM, a fin que se efectúen las gestiones correspondientes para su aprobación;

Que, en atención a ello, mediante Memorando N° D002655-2022-MIDIS/PNAEQW-UPPM, de fecha 14 de setiembre de 2022, la Unidad de Planeamiento, Presupuesto y Modernización señala que la propuesta de documento normativo cumple con los requisitos y formalidades establecidas en la "Directiva para la formulación, modificación y aprobación de documentos normativos del Programa Nacional de Alimentación Escolar Qali Warma"; asimismo, señala que la citada propuesta se enmarca y es congruente con las funciones señaladas en el Manual de Operaciones del PNAEQW, por lo que emite opinión favorable a la propuesta de documento normativo denominado "Lineamientos de seguridad de la información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo LIN-015-PNAEQW-UTI, Versión N° 01;

Que, mediante Informe N° D000585-2022-MIDIS/PNAEQW-UAJ, la Unidad de Asesoría Jurídica señala que a través de la Resolución Ministerial N° 004-2016-PCM se dispone la implementación obligatoria 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, debiendo tener en consideración que conforme a la Única Disposición Complementaria Derogatoria del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema de Transformación Digital, publicado el 09 de enero de 2020, para todos sus efectos, el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática;

Que, se indica en el Informe de la Unidad de Asesoría Jurídica que, conforme se describe en el numeral 4.1 del artículo 4 del citado Decreto de Urgencia N° 006-2020, *"El Sistema Nacional de Transformación Digital es un Sistema Funcional del Poder Ejecutivo, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos mediante los cuales se organizan las actividades de la administración pública y se promueven las actividades de las empresas, la sociedad*

civil y la academia orientadas a alcanzar los objetivos del país en materia de transformación digital." Dicho Sistema tiene como finalidad, entre otras *"Fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital fomentando la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital para la sostenibilidad, prosperidad y bienestar social y económico del país;"* (subrayado agregado). Se dispone también que los principios, normas y procedimientos que rigen la materia de Transformación Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS, (dentro de los cuales se encuentran los Programas estatales) y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia en lo que corresponda;

Que, señala también la Unidad de Asesoría Jurídica que en el Decreto de Urgencia N° 006-2020 se establece que forman parte del Sistema Nacional Transformación Digital, entre otros los Comités de Gobierno Digital de las entidades públicas a nivel nacional. En tal sentido, teniendo en cuenta que el PNAEQW, a través del Comité de Gobierno Digital creado mediante Resolución de Dirección Ejecutiva N° 357-2018-MIDIS/PNAEQW, forma parte integrante del Sistema Nacional Transformación Digital, corresponde que se adopten las acciones necesarias a fin de implementar en el Programa 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", conforme lo dispuesto en el artículo 1 de la Resolución Ministerial N° 004-2016-PCM;

Que, por otro lado, mediante Resolución Ministerial N° 002-2021-MIDIS, de fecha 07 de enero de 2021, se aprueban los *"Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social"*, estableciéndose en el artículo 3 que los Programas Nacionales adscritos a dicho Ministerio deben adecuar sus protocolos o lineamientos internos, a las disposiciones previstas en dicho documento normativo;

Que, en consecuencia se verifica que el proyecto de documento normativo se ha elaborado en concordancia con lo previsto en las normas antes citadas y, conforme a lo señalado en el literal i) del artículo 15, del Manual de Operaciones del PNAEQW, la Unidad de Asesoría Jurídica opina favorablemente a la emisión de la Resolución de Dirección Ejecutiva que apruebe el proyecto de "Lineamientos de seguridad de la información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo LIN-015-PNAEQW-UTI, Versión N° 01, propuesto por la Unidad de Tecnologías de la Información, el cual no colisiona ni se superpone a otra norma técnica sobre la materia;

Con el visado de la de la Unidad de Tecnologías de la Información, de la Unidad de Planeamiento, Presupuesto y Modernización y de la Unidad de Asesoría Jurídica;

En uso de las atribuciones establecidas en el Decreto Supremo N° 008-2012-MIDIS y normas modificatorias, la Resolución Ministerial N° 283-2017-MIDIS, y la Resolución Ministerial N° 081-2019-MIDIS;

SE RESUELVE:

Artículo 1.- APROBAR los "Lineamientos de seguridad de la información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo LIN-015-PNAEQW-UTI, Versión N° 01, el mismo que forma parte integrante de la presente resolución.

Artículo 2.- ENCARGAR a la Coordinación de Gestión Documentaria y Atención al Ciudadano, la notificación de la presente Resolución a las Unidades Territoriales, las Unidades de Asesoramiento, Apoyo, y Técnicas del Programa Nacional de Alimentación Escolar Qali Warma, a través de medios electrónicos.

Artículo 3- DISPONER que la Unidad de Comunicación e Imagen efectúe la publicación de la presente Resolución de Dirección Ejecutiva y los "Lineamientos de seguridad de la información del Programa Nacional de Alimentación Escolar Qali Warma", con código de documento normativo LIN-015-PNAEQW-UTI, Versión N° 01, en el Portal Institucional del Programa Nacional de Alimentación Escolar Qali Warma (https://www.gob.pe/qaliwarma).

Regístrese y comuníquese.

PERÚ | Ministerio de Desarrollo e Inclusión Social | Viceministerio de Prestaciones Sociales | Programa Nacional de Alimentación Escolar QALI WARMA

LINEAMIENTOS

Código de documento normativo	Versión N°	Total de páginas	Resolución de aprobación	Fecha de aprobación
LIN-015-PNAEQW-UTI	01	20	Resolución de Dirección Ejecutiva Nº D000390-2022 MIDIS/PNAEQW-DE	28 / 09 / 2022

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR QALI WARMA

ELABORADO POR:	REVISADO POR:	REVISADO POR:
Nombres y Apellidos Jefa/e de la Unidad de Tecnologías de la Información	Nombres y Apellidos Jefa/e de la Unidad de Planeamiento, Presupuesto y Modernización	Nombres y Apellidos Jefa/e de la Unidad de Asesoría Jurídica
Firma Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard Motivo: Soy el autor del documento Fecha: 28.09.2022 12:11:58 -05:00	Firma Firmado digitalmente por VERA DIAZ Edgar Alejandro FAU 20550154065 soft Motivo: Soy el autor del documento Fecha: 28.09.2022 13:07:06 -05:00	Firma Firmado digitalmente por RAMIREZ GARRO Jose Aurelio FAU 20550154065 soft Motivo: Soy el autor del documento Fecha: 28.09.2022 12:22:00 -05:00

ÍNDICE

Página

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 12:12:04 -05:00

I. Objetivo

Establecer las orientaciones a fin de conducir al Programa Nacional de Alimentación Escolar Qali Warma hacia una adecuada gestión de la seguridad de la información.

II. Alcance

Los presentes lineamientos son de cumplimiento obligatorio para todas/os las/los servidoras/es civiles del Programa Nacional de Alimentación Escolar Qali Warma y proveedoras/es, que en el ejercicio de sus funciones interactúen con los recursos y servicios de tecnologías de información del Programa.

III. Base Normativa

3.1 Ley N° 27269, Ley de Firmas y Certificados Digitales.
3.2 Ley N° 27444, Ley del Procedimiento Administrativo General.
3.3 Ley N° 29733, Ley de Protección de Datos Personales.
3.4 Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento
3.5 Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.6 Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
3.7 Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.8 Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
3.9 Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
3.10 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC-27001:2014. Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición, en todas las entidades integrantes del Sistema Nacional de Informática.
3.11 Resolución Ministerial N° 087-2019-PCM, que aprueba las disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
3.12 Resolución Ministerial Nº 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
3.13 Resolución Ministerial N° 287-2017-MIDIS, que aprueba el Manual de Operaciones del Programa Nacional de Alimentación Escolar Qali Warma.
3.14 Resolución Ministerial N° 002-2021-MIDIS, que aprueba los Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social.
3.15 Resolución Ministerial N° 00138-2021- MIDIS, que aprueba al Manual para la Gestión de Riesgos de Procesos del Ministerio de Desarrollo e Inclusión Social.
3.16 Resolución de Secretaría de Gobierno Digital 004-2018-PCM/SEGDI, que aprueba los lineamientos del Líder de Gobierno Digital.
3.17 Resolución de Dirección Ejecutiva N° 357-2018-MIDIS/PNAEQW-DE, que crea el Comité Digital del Programa Nacional de Alimentación Escolar Qali Warma y funciones.

Las referidas normas incluyen sus respectivas modificaciones y/u otra norma que la sustituya o reemplace, de ser el caso.

IV. Documentos de Referencia

4.1 DIR-023-PNAEQW-UTI, Directiva para la gestión de copias de respaldo y resguardo de la Información del Programa Nacional de Alimentación Escolar Qali Warma.

4.2 DIR-024-PNAEQW-UTI, Directiva de acceso físico al centro de datos del Programa Nacional de Alimentación Escolar Qali Warma.

4.3 PRO-003-PNAEQW-UPPM, Procedimiento para la gestión de acciones correctivas y oportunidades de mejora del Programa Nacional de Alimentación Escolar Qali Warma.

4.4 PRO-004-PNAEQW-UPPM, Procedimiento para la revisión por la Dirección del sistema de gestión de la calidad y de seguridad de la información del Programa Nacional de Alimentación Escolar.

4.5 INS-003-PNAEQW-URH, Instructivo para la administración de legajos de personal del Programa Nacional de Alimentación Escolar Qali Warma.

4.6 Norma Internacional ISO 27001: 2013, Sistema de Gestión de Seguridad de la Información.

V. Definición de Términos

5.1 Activo
Se refiere a cualquier información o elemento relacionado con el tratamiento del mismo (sistemas, soportes, edificios o personas) que tenga valor para la organización.

5.2 Código Fuente
Es un archivo o conjunto de archivos que tienen instrucciones concretas escritas en un lenguaje de programación, que posteriormente se compilan y son las directrices que debe seguir la computadora.

5.3 Comité de Gobierno Digital
Mecanismo de gobernanza responsable de la gestión digital de la entidad.

5.4 Confidencialidad
Es la propiedad de la información de no estar accesible y utilizable cuando lo requieran individuos, entidades o procesos no autorizados.

5.5 Control
Medida que la entidad establece para afrontar o responder al riesgo.

5.6 Disponibilidad
Es la propiedad de la información de estar accesible y utilizable cuando lo requiera individuos, entidades o procesos autorizados.

5.7 Documento
Información contenida en cualquier medio de soporte y que ha sido creado o recibido como información y/o prueba por el Programa Nacional de Alimentación Escolar Qali Warma en el desarrollo de sus actividades o en virtud de sus obligaciones legales.

5.8 Medio Removible
Componente extraíble de hardware que es usado para el almacenamiento de información.

5.9 Incidente de Seguridad de la Información
Se refiere a una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones de la entidad y de amenazar la seguridad de la información.

5.10 Integridad
Presunción legal por la cual un documento electrónico no ha sido alterado desde su emisión hasta su recepción.

5.11 Plataforma Tecnológica
Conjunto de componentes de arquitectura tecnológica hardware y del software que cumplen un servicio en específico.

5.12 Plan de Continuidad Operativa de Tecnologías de la Información
Plan que garantiza la continuidad de operaciones de tecnologías de la información ante sucesos adversos, sin afectar los objetivos del Programa Nacional de Alimentación Escolar Qali Warma.

5.13 Procedimiento
Documento que describe cómo deben ejecutarse las actividades que conforman los procesos, tomando en cuenta los elementos que lo componen y su secuencialidad, permitiendo de esta manera una operación coherente.

5.14 Propietaria/o del Riesgo
Persona o entidad responsable a la que se ha dado la autoridad para valorar y gestionar un riesgo en particular, por lo que debe rendir cuentas por ello.

5.15 Registro
Documento que indique los resultados obtenidos o proporcione evidencia de las actividades desempeñadas.

5.16 Riesgo
Posibilidad de que suceda algún evento adverso que afecta el logro de los objetivos de la entidad.

5.17 Seguridad de la Información
Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

5.18 Sistema de Gestión de Seguridad de la Información
Sistema de gestión para preservar la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente.

VI. Abreviaturas y Siglas

IEC	:	International Electrotechnical Commission
ISO	:	International Organization for Standardization
NTP	:	Norma Técnica Peruana
PNAEQW	:	Programa Nacional de Alimentación Escolar Qali Warma
SGSI	:	Sistema de Gestión de Seguridad de la Información
SEGDI	:	Secretaria de Gobierno Digital
UTI	:	Unidad de Tecnología de la Información

VII. Orientaciones Generales

7.1 La gestión de la seguridad de la información del PNAEQW y su implementación, debe ser revisada de forma independiente a intervalos planeados o cuando ocurran cambios significativos en el Programa.

7.2 Liderazgo y Compromiso

Siendo el PNAEQW integrante del Sistema Nacional de Informática debe adecuarse a la NTP ISO/IEC 27001:2014, por ello la Dirección Ejecutiva asume el liderazgo y compromiso de implementar un SGSI que colabore en la consecución de los objetivos estratégicos del PNAEQW, así como de velar por el cumplimiento de los presentes lineamientos.

7.3 Política de Seguridad de la Información

El PNAEQW utiliza, procesa, genera o comparte información que utiliza durante el desarrollo de sus actividades, la cual se considera como un recurso estratégico y un activo crítico; asimismo, el aseguramiento de los principios de confidencialidad, disponibilidad e integridad son primordiales para realizar con normalidad sus operaciones y actividades institucionales. Es compromiso del PNAEQW establecer, implementar, mantener y mejorar continuamente su SGSI.

7.4 Objetivos de Seguridad de la Información

7.4.1. Proteger los activos de información del PNAEQW y la tecnología utilizada para su procesamiento, frente a amenazas internas y/o externas, reduciendo los riesgos para mantener la continuidad operativa de los distintos procesos que ejecuta el PNAEQW.
7.4.2. Determinar los requerimientos de seguridad de la información del PNAEQW, a partir de los cuáles se identifiquen los controles que se deberán adoptar, para protegerse contra amenazas que podrían afectar la seguridad de la información.
7.4.3. Identificar los activos de información del PNAEQW y definir las responsabilidades y medidas de protección adecuadas.
7.4.4. Establecer una respuesta efectiva ante incidentes de seguridad de la información.
7.4.5. Implementar mecanismos de medición de seguridad de la información, en función al nivel de exposición a los riesgos y la eficacia de los controles implementados.
7.4.6. Promover la comunicación oportuna de los lineamientos de seguridad de la información y los procedimientos de seguridad establecidos, asegurando que sean comprendidos y se encuentren disponibles para todas/os las/los servidoras/es civiles del PNAEQW.
7.4.7. Concientizar al personal del PNAEQW y proveedoras/es, en el proceso de preservar la seguridad de la información.

7.5 Roles y Responsabilidad respecto a la Seguridad de la Información

El PNAEQW ha definido roles y responsabilidades del SGSI, de acuerdo a lo siguiente:

7.5.1 La Dirección Ejecutiva es responsable de:

a) Asignar la responsabilidad y la autoridad para asegurar que el SGSI esté conforme a los requisitos de la NTP-ISO/IEC 27001:2014.
b) Asignar la responsabilidad y la autoridad para reportar sobre el desempeño del SGSI.
c) Liderar la implementación del SGSI del PNAEQW.
d) Brindar los lineamientos para la disponibilidad de los recursos necesarios para el cumplimiento de los objetivos de la seguridad de la

información en el PNAEQW.

e) Nombrar al Comité de Gobierno Digital.
f) Delegar autoridad y responsabilidad a cada una de las unidades orgánicas para el cumplimiento del presente documento.

7.5.2 El Comité de Gobierno Digital es responsable de ejecutar las funciones establecidas en la Resolución de Dirección Ejecutiva N° 357-2018-MIDIS/PNAEQW que conforma el mencionado Comité.

7.5.3 La/el oficial de seguridad de la información, es responsable de:

a) Dirigir, coordinar y controlar todas las actividades relacionadas con la seguridad de la información del PNAEQW.
b) Liderar y velar por el desarrollo, implementación, mantenimiento y cumplimiento de los lineamientos, y procedimientos para promover la seguridad de la información.
c) Coordinar y proponer la agenda de las sesiones del Comité de Gobierno Digital, respecto a la gestión de seguridad de la información.
d) Registrar en actas lo actuado por el Comité de Gobierno Digital, respecto a la gestión de seguridad de la información.
e) Custodiar los registros de los acuerdos tomados en las sesiones del Comité de Gobierno Digital, respecto a la gestión de seguridad de la información.
f) Gestionar el Sistema de Gestión de Seguridad de la Información, llevando a cabo las siguientes actividades:

i. La administración operativa del SGSI:

- Presentar al Comité de Gobierno Digital, los avances en la implementación del SGSI, la gestión de los incidentes de seguridad de la información, los indicadores y métricas de desempeño del SGSI.
- Elaborar los informes de gestión del SGSI, para su revisión por el Comité de Gobierno Digital.
- Dirigir, coordinar y supervisar la implementación del SGSI
- Realizar el control de los documentos (revisión, modificación y distribución) del SGSI.
- Asegurar el mantenimiento del SGSI.
- Supervisar el funcionamiento del SGSI en cada lugar de trabajo.
- Elaborar y monitorear el cumplimiento del plan anual de implementación del SGSI.

ii. La administración de las oportunidades de mejora y gestión de riesgos:

- Registrar la oportunidad de mejora o hallazgo identificado en el proceso de auditoría.
- Realizar el seguimiento y monitoreo de las acciones propuestas para la implementación de la mejora.
- Capacitar y/o sensibilizar a las/los servidoras/es civiles del PNAEQW respecto a la metodología de la gestión de riesgos y oportunidades de procesos, en el marco del “Manual para la gestión de riesgos de procesos en el Ministerio de Desarrollo e Inclusión Social”.

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 12:12:35 -05:00

iii. Control sobre las no conformidades y oportunidades de mejora derivadas de auditorías:

- Administrar las auditorías internas (programación, ejecución, control y seguimiento del programa anual de auditorías internas).
- Distribuir las no conformidades a las/los responsables de las unidades orgánicas auditadas.
- Conducir las causas de las no conformidades identificadas en el proceso de auditoría, en coordinación con las/los responsables de las unidades orgánicas auditadas.
- Conducir la aplicación del "Procedimiento para la gestión de acciones correctivas y oportunidades de mejora del Programa Nacional de Alimentación Escolar Qali Warma", para el levantamiento de las no conformidades relacionadas al SGSI.
- Monitorear la efectividad de los planes de acción y mantener informado de los resultados obtenidos al CGD.
- Coordinar la reformulación del plan de acción para garantizar su efectividad.

iv. Apoyo en la revisión por la Dirección, en el marco del SGSI:

- Generar información sobre el mantenimiento y eficacia del SGSI para su presentación y análisis en la reunión de revisión por la Dirección.
- Elaborar las actas de los resultados de la revisión por la Dirección.
- Efectuar el seguimiento a los acuerdos de la reunión, en coordinación con las/los responsables de las unidades orgánicas.
- Ejecutar acciones en cumplimiento del "Procedimiento para la revisión por la Dirección del sistema de gestión de la calidad y de seguridad de la información del Programa Nacional de Alimentación Escolar".

g) Tomar conocimiento de los incidentes de seguridad que se presenten, con el fin de evaluar la efectividad de los controles implementados.
h) Asesorar a las distintas unidades orgánicas del PNAEQW en temas relacionados a la seguridad de la información.
i) Elaborar y/o actualizar el plan de continuidad operativa de tecnologías de la información del PNAEQW.
j) Otras funciones que se le asigne en el ámbito de su competencia.

7.5.4 La/el servidora/or civil encargada/o de la coordinación del SGSI designada/o por cada unidad orgánica involucrada dentro del alcance del SGSI es responsable de:

a) Participar en las actividades de implementación del SGSI.
b) Identificar y clasificar los activos de información, así como analizar y evaluar los riesgos de seguridad de la información siguiendo la metodología aplicada.
c) Monitorear e informar sobre la efectividad de las medidas de mitigación implantadas en su unidad orgánica.
d) Participar de las actividades de capacitación y concientización en temas relacionados al SGSI.
e) Participar en las auditorías internas y externas del SGSI.
f) Asegurar la generación oportuna y exacta de evidencias respecto a la implementación de acciones de mitigación de riesgo implementadas por su unidad orgánica.

g) Identificar y formular las acciones correctivas y oportunidades de mejora como parte del SGSI.
h) Otras funciones necesarias para garantizar la implementación del SGSI.

7.5.5 Las/los servidoras/es civiles del PNAEQW son responsables de:

a) Conocer, comprender y cumplir los lineamientos, política, procedimientos y/u otros documentos normativos de seguridad de la información del PNAEQW.
b) Notificar incidentes y riesgos de seguridad de la información a la/al jefa/e inmediata/o superior y/o a la/al oficial de seguridad de la información o quién haga sus veces.
c) Utilizar la información, sistemas y todos los recursos del PNAEQW únicamente para los propósitos autorizados e inherentes a la función asignada.
d) Reportar incumplimientos de seguridad de la información.
e) Resguardar y hacer uso adecuado de la información y los activos asociados a ella, en coordinación con las unidades orgánicas competentes para la correcta aplicación de los controles de seguridad de la información que corresponden.
f) Cumplir con las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego del término de la relación contractual con el PNAEQW.
g) Almacenar su información restringida, critica o confidencial en las unidades compartidas de red, para su respectivo respaldo.
h) Mantener en orden su área de trabajo y asegurarse que la información confidencial se encuentre en un lugar seguro cuando se ausente del lugar asignado para el desarrollo de sus funciones.
i) Verificar previamente el contenido de la información transmitida a través de cualquier medio asignado, como es el caso del correo electrónico o cualquier otro medio de difusión de mensajes empleado por el PNAEQW.
j) Evitar conectarse a internet desde Wi-Fi público a la red institucional.

7.5.6 La/el propietaria/o del riesgo es responsable de:

a) Velar por la integridad, confidencialidad y disponibilidad de la información.
b) Apoyar en la difusión de las normas relacionadas a la seguridad de la información en el PNAEQW.
c) Comunicar requerimientos de control y protección de la información a la/al oficial de seguridad de la información o quién haga sus veces.
d) Identificar los riesgos asociados a la seguridad de la información inherente a su gestión, según las normas del PNAEQW, así como solicitar el apoyo de las unidades orgánicas pertinentes para evaluar dichos riesgos y establecer medidas de mitigación.
e) Apoyar y facilitar las revisiones periódicas para la verificación del cumplimiento de las normas relacionadas a la seguridad de la información.
f) Determinar los criterios y niveles de acceso a la información de la cual son responsables y notificar el cambio de función/ubicación de cualquier/a servidor/a civil, a su cargo, sea por reasignación o retiro, con la finalidad de modificar o cancelar sus accesos.
g) Autorizar la asignación de accesos sobre la información.
h) Reportar inmediatamente el incumplimiento o infracciones a las normas relacionadas a la seguridad de la información.

7.5.7 Las/los servidoras/es civiles de la UTI, son responsables de:

a) Definir los requerimientos de seguridad de la información en coordinación con la/el oficial de seguridad de la información, tan pronto como se inicie la adquisición, desarrollo o adecuación de aplicativos y/o sistemas de información.
b) Asegurar que los requerimientos y proyectos se realicen usando métodos, técnicas y procedimientos para mantener la seguridad de la información de los mismos, garantizando la confidencialidad, integridad y disponibilidad de la información.
c) Realizar los procesos de respaldo de información, así como la creación de procesos de recuperación de acuerdo a lo coordinado con las/los propietarias/os de la información.
d) Asegurar un adecuado mantenimiento de los equipos informáticos y de los dispositivos magnéticos u ópticos utilizados para las copias de respaldo.

VIII. Acciones Prioritarias

8.1 Sobre la Organización de la Seguridad de la Información

El PNAEQW en materia de organización de seguridad de la información se compromete a:

8.1.1 Determinar los roles y funciones para la gestión de seguridad de la información, las cuales le corresponden al Comité de Gobierno Digital, a la/al oficial de seguridad de la información, propietarias/os del riesgo y a todas/os las/los servidoras/es civiles, para reducir el riesgo de modificación no autorizada o el mal uso de los activos de información del PNAEQW.

8.1.2 Mantener una lista actualizada con autoridades (es decir, de cumplimiento de la ley, organismos reguladores, autoridades de supervisión, proveedoras/es de servicios, departamento de bomberos, etc.) a contactar, a fin de reportar en el momento oportuno cualquier tipo de incidentes que comprometan a la seguridad de la información.

8.1.3 Establecer e implementar un procedimiento para la asignación de dispositivos móviles, manteniendo un adecuado control de la entrega y devolución de los mismos.

8.1.4 Establecer las disposiciones para la no divulgación de la información sensible almacenada en los dispositivos móviles, a la cual tengan acceso las/los servidoras/es civiles del PNAEQW. Asimismo, dichas disposiciones también deben estar contempladas en los acuerdos y contratos con terceros o proveedoras/es de servicios.

8.1.5 Verificar que los dispositivos móviles proporcionados por el PNAEQW cuenten con lo siguiente:

- Registro actualizado de los dispositivos móviles.
- Restricción de la instalación de software no autorizado y la conexión a una PC que no tenga actualizado su antivirus.
- Controles de acceso para servicios y aplicaciones web.
- Protección contra software malicioso.

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 12:12:58 -05:00

8.1.6 Reportar inmediatamente toda pérdida o robo de dispositivos móviles a su jefatura inmediata y a la UTI del PNAEQW.

8.1.7 Disponer de una adecuada infraestructura tecnológica que permita la inclusión de políticas para asegurar el acceso remoto, para ello, es necesario utilizar una conexión VPN pues a través de ella, se establece una conexión remota segura (encriptada) a la red institucional. La conexión VPN son personalizadas para sólo acceder a tomar control remoto del equipo asignado al interior del PNAEQW y utilizar los permisos de acceso ya asignados a dicho equipo.

8.1.8 Establecer requisitos de protección de malware y reglas de firewall (cortafuegos).

8.1.9 Sensibilizar a las/los servidoras/es civiles sobre la importancia de permanecer alerta, respecto a correos electrónicos fraudulentos. Ante cualquier duda o sospecha sobre una amenaza, phishing o malware, debe contactarse con la UTI.

8.1.10 Tener equipos de conexión remota fuera de la oficina con softwares y sistema operativo actualizados, y con software antivirus

8.1.11 Contratar servicios de videoconferencia con niveles de seguridad alto para la sustitución de reuniones presenciales.

8.1.12 Aplicar la lógica de respaldo de la información en este nuevo escenario de conexión remota.

8.1.13 Verificar los accesos a las aplicaciones informáticas según el rol que posea cada servidor/a civil.

8.1.14 Establecer la revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de trabajo a distancia.

8.1.15 Verificar la devolución del equipo asignado en las mismas condiciones en que fue entregado, en el caso que cese la necesidad de trabajar en forma remota.

8.2 Sobre la Seguridad de los Recursos Humanos

El PNAEQW en materia seguridad de recursos humanos se compromete a:

8.2.1 Verificar la veracidad de la información suministrada por la/el candidata/o a ocupar un cargo en el PNAEQW, antes de su vinculación laboral, de acuerdo a lo señalado en el "Instructivo para la administración de legajos de personal del Programa Nacional de Alimentación Escolar Qali Warma".

8.2.2 Informar a la UTI, a través de la Unidad de Recursos Humanos, cuando las/los servidoras/es civiles dejan de laborar en el PNAEQW, para realizar la baja de los accesos a recursos y servicios informáticos que tenían asignados.

8.2.3 Asegurar que las/los servidoras/os civiles del PNAEQW, independientemente del régimen laboral, puesto, nivel jerárquico o función que desarrollen, conozcan, entiendan, cumplan y asuman sus responsabilidades con respecto a la seguridad de la información, de conformidad con lo establecido en el presente documento.

8.2.4 Asignar a las/los servidoras/es civiles del PNAEQW la respectiva identificación de acceso al local del Programa, desde el inicio de sus labores.

8.2.5 Incluir el acuerdo y/o cláusula de confidencialidad en los contratos de las/los servidoras/es civiles del PNAEQW y terceros, con acceso a información sensible del Programa.

8.2.6 Convocar a todas/os las/los servidoras/es civiles del PNAEQW a las charlas y eventos programados como parte del programa de sensibilización y capacitación en seguridad de la información.

8.2.7 Velar por el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre la plataforma tecnológica del PNAEQW al darse por concluido el vínculo contractual o de haber cambios o rotación de sus funciones.

8.3 Sobre la Seguridad de Gestión de Activos de la Información

El PNAEQW en materia seguridad de gestión de activos de la información se compromete a:

8.3.1 Elaborar y mantener un inventario de los activos de información para el proceso de evaluación de riesgos de seguridad de la información, de acuerdo al alcance del SGSI establecido, asignando responsables de velar por la protección de dichos activos.

8.3.2 Verificar que cada activo de información tenga un/una propietario/a que sea responsable de su correcta gestión.

8.3.3 Identificar, documentar e implementar las reglas para el uso aceptable de los activos informáticos y las instalaciones de procesamiento de información.

8.3.4 Clasificar la información en función de los requisitos legales, valor, criticidad y la sensibilidad a la divulgación o modificación no autorizada. Para ello el nivel de protección debe evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad y cualquier otro requisito para la información considerada. La clasificación se hace según lo definido por la/el propietaria/o de la información, la misma que es aprobada por la/el jefa/e del área responsable y distribuida a las diferentes unidades orgánicas.

8.3.5 Clasificar la información que administra el PNAEQW por categorías en función de su valor, requisitos legales, criticidad y sensibilidad, de acuerdo a lo siguiente:

- Pública: Información de acceso libre a cualquier persona que lo requiera, haciendo uso del procedimiento establecido en la Ley Nº 27806, Ley de transparencia y acceso a la información pública.
- Uso interno: Información de acceso interno, cuya divulgación o uso no autorizado, puede generar algún riesgo a la institución o terceros.
- Información confidencial: Información de acceso restringido, cuyo uso o divulgación no autorizada puede ocasionar un alto impacto a la institución o terceros.

8.3.6 Etiquetar la información de acuerdo con el esquema de clasificación de la información adoptado por el PNAEQW.

PERÚ Ministerio de Desarrollo e Inclusión Social
QaliWarma
PROGRAMA NACIONAL DE ALIMENTACIÓN ESCOLAR

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 12:13:11 -05:00

8.3.7 Controlar los medios removibles (cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, etc.) de acuerdo con el esquema de clasificación adoptado.

8.3.8 Comprobar, a través de la UTI, antes de reasignar o dar de baja algún dispositivo de almacenamiento, que la información contenida sea eliminada o sobrescrita de manera segura, de modo que resulte imposible recuperar dicha información.

8.3.9 Respaldar la información según lo establecido en la "Directiva para la gestión de copias de respaldo y resguardo de la información del Programa Nacional de Alimentación Escolar Qali Warma".

8.3.10 La UTI o quien haga sus veces en las unidades territoriales debe proteger a los medios que contienen información, contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte de los mismos.

8.4 Sobre los Controles de Acceso

El PNAEQW en materia de control de acceso se compromete a:

8.4.1 Establecer perfiles estandarizados y adecuadamente registrados, los que deben estar definidos según roles y asignados de manera individual a cada usuaria/o.

8.4.2 Establecer los procedimientos de acceso a los sistemas, aplicaciones y demás recursos informáticos, creando perfiles y registrando actividades.

8.4.3 Asignar de manera personal a la/al usuaria/o su cuenta y contraseña por cada servicio y/o aplicación, en base a la necesidad y en relación a las funciones de la/el misma/o, quien a su vez es responsable de todo lo que se registre con la cuenta asignada. Para el caso del acceso no autorizado a los sistemas de información, servicios de red y plataforma tecnológica del PNAEQW, emplea mecanismos para prevenirlos.

8.4.4 Inhabilitar de oficio las cuentas de usuario de servicio y/o aplicaciones cuando estas no hayan sido utilizadas en los últimos noventa (90) días.

8.4.5 Actualizar la contraseña de las cuentas de usuario cada sesenta (60) días y evitar su reutilización.

8.4.6 Concientizar a la/al usuaria/o sobre el buen uso de sus credenciales de acceso.

8.4.7 Prohibir el ingreso a equipos de cómputo utilizando credenciales distintas a las asignadas.

8.4.8 Limitar que el personal del PNAEQW tenga acceso de escritura a los datos de los sistemas en producción por fuera de las interfaces de usuarios.

8.4.9 Cubrir eventualidades causadas por ausencia imprevista o por razones de fuerza mayor del/de la servidor/a civil que tiene a cargo operaciones críticas.

8.4.10 Implementar un proceso de autorización y registro de los privilegios asignados, así como controlar la asignación y uso de los derechos de acceso.

8.4.11 Prohibir la instalación de herramientas o software que permitan accesos privilegiados a recursos, servicios o sistemas. Excepto a las/los

administradoras/es de la plataforma tecnológica y/o servidor/a civil que por sus funciones lo requiera.

8.4.12 Mantener disponibles las bibliotecas de programas fuente en los ambientes de producción, calidad y desarrollo, e implementar controles para controlar el acceso al código fuente.

8.4.13 Implementar una política de bloqueo de pantalla, a fin de evitar el acceso no autorizado a la información almacenada en los equipos informáticos de las/los usuarias/os.

8.4.14 Restringir y controlar el uso de programas utilitarios que puedan ser capaces de anular los controles del sistema operativo y de los softwares de aplicación.

8.4.15 Revisar periódicamente los accesos concedidos para validar su vigencia o caducidad.

8.5 Sobre los Controles Criptográficos

El PNAEQW en materia de controles criptográficos se compromete a:

8.5.1 Establecer un mecanismo respecto a la administración de claves y la recuperación de la información cifrada en caso de pérdida, compromiso, daño y reemplazo de las claves antes mencionadas.

8.5.2 En los casos que se requiera el cifrado de la información, se debe evaluar los riesgos con la finalidad de identificar el nivel requerido de protección

8.5.3 Para los casos de la contratación de servicios informáticos en la nube, establecer o solicitar conexiones encriptadas, conforme a los lineamentos vigentes establecidos por la SEGDI.

8.6 Sobre la Seguridad Física y Ambiental

El PNAEQW en materia de seguridad física y ambiental se compromete a:

8.6.1 Controlar que el personal porte permanentemente y de forma visible su fotocheck que lo autorice a permanecer en las instalaciones.

8.6.2 Asegurar que todas las áreas que cuenten con instalaciones de procesamiento de información consideradas críticas para el correcto funcionamiento de los sistemas de información del PNAEQW, estén protegidas por un perímetro de seguridad física.

8.6.3 Restringir el acceso a los ambientes críticos del PNAEQW a todo personal no autorizado.

8.6.4 Mantener un registro de visitas al centro de datos.

8.6.5 En relación al centro de datos, gestionar y asegurar la implementación y validación de las medidas de protección contra amenazas externas, las mismas que son:

- Elaborar y ejecutar un plan de mantenimiento de equipos informáticos.
- Controles de acceso y seguridad física
- Sistema contra incendios, que incluyen extintores funcionales.
- Sistema de alimentación ininterrumpida (UPS)

- Sistema de puesta a tierra
- Medidas contra aniegos
- Grupo electrógeno.
- Disposiciones de salubridad

Con la finalidad de garantizar la entrega de los servicios de tecnologías de la información a las/los usuarias/os internas/os y usuarias/os externas/os.

8.6.6 Establecer o trasladar las exigencias de seguridad aplicables de los presentes lineamientos y/o política a las empresas proveedoras que presten servicio de alojamiento, procesamiento o almacenamiento de información del PNAEQW.

8.6.7 Retirar de manera inmediata los privilegios de acceso físico al centro de datos cuando el personal autorizado deje de prestar servicios en el PNAEQW.

8.6.8 Prohibir el acceso de visitantes con equipos electrónicos tales como videograbadoras, cámaras fotográficas, celulares, dispositivos de almacenamiento, equipos de transmisión o recepción de señales u otros dispositivos en los ambientes críticos o restringidos del PNAEQW, que puedan vulnerar la seguridad del área y activos de información.

8.6.9 Controlar que cualquier elemento u objeto (hardware o software) que ingrese o salga de las instalaciones del PNAEQW sea anunciado al personal de vigilancia para que este proceda a hacer el registro correspondiente y emitirse el formato de autorización por el área competente.

8.6.10 Velar por el cumplimiento a la normativa interna relacionada al mantenimiento preventivo y correctivo de los equipos de cómputo y de comunicaciones, con la finalidad de asegurar la continuidad, disponibilidad e integridad de los mismos. Asimismo, se debe dar cumplimiento a la normativa interna relacionada al respaldo y restauración de la información.

8.6.11 Establecer controles para proteger los equipos informáticos, respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas.

8.6.12 Verificar que en todas las instalaciones del PNAEQW, el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios informáticos, cuente con mecanismos que lo protejan contra intercepción o daño. Asimismo, el cableado eléctrico debe estar separado del cableado de datos, es decir, no deben estar en el mismo ducto o canaleta con el fin de evitar interferencias.

8.6.13 Verificar que el cableado de red de comunicaciones del PNAEQW cumpla con los estándares nacionales e internacionales de cableado estructurado; asimismo solo el personal técnico autorizado por la UTI puede realizar trabajos de instalación o mantenimiento del cableado eléctrico o de comunicaciones.

8.6.14 Verificar que todas las estaciones de trabajo del PNAEQW tengan un mecanismo automático de bloqueo de pantalla con clave cuando no lo estén utilizando.

8.7 Sobre la Seguridad de las Operaciones

El PNAEQW en materia de seguridad de las operaciones se compromete a:

8.7.1 Mantener documentado el procesamiento de la información y los recursos y servicios informáticos del PNAEQW, estableciendo las correspondientes

responsabilidades, asimismo dicha documentación debe encontrarse disponible y accesible para todas/os las/los usuarias/os interesadas/os que lo requieran.

8.7.2 Controlar que los recursos informáticos del PNAEQW sean utilizados únicamente para fines propios de la labor del personal.

8.7.3 Establecer procedimientos y tareas para la actualización de software utilizados por el PNAEQW, y monitorear la vigencia de licencias de software a fin de realizar las renovaciones respectivas para prevenir caer en el uso ilegal de software y la inoperatividad del mismo.

8.7.4 Probar los cambios en los sistemas y aplicaciones de producción en un ambiente de calidad, antes de su pase a producción.

8.7.5 Prohibir el uso de compiladores, editores, y otros utilitarios del sistema de información en el ambiente de producción, sin autorización de la UTI.

8.7.6 Monitorear permanentemente la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse de ataques de códigos maliciosos en la plataforma tecnología; lo cual debe estar acompañado de una concientización adecuada a la/al usuaria/o.

8.7.7 Implementar mecanismos para el registro y revisión de los registros de auditoría, orientados a producir informes de las amenazas detectadas contra los sistemas de información y métodos utilizados. Además, planificar y establecer los requisitos de auditorías y las actividades que involucran la verificación de los sistemas de información, con el propósito de minimizar la interrupción a los procesos de negocio del PNAEQW.

8.7.8 Realizar el monitoreo de la red interna, así como detectar actividades no autorizadas y generar evidencia de los registros (Logs). Además, los registros (Logs) y la información de los mismos, deben ser protegidos contra la adulteración y el acceso no autorizado.

8.7.9 Obtener de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de información a ser utilizados, y evaluar la exposición del PNAEQW a dichas vulnerabilidades, así como tomar las medidas adecuadas para manejar los riesgos asociados.

8.7.10 Revisar los medios magnéticos extraíbles con un antivirus provisto por el PNAEQW, antes de introducirlos en los computadores personales o servidores.

8.7.11 Definir la información que debe ser respaldada por medio de copias de seguridad.

8.7.12 Prohibir que el personal borre información que pertenece al PNAEQW de la computadora a su cargo como usuaria/o.

8.7.13 Prohibir instalar o utilizar software o productos sin licencias no autorizadas por el PNAEQW. Se exceptúan de estos lineamientos y/o política los productos de software con licencia de libre utilización o que sean soportados con certificado de propiedad de licencia de terceros o que hayan sido resultado de un desarrollo propio, en cuyo caso, cualquier instalación de software debe ser solicitada y obtenida a través de la UTI.

8.7.14 Definir un mecanismo para el control de los cambios en los sistemas de información y recursos informáticos, el cual debe incluir responsabilidades y canales de comunicación.

8.7.15 Monitorear continuamente la plataforma tecnológica del PNAEQW, con el fin de establecer niveles de capacidad y desempeño, así como también realizar proyecciones para determinar requisitos futuros de capacidad.

8.8 Sobre la Seguridad de las Comunicaciones

El PNAEQW en materia de seguridad de las comunicaciones se compromete a:

8.8.1 Identificar, justificar y documentar los servicios, protocolos y puertos permitidos en las redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

8.8.2 Asegurar que la infraestructura de comunicaciones tecnológicas esté adecuadamente identificada y diagramada; así también los equipos informáticos que la componen deben poseer los elementos de seguridad mínima como claves de acceso, manejo de protocolos de cifrado, monitoreo de operatividad, log de eventos y respaldo de configuraciones.

8.8.3 Controlar el acceso a los componentes de red, tanto internos como externos, como routers y switches, de manera que las/los usuarias/os no comprometan la seguridad de los activos de información.

8.8.4 Establecer controles y mecanismos de autorización para otorgar acceso a las/los usuarias/os, a las redes y servicios informáticos autorizados.

8.8.5 El acceso externo a la red del PNAEQW, se debe realizar solamente a través de una VPN (Red Privada Virtual) configurada para tal fin.

8.8.6 Utilizar equipos institucionales con los resguardos de seguridad correspondientes. De no ser posible, el/la servidor/a civil debe utilizar su equipo personal y, en conjunto con el PNAEQW, verificar que su dispositivo se encuentre en condiciones de seguridad aptas: antivirus reconocido y actualizado, sistema operativo debidamente licenciado y con sus parches al día, y aplicaciones debidamente licenciadas y actualizadas.

8.8.7 Si las/los servidoras/es civiles utilizan un equipo compartido en el hogar, el PNAEQW debe verificar que se cree un perfil específico para la ejecución de las actividades asignadas.

8.8.8 Establecer medidas para evitar el acceso de forma fortuita a la información del PNAEQW por otras/os usuarias/os del equipo del/de la servidor/a civil, como familiares o conocidas/os.

8.8.9 Difundir buenas prácticas de seguridad referente al uso del servicio de internet y el correo institucional.

8.8.10 Limitar la conexión de dispositivos de almacenamiento externo (ej. Memorias USB, discos externos, lectoras/quemadoras externas).

8.9 Sobre la Adquisición, Desarrollo y Mantenimiento de Sistemas

El PNAEQW en materia de adquisición, desarrollo y mantenimiento de sistemas se compromete a:

8.9.1 Velar para que los aplicativos, desarrollados interna o externamente que se pongan en operación en el PNAEQW cumplan los requerimientos de seguridad mínimos, controles de cambios, protección de código fuente y datos en producción, establecidos para asegurar la confidencialidad, integridad y disponibilidad en la información que manejan.

8.9.2 Mantener por separado los ambientes de producción, calidad y desarrollo, y que cada uno de ellos tenga los elementos que se consideren adecuados con el fin de mitigar riesgos.

8.9.3 Proteger la información confidencial de producción a ser entregada a los desarrolladores para sus pruebas.

8.9.4 Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del PNAEQW.

8.9.5 Aplicar una capa de seguridad en los aplicativos dentro del ciclo de vida de desarrollo del software.

8.9.6 Garantizar que el desarrollo y mantenimiento de los sistemas de información en el PNAEQW esté basado en la NTP vigente y/o por lo establecido por el Ministerio de Desarrollo e Inclusión Social, referido al ciclo de vida del software, entre otros estándares aplicables, siendo de uso obligatorio para todo el PNAEQW.

8.9.7 Garantizar que los datos de prueba pueden ser seleccionados, protegidos y controlados de manera adecuada.

8.10 Sobre la Relación con las/los Proveedoras/es de Servicio

El PNAEQW en materia de relación con las/los proveedoras/es de servicio se compromete a:

8.10.1 Incluir en los contratos u órdenes de servicio de las/los proveedoras/es de servicios de tecnologías de la información y comunicaciones una cláusula de confidencialidad. Asimismo, debe controlar el acceso de las/los mismas/os a las instalaciones del PNAEQW.

8.10.2 Acordar con el/la proveedor/a y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del/de la mismo/a a los activos del PNAEQW.

8.10.3 Establecer y acordar con cada proveedor/a que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura tecnológica para el PNAEQW, todos los requisitos relevantes de seguridad de la información.

8.10.4 Incluir en los contratos con terceros, controles de seguridad de la información, que garanticen la confidencialidad de la información del PNAEQW.

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 12:15:19 -05:00

8.10.5 Incluir en los acuerdos con proveedoras/es requisitos para abordar los riesgos de seguridad de la información asociados con los servicios informáticos y la cadena de suministro de productos.

8.10.6 Hacer seguimiento y revisar regularmente la prestación de los servicios del/de la proveedor/a, relacionados a los recursos o servicios de tecnologías de la información.

8.11 Sobre la Gestión de Incidentes de Seguridad de la Información

El PNAEQW en materia de gestión de incidentes de seguridad de la información se compromete a:

8.11.1 Establecer procedimientos documentados para informar, evaluar, clasificar y dar respuesta a los incidentes y debilidades de seguridad de la información.

8.11.2 Reportar cualquier incidente o debilidades de seguridad de la información a la/al oficial de seguridad de la información o a quién haga sus veces de forma oportuna, cuando se detecte una posible amenaza que atente contra los activos de información.

8.11.3 Promover que el conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información, sea considerado para reducir la probabilidad o el impacto de incidentes futuros.

8.11.4 Programar revisiones semestrales, orientadas a obtener información oportuna e identificar incidentes de seguridad en los servicios de tecnologías de la información del PNAEQW.

8.11.5 Definir y aplicar mecanismos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

8.12 Sobre Aspectos de Seguridad de la Información en la Gestión de la Continuidad Operativa

El PNAEQW en materia de aspectos de seguridad de la información en la gestión de la continuidad operativa se compromete a:

8.12.1 Determinar los requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas como en una crisis o desastre.

8.12.2 Diseñar y mantener vigente el plan de continuidad operativa de tecnologías de la información que atienda los requerimientos de seguridad de la información en el PNAEQW según el análisis de riesgos determinado para tal fin.

8.12.3 Realizar pruebas periódicas de acuerdo al plan de continuidad operativa de tecnologías de la información, con la finalidad de asegurar la validez y efectividad durante situaciones adversas.

8.12.4 Conformar y designar un equipo de respuesta ante incidentes de seguridad de la información y/o ciberseguridad.

8.12.5 Implementar en las instalaciones de procesamiento de la información, la suficiente redundancia para cumplir con los requisitos de disponibilidad necesarios.

8.13 Sobre el Cumplimiento de Requisitos Legales y Contractuales

El PNAEQW en materia de cumplimiento de requisitos legales y contractuales se compromete a:

8.13.1 Garantizar el cumplimiento de requisitos legales, regulatorios y contractuales relevantes que afecten los activos de información del PNAEQW.

8.13.2 Asegurar el cumplimiento de los derechos de propiedad intelectual, y garantizar que los equipos de cómputo utilicen software que cuente con licencia de uso.

8.13.3 Garantizar la privacidad y protección de datos personales de acuerdo a la normativa vigente.

8.13.4 Velar por la correcta implementación y cumplimiento de los lineamientos y/o política y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

Firmado digitalmente por SANCHEZ DE LA CRUZ Edgar Anddy FAU 20550154065 hard
Motivo: Doy V° B°
Fecha: 28.09.2022 12:13:55 -05:00