

**PERÚ**Ministerio de Desarrollo
e Inclusión SocialViceministerio
de Prestaciones SocialesPrograma Nacional de Apoyo
Directo a los Más Pobres
JUNTOS

*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la universalización de la salud"*

VISTOS:

El Informe 120-2020-MIDIS/PNADP-UTI de fecha 21 de julio de 2020, de la Unidad de Tecnologías de la Información; el Memorando N° 748-2020-MIDIS/PNADP-UPPM de fecha 29 de julio de 2020, de la Unidad de Planeamiento, Presupuesto y Modernización; el Informe N° 107-2020-MIDIS/PNADP-UPPM-CMG de la Coordinadora de Modernización de la Gestión; y, el Informe N° 224-2020-MIDIS/PNADP-UAJ de fecha 30 de agosto de 2020 de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 032-2005-PCM, modificado por el Decreto Supremo N° 062-2005-PCM y el Decreto Supremo N° 012-2012-MIDIS, se crea el Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", adscrito al Ministerio de Desarrollo e Inclusión Social-MIDIS, el cual tiene por finalidad ejecutar transferencias directas en beneficio de los hogares en condición de pobreza, priorizando progresivamente su intervención en los hogares rurales a nivel nacional; el Programa facilita a los hogares, con su participación y compromiso voluntario, el acceso a los servicios de salud - nutrición y educación, orientados a mejorar la salud y nutrición preventiva materno-infantil y la escolaridad sin deserción;

Que, mediante Resolución Ministerial N° 278-2017-MIDIS, se aprueba el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", el cual constituye el documento técnico normativo de gestión institucional, que determina la estructura orgánica, describe sus funciones generales, las funciones específicas de las unidades que lo integran, así como la descripción de los procesos estratégicos, misionales y de apoyo del Programa;

Que, en virtud de las normas antes señaladas, la Dirección Ejecutiva es la máxima autoridad ejecutiva y administrativa del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", y dentro de sus funciones se encuentra la de emitir Resoluciones de Dirección Ejecutiva en asuntos de su competencia;

Que, de acuerdo al artículo 20 del Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", "La Unidad de Tecnologías de la Información es responsable de planificar, ejecutar, monitorear y evaluar el desarrollo, implementación y mantenimiento de soluciones Tecnológicas de la Información (TI) en apoyo a las Unidades del Programa, para el cumplimiento de los objetivos y en el marco de las políticas y lineamientos del MIDIS y de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM)";

Que, mediante Resolución Ministerial N° 004-2016-PCM se 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, apreciándose que en la tabla A.12, numeral A.12.6 comprende la gestión de vulnerabilidades técnicas, señalando que "la información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado";

Que, mediante Decreto de Urgencia N° 006-2020 se crea el Sistema Nacional de Transformación Digital, como un Sistema Funcional del Poder Ejecutivo, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos para organizar, entre otros, las actividades de la administración pública, a efectos de alcanzar los objetivos del país en materia de transformación digital; habiendo establecido en su Única Disposición Complementaria Derogatoria,





PERÚ

Ministerio de Desarrollo
e Inclusión Social

Viceministerio
de Prestaciones Sociales

Programa Nacional de Apoyo
Directo a los Más Pobres
JUNTOS

que para todos sus efectos, el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática;

Que, el artículo 6 del Decreto de Urgencia N° 006-2020 regula el ámbito de aplicación de dicha norma, disponiendo 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 N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia en lo que corresponda;

Que, con la Resolución Ministerial N° 028-2019-MIDIS se aprueban los 'Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social', considerando dentro de sus alcances a los Programas Sociales; y, señalando en el numeral 1 que dichos lineamientos constituyen una actualización de la normativa 'Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social' de acuerdo a lo establecido en la NTP ISO/IEC 27001:2014; habiendo establecido en el literal c) del numeral 5.15 que "Cualquier servidor del MIDIS y de sus Programas Sociales debe comunicar al Oficial de Seguridad de la Información del MIDIS, o la que haga sus veces en los Programas Sociales, sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que puede tener relación con la seguridad de la información";

Que, mediante Informe N° 120-2020-MIDIS/PNADP-UTI de fecha 21 de julio de 2020, la Unidad de Tecnologías de la Información formula la propuesta de Procedimiento de Gestión de Vulnerabilidades e Incidentes de Seguridad de la Información del Programa Juntos, señalando que tiene por objetivo establecer el marco de trabajo para la gestión de incidentes de seguridad de la información;

Que, con Memorando N° 748-2020-MIDIS/PNADP-UPPM de fecha 29 de julio de 2020, la Unidad de Planeamiento, Presupuesto y Modernización adjunta el Informe N° 107-2020-MIDIS/PNADP-UPPM-CMG de la Coordinadora de Modernización de la Gestión, concluyendo que la propuesta normativa se encuentra acorde a la normativa vigente y se articula al macro proceso Gestión de Sistemas y Tecnologías de la Información, emitiendo opinión favorable para su aprobación;

Que, con Informe N° 224-2020-MIDIS/PNADP-UAJ de fecha 30 de agosto de 2020, la Unidad de Asesoría Jurídica estima viable la emisión de la Resolución de Dirección Ejecutiva que apruebe el Procedimiento de Gestión de Vulnerabilidades e Incidentes de Seguridad de la Información, al encontrarse enmarcado en la normativa sobre la materia;

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

De conformidad con lo dispuesto por el Decreto Supremo N° 032-2005-PCM, modificado por el Decreto Supremo N° 062-2005-PCM y por el Decreto Supremo N° 012-2012-MIDIS; la Resolución Ministerial N° 068-2020-MIDIS; y, estando a lo establecido por el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", aprobado por Resolución Ministerial N° 278-2017-MIDIS.

SE RESUELVE:

Artículo 1.- Aprobar el Procedimiento de Gestión de Vulnerabilidades e Incidentes de Seguridad de la Información del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", y formatos que lo acompañan, que en anexo forman parte integrante de la presente Resolución.

Artículo 2.- Encargar a la Unidad de Tecnologías de la Información la implementación y socialización del documento aprobado en el artículo 1 de la presente Resolución, entre los integrantes del Programa, y que las Unidades realicen las acciones necesarias para la aplicación y cumplimiento del documento aprobado.





PERÚ

Ministerio de Desarrollo
e Inclusión Social

Viceministerio
de Prestaciones Sociales

Programa Nacional de Apoyo
Directo a los Más Pobres
JUNTOS

Artículo 3.- Disponer que la Unidad de Comunicación e Imagen publique la presente Resolución en el Portal de Transparencia Estándar y en el Portal Institucional del Programa Nacional de Apoyo Directo a los Más Pobres “JUNTOS” (www.gob.pe/juntos), en el plazo de dos (02) días desde su emisión.

Regístrese y comuníquese.





PERÚ

Ministerio de Desarrollo e Inclusión Social



Código: PNADP-UTI-GTI-P-005

Versión: 01

Páginas: 1 de 13

PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES “JUNTOS”

Ministerio de Desarrollo e Inclusión Social

PROCEDIMIENTO

GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Karin Patiño Oficial de Seguridad de la Información Silvia Villanueva Gavidia Coordinadora de Modernización de la Gestión	Edwing Pinedo Añazgo Jefe de la Unidad de Tecnologías de la Información Diana Silva Pretel Jefa de la Unidad de Planeamiento, Presupuesto y Modernización	Jessica Niño de Guzmán Esaine Directora Ejecutiva

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



  	GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Código:	PNADP-UTI-GTI-P-005
	Versión:	01
	Páginas:	2 de 13

1. Objetivo

Garantizar la detección temprana de eventos, incidentes y vulnerabilidades de seguridad de la información, así como la rápida reacción y respuesta ante dichas situaciones en el Programa Nacional de Apoyo Directo a los Más Pobres “JUNTOS”, en adelante el Programa JUNTOS.

2. Alcance

Aplica a los/as servidores/as del Programa JUNTOS, con responsabilidad en la gestión de incidentes de seguridad de la información dentro del alcance del SGSI frente a la ocurrencia de incidentes de seguridad. Asimismo, es de cumplimiento de todas las Unidades de la Sede Central del Programa JUNTOS, en el ámbito de sus competencias.

3. Base legal

- 3.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y modificatoria.
- 3.2. Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- 3.3. Ley N° 29792, Ley de creación, organización y funciones del Ministerio de Desarrollo e Inclusión Social.
- 3.4. Decreto Supremo N° 032-2005-PCM, que crea el Programa Nacional de Apoyo Directo a los Más Pobres “JUNTOS”, modificado por los Decretos Supremos N° 062-2005-PCM y N° 012-2012-MIDIS.
- 3.5. Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- 3.6. Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- 3.7. Resolución Ministerial N° 278-2017-MIDIS, que aprueba el Manual de Operaciones del Programa JUNTOS.
- 3.8. 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’
- 3.9. Norma Internacional ISO 9001:2015. Requisitos de un Sistema de Gestión de la Calidad.
- 3.10. Norma Internacional ISO 37001:2016. Requisitos del Sistema de Gestión Antisoborno.
- 3.11. Norma Internacional ISO/IEC 27001: 2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.

4. Siglas y definiciones

- 4.1 **Activo de información:** Dato, dispositivo u otro componente del entorno que apoya actividades relacionadas con la información.
- 4.2 **Definiciones:** Acción de asignar una Categoría a algo. La Clasificación se usa con el objeto de asegurar la integridad, confidencialidad y disponibilidad de la información y una gestión consistente para resguardarla.
- 4.3 **Estado:** Muestra la situación actual de una Vulnerabilidad o Incidente.
- 4.4 **Evento:** Ocurrencia identificada de un estado de la red, servicio o sistema que indica una posible violación de una política de seguridad de la información, la falla de los

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



  	GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Código: PNADP-UTI-GTI-P-005	
	Versión: 01	Páginas: 3 de 13

controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

- 4.5 **Gestión de incidencias:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de las incidencias de seguridad de la información.
- 4.6 **Impacto:** Una medida del efecto de un Incidente, Problema o Cambio en los Procesos de Negocio. En el caso de una vulnerabilidad, se refiere al impacto potencial.
- 4.7 **Incidente de Seguridad de la Información:** Cualquier evento real o sospechoso o serie de eventos indeseados o inesperados, que pudiese comprometer la información que se maneja dentro del ámbito del SGSI del Programa JUNTOS, sus sistemas o las redes computacionales o el acto de violar explícita o implícitamente las políticas de seguridad.
- 4.8 **Prioridad:** Categoría empleada para identificar la importancia relativa de un Incidente.
- 4.9 **Sistema de Gestión (SG):** Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.
- 4.10 **Sistema Integrado de Gestión (SIG):** Sistema Integrado que, comprende al Sistema de Gestión de Calidad, Seguridad de la Información, Antisoborno, y cualquier otro que la organización crea pertinente.
- 4.11 **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. Política específica

Para la gestión de las vulnerabilidades e incidentes de seguridad de la información, el Programa JUNTOS se compromete a:

- Gestionar los incidentes considerando la clasificación y priorización de estos y evaluando tanto el impacto como la urgencia de la solicitud de servicio.
- Informar oportunamente a todas las partes interesadas y escalar de acuerdo con los procedimientos correspondientes.
- Informar e identificar las causas y cualquier oportunidad de mejora del servicio, luego de la resolución del incidente.
- Mantener registros de las vulnerabilidades e incidentes reportados y su seguimiento.

6. Requisitos para iniciar el procedimiento

Descripción del requisito	Fuente
Anexo A (A.16) – Gestión de incidentes de seguridad de la información	Norma ISO/IEC 27001:2013

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**





7. Procedimiento

N°	Descripción de la Actividad	Unidad responsable	Responsable (Cargo)	Registro asociado	Plazo
Detección de la vulnerabilidad o incidente					
1.	<p>Detectar un incidente o vulnerabilidad que pueda afectar la confidencialidad, disponibilidad y/o integridad de la información. Los incidentes pueden responder a las siguientes categorías detalladas en el Anexo n° 01:</p> <p>a) Infracción a leyes y reglamentos b) Incumplimiento del SGSI c) Código malicioso d) Denegación de servicios e) Acceso no autorizado f) Uso inapropiado. g) Fraudes informáticos.</p>	Unidades de sede central	Servidores/as sede central	No aplica	No aplica
Notificación de la vulnerabilidad o incidente					
2.	Reportar ambos casos, quien notifique indicará con detalle los hechos ocurridos, y cuál fue el efecto del problema, vía aplicativo MDA.	Unidades de sede central	Servidores/as sede central	<ul style="list-style-type: none"> MDA Reporte de incidencias y vulnerabilidades (PNADP-UTI-GTI-F-009) 	No aplica
3.	Evaluar si el reporte emitido por el servidor realmente califica dentro de las categorías de vulnerabilidades o incidencias; caso contrario desestimar el reporte y registrar que el reporte no es válido, indicando los motivos.	UTI	Oficial de Seguridad de la Información	MDA	No aplica

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**





Nº	Descripción de la Actividad	Unidad responsable	Responsable (Cargo)	Registro asociado	Plazo
4.	Verificar que la información del reporte esté completa; en caso no lo esté, deberá comunicarse con el servidor del Programa que emitió el reporte a fin de solicitar más información sobre el suceso.	UTI	Oficial de Seguridad de la Información	Correo electrónico o llamada telefónica	No aplica
5.	Registrar las incidencias o vulnerabilidades detectadas, colocando la siguiente información: a) Tipo de evento (vulnerabilidad o incidencia) b) Fecha y hora del suceso c) Apellidos y Nombres de la persona que emitió el reporte d) Detalle del suceso	UTI	Oficial de Seguridad de la Información	Registro de incidencias y vulnerabilidades (PNADP-UTI-GTI-F-010)	No aplica
Revisión de antecedentes					
7.	Revisar los antecedentes del caso y de requerir información adicional o determinar que los antecedentes no son suficientes, deberá remitir la petición al solicitante. En caso contrario deberá continuar con lo señalado en la siguiente actividad.	UTI	Oficial de Seguridad de la Información	Registro de incidencias y vulnerabilidades (PNADP-UTI-GTI-F-010)	No aplica
Evaluación y clasificación del evento					
	Evaluar la información y determinar la severidad del evento, tipificándolo como: • Grave • Mediana • Baja Los lineamientos para determinar la severidad del evento se indican en el Anexo n° 02 del presente documento.	UTI	Oficial de Seguridad de la Información	Registro de incidencias y vulnerabilidades (PNADP-UTI-GTI-F-010)	No aplica

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**





Nº	Descripción de la Actividad	Unidad responsable	Responsable (Cargo)	Registro asociado	Plazo
	Solicitar apoyo para la evaluación y clasificación del evento a especialistas externos o propios del Programa JUNTOS, de creerse conveniente.	UTI	Oficial de Seguridad de la Información	No aplica	No aplica
Acción a tomar					
12.	Determinar si es necesario y/o factible realizar una acción para abordar la incidencia o vulnerabilidad ¹ , de acuerdo con la severidad ² del evento, y al criterio del Oficial de Seguridad de la Información.	UTI	Oficial de Seguridad de la Información	No aplica	No aplica
13.	Coordinar con los/as especialistas de la institución, para el análisis de los incidentes de seguridad, a objeto de que elaboren y promuevan los procedimientos respectivos de respuesta a incidentes de seguridad.	UTI	Oficial de Seguridad de la Información	No aplica	No aplica
14.	Establecer y coordinar contactos extra institucionales, en caso sea necesario, para la respuesta ante incidentes, como: - Proveedores de hardware y software. - Especialistas en delitos informáticos.	UTI	Responsables de planes de acción	No aplica	No aplica
15.	Realizar el escalamiento del incidente a la unidad que sea especialista en el tipo de evento detectado, a fin de poder establecer las acciones necesarias para afrontar el evento	UTI	Oficial de Seguridad de la Información	No aplica	No aplica

¹ Si el evento es una vulnerabilidad, las acciones se basarán en erradicación de esta, a fin de que no produzcan incidencias en el futuro. Si el evento es una incidencia, las acciones a tomar deberán incluir sin limitarse, lo siguiente: a) Contención del incidente: acciones que mitigarán o eliminara los efectos no deseados, producto del incidente b) Erradicación del incidente: acciones que eliminarán las causas que produjeron el incidente. c) Recuperación del incidente: una vez erradicado el incidente, se deberán tomar acciones para la recuperación oportuna de los activos de información que pudieran haber sido afectados.

² No aplica para eventos con severidad "Grave" ya que estos deben contar con un plan de acción para su mitigación
 Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.



**PERÚ**

Ministerio de Desarrollo e Inclusión Social

**GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

Código: PNADP-UTI-GTI-P-005

Versión: 01

Páginas: 7 de 13

Nº	Descripción de la Actividad	Unidad responsable	Responsable (Cargo)	Registro asociado	Plazo
	reportado, en caso sea necesario.				
16.	Supervisar de manera permanente las acciones que se tomen ante la vulnerabilidad o incidente.	UTI	Oficial de Seguridad de la Información	No aplica	No aplica
17.	Registrar la siguiente información: <ul style="list-style-type: none"> • Descripción de las acciones a tomar. • Responsables de la ejecución de las acciones. • Fecha de ejecución de las acciones. • Verificación de la ejecución de las acciones (colocar detalle). Estado actual de la acción, si ya se tomó una acción y se verificó la realización de esta, se coloca "CERRADA", caso contrario, se coloca "ABIERTA".	UTI	Oficial de Seguridad de la Información	No aplica	No aplica
Actividad Post-incidente					
18.	Almacenar la evidencia correspondiente al incidente ocurrido en una carpeta que tendrá como nombre el código del evento que se indica en el Registro de Incidencias y Vulnerabilidades	UTI	Oficial de Seguridad de la Información	Carpeta compartida UTI	No aplica
19.	Analizar cada incidente registrado en el Registro de Incidencias y Vulnerabilidades y cuando aplique, sugerir medidas preventivas o correctivas a las partes interesadas.	UTI	Oficial de Seguridad de la Información	No aplica	Mensual
20.	Revisar todos los incidentes ingresados en el Registro de Incidencias y Vulnerabilidades; a fin de identificar aquellos que son	UPPM	Coordinador/a de Modernización de la Gestión	<ul style="list-style-type: none"> • Informe • Registro y Reporte de Acciones de 	Trimestral

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**





PERÚ

Ministerio de Desarrollo e Inclusión Social



GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Código: PNADP-UTI-GTI-P-005

Versión: 01

Páginas: 8 de 13

Nº	Descripción de la Actividad	Unidad responsable	Responsable (Cargo)	Registro asociado	Plazo
	recurrentes, y solicitar la implementación de medidas adicionales para prevenir la ocurrencia de nuevos incidentes.			Mejora (PNADP-UPPM-GMC-F-034)	
21.	En el caso de que algún incidente vinculado con la temática de seguridad de la información y/o algún incumplimiento del SGSI; amerite una sanción ³ (administrativa o legal), se comunicará a las áreas correspondientes.	UTI	Líder de Gobierno Digital	Informe	No aplica
22.	Almacenar toda la evidencia necesaria que soporte la aplicación de cualquier medida tomada.	UTI	Oficial de Seguridad de la Información	Información documentada	No aplica

8. Control de Cambios

Versión	Fecha	Justificación	Textos Modificados	Responsable
01		Elaboración inicial del documento		UPPM-CMG

9. Formatos

- Reporte de incidencias y vulnerabilidades (PNADP-UTI-GTI-F-009)
- Registro de incidencias y vulnerabilidades (PNADP-UTI-GTI-F-010)

10. Procesos relacionados

- Gestión de tecnologías de la información
- Gestión de la mejora continua

11. Anexos

- Anexo nº 01: Categorías de incidentes de seguridad de la información
- Anexo nº 02: Severidad de un incidente de seguridad de la información
- Anexo nº 03: Matriz de requisitos de calidad, antisoborno y seguridad de la información
- Anexo nº 04: Flujograma de información

³ Si la sanción requiere medidas disciplinarias, se recurrirá a la URH para el análisis y ejecución de las mismas, de corresponder. Si la sanción requiere acciones legales, se recurrirá a la UAJ, a fin de tomar las acciones respectivas.

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.



 PERÚ Ministerio de Desarrollo e Inclusión Social			GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
			Código: PNADP-UTI-GTI-P-005	
	Versión: 01	Páginas: 9 de 13		

Anexo nº 01: Categorías de incidentes de seguridad de la información

1. Infracción de leyes y reglamentaciones

- a) Infracción de las leyes o reglamentaciones identificadas en la matriz de cumplimiento legal para el Sistema de Gestión de Seguridad de la Información.
- Instalar software sin licenciamiento.
 - Divulgación de datos e imágenes personales con los cuales se infringen las leyes de protección de los datos personales.
 - Fraudes informáticos (ver ejemplos en el ítem 7).

2. Incumplimiento del Sistema de Gestión de Seguridad de la Información

- a) Incumplimiento de las políticas de seguridad de la información. Ejemplo: no cumplir con política de escritorio limpio:
- Dejar información confidencial en impresoras.
 - Anotar contraseñas de acceso en papeles y dejarlas visibles.
 - Dejar información confidencial en pizarras luego de utilizar las salas de reuniones.
- b) Incumplimiento de procedimientos de seguridad de la información.

3. Código malicioso

- a) Infecciones por malware, por ejemplo:
- Un gusano utiliza directorios compartidos en la red, para infectar rápidamente varias estaciones de trabajo dentro de la organización.
 - El Programa JUNTOS recibe un aviso de un proveedor de antivirus que un nuevo virus se está propagando rápidamente a través de correo electrónico a través de Internet. El virus se aprovecha de una vulnerabilidad que está presente en muchos de los servidores del Programa JUNTOS.

4. Denegación de servicio

- a) Interrupciones o denegaciones de servicio indeseadas dentro del ámbito del SGSI. Por ejemplo:
- Un atacante envía paquetes especialmente diseñados a un servidor web, provocando que se bloquee.
 - Un atacante dirige cientos de estaciones de trabajo “zombies” para enviar tantas solicitudes de inicio de conversación con un servidor, como sea posible, de manera de saturar la reserva de memoria para tales sesiones y provocar una disrupción de la máquina.

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



 PERÚ	Ministerio de Desarrollo e Inclusión Social		GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
			Código:	PNADP-UTI-GTI-P-005
			Versión:	01

5. Acceso no autorizado

- a) Intentos de acceso no autorizado a los sistemas o a la información de la institución. Ejemplo:
- Un atacante ejecuta una herramienta de explotación de vulnerabilidades para obtener acceso al archivo de contraseñas de un servidor.
 - Un tercero no autorizado ingresa a las oficinas de la sede del Programa JUNTOS, con el propósito de sustraer activos.
 - Un servidor del Programa JUNTOS utiliza la autorización de acceso de un compañero para acceder a un área restringida a la cual aún no ha sido autorizado.

6. Uso Inapropiado

- a) Uso no autorizado de sistemas para hacer procesamientos o almacenamiento de datos. Ejemplo:
- Una persona intenta usar información de la institución para obtener beneficios personales.
 - Un/a colaborador/a divulga información de manera no autorizada a otras personas o instituciones externas al Programa JUNTOS
 - Un/a colaborador/a utiliza el correo electrónico para propagar malware.

7. Fraudes Informáticos (ver Infracción de leyes y reglamentaciones)

- a) Suplantación de identidad: un servidor del Programa JUNTOS utiliza las credenciales de acceso de otro servidor para acceder a equipos y sistemas
- b) Ataques de phishing a clientes o servidores del Programa JUNTOS.

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



Anexo nº 02: Severidad de un incidente de seguridad de la información

Severidad	Descripción	Ejemplos de casos
Grave	Hay certeza de infracción de alguna ley o reglamentación según el ordenamiento jurídico identificado en la Matriz de requisitos legales del SGSI (PNADP-UTI-GMC-F-001) o de que existen uno o más activos afectados o evidencia de impacto en términos de su disponibilidad, integridad o confidencialidad.	<ul style="list-style-type: none"> - Software sin licenciamiento. - Reproducción y/o difusión de documentos protegidos, sin la autorización. - Divulgación de datos o imágenes que infrinjan la ley de protección de datos personales. - Intrusión en sistemas. - Propagación masiva de código malicioso en la red interna. - Alteración no autorizada del sitio web. - Divulgación y/o alteración de información confidencial. - Ataque de denegación de servicio. - Robo de dispositivos.
Mediana	Existe actividad agresiva o maliciosa, pero no es posible establecer con certeza si se darán las condiciones propicias para lograr una intrusión exitosa o afectar los activos, en términos de su disponibilidad, integridad o confidencialidad.	<ul style="list-style-type: none"> - Búsqueda de vulnerabilidades desde Internet. - Intentos de acceso no autorizados. - Intentos recurrentes de inyección de comandos de sistemas operativos
Baja	La actividad no corresponde a una acción agresiva o maliciosa en sí, pero se considera tráfico anormal, el que eventualmente podría afectar los activos.	<ul style="list-style-type: none"> - Accesos a aplicaciones web denegadas por condiciones de desbordamiento de memoria reservada o detección de caracteres en campo de texto. - Equipo con presencia de un programa o aplicación no deseados. - Altas tasas de tráfico, asociable a actividad de un malware.

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



   	GESTIÓN DE VULNERABILIDADES E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
	Código:	PNADP-UTI-GTI-P-005	
	Versión:	01	Páginas:

Anexo n° 03: Matriz de Requisitos de Calidad – Antisoborno – Seguridad de la información

Nombre del Proceso:	Gestión de Tecnologías de la Información	Responsable del proceso:	Jefe/a de UTI
----------------------------	--	---------------------------------	---------------

Subproceso	Requisitos			Control	Criterio de Aceptación	Frecuencia	Responsable	Acciones a tomar en caso de incumplimiento a los criterios de aceptación
	Tipo							
	Calidad	Antisoborno	Seg. Información					
Gestión de vulnerabilidades e incidentes	X			Oportunidad en la realización de la identificación de incidentes recurrentes.	De acuerdo a la frecuencia establecida en el presente procedimiento.	Trimestral	Coordinador/a de Modernización de la Gestión	Identificación de hallazgo y registro en el formato de Registro y Reporte de Acciones de Mejora (PNADP-UPPM-GMC-F-034).
			X	Confiabledad en los análisis de las incidencias	Análisis realizado de acuerdo al Anexo 01	Por cada incidencia	Oficial de seguridad de la información	Identificación de hallazgo y registro en el formato de Registro y Reporte de Acciones de Mejora (PNADP-UPPM-GMC-F-034).

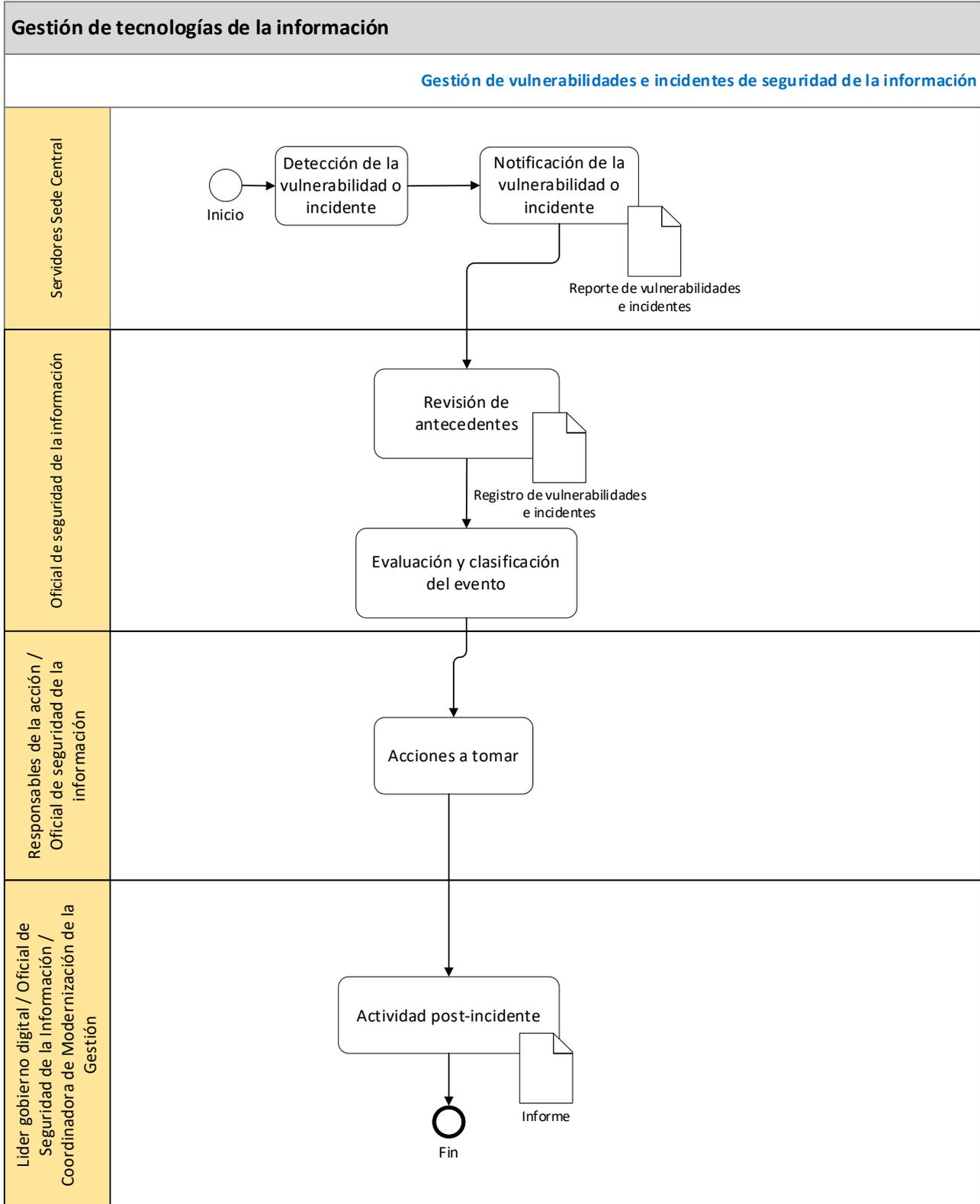
Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**





Anexo nº 04: Flujograma de información



Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



REPORTE DE INCIDENCIAS Y VULNERABILIDADES

PNADP-UTI-GTI-F-009/Rev.1

DATOS DEL REPORTE			
Apellidos y Nombres	[APELIDOS Y NOMBRES DEL EMISOR DEL REPORTE]		
Tipo Evento		Clase de incidencia (solo si es incidencia)	
Fecha del evento	[DIA/MES/AÑO]	Hora del evento	[COLOCAR HORA]
Activos afectados	[ACTIVOS DE INFORMACIÓN PERJUDICADOS]		
DESCRIPCIÓN DEL EVENTO			
COLOCAR LA INFORMACIÓN SOLICITADA, SEGÚN CORRESPONDA A) SINTOMAS O AFECTACION B) MEDIDAS DE MITIGACION ACCIONADAS FRENTE AL EVENTO C) CAUSA PROBABLE O EXACTA DEL EVENTO D) ACCIONES NECESARIAS PARA QUE NO VUELVA A OCURRIR EL EVENTO			
INFORMACIÓN ADICIONAL			
[COLOCAR LA INFORMACIÓN ADICIONAL QUE SE CONSIDERE PERTINENTE]			
DOCUMENTOS ADJUNTOS			
[EN CASO SE ADJUNTEN DOCUMENTOS, MENCIONARLOS]			

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

Esta es una copia auténtica imprimible de un documento electrónico archivado por Programa Nacional de Apoyo Directo a los Más Pobres, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026- 2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: <https://sgd.juntos.gob.pe/verifica/inicio.do> e ingresando el siguiente código de verificación: **SYEERAS**



REGISTRO DE INCIDENCIAS Y VULNERABILIDADES

PNADP-UTI-GTI-F-010/Rev.1

N°	Código	Tipo de evento	Fecha Incidente	Hora Incidente	Apellidos y Nombres de la persona que emitió el reporte	Activos afectados	Detalle del suceso	Severidad	Requiere acción	Acción a Tomar	Responsable	Fecha de ejecución	Verificación de la acción	Estado
001	VUL-001	VUL						GRAVE	SI					CERRADO
002	INC-002	INC						BAJA	SI					ABIERTO
003	VUL-003	VUL						GRAVE	NO					ABIERTO
004	VUL-004	VUL						MEDIANA	SI					ABIERTO
005	INC-005	INC						GRAVE	NO					ABIERTO
006	VUL-006	VUL						GRAVE	SI					ABIERTO
007	VUL-007	VUL						GRAVE	SI					ABIERTO

Toda copia de este documento que se encuentre fuera del entorno del Portal Web JUNTOS PODEMOS es una COPIA NO CONTROLADA.

