INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

PROCEDIMIENTO ADMINISTRATIVO

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

Código: PRA-018-OTIN-2018
Versión 1.0.0

PROCEDIMIENTO		
NOMBRE DEL PROCEDIMIENTO: PROCEDIMIENTO ADMINISTRATIVO PARA LA GESTIÓN DE INCIDENTES, AMENAZAS Y DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN – OTIN		
CODIGO: PRA-018-OTIN-2018		**VERSION:** 2.0.0
PROCESO AL QUE PERTENECE: Gestión de la Seguridad		
Elaborado por: Unidad Funcional de Infraestructura Tecnológica	**Coordinado con:** Unidad Funcional de Calidad, Procesos y Seguridad de la Información	**Aprobado por:** Director Técnico de la Oficina Técnica de Informática
Nombre: Ing. Juan Padilla	**Nombre:** Ing. Katherine Montenegro	**Nombre:** Ing. CIP Manuel Matos Alvarado
Fecha: 9/11/2018	**Fecha:** 19/11/2018	**Fecha:**
Firma	**Firma**	**Firma**
		

Información del Documento

Fecha de Creación:	Código:	Versión:	Elaborado por:	Aprobado por:
04/10/2016	PRA-011-OTIN-2016-V01	1.0.0	Jhino Arias Moreno	Manuel Amador Mattos Alvarado - Director Técnico de la Oficina Técnica de Informática - OTIN
	PRA-018-OTIN-2018	2.0.0	Juan Padilla Padilla	Manuel Amador Mattos Alvarado - Director Técnico de la Oficina Técnica de Informática - OTIN

Historial del Documento

Fecha de Creación:	Versión:	Modificado/Creado por:	Descripción de la modificación:
04/10/2016	1.0.0	Jhino Arias Moreno	Creación del primer documento
	2.0.0	Juan Padilla Padilla	Actualización del documento conforme observaciones

TABLA DE CONTENIDO

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

1. OBJETIVO

Gestionar adecuadamente los incidentes y eventos de seguridad de la información, mediante el reporte oportuno de los usuarios, y el análisis de la información para reducir la afectación negativa de la seguridad de la información y/o la continuidad de las operaciones de la entidad, esto con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información ante los incidentes, 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 que puedan presentarse en el Instituto Nacional de Estadística e Informática – INEI. Asimismo, se aplica a todos los usuarios y/o trabajadores que tienen acceso a activos de información del INEI, el cual se inicia con la detección del incidente de seguridad de la información, continúa con la estrategia de contención y termina con el análisis post-incidente.

3. RESPONSABLES

Unidad Funcional de Calidad, Procesos y Seguridad de la Información

- Velar por el cumplimiento de este procedimiento, realizando el seguimiento de los incidentes de seguridad de la información presentados en la institución.
- 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 las actividades de la Unidad Funcional de Infraestructura TIC, evaluando el uso de herramientas tecnológicas de auditoria.
- El responsable de realizar el testing a las aplicaciones deberá elaborar informes sobre el estado de vulnerabilidades en la seguridad de la información y reportarlos a su Jefe inmediato para ser elevados a la Dirección de la OTIN.

Unidad Funcional de Operaciones

- Responder oportunamente ante incidentes y/o amenazas reportadas a través del Sistema de Servicios Informáticos (SSI), y las recepcionadas por el personal de Soporte Técnico.
- Recibir, reportar, investigar, clasificar e informar del incidente.

- Comunicar a la Unidad Funcional de Calidad y Seguridad de la Información y a la Unidad Funcional de Infraestructura Tecnológica si el incidente afecta a la seguridad de la información o representa una amenaza en la continuidad de las operaciones.
- Si el incidente puede ser solucionado dentro de la Unidad Funcional de Operaciones, informa a la Unidad Funcional de Calidad, Procesos y Seguridad de la Información sobre la atención realizada en la Institución; caso contrario deriva el incidente a la Unidad Funcional respectiva.
- Brindar una solución y explicación al usuario o grupo de usuarios que fueron afectados.
- Mantener un registro actualizado de incidencias dentro de la Institución en formato digital y físico.

Unidad Funcional de Infraestructura TIC

- Monitorear la infraestructura, revisar logs periódicamente y si en caso los incidentes, afecten la seguridad de la información o representen una amenaza comunicar a la Unidad Funcional de Calidad, Procesos y Seguridad de la información:

  - ✓ Realizar las actualizaciones del firmware de los equipos de comunicaciones.
  - ✓ Realizar los backups diarios, mensuales y anuales de la data de la Institución.
  - ✓ Mantener actualizados los sistemas operativos de servidores, previamente testeados por el área de seguridad y producción.
  - ✓ Actualizar las PC's mediante el servicio de actualización de Windows Server (WSUS).
  - ✓ Actualizar del software 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).
  - ✓ Actualizar las políticas de firewall de acuerdo a las buenas practicas (hardening).
  - ✓ Realizar el mantenimiento anual preventivo de los servidores y switches.

- Atender aquellos incidentes relacionados con la seguridad informática y el centro de datos del INEI.
- Mantener registros de los incidentes y/o amenazas ocurridas, incluyendo las soluciones que se implementen.
- Informar a la Unidad Funcional de Calidad, Procesos y Seguridad de la Información sobre la solución brindada al incidente reportado en la Institución.

Usuario:

- Informar a la Unidad Funcional de Operaciones, mediante el Sistema de Servicios Informáticos (SSI) cada vez que sospeche o tenga certeza de la presencia de algún tipo de incidente que afecte la seguridad de la información, con su respectiva evidencia.

4. DEFINICIONES

- **Amenaza:** Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas.
- **Confidencialidad:** Hace referencia a que la información debe ser solo accesible a sus destinatarios predeterminados.
- **Debilidad:** Aquello que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.
- **Disponibilidad:** Principio por el cual se debe tener acceso a la información cuando se solicite.
- **Integridad:** La información debe ser correcta y completa.
- **Incidente:** Circunstancia o suceso de manera inesperada y que puede afectar al desarrollo de un asunto o negocio, aunque no forme parte de él.
- **Registro:** Documento donde se relacionan ciertos acontecimientos o cosas; especialmente aquellos que deben constar permanentemente de forma oficial.
- **Seguridad:** Es una forma de protección contra los riesgos.
- **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 productos que realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.
- **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.
- **Vulnerabilidad:** Es la debilidad en un sistema permitiendo a un atacante violar la confidencialidad del sistema o de sus datos y aplicaciones.
- **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 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 y 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:

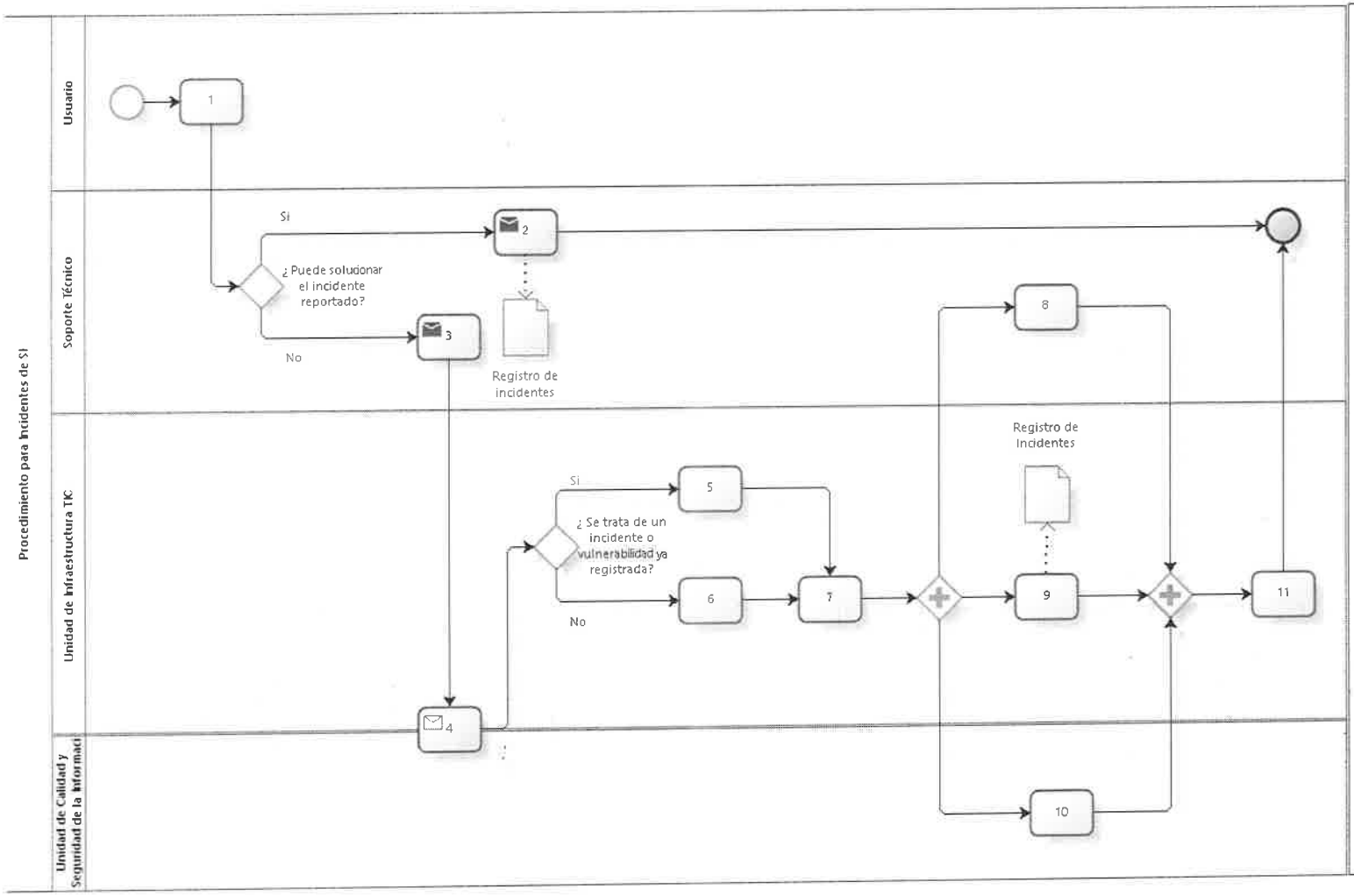
  - ✓ Incendio o inundación en la sala de servidores.
  - ✓ Robo de computadores personales.
  - ✓ Robo de información electrónica.
  - ✓ Ingreso de personal no autorizado en la sala de servidores o estaciones de trabajo.
  - ✓ Corte eléctrico o defectos en el sistema eléctrico.
  - ✓ Hacking y técnicas 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 Funcional 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, también pueden llamar al Anexo 9397 del INEI o asistir personalmente con algún personal de Soporte Técnico.
- 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 coordinar personalmente a la Unidad Funcional de Operaciones, sin necesidad de enviar un correo electrónico.

- La Unidad Funcional de Operaciones y/o personal de Soporte Técnico de la OTIN deberá informar a la Unidad Funcional de Calidad, Procesos 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, el personal de 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



1: Reportar ocurrencias de incidencias o la detección de amenazas y/o debilidades a través del link: http://webinei.inei.gob.pe/ssi/, por teléfono o personalmente a Soporte Técnico de la OTIN.
¿Soporte Técnico puede solucionar el incidente reportado?
2: Si: Registrar el incidente, solucionar e informar sobre la incidencia a la Unidad Funcional de Calidad, Procesos de Seguridad. Fin del Procedimiento.
3: No: Informar a la Unidad Funcional de Infraestructura TIC y a la Unidad Funcional de Calidad, Procesos y Seguridad de la Información para iniciar una investigación asimismo tomar las acciones correspondientes.
4: Detectar las causas del problema y los elementos afectados.
¿Se trata de un incidente o vulnerabilidad antes registrada?
5: Si: Actualizar el número de veces del incidente identificado.
6: No: Registrar el nuevo incidente.
7: Solucionar el incidente, informar sobre la incidencia a la Unidad Funcional de Calidad, Procesos de Seguridad de la Información y comunicar al personal de Soporte Técnico que la incidencia ha sido solucionada.
8: Informar y atender a los usuarios afectados.
9: Mantener un registro actualizado de incidentes o vulnerabilidad.
10: Recepcionar el reporte y llevar el control del incidente.
11: Informar al Director Técnico de la OTIN sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema.
Fin del Procedimiento

5.3. DESCRIPCIÓN DE ACTIVIDADES

N°	Responsable	Actividades
Inicio del Procedimiento		
1	Usuario	Reportar 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) a través del link: http://webinei.inei.gob.pe/ssi/, por teléfono o personalmente a Soporte Técnico de la OTIN.
		¿Soporte Técnico puede solucionar el incidente reportado?
2	Soporte Técnico	Si: Registrar el incidente, solucionar e informar sobre la incidencia a la Unidad Funcional de Calidad, Procesos y Seguridad mediante un correo electrónico. Fin del Procedimiento.
3	Soporte Técnico	No: Informar mediante un correo electrónico a la Unidad Funcional de Infraestructura TIC y a la Unidad Funcional de Calidad, Procesos y Seguridad de la Información para iniciar una investigación asimismo tomar las acciones correspondientes.
4	Unidad Funcional de Infraestructura TIC // Unidad Funcional de Calidad y Seguridad de la Información	Detectar las causas del problema y los elementos afectados.
		¿Se trata de un incidente o vulnerabilidad antes registrada?
5	Unidad Funcional de Infraestructura TIC	Si: Actualizar el número de veces del incidente identificado.
6	Unidad Funcional de Infraestructura TIC	No: Registrar el nuevo incidente.
7	Unidad Funcional de Infraestructura TIC	Solucionar el incidente, informar sobre la incidencia a la Unidad Funcional de Calidad, Procesos y Seguridad mediante un correo electrónico y comunicar a Soporte que la incidencia ha sido solucionada.
8	Unidad Funcional de Infraestructura TIC	Informar y atender a los usuarios afectados.
9	Soporte Técnico	Mantener un registro actualizado de incidentes o vulnerabilidad. Incluyendo todas la acciones o medidas que se implementen para solucionarlos ya sea de forma parcial o total.
10	Unidad Funcional de Calidad y seguridad	Recepcionar el reporte y llevar el control del incidente.

N°	Responsable	Actividades
11	Unidad Funcional de Infraestructura TIC	Informar al Director Técnico de la OTIN sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema.
Fin del procedimiento		

6. REGISTROS ASOCIADOS

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

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 políticas 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.