INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

PROCEDIMIENTO ADMINISTRATIVO PARA LA GESTIÓN DE INCIDENTES, AMENAZAS Y DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN – OTIN

Código: PRA-011-OTIN-2016-V01

PROCEDIMIENTO	
NOMBRE DEL PROCEDIMIENTO: PROCEDIMIENTO ADMINISTRATIVO PARA LA GESTIÓN DE INCIDENTES, AMENAZAS Y DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN – OTIN	
CODIGO: PRA-011-OTIN-2016-V01	**VERSION:** 01
PROCESO AL QUE PERTENECE: Gestión de Seguridad de la Información	
Elaborado por: Unidad de Calidad y Seguridad de la Información	**Aprobado por:** Director Técnico de la Oficina Técnica de Informática
Nombre: Jhino Arias Moreno	**Nombre:** Manuel Matos Alvarado
Fecha: 04 OCT 2016	**Fecha:** 04 OCT 2016
Firma	**Firma**

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA – Oficina Técnica de Informatica – INEI

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA – V° B° – Oficina Técnica de Informática – INEI

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA – Oficina Técnica de Informática – FRANK BRAVO MENDOZA

TABLA DE CONTENIDO

"PROCEDIMIENTO ADMINISTRATIVO PARA LA GESTIÓN DE INCIDENTES, AMENAZAS Y DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN – OTIN"

1. OBJETIVO

Preservar la confidencialidad, integridad y disponibilidad ante los incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información de la Oficina Técnica de Informática – OTIN.

2. ALCANCE

El presente procedimiento tiene alcance a todos los incidentes, amenazas y debilidades asociados a la seguridad de la información y electrónica. Este procedimiento se aplica a todos los usuarios y/o trabajadores que tienen acceso a activos de información del Instituto Nacional de Estadística e Informática – INEI.

3. RESPONSABLES

3.1. Unidad de Calidad y Seguridad de la Información

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento, respondiendo oportunamente ante incidentes y/o amenazas que correspondan a la seguridad de la información.
- Informar inmediatamente a la Dirección Técnica de la Oficina Técnica de Informática – OTIN la ocurrencia de incidentes o la detección de amenazas y/o debilidades que afecten a la seguridad de la información o representen una amenaza.
- Auditar todas las actividades de la Unidad de Infraestructura TIC.
- El especialista en Seguridad de la Información deberá elaborar informes sobre el estado de vulnerabilidades en la seguridad de la información.

3.2. Unidad de Operaciones

- Recibe, reporte, investiga, clasifica e informa del incidente.
- Comunicar a la Unidad de Calidad y Seguridad de la Información si el incidente afecta a la seguridad de la información o representa una amenaza en la continuidad de las operaciones.
- Informar a la Unidad a la Unidad de Calidad y Seguridad de la Información sobre la atención realizada en la Institución.

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA V° B° Oficina Técnica de Informática OTIN Michael Malaga Matasich -INEI-

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA Oficina Técnica de Informática FRANK BRAVO MENDOZA

- Brindar una solución y explicación al usuario o grupo de usuarios que fueron afectados.
- Mantener un registro actualizado de incidencias dentro de la Institución.

3.3. Unidad de Infraestructura TIC

- Monitorear la infraestructura, revisar logs y si en caso, afecten la seguridad de la información o representen una amenaza comunicar a la Unidad de Calidad y Seguridad de la información:
  - Realizar las actualizaciones a los equipos de comunicaciones.
  - Realizar los backups de la Institución.
  - Mantener actualizadas los sistemas operativos de servidores.
  - Actualizaciones del WSUS para PC's.
  - Actualizaciones de antivirus.
  - Realizar backups de la Institución y entregarlos a la Escuela Nacional de Estadística e Informática (ENEI), Instituto Nacional de Estadística e Informática (INEI) y Banco Central de Reserva (BCR).
  - Actualización de las políticas de firewall.
  - Mantenimiento preventivo de los servidores y switches.
- Mantener registros de los incidentes y/o amenazas ocurridas, incluyendo las soluciones que se implementen.

3.4. Usuario:

- Informar a la Unidad de Operaciones, mediante el Sistema de Servicios Informáticos (SSI) cada vez que sospeche o tenga certeza de algún tipo de incidente que se presente.

4. DEFINICIONES

Entiéndase para efectos del presente procedimiento, lo siguiente:

a) Procedimiento Administrativo:

Es el cauce formal de la serie de actos en que se concreta la actuación administrativa para la realización de un fin, no se confunda con

proceso administrativo el cual es una instancia jurisdiccional bajo el fuero contencioso-administrativo.

b) Integridad:

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

c) Disponibilidad:

Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

d) Confidencialidad:

Es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

e) Seguridad:

Es una forma de protección contra los riesgos.

f) Incidente:

Circunstancia o suceso que sucede de manera inesperada y que puede afec tar al desarrollo de un asunto o negocio, aunque no forme parte de él.

g) Amenaza:

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

h) Debilidad:

Permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

i) Registro:

Documento donde se relacionan ciertos acontecimientos o cosas; especialmente aquellos que deben constar permanentemente de forma oficial.

j) Spyware:

Programa espía que es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware.

Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono. Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

k) Virus Informático:

Un virus tiene por objetivo alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

l) WSUS:

WSUS o Windows Server Update Services es una función más dentro del catálogo de roles disponible en Windows Server 2008 o superior. Este rol permite disponer de un sistema centralizado de actualizaciones para equipos de puesto de trabajo Windows a través de la red local de nuestra empresa. A través de WSUS es posible gestionar completamente la distribución de las

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA V° B° Mirtha Málaga Matasich INEI

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática FRANK BRAVO MENDOZA

últimas actualizaciones publicadas por Microsoft a través del servicio Windows Update así como de los parches de seguridad más recientes.

5. DESARROLLO

5.1. Disposiciones Generales

- Se protegerán los siguientes activos de información ante incidentes, amenazas:
  - Equipos de comunicaciones.
  - Sala de servidores.
  - Computadora asignada.
  - Impresoras.
  - Correo electrónico.
  - Sistema eléctrico.
  - Equipos telefónicos.
  - Portal Institucional.
  - Sistemas de Información, aplicaciones y software en general.
  - Cualquier otro servicio computacional entregado por el INEI
- Los tipos de incidencias que pueden representar una amenaza para la seguridad de la información son:
  - Incendio o inundación en la sala de servidores.
  - Robo de computadores personales.
  - Robo de información electrónica.
  - Ingreso de personal no autorizado en la sala de servidores o estaciones de trabajo.
  - Corte eléctrico o defectos en el sistema eléctrico.
  - Hacking y técnicas de suplantación.
  - Virus informáticos y spyware.
  - No disponibilidad de Portal Institucional y Sistemas de Información.

- La primera vía formal de reporte de incidentes o amenazas será mediante el uso del Sistema de Servicios Informáticos que es utilizado por la Unidad de Operaciones, cuya dirección web es: "http://webinei.inei.gob.pe/ssi/", colocando de título de la incidencia la frase **"Incidente de seguridad de información"** u otra similar que permita reconocer la situación rápidamente. Se deberá ser lo más claro y preciso en especificar el incidente o amenaza y a que recursos tecnológicos podría estar afectando.

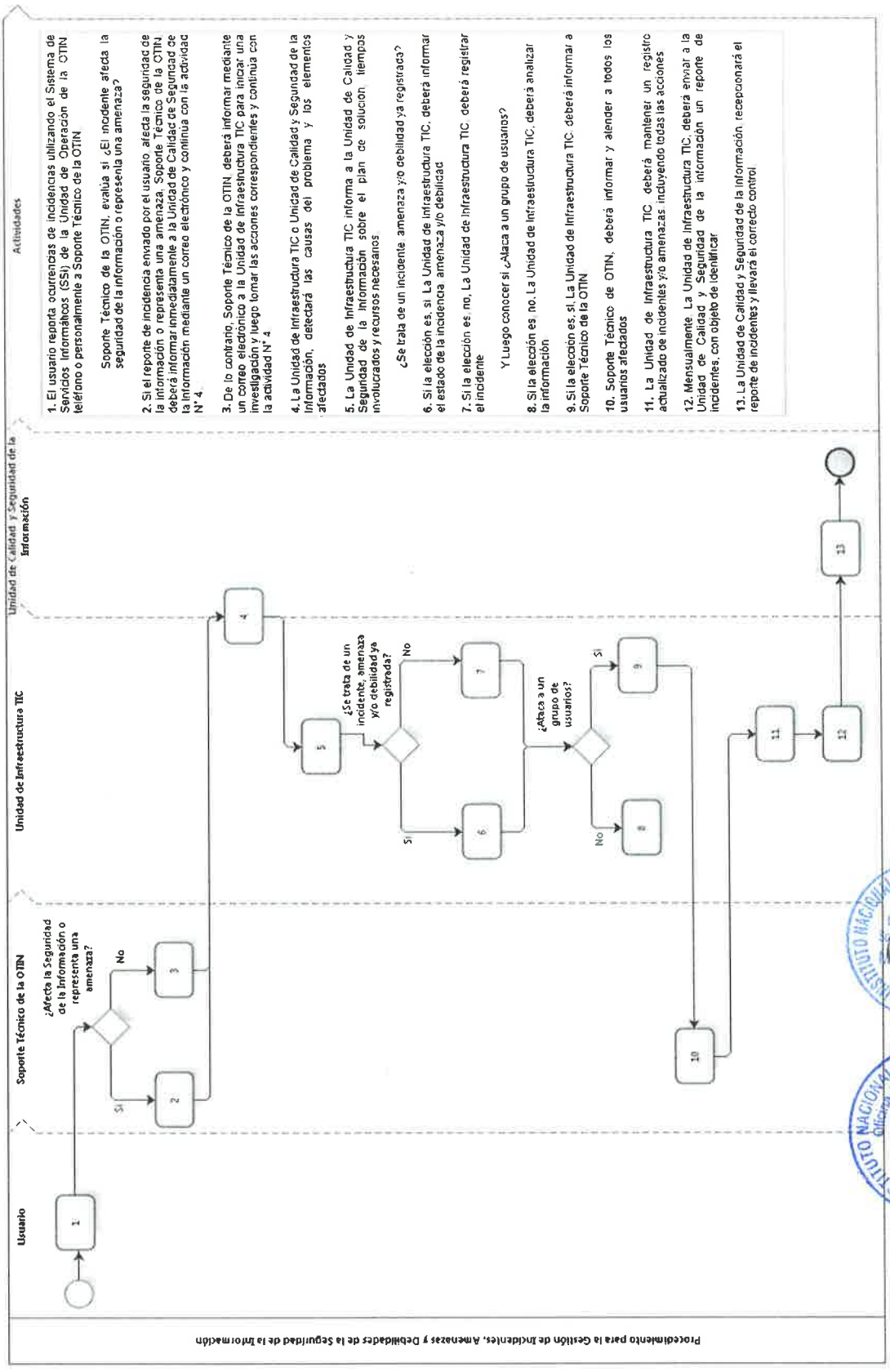
- En caso de que el incidente y/o amenaza, requiera de una intervención urgente, se deberá contactar a personal del Soporte Técnico de la OTIN vía telefónica (Anexo: 9397) o acudir personalmente a la Unidad de Operaciones, sin necesidad de enviar un correo electrónico.

- La unidad de Operaciones y/o Soporte Técnico de la OTIN deberá informar a la Unidad de Calidad y Seguridad de la Información mediante un correo electrónico a: GrupoSeguridad@inei.gob.pe si en caso, uno de los incidentes afecte a la seguridad de la información o representen una amenaza.

- Si el incidente afecta a varios usuarios, Soporte Técnico de la OTIN, realizará las comunicaciones pertinentes para informar a todos los afectados, indicando:

    - Características del Incidente.
    - Como se ven afectadas las actividades de los usuarios.
    - El estado del incidente.
    - Las acciones que se están llevando a cabo.
    - Los tiempos estimados de solución.

5.2. Diagrama de Flujo



5.3. Descripción de actividades

N° de Actividad	Desarrollo y Descripción
1	El usuario reporta ocurrencias de incidencias o la detección de amenazas y/o debilidades que pudiesen comprometer a la seguridad de activos de información de la institución, utilizando el Sistema de Servicios Informáticos (SSI) de la Unidad de Operación de la OTIN, teléfono o personalmente a Soporte Técnico de la OTIN.
	Soporte Técnico de la OTIN, evalúa si ¿El incidente afecta la seguridad de la información o representa una amenaza?
2	Si el reporte de incidencia enviado por el usuario, afecta la seguridad de la información o representa una amenaza, Soporte Técnico de la OTIN, deberá informar inmediatamente a la Unidad de Calidad de Seguridad de la Información mediante un correo electrónico y continúa con la actividad N° 4.
3	De lo contrario, Soporte Técnico de la OTIN, deberá informar mediante un correo electrónico a la Unidad de Infraestructura TIC para iniciar una investigación y luego tomar las acciones correspondientes y continúa con la actividad N° 4.
4	La Unidad de Infraestructura TIC o Unidad de Calidad y Seguridad de la Información, detectará las causas del problema y los elementos afectados.
5	La Unidad de Infraestructura TIC informa a la Unidad de Calidad y Seguridad de la Información sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema, quien deberá realizar las gestiones correspondientes incluyendo la comunicación al Director Técnico.
	¿Se trata de un incidente, amenaza y/o debilidad ya registrada?
6	Si la elección es, si, La Unidad de Infraestructura TIC, deberá informar el estado de la incidencia, amenaza y/o debilidad.
7	Si la elección es, no, La Unidad de Infraestructura TIC, deberá registrar el incidente.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA V° B° Oficina Técnica de OTIN Natalia Málaga Matalich -INEI-

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática FRANK BRAVO MENDOZA

	Y Luego conocer si ¿Ataca a un grupo de usuarios?
8	Si la elección es, no, La Unidad de Infraestructura TIC, deberá analizar la información.
9	Si la elección es, si, La Unidad de Infraestructura TIC, deberá informar a Soporte Técnico de la OTIN.
10	Soporte Técnico de OTIN, deberá informar y atender a todos los usuarios afectados.
11	La Unidad de Infraestructura TIC, deberá mantener un registro actualizado de incidentes y/o amenazas, incluyendo todas las acciones o medidas que se implementen para solucionarlos ya se de forma total o parcial.
12	Mensualmente, La Unidad de Infraestructura TIC, deberá enviar a la Unidad de Calidad y Seguridad de la información un reporte de incidentes, con objeto de identificar
13	La Unidad de Calidad y Seguridad de la Información, recepcionará el reporte de incidentes y llevará el correcto control.

6. REGISTROS

6.1 Reporte Generado por el Sistema de Servicios Informáticos que es utilizado por la Unidad de Operaciones.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA – INEI – V° B° Oficina Técnica de Informática Michael Calaga Matasich

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática FRANK BRAVO MENDOZA

7. ANEXOS

7.1 Guía para la clasificación de incidentes

Las siguientes categorías podrían utilizarse para la clasificación del incidente.

NOMBRE	EJEMPLO
Exposición de datos personales	Se han revelado datos personales confidenciales.
Denegación de servicio	Actividad maliciosa tendiente a dificultar el acceso a un servicio.
Actividad de software malicioso	Virus, worms, keylogger, phishing.
Violación de póliticas de seguridad	Uso inapropiado de recursos.
Servicios no autorizados	Servicio ftp no autorizado.
Acceso no autorizados lógico / físico	Abuso de privilegios / Acceso no autorizado a áreas definidas como criticas.

7.2 Guía de evaluación de la criticidad de un incidente

SEVERIDAD	DESCRIPCIÓN
ALTO	➢ Afecta gran parte del INEI ➢ Impacta activos críticos del INEI ➢ Afecta información confidencial del trabajador. ➢ Amenaza la vida de los trabajadores. ➢ Robo o alteración de información crítica. ➢ Destrucción de propiedad del INEI.

	➢ Aprovechamiento de brechas de seguridad detectadas y no informadas.
MEDIO	➢ Impacta un número moderado de sistemas o personas. ➢ Impacta activos importantes pero no críticos. ➢ Puede propagarse a otros activos ➢ Acceso lógico o físico a sitios no autorizados. ➢ No informar acerca de brechas en la seguridad detectadas.
BAJO	➢ Impacta un número pequeño de sistemas o personas. ➢ Afecta un segmento de red. ➢ Baja probabilidad de propagación. ➢ Instalación y/o descarga de software no autorizado. ➢ Visitas a páginas de Internet no autorizadas.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA V° B° Matasich

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática FRANK BRAVO MENDOZA