sunarp
V° B°
Firmado digitalmente por:
OBLITAS CENTENO Oswaldo Arturo FAU 20260998898 hard
Motivo: Doy Visto Bueno del Documento
Fecha: 2022/09/27 14:51:18-0500

sunarp
V° B°
Firmado digitalmente por:
NEYRA ZUMAETA Elizabeth Nilda FAU 20260998898 hard
Motivo: Doy Visto Bueno del Documento
Fecha: 2022/09/27 16:01:35-0500

sunarp
V° B°
Firmado digitalmente por:
MARCHETTI ESPEJO Armando Angel FAU 20260998898 soft
Motivo: Doy Visto Bueno del Documento
Fecha: 2022/09/27 15:00:27-0500

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°664-2022-SUNARP/ZRIX/JEF

sunarp
V° B°
Firmado digitalmente por:
MOGOLLON CHUMPITAZ Carlos Gregorio FAU 20260998898 hard
Motivo: Doy Visto Bueno del Documento
Fecha: 2022/09/27 16:36:57-0500

Lima, 27 de setiembre de 2022

VISTOS:

El Memorándum Nº00007-2022-SUNARP/ZRIX/JEF/JEF-SIG-SGSI del 07 de septiembre de 2022; el Memorándum Nº01246-2022-SUNARP/ZRIX/UPPM del 13 de septiembre de 2022; el Informe Nº00221-2022-SUNARP/ZRIX/UAJ del 15 de septiembre de 2022; el Memorándum Nº00027-2022-SUNARP/ZRIX/JEF/JEF-SIG del 23 de septiembre de 2022, y;

CONSIDERANDO:

Que, mediante el artículo 1° de la Ley N°26366, Ley de Creación del Sistema Nacional de los Registros Públicos y de la Superintendencia de los Registros Públicos, publicada en el Diario Oficial "El Peruano" el 16 de octubre de 1994, se crea el Sistema Nacional de los Registros Públicos con la finalidad de mantener y preservar la unidad y coherencia del ejercicio de la función registral en todo el país, orientado a la especialización, simplificación, integración y modernización de la función, procedimientos y gestión de todos los registros que lo integran;

Que, mediante el artículo único de la Ley N°27309, publicado en el Diario Oficial "El Peruano" el 17 de julio de 2000, se modifica el Título V del Libro Segundo del Código Penal, incorporándose los Delitos Informáticos;

Que, mediante el artículo 1° de la Ley N°27658, Ley Marco de Modernización de la Gestión del Estado, publicada en el Diario Oficial "El Peruano" el 30 de enero del 2002, se declaró al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, por Decreto Supremo N°052-2008-PCM, publicado en el Diario Oficial "El Peruano" el 19 de julio de 2008, se aprobó el Reglamento de la Ley de Firmas y Certificados Digitales, con el objeto de regular, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica;

Que, por Resolución Ministerial N°004-2016-PCM, publicado en el Diario Oficial "El Peruano" el 14 de enero de 2016, se aprobó 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 y su modificatoria;

Que, por Resolución Directoral N°056-2017-INACAL/DN, publicado en el Diario Oficial "El Peruano" el 29 de diciembre de 2017, se aprobó la Norma Técnica Peruana NTP-ISO/IEC 27002:2017, Tecnología de la Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición;

Que, mediante Resolución de la Superintendente Nacional de los Registros Públicos N°208-2008-SUNARP/SN del 17 de julio de 2008, se aprueba la Directiva N°004-2008- SUNARP/SN, denominada "Normas para la Administración, Uso y Control del Servicio de Publicidad Registral en Línea";

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°664-2022-SUNARP/ZRIX/JEF

Lima, 27 de setiembre de 2022

Que, mediante Resolución de la Gerencia General de la Superintendente Nacional de los Registros Públicos N°210-2022-SUNARP/GG del 04 de julio de 2022, se aprobó la Directiva DI-002-2022-UOM-OPPM, denominada *"Directiva que regula la emisión de los documentos normativos de la Sunarp",* que establece las disposiciones para la formulación, aprobación, emisión, revisión, actualización y derogación de los documentos normativos;

Que, de acuerdo al artículo segundo de la Resolución Jefatural N°350-2018-SUNARPZ.R.N°IX/JEF del 18 de junio de 2018, se designó como Supervisor de Seguridad de la Información de la Zona Registral N°IX-Sede Lima, al Analista de Producción de la Unidad de Tecnologías de la Información, Ingeniero Armando Ángel Marchetti Espejo; asimismo, con el artículo segundo de la Resolución Jefatural N°391-2020-SUNARP-Z.R.N°IX/JEF del 19 de noviembre de 2020, se modificó la denominación de Coordinador por la de "Oficial" a los responsables de cada uno de los sistemas de gestión a quienes a partir de esa fecha se les identificará conforme se detalla: Oficial del Sistema de Gestión de Calidad, Oficial del Sistema de Gestión de Seguridad de la Información, Oficial del Sistema de Seguridad y Salud en el Trabajo;

Que, mediante Resolución Jefatural N°245-2020-SUNARP-Z.R.N°IX/JEF del 03 de agosto de 2020, se designó Coordinador General del Sistema Integrado de Gestión a la Asesor de la Zona Registral N°IX-Sede Lima, Ingeniera de Sistemas Nancy Haydee Vílchez López;

Que, mediante Resolución Jefatural N°271-2020-SUNARP-Z.R.N°IX/JEF del 21 de agosto de 2020, se conformó el Comité del Sistema Integrado de Gestión – SIG de la Zona Registral N°IX-Sede Lima, cuya responsabilidad principal es actuar como un ente rector de gestión, a cargo de desarrollar las tareas de planificación y seguimiento del Sistema Integrado de Gestión, absorbiendo las funciones del Comité de Gestión de Calidad;

Que, mediante Resolución Jefatural N°598-2021-SUNARP-ZRIX/JEF del 09 de diciembre de 2021, se aprobó por cambio de versión, el Procedimiento de Gestión de Documentos de Soporte a los Procesos (Versión: 03, Código: PR-003-UPP-ZRIX);

Que, mediante Memorándum Nº00007-2022-SUNARP/ZRIX/JEF/JEF-SIG-SGSI, el Oficial del Sistema de Gestión de Seguridad de la Información remite a la Unidad de Planeamiento, Presupuesto y Modernización, el proyecto del Procedimiento de Gestión de Incidentes de Seguridad de la Información, versión 01, con el debido sustento técnico, para su revisión;

Que, mediante Informe N°00221-2022-SUNARP/ZRIX/UAJ, el Jefe de la Unidad de Asesoría Jurídica, remite a la Coordinador General del Sistema Integrado de Gestión, el proyecto del Procedimiento en mención, con la opinión legal favorable, en atención a lo requerido por Memorándum N°01246-2022-SUNARP/ZRIX/UPPM del 13 de septiembre de 2022, emitido por la Jefe de la Unidad de Planeamiento, Presupuesto y Modernización, con la opinión favorable de su Unidad respecto del contenido, estructura y sustento técnico del citado proyecto;

Que, mediante Memorándum N°00027-2022-SUNARP/ZRIX/JEF/JEF-SIG, la Coordinador General del Sistema Integrado de Gestión informa a la Unidad de Asesoría Jurídica que, en reunión de Comité del Sistema Integrado de Gestión de fecha 19 de septiembre de 2022, a través de Acta N°013-2022, se aprobó el Procedimiento de Gestión de Incidentes de Seguridad de la Información, en su primera versión; asimismo, solicita la emisión del documento normativo correspondiente a fin de concluir con el flujo de aprobación;

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°664-2022-SUNARP/ZRIX/JEF

Lima, 27 de setiembre de 2022

Que, esta Jefatura considera pertinente aprobar, por cambio de versión, el Procedimiento de Gestión de Incidentes de Seguridad de la Información (Versión: 01, Código: PR-011-UTI-ZRIX), el mismo que cuenta con la aprobación del Comité del Sistema Integrado de Gestión, según Acta N°013-2022 del 19 de septiembre de 2022;

Con las visaciones de la Coordinador General del Sistema Integrado de Gestión, del Oficial de Seguridad de la Información, del Jefe de la Unidad de Tecnologías de la Información, de la Jefe de la Unidad de Planeamiento, Presupuesto y Modernización, y del Jefe de la Unidad de Asesoría Jurídica;

En uso de las atribuciones conferidas por el Consolidad del Texto Integrado del Reglamento de Organización y Funciones de la Sunarp, aprobado por Resolución de la Superintendencia Nacional de los Registros Públicas N°035-2022-SUNARP/SN y en virtud de la Resolución de la Gerencia General de la Superintendencia Nacional de los Registros Públicos N°336-2021-SUNARP/GG del 16 de diciembre de 2021.

SE RESUELVE:

Artículo 1.- Aprobación de la primera versión del Procedimiento de Gestión de Incidentes de Seguridad de la Información

Apruébese la primera versión, del Procedimiento de Gestión de Incidentes de Seguridad de la Información (Versión: 01, Código: PR-011-UTI-ZRIX), el mismo que como anexo forma parte integrante de la presente Resolución.

Artículo 2.- Difusión

Disponer que, a través de la Unidad de Comunicaciones, se ejecuten las acciones respectivas destinadas a su publicación en la página web institucional con la finalidad de que todas las áreas tomen conocimiento y brinden las facilidades del caso, cuando corresponda.

Regístrese, comuníquese y publíquese en el portal institucional.

sunarp
Firmado digitalmente por:
PEREZ SOTO Jose Antonio FAU 20260998898 soft
Motivo: Soy Autor del Documento
Fecha: 2022/09/27 16:42:23-0500

Firmado digitalmente
JOSÉ ANTONIO PÉREZ SOTO
Jefe Zonal (e)
Zona Registral N°IX-Sede Lima - SUNARP

	Denominación:	Código:
sunarp Superintendencia Nacional de los Registros Públicos	**PROCEDIMIENTO**	**PR-011-UTI-ZRIX**
	Aprobación: **Resolución N°664-2022-SUNARP-ZRIX/JEF**	

Versión:	Fecha de aprobación	Páginas:
V.01	**27/09/2022**	**1/14**

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

I. OBJETIVO 3
II. ALCANCE 3
III. BASE LEGAL 3
IV. DEFINICIONES Y ABREVIATURAS 4
V. DISPOSICIONES GENERALES 5
VI. DESCRIPCIÓN DEL PROCEDIMIENTO 6
VII. ANEXOS 10
ANEXO N° 01: EJEMPLOS DE EVENTOS E INCIDENTES MENORES DE SEGURIDAD DE LA INFORMACIÓN 11
ANEXO N° 02: DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 13
CUADRO DE CONTROL DE CAMBIOS 14

I. OBJETIVO

Establecer la secuencia de actividades para la identificación, evaluación, atención y cierre de eventos e incidentes de seguridad de la información, para su gestión efectiva e identificación de lecciones aprendidas.

II. ALCANCE

El presente procedimiento es de cumplimiento obligatorio para el personal involucrado de la gestión de los eventos e incidentes de seguridad de la información de la Zona Registral N° IX – Sede Lima.

III. BASE LEGAL

La siguiente documentación contiene disposiciones que, al ser citadas en este texto, constituyen requisitos de este procedimiento.

3.1. Ley N° 26366 – Ley de Creación del Sistema Nacional de los Registros Públicos y de la Superintendencia de los Registros Públicos, de fecha 16 de octubre de 1994 y su modificatoria.

3.2. Decreto Supremo N° 008-2004-JUS, que aprueba el Texto Único de Procedimientos Administrativos – TUPA, de fecha 27 de Julio de 2004.

3.3. Decreto Supremo N° 052-2008-PCM que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, de fecha 19 de julio de 2008 y su modificatoria.

3.4. Resolución del Superintendente Nacional de los Registros Públicos N° 208-2008-SUNARP/SN, que aprueba la Directiva N° 004-2008-SUNARP/SN denominada “Normas para la Administración Uso y Control del Servicio de Publicidad Registral en Línea”, de fecha 17 de julio de 2008.

3.5. Resolución del Superintendente Nacional de los Registros Públicos N° 126-2012-SUNARP/SN, que aprueba el Texto Único Ordenado del Reglamento General de los Registros Públicos, de fecha 18 de mayo de 2012 y su modificatoria.

3.6. Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal, de fecha 17 de julio de 2000.

3.7. Resolución Ministerial Nº 004-2016-PCM Aprueban 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 y su modificatoria.

IV. DEFINICIONES Y ABREVIATURAS

Para los propósitos de este procedimiento se aplican las siguientes definiciones:

4.1. Confidencialidad: Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.

4.2. Disponibilidad: Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

4.3. Evento / Suceso: Ocurrencia o cambio de un conjunto particular de circunstancias.

Nota N° 01: Un evento puede ser una o más ocurrencias, y puede tener varias causas.

Nota N° 02: Un evento puede consistir en algo que no sucede (de manera preventiva).

Nota N° 03: Un evento a veces puede ser referido como un "incidente" o "accidente".

4.4. Evento de seguridad de la información: Ocurrencia identificada en un sistema, servicio o el estado de la red que indica una posible violación de la política de seguridad de la información (que se encuentran en la política del SIG y las políticas específicas de Seguridad de la Información) o la falla o fracaso de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la información.

4.5. Gestión de incidentes de seguridad de la información: Procesos para detectar, informar, evaluar, responder frente a, y aprender de incidentes de seguridad de la información.

4.6. Incidente de seguridad de la información: Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad significativa de comprometer las operaciones del negocio o institución y amenazar la seguridad de la información.

4.7. Integridad: Propiedad de la información del cual consiste en que esta sea exacta y completa.

4.8. Nivel 1: Personal de la Mesa de Ayuda que se encarga de recepcionar, analizar y evaluar los eventos e incidentes ingresados para su asignación a los especialistas correspondientes, ya sea del Nivel 2 o Nivel 3.

4.9. Nivel 2: Personal de la Mesa de la Ayuda que se encarga de la revisión y configuración de equipos de cómputo, periféricos y suministros, hasta su solución.

4.10. Nivel 3: Personal de la Unidad de Tecnologías de la Información que brinda el soporte a las aplicaciones registrales y/o administrativas de la Zona Registral N° IX – Sede Lima hasta su solución o gestión con la Oficina de Tecnologías de la Información.

4.11. Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman entradas en salidas.

ABREVIATURAS	
CGSIG	Coordinador General del Sistema Integrado de Gestión
SGCN	Sistema de Gestión de Continuidad del Negocio
SGSI	Sistema de Gestión de Seguridad de la Información
UTI	Unidad de Tecnologías de la Información

V. DISPOSICIONES GENERALES

5.1. Todos los usuarios (servidores civiles de la Zona Registral N° IX – Sede Lima o terceros) deberán reportar los eventos o incidentes de seguridad de la información a Mesa de Ayuda a través del aplicativo de web “SistemaNacional de Mesa de Ayuda” o, de manera excepcional, por correo electrónico, teléfono u otro medio.

Nota N° 04: En caso el evento o incidente de seguridad de la información sea identificado por un tercero, cualquier personal de la Zona Registral N° IX – Sede Lima, puede reportarlos a Mesa de Ayuda por los canales indicados.

5.2. Mesa de Ayuda deberá de realizar una evaluación para determinar si es un evento o incidente menor de seguridad de la información:

- **Evento de seguridad de la información:** Cuando no genera la pérdida de la información porque el control correspondiente lo identificó y evitó que se concrete.
- **Incidente menor de seguridad de la información:** Aquellos que no ponen en peligro el desarrollo de los procesos de la institución.

5.3. Mesa de Ayuda deberá clasificar el evento o incidente menor de seguridad de la información considerando los siguientes tipos:

- INC01 - Control de seguridad ineficaz
- INC02 - Afectación de la integridad o disponibilidad de la información
- INC03 - Errores Humanos
- INC04 - Incumplimientos de las políticas o directrices
- INC05 - Incumplimientos de las medidas de seguridad físicas
- INC06 - Afectación de la confidencialidad
- INC07 - Cambios no controlados del sistema
- INC08 - Mal funcionamiento de software o hardware
- INC09 - Acceso no autorizado
- INC10 - Otros eventos o incidentes

En el Anexo N° 01 se puede ver una relación de ejemplos de eventos e incidentes menores de seguridad de la información.

5.4. El Oficial del SGSI o especialistas de nivel 2 o 3 de la UTI puede escalar el incidente a mayor o disruptivo cuando se ve afectado el desempeño normal de las operaciones. En estos casos, deberá comunicar al Jefe de UTI y al Oficial del SGCN o CGSIG la necesidad de activar el "Procedimiento de gestión de incidentes disruptivos del plan de recuperación tecnológica ante desastres".

5.5. El Oficial del SGSI podrá solicitar y tener acceso a las evidencias del incidente y documentación de la solución de los mismos, la cual servirá para retroalimentar y fortalecer el proceso de gestión de incidentes de seguridad de la información.

5.6. El Oficial del SGSI deberá realizar el seguimiento y control de los eventos e incidentes de seguridad de la información. El Sistema Nacional de Mesa de Ayuda remite automáticamente la información del estado de los mismos en forma quincenal.

5.7. El personal involucrado en la gestión de los incidentes (Oficial del SGSI y especialistas de nivel 2 o 3 de la Unidad de Tecnologías de la Información), dentro del ámbito de su competencia, deben tener un cuidado adecuado respecto al recojo, custodia y conservación de la evidencia de los incidentes y de su gestión, de manera que se garantice su validez, sobre todo, en caso se requieran posteriormente para acciones disciplinarias o legales contra los autores de los incidentes.

VI. DESCRIPCIÓN DEL PROCEDIMIENTO

El proceso de gestión incidentes inicia cuando se produce alguno de los siguientes eventos:

- Cuando un evento o incidente de seguridad de la información es identificado, iniciar con la **actividad 1. Reportar evento o incidente**.
- Inicio de la **actividad 9. Generar reporte de eventos e incidentes**, la cual es una actividad automatizada y programada cada 15 días.

N°	ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
	INICIO		
1.	**Reportar evento o incidente**	Usuario	Identifica un evento o incidente de seguridad de la información y lo registra en el aplicativo web "Sistema Nacional de Mesa de Ayuda". Continuar con la actividad 3 "Evaluar evento o incidente". De no contar con acceso al aplicativo, reporta a través de correo electrónico, vía telefónica u otro medio al área de Mesa de Ayuda, para la atención correspondiente. Continuar con la actividad 2 "Generar ticket de atención".

N°	ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
2.	**Generar ticket de atención**	Personal de Mesa de Ayuda	Registra los datos consignados por el usuario en el Sistema Nacional de Mesa de Ayuda, de acuerdo a lo indicado en el “Procedimiento atención de servicio de mesa de ayuda y soporte a usuarios”.
3.	**Evaluar evento o incidente**	Personal de Mesa de Ayuda	**¿El ticket guarda relación con evento o incidente de Seguridad de Información (SI)?** • Si, marcar el indicador (checkbox) de “Evento o incidente de Seguridad de la Información” en el Sistema Nacional de Mesa de Ayuda” y lo clasifica según los tipos indicados en el numeral 5.3. Evalúa si corresponde a un evento o incidente: - De ser un evento, continuar con la actividad 4. Brindar solución al evento. - De ser un incidente, continuar con la actividad 5. Derivar a especialista e informar al Oficial del SGSI. • No, continuar con la atención de acuerdo a lo señalado en el “Procedimiento atención de servicio de mesa de ayuda y soporte a usuarios”. Fin del proceso.
4.	**Brindar solución al evento**	Personal de Mesa de Ayuda	Brinda solución inmediata al evento de seguridad de la información. • Si se brinda solución, continuar con actividad 8 “Registrar la solución del evento o incidente menor”. • En caso no sea factible una solución inmediata, deberá de escalarlo al Especialista, lo cual lo convierte en incidente. Continuar con actividad 5. “Derivar a especialista e informar al Oficial del SGSI”.

N°	ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
5.	**Derivar a especialista e informar al Oficial del SGSI**	Personal de Mesa de Ayuda	Asigna atención al especialista nivel 2 o 3, según corresponda, a través del Sistema Nacional de Mesa Ayuda y comunica vía correo electrónico la ocurrencia del incidente al Oficial del SGSI. Continuar con las actividades 6 y 7 en paralelo.
6.	**Evaluar incidente y realizar seguimiento del incidente**	Oficial del SGSI	Toma conocimiento del incidente y lo registra en el formato “Control de Incidente de Seguridad de la Información”, completando la sección “I. DE LA IDENTIFICACIÓN DEL INCIDENTE”. Posteriormente, evalúa el incidente: • Si es un incidente menor, realiza seguimiento y las coordinaciones correspondientes para dar solución al incidente y completa la sección “II. DE LA ATENCIÓN DEL INCIDENTE”. • Si es un incidente mayor, comunica al Jefe de UTI y al Oficial del SGCN o CGSIG la necesidad de activar el “Procedimiento de gestión de incidentes disruptivos del plan de recuperación tecnológica ante desastres”. Fin del proceso.
7.	**Brindar solución al incidente**	Especialista (Nivel 2 o 3)	Analiza el incidente, realiza el diagnóstico y aplica las posibles soluciones hasta que el incidente sea resuelto. **Nota N° 05:** De requerir escalar el incidente a mayor (disruptivo) comunica al Jefe de UTI y al Oficial del SGCN o CGSIG la necesidad de activar el “Procedimiento de gestión de incidentes disruptivos del plan de recuperación tecnológica ante desastres”.
8.	**Registrar la solución del evento o incidente menor**	Personal de Mesa de ayuda / Especialista (Nivel 2 o 3)	Registra la solución del evento o incidente menor de seguridad de la información en el Sistema Nacional de Mesa de Ayuda, de manera

N°	ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN
			obligatoria, y cierra la atención del ticket en el sistema. El Especialista (Nivel 2 o 3) recopila evidencia de la atención o solución del incidente y lo remite al Oficial de SGSI. Continuar con actividad 10 “Tomar conocimiento y evaluar lecciones aprendidas”.
9.	**Generar reporte de eventos e incidentes**	Sistema Nacional de Mesa de Ayuda	El Sistema Nacional de la Mesa de Ayuda genera y envía el “Reporte de Eventos e Incidentes de Seguridad de la Información” mediante correo electrónico al Oficial del SGSI. Esta información se enviará cada 15 días de manera automática. **Nota N° 06:** En caso de problemas con la información de manera automatizada, el personal de Mesa de Ayuda completará manualmente el formato del mismo nombre y lo remitirá al Oficial del SGSI.
10.	**Tomar conocimiento y evaluar lecciones aprendidas**	Oficial del SGSI	Toma conocimiento sobre el estado de los eventos e incidentes menores de seguridad de la información, revisa las acciones tomadas para identificar las lecciones aprendidas y evitar que el evento o incidente se vuelva a producir. Para el caso de los incidentes, registra la información correspondiente a la sección “III. DEL CIERRE DEL INCIDENTE” del formato “Control de Incidente de Seguridad de la Información, considerando la evidencia proporcionada por el Especialista (2 o 3), de ser el caso. **Nota N° 07:** Luego de realizar toda esta evaluación, el Oficial del SGSI podrá actualizar los controles de riesgos de seguridad de la información o realizar una acción correctiva dependiendo del análisis de las causas del incidente.
	FIN		

VII. ANEXOS

- Anexo N° 01: Ejemplos de eventos e incidentes menores de seguridad de la información.
- Anexo N° 02: Diagrama de Flujo del Procedimiento de gestión de incidentes de seguridad de la información.

ANEXO N° 01: EJEMPLOS DE EVENTOS E INCIDENTES MENORES DE SEGURIDAD DE LA INFORMACIÓN

INC01 - Control de seguridad ineficaz

- Cuando el control no evitó que se concrete la amenaza, pero afectó solo a un equipo o fue un hecho único, por ejemplo: Ataques por virus informáticos u otros códigos maliciosos (malware) que genera problemas en la información o en el funcionamiento del equipo pese a tener el antivirus instalado.

INC02 - Afectación de la integridad o disponibilidad de la información

- Perdida de la disponibilidad o integridad, pero se puede recuperar por respaldo.
- Borrado de información de terceros, pero que se puede recuperar mediante solicitud de restauración de copia de respaldo.

INC03 - Errores Humanos

- Robo de contraseñas por descuido del usuario (tener contraseña débil o por poner la contraseña en forma visible cerca de otras personas).
- Robo o pérdida de equipos en ambientes externos a la institución.
- Entrega de información sensible de la persona o de la institución por engaño o manipulación por correo, teléfono, SMS, WhatsApp u otro medio (ingeniería social).
- Instalación de virus informático en la computadora por phishing.
- Realización de una transacción perjudicial por engaño o manipulación por correo, teléfono, SMS, WhatsApp u otro medio (ingeniería social).

INC04 - Incumplimientos de las políticas o directrices

- No tener el antivirus instalado o actualizado.
- Compartir la contraseña de sus cuentas de red o de base de datos.
- Infracciones de derechos de autor o piratería.
- Uso no autorizado de recursos informáticos.
- Material con contenido abusivo, violencia o pornografía en ambientes o equipos de la institución.

INC05 - Incumplimientos de las medidas de seguridad físicas

- Accesos de personal no autorizados a algún área administrativa o registral.
- Robo de equipos, componentes de equipos o información por accesos no autorizados.

INC06 - Afectación de la confidencialidad

- Filtración de información de datos personales del personal.
- Filtración de información de los resultados de los exámenes médicos.

INC07 - Cambios no controlados del sistema

- Fallas en los programas informáticos por cambio de versión.

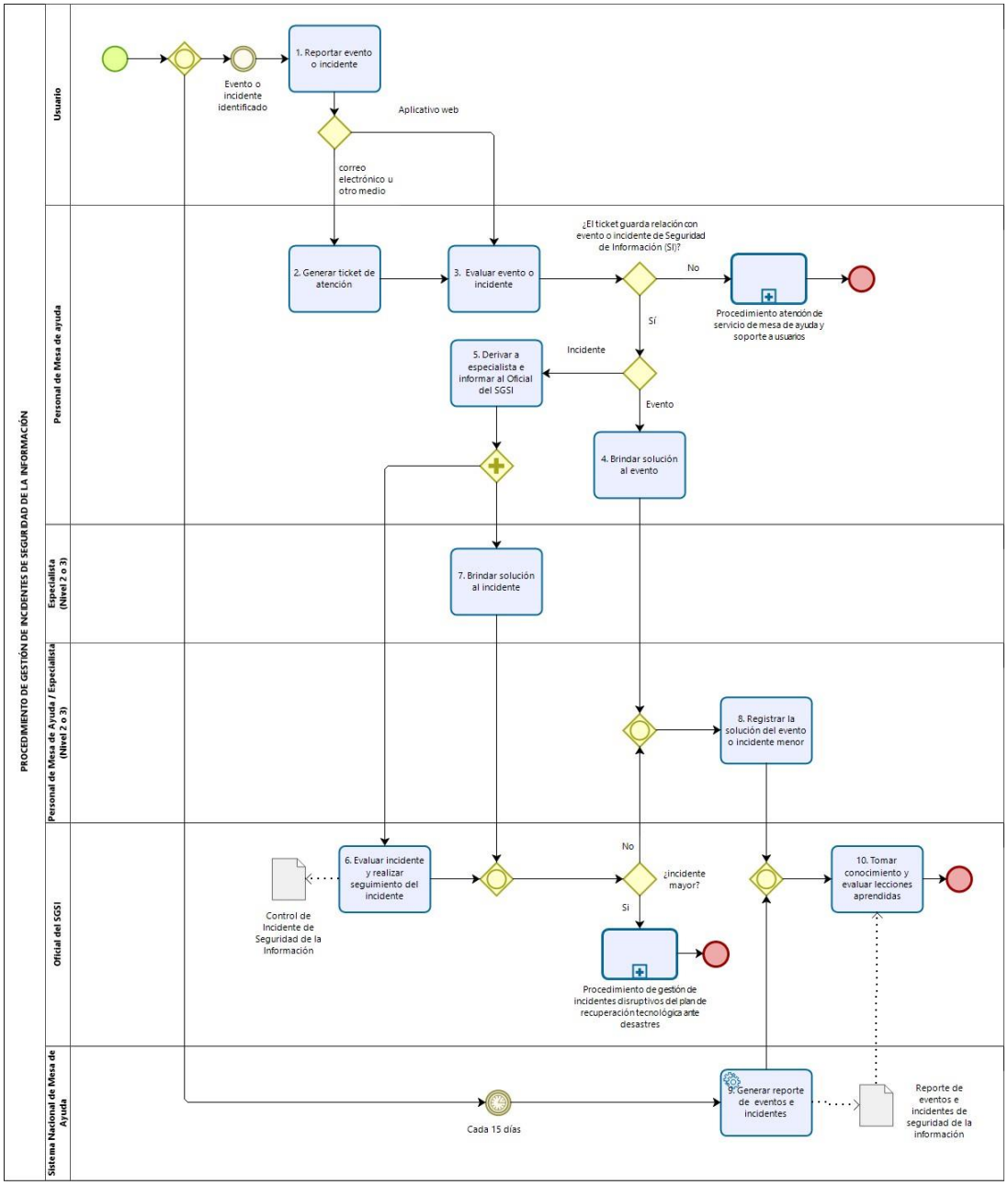
INC08 - Mal funcionamiento de software o hardware

- Perdida de información o encriptación de información por posible ciberataque.

INC09 - Acceso no autorizado

- La utilización de fallas en los procesos de autenticación para obtener accesos indebidos.
- Robo de información por persona que tiene excesivos privilegios.
- Robo de información por ciberataque.
- Falsificación de registros.
- Alteración de la información.
- Falsificación o usurpación de identidad.

ANEXO N° 02: DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN



CUADRO DE CONTROL DE CAMBIOS

Ítem	Descripción del cambio	Código / Versión
-	Elaboración inicial del documento	PR-011-UTI-ZRIX/V.01