REPUBLICA DEL PERU

Resolución Directoral

Nº 012 -2018-TP/DE

Lima, 29 ENE. 2018

VISTO: El Informe N° 0015-2018-TP/DE/UGPPME-CFPP, de fecha 12 de enero de 2018, de la Coordinación Funcional de Coordinación Funcional de Planificación y Presupuesto de la Unidad Gerencial de Planificación, Presupuesto, Monitoreo y Evaluación, el Informe N° 171-2017-TP/DE/UGA-CFS, de fecha 21 de diciembre de 2017, de la Coordinación Funcional de Sistemas de la Unidad Gerencial de Administración, y el Informe N° 045-2018-TP/DE/UGAL, de fecha 26 de enero de 2018, de la Unidad Gerencial de Asesoría Legal; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 012-2011-TR, modificado por los Decretos Supremos Nros. 004-2012-TR y 006-2017-TR, se crea el Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú", *en adelante el Programa*, con el objeto de generar empleo y promover el empleo sostenido y de calidad en la población desempleada y subempleada de las áreas urbanas y rurales, en condición de pobreza y pobreza extrema y/o afectada parcial o íntegramente por una emergencia o desastre natural, de acuerdo a la información que proporcione el organismo rector competente;

Que, con Resolución de Contraloría N° 149-2016-CG, se aprueba la Directiva N° 013-2016-CG/GPROD denominada "Implementación del Sistema de Control Interno en las Entidades del Estado", con la finalidad de fortalecer el control interno en las entidades del Estado para el eficiente, transparente y correcto ejercicio de la función pública en el uso de los recursos del Estado;

Que, en la Actividad 6 de la Etapa III de la Fase de Planificación de la Implementación del Sistema de Control Interno de la acotada Directiva se estableció al *Plan de Trabajo para el Cierre de Brechas* como aquel documento que define el curso de acción a seguir con la finalidad de cerras las brechas identificadas en el diagnóstico, donde por cada brecha identificada se debe indicar las acciones a desarrollar para cerrarla, encontrándose registradas las mismas en el plan de trabajo, consignando la unidad orgánica, funcionario o servidor público responsable, así como los recursos y plazos de inicio y fin para su implementación trazados en un cronograma de ejecución;

TRABAJA PERÚ V° B° Lic. César Edmundo Gálvez Pardavé Director Ejecutivo

TRABAJA PERÚ V° B° Abog. Dana Martin Delgado Hidalgo Gerente de la Unidad Gerencial de Asesoría Legal

TRABAJA PERÚ V° B° John Hairo Altamirano Martinez Responsable de la Coordinacion Funcional de Planificación y Presupuesto

TRABAJA PERÚ V° B° Ing. Richel Luis Zapata Lovey Responsable de la Coordinación Funcional de Sistemas

TRABAJA PERÚ V° B° Econ. Ynés Aurora Quispe Chavez de Lopez Gerente de la Unidad Gerencial de Planificación, Presupuesto, Monitoreo y Evaluación

TRABAJA PERÚ V° B° Mg. Emerson O. Loayza Allaga Gerente de la Unidad Gerencial de Administración

Que, mediante Resolución Directoral N° 123-2017-TP/DE, se aprueba el Plan de Trabajo para el Cierre de Brechas del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú" y el Programa Nacional de Promoción de la Responsabilidad Social Empresarial "Perú Responsable", quienes conforman la Unidad Ejecutora 005 del Ministerio de Trabajo y Promoción del Empleo, siendo modificado el aludido Plan, en cuanto al Programa "Trabaja Perú", mediante Resolución Directoral N° 214-2017-TP/DE;

Que, en el ítem 29) de la Norma 3.9: Controles para la Tecnología de la Información y Comunicación (TIC) del Componente 3: Actividades de Control Gerencial, del acotado Plan, se ha señalado como actividad la *elaboración de Lineamientos sobre la política de seguridad informática del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú";*

Que, una de las funciones de la Unidad Gerencial de Administración, conforme se señala en el literal o) del artículo 20° del referido Manual, consiste en diseñar, construir, implantar y mantener los sistemas de información y la infraestructura tecnológica de soporte a los sistemas de información, telecomunicaciones y demás servicios informáticos del Programa;

Que, de otra parte, mediante Resolución Directoral N° 016-2015-TP/DE, modificada con Resolución Directoral N° 084-2015-TP/DE, se constituyó a la Coordinación Funcional de Sistemas dentro de la Unidad Gerencial de Administración, estableciéndose entre sus funciones mantener un adecuado nivel de integración y seguridad de la información institucional así como gestionar la seguridad a la red de datos y comunicaciones del Programa, estableciendo niveles de acceso y permisos a nivel interno y externo, propendiendo la integridad, confidencialidad y disponibilidad de la información;

Que, la Coordinación Funcional de Sistemas de la Unidad Gerencial de Administración propone el documento de gestión denominado Lineamientos de Seguridad Informática del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú como un elemento de entrada y base para la elaboración posterior del Plan de Seguridad Informática, conforme se señala en el Informe N° 171-2017-TP/DE/UGA-CFS, agregando que los alcances vertidos en la propuesta se adecúa a las técnicas vigentes reguladas en la Resolución Ministerial N° 004-2016-PCM, que obliga el uso de la Norma Técnica Peruana NTP-ISO/IEC 27001-2014;

Que, asimismo, la Coordinación Funcional de Planificación y Presupuesto de la Unidad Gerencial de Planificación, Presupuesto, Monitoreo y Evaluación emite opinión sobre la propuesta de Lineamientos de Seguridad Informática del Programa "Trabaja Perú", indicando que el mismo se enmarca dentro del Plan de Trabajo de Cierre de Brechas aprobado mediante Resolución Directoral N° 123-2017-TP/DE, y modificado con Resolución Directoral N° 214-2017-TP/DE;

Que, mediante Informe Nº 045-2018-TP/DE/UGAL, la Unidad Gerencial de Asesoría Legal recomienda la aprobación del citado documento de gestión, a propósito de la implementación del Sistema de Control Interno;

Que, en los literales h) e i) del artículo 12° del Manual de Operaciones del Programa, se ha previsto entre las facultades de la Dirección Ejecutiva, expedir Resoluciones Directorales en asuntos de su competencia tales como aprobar directivas, reglamentos, instrumentos y procedimientos de carácter técnico operativo del Programa;

TRABAJA PERÚ V° B° Lic. César Edmundo Gálvez Pardavé Director Ejecutivo

TRABAJA PERÚ V° B° Abog. David Martín Delgado Arango Gerente de la Unidad Gerencial de Asesoría Legal

TRABAJA PERÚ V° B° John Hairo Altamirano Martínez Responsable de la Coordinación Funcional de Planificación y Presupuesto

TRABAJA PERÚ V° B° Ing. Richel Iván Zapatel Davey Responsable de la Coordinación Funcional de Sistemas

TRABAJA PERÚ V° B° Econ. Ynés Aurora Quispe Chávez de López Gerente de la Unidad Gerencial de Planificación, Presupuesto, Monitoreo y Evaluación

TRABAJA PERÚ V° B° Mg. Enrique A. Loayza Abaga Gerente de la Unidad Gerencial de Administración

Con la visación de las Coordinaciones Funcionales de Sistemas y de Planificación y Presupuesto; de las Unidades Gerenciales de Administración, de Planificación, Presupuesto, Monitoreo y Evaluación y de Asesoría Legal del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú"; y;

De conformidad con lo dispuesto por el Decreto Supremo N° 012-2011-TR, modificado por los Decreto Supremos N[ros.] 004-2012-TR y 006-2017-TR, que crea el Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú", los incisos h) e i) del artículo 12° del Manual de Operaciones del Programa, aprobado mediante Resolución Ministerial N° 226-2012-TR y modificado por Resoluciones Ministeriales N[ros.] 215, 234-2014-TR, 027-2017-TR y 003-2018-TR;

SE RESUELVE:

Artículo 1°.- Lineamientos de Seguridad Informática.

Aprobar los Lineamientos de Seguridad Informática del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú", que en anexo adjunto forman parte integrante de la presente Resolución Directoral.

Artículo 2°.- Difusión.

Disponer que la Unidad Gerencial de Administración difunda el contenido del documento de gestión aprobado, en el marco de la Implementación del Sistema de Control Interno en el Programa "Trabaja Perú".

Artículo 3°.- Notificación.

Encargar a la Unidad Gerencial de Administración la notificación de la presente Resolución a las unidades orgánicas del Programa, a la Secretaría General y al Órgano de Control Institucional del Ministerio de Trabajo y Promoción del Empleo.

Artículo 4°.- Publicación.

La presente Resolución deberá ser publicada en el Portal de Transparencia del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú".

Regístrese y comuníquese.

TRABAJA PERÚ V° B° Abog. David Martín Delgado Hidalgo Gerente de la Unidad Gerencial de Asesoría Legal

TRABAJA PERÚ V° B° John Hairo Altamirano Martínez Responsable de la Coordinación Funcional de Planificación y Presupuesto

TRABAJA PERÚ V° B° Ing. Richal Ivain Zapatel Davey Responsable de la Coordinación Funcional de Sistemas

TRABAJA PERÚ V° B° Econ. Ynes Aurora Quispe Chávez de Lopez Gerente de la Unidad Gerencial de Planificación, Presupuesto, Monitoreo y Evaluación

TRABAJA PERÚ V° B° Mg. Enrique D. Loayza Aliaga Gerente de la Unidad Gerencial de Administración

PROGRAMA TRABAJA PERU

Lic. César Edmundo Gálvez Pardavé
Director Ejecutivo

LINEAMIENTOS DE SEGURIDAD INFORMÁTICA

DEL PROGRAMA TRABAJA PERÚ

CONTENIDO

I. INTRODUCCIÓN

1. Finalidad

Los presentes Lineamientos de Seguridad Informática del Programa para la Generación de Empleo Social Inclusivo "Trabaja Perú" tienen por finalidad establecer el marco general de gestión para proteger adecuadamente la información digital del Programa, definiendo las directrices generales de actuación que aseguren el tratamiento adecuado de los riesgos y que conduzcan al fortalecimiento de una cultura en Seguridad Informática.

2. Alcance

Los presentes Lineamientos de Seguridad Informática y las disposiciones emanadas en el marco de la misma, son de cumplimiento obligatorio por parte de todo el personal del Programa Trabaja Perú, sin distingo de régimen laboral o contractual, o nivel jerárquico, al que en adelante se denominará "colaborador de Trabaja Perú", así como de las personas naturales o jurídicas que presten servicios en general, en adelante "terceros", que tengan acceso a la información de Trabaja Perú.

3. Base Legal y Administrativa

- 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. 2da Edición."*, en todas las entidades integrantes del Sistema Nacional de Informática, así como los nuevos plazos de implementación.

II. PRINCIPIOS

1. Protección

Los activos de información deben de ser protegidos con el nivel de seguridad necesario, guardando proporción entre el valor y el riesgo de pérdida para el Programa. La protección debe enfocarse en la confidencialidad, integridad y disponibilidad de estos activos.

2. Uso apropiado

Los activos de información disponibles en el Programa deben ser utilizados en forma adecuada, eficiente, racional y exclusivamente para el desarrollo de las actividades institucionales.

3. Acceso autorizado

Todos los usuarios de sistemas de información del Programa deben ser identificados individualmente, y sus permisos de acceso deben de concederse en forma específica de acuerdo a su rol y responsabilidades. Los métodos de acceso de los usuarios deben exigir un proceso de autenticación, autorización y auditoría.

4. Auditabilidad

Se debe asegurar que los sistemas informáticos, de acuerdo a su criticidad, registren eventos pertinentes a la seguridad informática para su control posterior. Las evidencias de auditoría generadas deben permitir identificar usuarios y documentar las situaciones relacionadas con dichos eventos.

5. Disponibilidad

Los activos de información deben estar disponibles para su uso por parte de los usuarios autorizados toda vez que lo requieran, garantizando el acceso oportuno a la información y a los recursos relacionados con la misma.

6. Integridad

Los activos de la información deben estar adecuadamente protegidos para asegurar su integridad. Las medidas de validación definidas deben permitir detectar la modificación inadecuada, adulteración o eliminación de los activos de información.

7. Confidencialidad

Los activos de información deben mantenerse protegidos para asegurar la confidencialidad y privacidad entre usuarios con acceso autorizado a los mismos. En todo

momento deben de mantenerse esquemas de seguridad que prevengan la divulgación no autorizada de información.

8. Colaboración

La conservación de la seguridad informática es un esfuerzo de equipo en el que participan los colaboradores del Programa y terceros que tengan acceso a los activos de información, por el cual estas personas deben desempeñar un papel activo en el cumplimiento y divulgación de las políticas y normas vigentes de seguridad informática.

9. Supervisión

Periódicamente se deben revisar las plataformas tecnológicas (hardware y software) disponibles en el Programa, a fin de verificar el cumplimiento de las políticas de seguridad y la implementación de los estándares de configuración establecidos.

10. Propiedad

La información registrada, almacenada y procesada por las operaciones de la organización es propiedad del Programa, a menos que en una relación contractual se establezca lo contrario, y la facultad de otorgar acceso a ella es del propietario de la información.

III. LINEAMIENTOS

3.1 Sobre la seguridad informática

1. Política de seguridad informática

Los presentes lineamientos constituyen la Política de Seguridad Informática, y define las líneas de acción y dirección a observar para la gestión adecuada de la seguridad informática. Es necesario revisar y actualizar periódicamente esta política cuando surjan nuevas exigencias regulatorias en la materia o en caso de un cambio significativo dentro del Programa.

2. Organización de la seguridad

El Programa debe administrar la seguridad de la información dentro del organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades en forma adecuada.

Se debe conformar el Comité de Gestión de Seguridad de la Información (CGSI) del Programa para la atención de temas en materia de seguridad de la información que requieran de una definición o aprobación institucional.

Se debe designar a un Oficial de Seguridad de la Información, o quien haga sus veces, con el perfil técnico adecuado para garantizar el cumplimento de la política de seguridad de la información.

3. Gestión de los activos

El Programa Trabaja Perú debe elaborar y mantener un inventario de sus activos de información en medios informáticos para el proceso de evaluación de riesgos de seguridad, asignando responsables de velar por la protección de dichos activos.

Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos relacionados con su procesamiento.

4. Seguridad de los recursos humanos

Se debe de verificar la idoneidad de las personas a contratar para laborar en la entidad, e incluir la firma de acuerdos de cumplimiento de seguridad informática para colaboradores del Programa y terceros que puedan tener acceso a información sensible.

Se deben realizar programas de concientización y entrenamiento para asegurar que los colaboradores del Programa asuman sus responsabilidades relacionadas con la

seguridad informática, estableciéndose procesos disciplinarios para casos de incumplimiento. Los terceros que incumplan las políticas de seguridad se sujetarán a lo establecido en los respectivos contratos.

Al término de la vinculación laboral o contractual, debe asegurarse la devolución de activos de información asignados y el retiro de los accesos a sistemas informáticos del Programa que se hayan otorgado. Toda alta, modificación de puesto o baja de usuarios debe de ser comunicada a la unidad orgánica correspondiente para administrar sus accesos respectivos.

5. Seguridad física y ambiental

Las áreas e instalaciones de procesamiento, gestión o almacenamiento de información del Programa deben de contar con mecanismos de control de acceso y protecciones físicas y ambientales apropiadas para prevenir el daño o pérdida de los activos de información. Se deben establecer procedimientos de mantenimientos de los equipos de procesamiento de información con el fin de asegurar su continua disponibilidad e integridad.

6. Gestión de las comunicaciones y las operaciones

En resguardo de la operación correcta y segura de las instalaciones de tecnologías de la información, se deben de mantener documentados y actualizados los procedimientos operativos informáticos, controlar y documentar los cambios previamente autorizados sobre la plataforma tecnológica, y efectuar una separación de tareas y áreas de responsabilidad.

Se deben aplicar medidas efectivas de protección para el software utilizado en los sistemas de cómputo, la información que estos procesan, y la información transmitida por sistemas de comunicación de datos en la red interna del Programa, incluyendo la mensajería electrónica y los intercambios de información con cualquier entidad externa.

Se debe monitorear el uso de las redes y sistemas de información a fin de detectar actividades no autorizadas de procesamiento de información. Se deben generar evidencias de auditoría (logs) sobre sistemas críticos o sensibles cuya revisión periódica permita el análisis de eventos anómalos.

7. Control de acceso

Deben establecerse mecanismos para prevenir el acceso no autorizado a los sistemas de información, servicios de red interna y plataformas de tecnología informática del Programa, así como garantizar la seguridad de la información de la entidad en entornos computacionales móviles, instalaciones de trabajo remoto y conexiones de redes externas.

Todo usuario autorizado debe poseer un identificador único para el acceso a los sistemas y servicios de información del Programa, debiéndose controlar la asignación y retiro de los correspondientes privilegios de uso.

8. Adquisición, desarrollo y mantenimiento de sistemas de información

Se deben determinar los requisitos de seguridad para los nuevos sistemas de información de Trabaja Perú o para los cambios en los existentes, ya sean desarrollados internamente o por terceros, que incluyan las verificaciones del procesamiento correcto de las aplicaciones y la protección del código y datos en producción.

Todo sistema de información nuevo o actualizado debe cumplir con el ciclo de vida establecido para el desarrollo, desde su requerimiento hasta la validación y aceptación formal por parte de los usuarios solicitantes antes de su puesta en producción, respetando la normativa correspondiente.

Los cambios en las aplicaciones y en el entorno de producción deben ser controlados adecuadamente, a fin de minimizar el riesgo de daños en la información o en los sistemas en donde se procesa la información.

9. Gestión de incidentes de seguridad de la información

Se deben establecer medidas para asegurar que las vulnerabilidades y eventos detectados que afecten negativamente a la seguridad informática o procesos de negocio del Programa sean reportados, registrados y gestionados de manera que permita la adopción de acciones preventivas y correctivas oportunas.

10. Gestión de la continuidad de negocio u operativa

El proceso de gestión de la continuidad de negocio u operativa debe tomar en cuenta los aspectos necesarios para el tratamiento de los riesgos en seguridad de la información. Se debe contar con planes de continuidad operativa y contingencia que cubran los recursos informáticos e infraestructuras tecnológicas que dan soporte a los procesos esenciales de Trabaja Perú, a fin de garantizar la continua disponibilidad de estos.

11. Cumplimiento de las normas legales y técnicas

Se deben establecer mecanismos para garantizar el cumplimiento de toda norma legal, directiva, regulación técnica u obligación contractual y de los requisitos de seguridad aplicables a los sistemas y activos de información del Programa.

3.2 Sobre el Sistema de Gestión de Seguridad de la Información

1. El Sistema de Gestión de la Seguridad de la Información (SGSI) de Trabaja Perú está conformado por la estructura organizativa, políticas, actividades de planeamiento, responsabilidades, prácticas, procesos, procedimientos y recursos destinados a la preservación de la seguridad de la información.

2. El Sistema de Gestión de Seguridad de la Información está sujeto a un proceso de mejora continua sobre la base de resultados de evaluaciones periódicas de riesgos, la respuesta ante incidentes que afecten la seguridad, o por la revisión periódica de las políticas vigentes.

3. Todo proceso de gestión de riesgo relacionado con la seguridad de la información se implementa con la metodología establecida por los responsables de gestión de riesgos asignados en el Programa y aprobada por la Dirección, en el ámbito de sus competencias, asegurándose así que dichos procesos se encuentren alineados con la gestión del riesgo institucional.

4. El Sistema de Gestión de la Seguridad de la Información de Trabaja Perú establece los requisitos de seguridad tomando en cuenta los resultados de la evaluación metódica de los riesgos relevantes, los dispositivos legales pertinentes y los métodos y mecanismos de procesamiento de la información desarrollados en el Programa para el apoyo a sus operaciones, entre otros aspectos.

IV. RESPONSABILIDADES

Para el cumplimiento de los presentes Lineamientos de Seguridad Informática en Trabaja Perú, se establecen las siguientes responsabilidades:

1. **Dirección:** Aprobar los Lineamientos y Políticas de Seguridad de la Información, y sus futuras modificaciones, con la asesoría del Comité de Gestión de Seguridad de la Información del Programa.

2. **Comité de Gestión de Seguridad de la Información (CGSI):** Dirigir, coordinar y revisar la puesta en práctica de la seguridad de la información en el Programa, comprometiendo el apoyo de la Dirección.

3. **Oficial de Seguridad de la información:** Supervisar el cumplimiento de los presentes lineamientos en coordinación con las distintas dependencias del Programa, y liderar el establecimiento, implementación y mantenimientos del Sistema de Gestión de Seguridad de la Información.

4. **Unidades Gerenciales y Coordinaciones Funcionales:** Aplicar las políticas de seguridad de la información al interior de cada órgano o unidad orgánica, en los ámbitos funcional, técnico y administrativo, según corresponda. Fomentar las políticas de seguridad informática al personal a su cargo.

5. **Propietario de la información:** Determinar el grado de confidencialidad y criticidad de la información, definir a cuáles usuarios se les otorgará el acceso y autorizar las peticiones sobre las distintas formas de utilizar la información.

6. **Custodio de la información:** Preservar y proteger la información que le ha sido confiada en custodia.

7. **Usuario:** Responder por los resultados derivados del uso de los activos de información a los que tiene acceso autorizado.

IV. GLOSARIO DE TÉRMINOS

1. **Activo de Información:** sistemas de información, aplicaciones o herramientas de tipo software, base de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos esenciales del Programa.

2. **Confidencialidad:** característica por la cual se garantiza que la información sea accesible sólo por las personas debidamente autorizadas para su acceso.

3. **Custodio de la información:** persona o grupo que, para efectos de custodia, detenta la posesión física de la información generada en Trabaja Perú o de aquella confiada al Programa.

4. **Determinación de riesgos:** evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatividad de Trabaja Perú.

5. **Disponibilidad:** característica por la cual se garantiza que los usuarios autorizados tengan acceso a la información cuando se requiera y previene contra intentos de denegar su uso autorizado.

6. **Evento de seguridad:** ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de las políticas de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser pertinente de seguridad.

7. **Incidente de seguridad:** uno o varios eventos de seguridad de información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones esenciales y de amenazar la seguridad de la información.

8. **Integridad:** característica por la cual se garantiza que la información y los correspondientes métodos de procesamiento sean exactos y estén completos, asegurando que la información no es transformada ni modificada de forma no autorizada durante su procesamiento, transporte o almacenamiento.

9. **Propietario de la información:** persona o grupo bajo cuya autoridad la información es producida y que dispone las reglas de uso de la misma. Toda información de Trabaja Perú contenida en activos o sistemas en producción debe de tener un propietario designado.

10. **Usuario:** persona que utiliza directamente los activos de información a los que tiene acceso autorizado.

11. **Seguridad de la Información:** conjunto de acciones destinadas a asegurar la confidencialidad, integridad y disponibilidad de los activos de información y tecnologías para su procesamiento, apoyando finalmente a la continuidad de las operaciones de Trabaja Perú.