CUT: 150478

REPUBLICA DEL PERU

RESOLUCIÓN JEFATURAL N° 282 -2016-ANA

Lima, 27 OCT. 2016

VISTOS:

La Carta N° 008-2016-ANA-SGSI del Presidente del Comité de Gestión de Seguridad de la Información de la Autoridad Nacional del Agua y el Acta de Reunión N° 06-2016-ANA-CGSI de fecha 29 de setiembre de 2016, y;

CONSIDERANDO:

Que, por Resolución Ministerial N° 004-2016-PCM de fecha 08 de enero de 2016, se aprobó el uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática, la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnologías de la Información. Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición";

Que, mediante Resolución Jefatural N° 71-2016-ANA, de fecha 16 de marzo de 2016, se modificó la conformación del Comité de Gestión de Seguridad de la Información de la Autoridad Nacional del Agua, constituido por Resolución Jefatural N° 660-2011-ANA, en virtud a lo dispuesto en la precitada Resolución Ministerial N° 004-2016-PCM;

Que, de acuerdo al artículo 6° de la Resolución Ministerial N° 004-2016-PCM, la responsabilidad de la implementación de la norma será del titular de cada entidad;

Que, el numeral 5.3 del artículo 5° de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnologías de la Información. Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", referida a los Roles, responsabilidades y autoridades organizacionales; establece que la alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas;

Que, mediante la Carta de Vistos, el Presidente del Comité de Gestión de Seguridad de la Información de la Autoridad Nacional del Agua, solicita la aprobación del documento denominado "SGSI-DOC-04 Roles y Responsabilidades del SGSI", el mismo que ha sido elaborado, revisado y validado con Acta de Reunión N° 06-2016-ANA-CGSI de fecha 29 de setiembre de 2016 por el referido Comité, sobre la base de lo estipulado en la Norma Técnica Peruana aprobada por la Resolución Ministerial N° 004-2016-PCM;

Que, en cumplimiento al marco legal expuesto, resulta necesario la aprobación del documento denominado "SGSI-DOC-04 Roles y Responsabilidades del SGSI", por la Jefatura Institucional;

Con los vistos de la Oficina de Planeamiento y Presupuesto, de la Oficina del Sistema Nacional de Información de Recursos Hídricos, de la Oficina de Asesoría Jurídica y de la Secretaría General, y en uso de las facultades conferidas en el artículo 11° del Reglamento de Organización y Funciones de la Autoridad Nacional del Agua aprobado por Decreto Supremo N° 006-2010-AG;

SE RESUELVE:

Artículo 1º.- Aprobación

Aprobar el documento denominado "SGSI-DOC-04 Roles y Responsabilidades del SGSI, elaborado por el Comité de Gestión de Seguridad de la Información de la Autoridad Nacional del Agua, que en Anexo forma parte integrante de la presente Resolución.

Artículo 2°.- Difusión

Disponer la publicación de la presente Resolución y de su Anexo en el portal web institucional de la Autoridad Nacional del Agua: www.ana.gob.pe.

Regístrese, comuníquese y publíquese,

Ing. ABELARDO DE LA TORRE VILLANUEVA
Jefe
Autoridad Nacional del Agua

ANA

Autoridad Nacional del Agua

ROLES Y RESPONSABILIDADES DEL SGSI

[SGSI-DOC-04]

SETIEMBRE/ 2016

USO PÚBLICO

DATOS DEL DOCUMENTO			
Nombre		**Fecha**	**FIRMA**
Creado por:	Oficial de Seguridad de la Información	21/09/2016	
Revisado por:	Comité de Seguridad de la Información	29/09/2016	
Aprobado por:	Jefe de la ANA		

REGISTRO DE REVISIONES Y MODIFICACIONES			
Revisión		**Emisor**	**Descripción**
N°	**Fecha**	**Nombre/Dpto.**	**De la Modificación**
01	21/09/2016	Oficial de Seguridad de Información	Creación del documento y propuesto a Comité para su revisión
02	29/09/2016	Comité de Seguridad de la Información	Revisado por el Comité de Gestión de Seguridad de la Información de la Autoridad Nacional del Agua

Contenido

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

1. INTRODUCCIÓN

El presente documento contiene la estructura organizativa de la organización de los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información (SGSI) de la Autoridad Nacional del Agua (ANA en adelante), alineado a lo establecido en la NTP ISO/IEC 27001:2014.

2. OBJETIVOS

Establecer los roles y responsabilidades relevantes a la seguridad de la información para asegurar la eficacia del sistema de gestión de seguridad de la información.

3. ALCANCE

La organización interna de seguridad de la información en la ANA, involucra al personal que forma parte de los procesos dentro del alcance del SGSI y en todas las actividades desarrolladas en la institución y para la institución.

4. ESTRUCTURA ORGANIZATIVA

La ANA dirige el SGSI de forma centralizada a través de la Jefatura y Secretaría General, la cual se apoya en un Comité de Seguridad de Información para gestionarlo, y en un Oficial de Seguridad de Información para operarlo. La totalidad de los roles involucrados son descritos a continuación:

- Jefatura de la ANA
- Secretaría General
- Directores y Jefes de Oficina de la ANA
- Comité de Gestión de Seguridad de la Información
- Oficial de Seguridad de la Información
- Propietarios de la Información
- Custodios de la Información
- Usuarios
- Auditor
- Auditado

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

5. ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Los roles y responsabilidades relacionadas al Sistema de Gestión de Seguridad de la Información establecidos por la ANA son las siguientes:

5.1. Jefatura de la ANA

Establece los lineamientos de liderazgo y empoderamiento para la operación del SGSI. Es el impulsor de la gestión de la seguridad de la Información en la ANA. Tiene como responsabilidad:

- Aprobar las Políticas, Objetivos y Responsabilidades del SGSI, disponiendo su publicación y distribución.
- Facilitar los recursos (humanos, de infraestructura, financieros y tecnológicos) para la implementación del SGSI, de acuerdo al marco de disponibilidad presupuestal de la entidad.
- Designar a los miembros del Comité de Gestión de Seguridad de la Información.

5.2. Secretaría General

Establece la dirección para la operación del SGSI, dando evidencia de su liderazgo y compromiso con la implementación, mantenimiento y la mejora continua de la eficacia del SGSI. Tiene como responsabilidad:

- Promover revisiones periódicas del SGSI, según el procedimiento definido.
- Velar por el cumplimiento de las políticas específicas de seguridad de la información aprobadas por el CGSI.
- Asignar funciones en torno a temas de Seguridad de Información al personal de la ANA.

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

5.3. Directores y Jefes de Oficina de la ANA

Directores y jefes de las diversas oficinas de la ANA, quienes cumplirán roles de facilitadores e impulsadores de la operación del SGSI. Tienen como responsabilidades:

- Modificar la vigencia y disponibilidad de todos los documentos relacionados a su área según corresponda, en los lugares donde se realicen actividades referidas al SGSI, para evitar la ocurrencia de no conformidades por el uso de documentos obsoletos.

- Participar activamente y asegurar su disposición para brindar la información requerida para la medición de los indicadores en el momento que le sea solicitada por el Oficial de Seguridad de Información (OSI), y bajo las especificaciones indicadas.
- Poner a disposición del equipo auditor los medios necesarios para la auditoría, así como también facilitar el acceso a las instalaciones y documentos relevantes para la auditoría.
- Elaborar y aprobar los procedimientos operacionales relacionados a su área según corresponda.

5.4. Comité de Gestión de Seguridad de la Información

Es un grupo formado por un representante de las Direcciones y Oficinas de la ANA, y son los encargados de supervisar y aprobar la implementación, mantenimiento y la mejora continua del SGSI. Tiene como responsabilidades:

- Revisar y presentar para aprobación de la Jefatura las Políticas, Objetivos, Roles y Responsabilidades de seguridad de la información.
- Asegurar que las metas de la seguridad de la información sean identificadas, relacionadas con las exigencias organizacionales y que sean integradas en procesos relevantes.
- Aprobar y revisar periódicamente la efectividad del SGSI.
- Proveer direcciones claras y un visible apoyo en la gestión para iniciativa de seguridad.
- Decidir el criterio para la aceptación de riesgos de seguridad de la información y los niveles de riesgo aceptables.
- Promover la difusión, apoyo y concientización de la seguridad de la información
- Asegurar y controlar la implementación de controles de seguridad de la información en la organización.
- Aprobar los Procedimientos, Planes, Instructivos, Metodologías, Guías y Formatos del SGSI.
- Oficiar como vínculo entre la Jefatura de la ANA, Secretaría General y el Oficial de Seguridad de Información.
- Proveer la dirección estratégica del SGSI.
- Aprobar la ejecución de las auditorías internas y externas de la seguridad de la información.

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

5.5. Oficial de Seguridad de la Información

Es el máximo responsable operativo de la implementación del SGSI y coordinador de la seguridad de la información en la ANA. Su aporte en la organización es el de un especialista en el tema, que trabaja estrechamente con el Comité de Seguridad de la Información. Tiene como responsabilidad:

- Asumir el rol de Jefe del proyecto de implementación del SGSI.
- Participar en la creación y revisión de las políticas, objetivos, normas, metodologías, procedimientos, manuales, planes, guías y formatos del SGSI.
- Administrar y revisar los documentos del SGSI, validar su contenido, versión y gestionar su aprobación.
- Coordinar las actividades relacionadas al proceso de implementación del SGSI, desde la etapa de la planificación, hasta la operación del mismo.
- Brindar orientación en el proceso de gestión de riesgos a los propietarios de activos dentro del alcance del SGSI.
- Evaluar, coordinar y monitorear la implementación del Plan de Tratamientos de Riesgos.
- Dar seguimiento a los incidentes de seguridad de la información, evaluar riesgos y eventuales impactos.
- Supervisar y apoyar la difusión de los temas en Seguridad de la Información.
- Coordinar las reuniones del Comité de Seguridad y comunicar los avances de la implementación del SGSI y sus controles.
- Apoyar en el cumplimiento de las actividades de elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI y en general a todas las actividades pertinentes establecidas por la norma NTP ISO/IEC 27001:2014 y su debido cumplimiento.
- Elaborar el Programa Anual de Auditorías del SGSI para el año en curso.

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

5.6. Propietarios de la Información

Son responsables de la información que se genera y se utiliza en los procesos diarios de la ANA, así como también de los riesgos a los que se encuentran expuestos. Tiene como responsabilidades:

- Elaborar el inventario de activos de información

- Participar en las actividades de análisis, evaluación y tratamiento de riesgos, convocadas por el Oficial de Seguridad de la Información.
- Aprobar los análisis de riesgo y el plan de tratamiento de riesgos de sus procesos.
- Sugerir y apoyar en la elaboración de las políticas, normas y procedimientos de Seguridad de la Información dentro de sus respectivas áreas y procesos.
- Determinar los criterios y niveles de acceso a la información.
- Definir y revisar periódicamente la clasificación de la información con el propósito de verificar que se cumpla con los requerimientos de la ANA.
- Contribuir a la implementación de los controles de seguridad que estén relacionados a sus funciones.
- Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI y en general a todas las actividades requeridas por la norma NTP ISO/IEC 27001:2014 y su debido cumplimiento.

5.7. Custodios de la Información

Se encarga de la administración diaria de la seguridad y monitoreo del cumplimiento de las políticas y los controles de seguridad en los activos que se encuentren bajo su administración. Tiene como responsabilidades:

- Administrar los controles relevantes a la Seguridad de la Información, acorde a las instrucciones establecidas por los Propietarios de la Información.
- Cumplir con los controles implementados para la protección de la información asignada para su custodia.
- Controlar el acceso a los activos por parte de los usuarios de acuerdo con las especificaciones establecidas por los propietarios.
- Reportar oportunamente incidentes y debilidades de seguridad de la información y oportunidades de mejora relacionadas a los activos bajo su custodia y colaborar en su investigación.
- Evaluar la efectividad de los controles sobre la base de la clasificación asignada por los Propietarios de la Información

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

5.8. Usuarios

Son los empleados de la ANA o personal externo de apoyo, quienes utilizan la información en actividades habituales y quienes están obligados a respetar las normas establecidas por la Entidad. Tienen como responsabilidades:

- Cumplir con las políticas, normas y procedimientos de seguridad de la información.
- Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información de la ANA únicamente para los propósitos autorizados.
- Participar en los entrenamientos, capacitaciones y programas de sensibilización en temas de seguridad de la información.
- Reportar cualquier incidente[1], potencial incidente u oportunidades de mejora de seguridad de la información.

5.9. Auditor

El Auditor es el responsable de preparar y llevar a cabo los procesos de Auditoría para determinar la extensión en que se cumplen los criterios de auditoria, en nombre de la propia organización, para la revisión por la dirección y con otros fines internos.

5.10. Auditado

El auditado es cualquier personal de la ANA que se encuentra sujeto a una revisión por parte de los auditores internos del SGSI, y debe cumplir con:

- Proporcionar al equipo auditor la información necesaria y objetiva para asegurar un proceso de auditoría eficiente y eficaz.

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

6. GLOSARIO DE TERMINOS

- Activo de información: En seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.

[1] Según la ISO/IEC 31000 Incidente: Situación que pudiera generar una alteración.

- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Auditor: Persona que lleva a cabo una auditoria.
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en que se cumplen los criterios de auditoría
- Criterios de auditoria. Grupo de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la evidencia de auditoria.
- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Custodio de la información: Persona con responsabilidad de la administración y resguardo de los activos de información
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- Evidencia de auditoria. Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoria y que son verificables.
- Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos.
- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar a la seguridad de la información.
- Información: Toda forma de conocimiento objetivo con representación física o lógica explícita.
- Integridad: Propiedad de la información relativa a su exactitud y completitud.
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- Propietario del riesgo: Persona con responsabilidad y autoridad para gestionar un riesgo.

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica

- Propietario de la información: Son los principales representantes de los órganos de la ANA que forman parte del alcance del SGSI.
- Proyecto de Gestión de Seguridad de la Información: Proyecto que se implementa en el marco de la NTP ISO/IEC 27001:2014 y contempla la implementación de un SGSI para el proceso definido en el alcance. Es un proyecto del negocio, no un proyecto de TI.
- Riesgo de la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- Sistema de Gestión de la Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión de riesgo y de mejora continua.

AUTORIDAD NACIONAL DEL AGUA
Abg. José A. Ramírez Garro
DIRECTOR
Oficina de Asesoría Jurídica