Resolución Ministerial

N° 221-2013-MINAM

Lima, 24 JUL. 2013

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM, publicada el 25 de agosto de 2007, se aprobó el uso obligatorio de la "Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", en todas las entidades integrantes el Sistema Nacional de Informática, con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública;

Que, la referida Norma Técnica Peruana señala que la Política de Seguridad de Información, tiene como objeto dirigir y dar soporte a la gestión de seguridad de la información en concordancia con los requerimientos de la institución, las leyes y las regulaciones, correspondiendo a la Alta Dirección establecer las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una Política de Seguridad en toda la organización;

Que, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros recomienda la aplicación y el uso de la "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", de manera progresiva, en todas las entidades que integran el Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico; la cual a su vez, se complementa con la Resolución Ministerial N° 246-2007-PCM

Que, en tal sentido, mediante Resolución Ministerial N° 129-2012-PCM, publicada el 25 de mayo de 2012, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", en todas las entidades integrantes del Sistema Nacional de Informática, cuyo control deberá ser implementado de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información";

Que, la segunda parte del artículo 5° de la Resolución Ministerial citada en el considerando precedente, establece que cada entidad designará un coordinador que hará las veces de oficial de seguridad de la información hasta la adecuación de su estructura organizacional donde se incorpore esta función, siendo que tal designación deberá realizarse mediante resolución del Titular de cada Entidad;

Que, mediante Resolución de Secretaría General N° 061-2011-MINAM, de 27 de julio de 2011, se conformó el Comité de Gestión de Seguridad de la Información del Ministerio del Ambiente – MINAM, con la finalidad de impulsar y realizar las acciones destinadas a mantener y mejorar la seguridad de la información en la entidad, el cual propone la aprobación de la Política de Seguridad

de la Información del Ministerio del Ambiente, la aprobación de los Lineamientos de la Política de Seguridad de la Información del Ministerio del Ambiente, así como la designación del Oficial de Seguridad de la Información; por lo que, corresponde emitir la presente resolución;

Con el visado de la Secretaría General, de la Oficina de Planeamiento y Presupuesto, de la Oficina General de Administración, y de la Oficina de Asesoría Jurídica; y,

De conformidad con lo establecido en el Decreto Legislativo N° 1013, Ley de Creación, Organización y Funciones del Ministerio del Ambiente y el Decreto Supremo N° 007-2008-MINAM, que aprueba su Reglamento de Organización y Funciones; y, las Resoluciones Ministeriales N° 246-2007-PCM y N° 129-2012-PCM.

SE RESUELVE:

Artículo 1°.- Aprobar la "Política de Seguridad de la Información del Ministerio del Ambiente – MINAM", que como Anexo 1 forma parte integrante de la presente resolución.

Artículo 2°.- Aprobar los "Lineamientos de la Política de Seguridad de la Información del Ministerio del Ambiente", que como Anexo 2 forma parte integrante de la presente resolución.

Artículo 3°.- Designar al Responsable del Sistema de Informática y Tecnologías de la Información, como Oficial de Seguridad de la Información del Ministerio del Ambiente – MINAM.

Artículo 4°.- El Oficial de Seguridad de la Información del Ministerio del Ambiente – MINAM, desarrollará las funciones siguientes:

a) Realizar las coordinaciones con la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).
b) Establecer la Información de cada órgano del MINAM, para definir los controles y procedimientos que mitiguen los posibles riesgos existentes y que puedan afectar los procesos críticos de la entidad.
c) Asegurar, a través de la Oficina de Planeamiento y Presupuesto, que los aspectos de seguridad, sean considerados dentro del planeamiento estratégico del MINAM.
d) Verificar el cumplimiento y efectividad de las medidas de administración de riesgos relacionados con: seguridad lógica, seguridad física, seguridad del recurso humano, administración de operaciones, clasificación de seguridad y procedimientos de respaldo.
e) Verificar y evaluar que el Sistema de Informática y Tecnologías de la Información realice un inventario periódico de activos asociados a la tecnología de información según la clasificación del nivel de seguridad requeridos por dichos activos.
f) Verificar que el proceso para la aprobación de propuestas de desarrollo y/o adquisición de sistemas cuente con una descripción general de los riesgos identificados, requerimientos de seguridad y las acciones a tomar para controlar dichos riesgos.
g) Verificar el cumplimiento y efectividad de los procedimientos de control y actualización de versiones y pases a producción.
h) Garantizar la correcta implementación de los "Lineamientos Generales de Seguridad de la Información del Ministerio del Ambiente", una vez que sean aprobados.

Artículo 5.- Disponer la publicación de la presente Resolución Ministerial en el Diario Oficial El Peruano. La Política de Seguridad de la Información del Ministerio del Ambiente – MINAM, se publicará en el Portal Web Institucional www.minam.gob.pe.

Regístrese, comuníquese y publíquese.

Manuel Pulgar-Vidal Otálora
Ministro del Ambiente

PERÚ | Ministerio del Ambiente

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL AMBIENTE - MINAM

El Ministerio del Ambiente reconoce como activo vital a toda la información generada en sus procesos, por ello se encuentra comprometido en salvaguardar su integridad y disponibilidad, por medio de la aplicación de las recomendaciones de normas técnicas peruanas, estándares internacionales y de las mejores prácticas de seguridad de la información, a fin de asegurar la continuidad de sus operaciones y mantener un nivel óptimo de calidad en los servicios que brinda.

Como entidad, el Ministerio del Ambiente, a través del presente documento, exhorta a reconocer que la información es uno de sus principales activos, así como motor de intercambio y desarrollo en el ámbito de sus funciones; por tanto, se debe adoptar una posición consciente y vigilante respecto al uso y limitaciones de los recursos y servicios informáticos críticos de la organización.

Los usuarios deben ser conscientes que la importancia de la información es proporcional al valor de sus procesos, lo que hace necesario adoptar mecanismos de gestión de seguridad de la información, entre los que se pueden contar la política, reglamento, procedimientos, estructura organizacional y soluciones tecnológicas sobre la base de estándares probados y reconocidos, tanto a nivel nacional como internacional.

Se debe tener en cuenta que la seguridad de la información se define como la salvaguarda de la información para su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información; su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos; y, su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando la requieran.

MINISTERIO DEL AMBIENTE - Oficina de Asesoría Jurídica - C. LÓPEZ - MINAM

MINISTERIO DEL AMBIENTE - Dirección General de Administración - MINAM

MINISTERIO DEL AMBIENTE - PLANEAMIENTO Y PRESUPUESTO - MINAM

Lima, 24 de julio de 2013.

LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL AMBIENTE – MINAM

1. OBJETO

Es objeto de los Lineamientos de la Política de Seguridad de la Información del Ministerio del Ambiente, en adelante los "Lineamientos", establecer el marco general de seguridad de la información que permita fortalecer los niveles de seguridad en el Ministerio del Ambiente - MINAM, en base a las necesidades y riesgos de sus procesos.

2. FINALIDAD

Los Lineamientos tienen por finalidad proteger los activos de la información, asegurando la confidencialidad, disponibilidad e integridad de la información del Ministerio del Ambiente, minimizando los riesgos y asegurando la continuidad operativa.

3. ALCANCE

Los Lineamientos son de cumplimiento obligatorio por el personal del Ministerio del Ambiente, independientemente de su vínculo laboral o contractual con el MINAM, así como de las personas naturales o jurídicas que brindan servicios a la entidad y que tengan acceso a la información.

4. BASE LEGAL

4.1 Ley N° 27444 – Ley de Procedimiento Administrativo General.

4.2 Ley N° 27927 –Ley de Transparencia y Acceso a la Información Pública.

4.3 Ley N° 27806 – Modificatoria de la Ley de Transparencia y Acceso a la Información Pública.

4.4 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.

4.5 Ley N° 27815, Ley del Código de Ética de la Función Pública.

4.6 Ley N° 28716, Ley de Control Interno de las Entidades del Estado.

4.7 Decreto Legislativo N° 822, Ley sobre el Derecho de Autor.

4.8 Decreto Legislativo N° 1013 – Ley de Creación, Organización y Funciones del Ministerio del Ambiente.

4.9 Decreto Supremo N° 007-2008-MINAM - Aprueba el Reglamento de Organización y Funciones (ROF) del Ministerio del Ambiente.

4.10 Decreto Supremo N° 043-2003-PCM - Aprueba el TUO de la Ley N°27806, Ley de Transparencia y Acceso a la Información Pública.

4.11 Decreto Supremo N° 070-2013-PCM - Modifica el Reglamento de la Ley de Transparencia y Acceso a la Información Pública aprobado por Decreto Supremo N° 072-2003-PCM, recientemente publicado en el Diario Oficial El Peruano el 14 de junio de 2013.

4.12 Resolución Ministerial N° 085-2012-MINAM - Aprueba el Manual de Procedimientos del MINAM.

4.13 Resolución Ministerial N° 129-2012-PCM - Aprueba el uso obligatorio de la Norma Técnica Peruana "*NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos*" en todas las entidades integrantes del Sistema Nacional de Informática.

4.14 Resolución Ministerial N° 224-2004-PCM – Uso Obligatorio de la NTP-ISO/IEC 17799: Código de Buenas Prácticas para Gestión de la Seguridad de la Información.

4.15 Resolución Ministerial N° 246-2007-PCM - Aprueba el Uso Obligatorio de la Norma Técnica Peruana "*NTP-ISO/IEC 17799:2007 EDI Tecnología de la Información Código de buenas prácticas para la Gestión de la Seguridad de la Información. 2ª Edición*", en todas las entidades integrantes del Sistema Nacional de Informática.

4.16 Resolución de Contraloría General N° 320-2006-CG - Normas de Control Interno.

4.17 Resolución N° 001-2007/INDECOPI-CTR - Aprueba Normas Técnicas Peruanas.

4.18 Resolución de Secretaria General N° 061-2011-MINAM - Conforma el Comité de Gestión de Seguridad de la información del Ministerio del Ambiente.

4.19 Directiva N° 004-2010-SG-MINAM – Directiva General para la Formulación, Aprobación, Modificación de Directivas en el Ministerio del Ambiente.

MINISTERIO DEL AMBIENTE Oficina de Asesoría Jurídica C. LOPEZ MINAM

MINISTERIO DEL AMBIENTE Oficina General de Administración MINAM

MINISTERIO DEL AMBIENTE PLANEAMIENTO Y PRESUPUESTO MINAM

5. DISPOSICIONES GENERALES:

Los Lineamientos se enmarcan en lo dispuesto por la Resolución Ministerial N° 129-2012-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "*NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información Técnicas de Seguridad - Sistemas de gestión de seguridad de la Información - Requisitos*", en todas las entidades integrantes del Sistema Nacional de Informática, cuyo control deberá ser implementado de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información".

La información y los sistemas de información son activos importantes para el Ministerio del Ambiente así como para la toma de decisiones de sus órganos.

La seguridad de la información, en su concepción moderna y técnica, busca, fundamentalmente, alcanzar los siguientes Objetivos: confidencialidad, integridad y disponibilidad de la información en general.

5.1 RESPONSABILIDADES

5.1.1 Es responsabilidad de la Oficina General de Administración, a través del Sistema de Informática y Tecnología de la Información, velar por el cumplimiento de los Lineamientos.

5.1.2 Es responsabilidad del personal del Ministerio del Ambiente (MINAM), detectar cualquier incumplimiento de las obligaciones y prohibiciones señaladas en los Lineamientos y comunicarlas a la Oficina General de Administración – Sistema de Informática y Tecnología de la Información, quien gestionará la investigación del hecho y reportará al Comité de Gestión de Seguridad de la Información del Ministerio del Ambiente el resultado de dicha investigación.

En caso de comprobarse alguna vulnerabilidad a los Lineamientos, el Comité de Gestión de Seguridad de la Información comunicará a la Oficina General de Administración – Sistema de Recursos Humanos, para que adopte las acciones pertinentes.

5.1.3 Es responsabilidad de la Alta Dirección del Ministerio del Ambiente:

- Que el personal, independientemente de su vínculo laboral o contractual, reciba una adecuada capacitación relacionada a la Seguridad de la Información.
- Que el personal se comprometa a cumplir con los presentes Lineamientos.
- Que todos los órganos se responsabilicen para que el personal externo que preste sus servicios en sus ambientes de información, conozcan y cumplan lo normado con los Lineamientos.

5.1.4 El Ministerio del Ambiente cuenta con una estructura que soporta los aspectos de seguridad de información, considerándose, principalmente, los siguientes:

5.1.4.1 **Comité de Gestión de Seguridad de la Información** (CGSI). Conformado en el MINAM, mediante Resolución de Secretaria General N° 061-2011-MINAM de fecha 27 de julio de 2011, el cual se encuentra integrado por:

- Un representante de la Alta Dirección, quien lo preside,
- El Director de la Oficina General de Administración,
- El Director de la Oficina de Asesoría Jurídica,
- El Director de la Oficina de Planeamiento y Presupuesto,
- El Especialista responsable de Recursos Humanos; y,
- El Especialista responsable de Informática y Tecnologías de Información, quien actúa como Secretaría Técnica.

Los roles y responsabilidades que asume el citado Comité son los siguientes:

- Asegurar que las metas de la seguridad de información sean identificadas, relacionadas con las exigencias organizacionales y que sean integradas en procesos relevantes.
- Formular, revisar y aprobar la política de seguridad de la información.

- Revisar la efectividad en la implementación de la Política de la Información.
- Proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad.
- Proveer los recursos necesarios para la seguridad de la información.
- Aprobar asignaciones de roles específicos y responsabilidades para seguridad de información a través de la organización.
- Iniciar planes y programas para mantener la conciencia en seguridad de información.
- Asegurar que la implementación de los controles de la seguridad de información sea coordinada a través de la organización.
- Implementar el Plan de Sensibilización para que el personal interno y externo del MINAM, se alinee a lo definido en los Lineamientos.
- Proponer normas, procedimientos y controles sobre aspectos de seguridad de información.
- Monitorear el cumplimiento del Plan de Seguridad de la Información.
- Establecer una metodología de evaluación de riesgos que se adecue al SGSI y a requisitos legales y regulatorios de la información de seguridad de la institución identificada; o de ser el caso del MINAM.
- Revisar las directivas y procedimientos de seguridad de la información verificando su efectividad y correcta implementación, proponiendo oportunamente su modificación o actualización.
- Determinar criterios para identificar los niveles aceptables del riesgo.
- Implementar el Plan de Tratamiento de Riesgos.

- Implementar procedimientos y otros controles.
- Revisar la evaluación de riesgos en intervalos planificados y revisar el nivel del riesgo residual y riesgo aceptable.
- Elaborar los Planes de Contingencia para la respuesta oportuna frente a una situación de emergencia, de modo que las operaciones se reanuden en el tiempo más breve posible.
- Supervisar que el Sistema de Informática y Tecnologías de la Información realice un inventario periódico de activos asociados a la tecnología de información según la clasificación del nivel de seguridad requeridos por dichos activos.

5.1.4.2 **Propietario de la Información**

Los titulares de los distintos órganos del Ministerio del Ambiente, son responsables de generar y hacer uso de dicha información. El propietario de la información es quien define la clasificación de la data y es responsable del mantenimiento y actualización de dicha clasificación, sin perjuicio de la responsabilidad por las funciones que por delegación le sean asignadas al personal subalterno.

Esta responsabilidad no puede ser delegada a terceros, con excepción de la custodia de la información que puede darse a un colaborador perteneciente al órgano en particular, quien apoya en las tareas operativas de administración y control de seguridad correspondiente a la información.

Es de responsabilidad del titular del órgano designar al custodio de la información del ámbito de su competencia.

5.1.4.3 Custodio de la Información

Es el personal de cada órgano que tiene la responsabilidad de mantener y proteger la información que ha sido generada. Cabe señalar que los custodios no necesitan de la información para el

- Utilizar la información sólo para el propósito para el que recibió autorización de uso.
- Cumplir los controles establecidos en la normativa interna.
- Adoptar las medidas adecuadas para evitar que la información se divulgue o utilice sin autorización.
- Informar de inmediato al propietario de la información y al Responsable del Sistema de Informática y Tecnologías de la Información sobre cualquier exposición de seguridad de los activos de información, sea esta real o potencial.

5.2 PROPIEDAD DE LA INFORMACIÓN

Toda la información generada, almacenada y soportada por el Ministerio del Ambiente, pertenece a la entidad y no puede ser utilizada en beneficio personal o de terceros.

5.3 REQUISITOS DE DOCUMENTACIÓN

La documentación debe incluir registros de las decisiones de los órganos del MINAM, que asegure que las acciones realizadas respondan a las decisiones adoptadas y a las normas establecidas.

La documentación del Sistema de Gestión de Seguridad de Información (SGSI) deberá incluir lo siguiente:

- Declaraciones documentadas de las normas y procedimientos que correspondan a la Seguridad de la Información.
- Alcance del SGSI.
- Descripción de la metodología de evaluación del riesgo.
- Informe de evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Procedimientos documentados necesarios en la organización para garantizar la planificación efectiva, funcionamiento y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.

desarrollo de su trabajo, simplemente la procesan, la gestionan y la hacen accesible a los demás usuarios.

Las funciones más importantes que debe cumplir son:

- Asegurar el establecimiento y aplicación de los controles establecidos en los Lineamientos.
- Asegurar que la información entregada al usuario sea actualizada e íntegra.

5.1.4.4 Usuario de la Información

Persona o conjunto de personas internas, autorizadas para consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento.

Los usuarios sólo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitarán su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.

Toda vez que se confíe información a un tercero, previamente, deberá suscribir el Acuerdo de Confidencialidad, el mismo que incluirá las instrucciones precisas para el manejo de los datos y la eliminación o borrado de los mismos, cumplido el periodo circunstancial que llevo a confiar en el tercero.

En el caso que se requiera que el MINAM firme un **Acuerdo de Confidencialidad** con terceros, debe hacerse uso del modelo que se muestra en el ***Apéndice Nº 02***.

Las principales responsabilidades de los usuarios de información son las siguientes:

6. DISPOSICIONES ESPECÍFICAS

6.1 CONTROL DE DOCUMENTOS

- Los documentos exigidos por el SGSI estarán protegidos y controlados. Se establecerá un procedimiento documentado para definir las acciones administrativas necesarias para:

  - Revisar y actualizar los documentos que sean necesarios.
  - Emitir visto bueno en la documentación para su implementación.
  - Asegurar que los cambios y el estado de la versión actual de los documentos sean identificados.
  - Asegurar que las versiones más recientes de los documentos pertinentes estén disponibles en los puntos de uso.
  - Asegurar que los documentos sean legibles y fácilmente identificables.
  - Asegurar que los documentos se encuentren disponibles para quienes los necesiten y sean transferidos, almacenados y dispuestos en concordancia con los procedimientos aplicables para su clasificación.
  - Asegurar que los documentos de origen externo sean identificados.
  - Asegurar que la distribución de documentos sea controlada.
  - Proponer documentos normativos relacionados al ámbito de su competencia.

6.2 CONTROL DE REGISTROS

Se establecerán y mantendrán registros para ofrecer evidencia de la conformidad con los requisitos y el funcionamiento efectivo del SGSI. Estos registros deberán ser controlados. El SGSI tomará en cuenta cualquier requisito legal pertinente. Los registros deben ser legibles, fácilmente identificables y accesibles.

Los controles necesarios para la identificación, almacenamiento, protección, acceso, tiempo de retención y disposición de registros deberán ser implementados y documentados.

6.3 CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Permite gestionar los privilegios de usuarios autorizados, controlar los accesos a los sistemas de información y generar reportes que faciliten controlar y auditar las diversas plataformas del Ministerio del Ambiente; los mismos que comprenden:

6.3.1 Gestión de privilegios de usuario autorizados

Los propietarios de la información son los encargados de definir los perfiles y privilegios para los usuarios autorizados que necesiten acceder a dicha información, los mismos que son controlados y evaluados por el Sistema de Informática y Tecnologías de la Información.

6.3.2 Control de accesos a los sistemas de información

Todos los usuarios de los sistemas informáticos conectados a la red del Ministerio del Ambiente, deben manejar una cuenta de usuario y una clave que les permita acceder a la información asignada según sus funciones, y deben estar regulados por procedimientos y estándares de identificación, autenticación, autorización, registros de acceso y monitoreo.

6.3.3 Gestión de claves de acceso de usuarios

Las claves de acceso de usuario tienen carácter personal, intransferible y confidencial, por lo que cada usuario es responsable de toda actividad que realice con su clave de acceso y es administrada de acuerdo a los privilegios asignados.

6.3.4 Acceso a la información por terceros

El acceso a la información del Ministerio del Ambiente por terceros debe limitarse a lo indispensable para cumplir con el servicio asignado y debe ser autorizado por el propietario de la información, así como supervisado por el custodio de la información.

6.3.5 Generación y accesos a registros

Todos los sistemas informáticos que manejen información clasificada, deben incluir reportes que identifiquen a los usuarios, las horas de inicio y cierre de sesión y acciones realizadas, a dichos reportes. Estos sólo son accesibles y auditables por los órganos de control del Ministerio del Ambiente.

6.4 AUDITORIAS INTERNAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio del Ambiente conducirá auditorías internas del Sistema de Gestión de Seguridad de la Información de forma periódica, para determinar si los objetivos de control, controles, procesos y procedimientos identificados de su SGSI están conformes a los requisitos de la NTP y la legislación o reglamentos relevantes y a los requisitos de seguridad de la información identificados, así como si se han implementado y mantenido efectivamente.

6.5 SEGURIDAD FÍSICA Y AMBIENTAL

Permite asegurar la confidencialidad, integridad y disponibilidad de los activos de información y los accesos a los ambientes de procesamiento, almacenamiento y comunicación de información del Ministerio del Ambiente, la misma que comprende:

6.5.1 Controles de acceso perimetral

- El personal del MINAM deberá portar, durante el horario de trabajo, de forma permanente, en un lugar visible, su fotocheck que lo identifique.
- Los visitantes o terceros que presten servicios para la entidad, a su ingreso a las instalaciones del MINAM, deberán estar adecuadamente identificados y anunciada su llegada a través del personal de Vigilancia, previo a su desplazamiento por las oficinas.
- Cualquier bien que ingrese o salga de las instalaciones del MINAM, debe ser registrado por el personal de Vigilancia.
- Las puertas de acceso a las áreas de manipulación o administración de información confidencial o privada, deberán permanecer cerradas en todo momento.

- Para el ingreso o salida de cualquier bien, deberá tramitarse el formato de actualización que tiene establecida la entidad con el registro completo de la información que se necesita.

- Las personas que ingresen a las áreas restringidas del MINAM, deberán cumplir los controles establecidos para los accesos específicos a dichas áreas.

6.5.2 Controles Ambientales

Los ambientes donde se procese, almacene y comunique la información del Ministerio del Ambiente deben ser implementados teniendo en cuenta los estándares y recomendaciones de seguridad física y ambiental de organizaciones y/o profesionales especialistas en el tema (ambientes, materiales, energía, cercanía a medios inseguros, mecanismos de seguridad y respaldo, etc.).

- El MINAM proporcionará un ambiente adecuado para la conservación de medios magnéticos y equipos.
- El MINAM mantendrá en condiciones óptimas la limpieza, la seguridad, el mantenimiento y la funcionalidad de cada uno de los elementos que forman parte del DATACENTER de la Entidad.
- El MINAM proporcionará el ambiente adecuado para la conservación de los documentos de tipo archivístico y bibliográfico.

6.5.3 Control de accesos a los ambientes

Las visitas a los ambientes donde se procese, almacene y comunique la información del Ministerio del Ambiente, deben de ser identificadas, autorizadas, registradas y supervisadas por un empleado autorizado durante la permanencia en dichos ambientes.

6.6. SEGURIDAD DE PERSONAL

Permite conocer al personal del MINAM, cuál es el rol y participación respecto a la seguridad de la información.

6.6.1 Concientización del personal

La Oficina General de Administración comunicará y capacitará a todo el personal, independientemente de su régimen laboral o contractual, respecto de las Normas y Procedimientos de Seguridad de Información de la Institución, asimismo, velará por su cumplimiento.

6.6.1.1 Ética y disciplina

El personal del MINAM, independientemente de su régimen laboral o contractual, deberá firmar el **Compromiso de Aceptación y Cumplimiento** (***Ver Apéndice N° 01***). Además, deberá cumplir con las disposiciones contenidas en el Código de Ética de la Función Pública y demás normativa relacionada.

6.6.1.2 Responsabilidades del personal

El personal del Ministerio del Ambiente, independientemente de su régimen laboral o contractual, es responsable de la seguridad de la información a la que tiene acceso, según las funciones que realice.

6.6.1.3 Proceso de selección del personal

Como parte de las Bases Administrativas de los procesos de selección que convoca el Ministerio del Ambiente, se deben establecer criterios de evaluación relacionados a la seguridad de información.

6.7 CONTRATOS CON TERCEROS

En los contratos que se celebren con terceros se deberá incluir la prohibición de divulgar los aspectos relativos a la confidencialidad, integridad y disponibilidad de la información a la que fuera autorizado a tener acceso, los cuales se rigen bajo el **Acuerdo de Confidencialidad** (***Ver Apéndice N° 02***).

6.8 ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

Permite proteger adecuadamente los activos de información del Ministerio del Ambiente, de acuerdo a su clasificación, la misma que comprende:

6.8.1 Clasificación de información

Toda la información utilizada por el MINAM deberá ser clasificada y administrada de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.

6.8.2 Inventario de activos de información

Los activos de información del Ministerio del Ambiente deben ser identificados e inventariados, según su clasificación por los propietarios y responsables de dichos activos.

6.8.3 Dispositivos de almacenamiento

El uso de dispositivos para el almacenamiento de información debe ser autorizado por los propietarios de la información y debe ser, exclusivamente, para fines de gestión o laborales y relacionados a las actividades propias del Ministerio del Ambiente.

6.8.4 Reasignación o dada de baja de equipos

Los equipos que contengan dispositivos de almacenamiento de información del Ministerio del Ambiente, deben de comprobarse que dicha información haya sido sobrescrita o eliminada antes de su reasignación o dada de baja.

6.9 SEGURIDAD DE LAS COMUNICACIONES

Permite el control de las conexiones a las redes del Ministerio del Ambiente, encriptar y desencriptar la información de acuerdo a su clasificación y regular el uso de los servicios de telefonía fija, correo electrónico, Internet e Intranet; la misma que comprende:

6.9.1 Conexión de componentes de red

La conexión de todo componente de la red debe ser realizada bajo procedimientos y estándares de seguridad que protejan a los equipos y a la información que circula por las redes internas y externas del Ministerio del Ambiente.

6.9.2 Retiro o desplazamiento de activos de información

El retiro y/o desplazamiento de activos de información de los ambientes de procesamiento, almacenamiento y comunicación de información sólo procede con la autorización del responsable de los activos y utilizando los medios de transporte autorizados por el Ministerio del Ambiente.

6.9.3 Sistemas de telefonía

Los equipos de anexos internos y teléfonos directos deberán ser utilizados, exclusivamente, para los fines propios de la gestión o trabajo, salvo casos de llamadas de emergencia.

6.9.4 Protección de la información en la red

Se debe implementar controles o mecanismos de prevención, detección y eliminación de software malicioso que ingrese a la red del Ministerio del Ambiente.

6.9.5 Conexión a Internet

Los accesos a Internet a través de las redes del Ministerio del Ambiente, son exclusivamente para fines de gestión o laborales, los que serán asignados solo al personal que por su función lo amerite, previa autorización del jefe del órgano correspondiente.

6.9.6 Conexión a Intranet

La Intranet es de uso exclusivo del personal del Ministerio del Ambiente. La información publicada en este medio debe contar con la autorización del propietario de la información y es solo de uso interno.

6.9.7 Correo electrónico

Se otorga el uso del correo electrónico al personal del Ministerio del Ambiente, solo para fines de gestión o laborales, debiendo contar con mecanismos de protección contra archivos adjuntos y mensajes no autenticados.

Todo correo electrónico que contenga información confidencial deberá indicar en el asunto la palabra "CONFIDENCIAL", a modo de rotulación.

Solo el personal debidamente autorizado tendrá la potestad de enviar correos electrónicos a destinatarios externos, en representación del Ministerio del Ambiente.

6.9.8 Encriptación

Toda la información clasificada, debe ser protegida en su almacenamiento y transporte electrónico, con algoritmos de encriptación vigentes y aprobados para su utilización por el Ministerio del Ambiente, de acuerdo a la clasificación que se le asigne.

Se debe implementar medidas de seguridad que garanticen la confidencialidad de las claves de encriptación usadas por el Ministerio del Ambiente.

6.10 DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Los Sistemas desarrollados por el MINAM o Contratados a terceros, deben contar con normas y procedimientos de seguridad para el desarrollo, adquisición y mantenimiento de sistemas de información, que permita proteger la información de agentes no autorizados; la misma que comprende:

6.10.1 Proceso de desarrollo y mantenimiento

El proceso de desarrollo y mantenimiento de sistemas de información debe ajustarse a las normas y procedimientos, estándares y metodologías implantadas en el Ministerio del Ambiente, así como con los acuerdos establecidos con los proveedores del servicio.

6.10.2 Adquisición de sistemas de información

En el proceso de adquisición de sistemas de información se debe especificar y cumplir los requisitos de seguridad de información, que garanticen la integridad de los sistemas existentes en el Ministerio del Ambiente, lo cual debe estar especificado en los contratos con los proveedores.

6.10.3 Ambientes de desarrollo y producción

El ambiente de desarrollo debe de mantenerse siempre separado del ambiente de producción, debiendo existir controles de acceso adecuados para cada uno de ellos.

6.10.4 Control de cambios

Se debe garantizar la operatividad de los sistemas informáticos a través de la implementación de controles, pruebas y verificación, antes de su pase a producción, bajo un adecuado nivel de segregación de funciones.

6.10.5 Derecho de propiedad intelectual

El Ministerio del Ambiente tiene la propiedad exclusiva sobre la patente, derechos de autor y otros derechos de propiedad intelectual de todo aquello que sus empleados y servicios contratados de terceros desarrollen para el Ministerio del Ambiente. "Esta cláusula debe incluirse expresamente en los contratos".

Se debe asegurar que el software del Ministerio (adquirido o desarrollado internamente) cumpla con la normativa vigente.

Los productos de software o modificados internamente a nombre del Ministerio del Ambiente, son propiedad exclusiva del MINAM.

El software desarrollado internamente por el personal del MINAM, deberá inscribirse a nombre del Ministerio del Ambiente en el registro intelectual respectivo, cuya función está bajo la responsabilidad de la Dirección General de Investigación e Información Ambiental – Centro de Documentación Ambiental, con objeto de acogerse a los resguardados que estipula la Ley de Propiedad Intelectual.

6.11 CONTINUIDAD DE SERVICIOS DE SISTEMAS DE INFORMACIÓN

Asegurar un nivel aceptable de operatividad y disponibilidad de los servicios críticos, ante fallas de los sistemas de información que sostienen a los procesos del Ministerio del Ambiente; la misma que comprende:

6.11.1 Plan de continuidad

El Ministerio del Ambiente debe implementar un Plan de Continuidad de los Sistemas y Servicios de información, para garantizar la operatividad y disponibilidad de los sistemas y servicios brindados, ante cualquier falla o interrupción en los mismos.

6.11.2 Respaldo de la información

Toda información crítica o sensible del Ministerio del Ambiente debe ser almacenada y respaldada en medios magnéticos mientras dure su vigencia.

6.12 MANEJO DE INCIDENCIAS DE SEGURIDAD DE INFORMACIÓN

Administrar adecuadamente las incidencias y debilidades de seguridad de información presentadas en los sistemas de información, minimizando sus ocurrencias e impacto sobre los procesos del Ministerio del Ambiente; la misma que comprende:

6.12.1 Respuesta ante incidencias

Se debe contar con planes de respuesta ante incidencias y debilidades de seguridad que afecten la operatividad de los sistemas informáticos del Ministerio del Ambiente, y que permita restaurar los servicios afectados en el menor tiempo posible.

6.12.2 Administración de las incidencias

Se deben instalar mecanismos para monitorear y cuantificar los tipos, ocurrencias e impacto de las incidencias, que permita implementar controles para minimizar su frecuencia e impacto en el Ministerio del Ambiente.

6.13 MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION

El MINAM mejorará continuamente la efectividad del sistema de gestión de la seguridad de la información a través del uso de la norma y procedimientos de

seguridad de la información, objetivos de seguridad, resultados de auditorías, análisis de eventos monitoreados, acciones correctivas y preventivas, y revisión gerencial.

7. GLOSARIO DE TÉRMINOS

Con la finalidad de facilitar la lectura y aplicación de los Lineamientos, éstos contienen un Glosario de Términos (***Ver Apéndice N° 03)***

8. DISPOSICION COMPLEMENTARIA:

Los procedimientos correspondientes al Sistema de Informática y Tecnologías de la Información, aprobados mediante Resolución Ministerial Nº 085-2012-MINAM, que detallan algunos de los aspectos citados en los presentes Lineamientos, no han sido alterados y siguen teniendo vigencia y su cumplimiento es obligatorio por todos los órganos integrantes del Ministerio (***Ver Apéndice N° 04)***.

MINISTERIO DEL AMBIENTE C. LOPEZ Oficina de Asesoría Jurídica MINAM

MINISTERIO DEL AMBIENTE Oficina General de Administración MINAM

MINISTERIO DEL AMBIENTE LINEAMIENTO Y PRESUPUESTO MINAM

APÉNDICE N° 01

COMPROMISO DE ACEPTACIÓN Y CUMPLIMIENTO

Yo.....
..... identificado con DNI .....
Domiciliado en .....
.....

DECLARO BAJO JURAMENTO tener pleno conocimiento de la Directiva **"Normas y Procedimientos Generales de Seguridad de Información"**; y demás responsabilidades y conductas no aceptadas respecto a la seguridad de la información del MINAM, comprometiéndome a salvaguardar la integridad, disponibilidad y confidencialidad de la información.

Responsabilidades

- Me comprometo a conocer y cumplir con la Directiva "Normas y Procedimientos Generales de Seguridad de Información" y todo otro documento normativo que el MINAM considere necesario implantar para cumplir con los requisitos legales y/o salvaguardar la integridad, disponibilidad y confidencialidad de la información.
- Asumo la responsabilidad sobre los sistemas y recursos puestos a mi disposición por el MINAM para el desarrollo de las funciones que se me encomendó. Me responsabilizo por la seguridad de los mismos.
- Me responsabilizo por la notificación a la OGA – Sistema de Informática y Tecnologías de la Información y a mis jefes inmediatos, en caso de verificar el mal uso de los recursos por parte de algún otro personal interno o externo al MINAM.
- Me comprometo a utilizar sólo aquel software que este autorizado por el órgano competente y que me haya sido asignado para el desarrollo de las funciones encomendadas
- Asumo la responsabilidad en el uso y manipulación de la información sobre la que tengo autorización, la que me comprometo a efectuar y proteger en base a los niveles de clasificación que tenga dicha información.
- Me comprometo a no acceder, copiar ni transferir información para la cual no tengo la autorización adecuada.

MINISTERIO DEL AMBIENTE Oficina de Asesoría Jurídica C. LÓPEZ MINAM

Conductas No Aceptadas

MINISTERIO DEL AMBIENTE Oficina General de Administración MINAM

Todas aquellas indicadas en la Ley como figuras penales relativas a Informática, tales como:

- Distribución maliciosa o inutilización de sistemas de información, sus partes o componentes, obstaculización o modificación de su funcionamiento o modificación no autorizada de los datos contenidos en el sistema.
- Acceso o intromisión en sistemas para apoderarse, usar o conocer indebidamente la información contenida en él.
- Daño, alteración o destrucción maliciosa de los datos contenidos en un sistema de información.
- Revelación o difusión maliciosa de datos contenidos en un sistema.

MINISTERIO DEL AMBIENTE PLANEAMIENTO Y PRESUPUESTO MINAM

- Conductas contrarias a la Ley, en base a lo establecido en el Decreto Legislativo Nº 822, Ley sobre el Derecho de Autor, acerca de la legislación de derechos de autor y propiedad intelectual, que regula la adquisición y el uso de software, o cualquier otra ley promulgada al respecto.
- Copiar o distribuir software, datos, códigos y manuales sin la expresa autorización del titular de los derechos de autor.
- Usar copias no autorizadas de Software (sin la debida licencia). Esto incluye la ejecución simultánea de software en dos o más computadores salvo que conste debidamente autorizado en la licencia de uso.
- Fabricar, adquirir o utilizar cualquier elemento que sirva para remover o burlar, aspectos de seguridad del software legalmente adquirido.
- El no cumplimiento de este compromiso formal, será considerado por el MINAM como una falta grave que atenta tanto contra la legalidad vigente como contra las normas internas, y lo faculta para adoptar las medidas administrativas que estime pertinente.

Lima, ___ de _____ del 20__

_____

NOMBRES Y APELLIDOS:
DNI:

MINISTERIO DEL AMBIENTE - Oficina de Asesoría Jurídica - C. LÓPEZ - MINAM

MINISTERIO DEL AMBIENTE - Oficina General de Administración - MINAM

MINISTERIO DEL AMBIENTE - PLANEAMIENTO Y PRESUPUESTO - MINAM

Este Apéndice deberá formar parte de los documentos que el personal debe firmar a su ingreso a prestar sus servicios o laborar en el MINAM.

APÉNDICE N° 02

ACUERDO DE CONFIDENCIALIDAD

Este Acuerdo de Confidencialidad (el "Acuerdo") efectivo el día.....,es firmado entre EL MINAM y EL TERCERO.

Por cuanto **EL TERCERO** ha recibido la solicitud para realizar ciertos servicios (los "Servicios") para el MINAM; y por cuanto, en conexión con la provisión de tales Servicios, el MINAM puede proporcionar a EL TERCERO cierta información considerada "Información Confidencial". En consecuencia, por lo anterior **El MINAM y EL TERCERO** Acuerdan lo siguiente:

1) Toda Información Confidencial debe ser etiquetada como "Información Confidencial" en forma escrita por EL MINAM antes de ser proporcionada a EL TERCERO para propósito de este documento, siendo EL TERCERO responsable de no revelar la **"Información Confidencial"** a ningún tercero, sujeto a los términos y condiciones establecidos en este documento.

2) El término "Información Confidencial" no debe incluir ninguna información:

   (a) Que no esté designada como "Información Confidencial", según lo señala el párrafo 1 de este Acuerdo.

   (b) Disponible al público (incluyendo sin limitación cualquier información obtenida de cualquier agencia gubernamental y disponible al público).

   (c) **EL TERCERO** tenga disponibilidad sobre una base no confidencial de una tercera parte.

   (d) Revelada por el cliente a una tercera parte sin sustancialmente la misma restricción establecida en este Acuerdo.

   (e) Solicitada a ser revelada por **EL TERCERO** por orden de una corte o jurisdicción competente, agencia administrativa o entidad del gobierno, o por cualquier ley, norma o regulación, o por mandato de comparecencia, o cualquier otro proceso legal o administrativo, o mediante normas profesionales o regulatorias aplicables.

   (f) Revelada por **EL TERCERO** en conexión con cualquier procedimiento judicial u otro que involucre a **EL TERCERO y al MINAM** relacionado con este Acuerdo y los Servicios.

   (g) Revelada con el consentimiento escrito de EL MINAM.

3) **EL TERCERO** está de acuerdo que la Información Confidencial entregada por EL MINAM y será usada por EL TERCERO solamente en conexión con la provisión de estos Servicios.
4) **EL TERCERO** debe llevar a cabo sus obligaciones bajo este Acuerdo usando las mismas normas de seguridad que utiliza para proteger su propia información, o por lo menos un razonable grado de seguridad.
5) Las obligaciones establecidas en este documento con respecto a esta "Información Confidencial", continuará en toda su extensión y efectos por un período de 5 años desde la fecha efectiva de este Acuerdo, o un período menor a 3 años en caso que así lo acuerden las partes.

6) Este Acuerdo se rige por las leyes de la República de Perú.

Encontrándose las partes conformes con la ejecución de este Acuerdo, los representantes autorizados de las partes firman este documento en duplicado en señal de conformidad.

En la ciudad de Lima, el _____de _____ de _____ 20__.

EL MINAM

Por: _____

Título _____

EL TERCERO

Por: _____

Este Apéndice deberá ser incluido en los contratos que el MINAM formalice con terceros para la prestación de servicios.

APÉNDICE N° 03

GLOSARIO DE TÉRMINOS

ACEPTACIÓN DEL RIESGO.- Decisión de aceptar el riesgo

ACTIVO.- (Seguridad de la información) Es cualquier información o sistema relacionado con la captura, generación, tratamiento, almacenamiento y presentación de la misma, el cual tienes un valor para la organización. Estos pueden ser:

- **Activo de información**.- Archivos, bases de datos, manuales procedimientos operativos o de soporte, contratos y acuerdos, material de formación, información financiera, documentos con información de investigación y desarrollo, correo físico y electrónico, libros revistas, etc.

- **Activos de software**.- Software de aplicación software del sistema, herramientas y programas de desarrollo.

- **Activos físicos:** Instalaciones (cuarto de servidores, closets de cableado y LAN, sistemas de alarma ubicación de proveedor terremark), equipos de computo, de comunicaciones, medios magnéticos, u otro equipo técnico.

- **Activos de servicios:** Servicios de comunicaciones, informáticos, documentarios, de información y informáticos (VPN, FTP, web, proxy, mail, seguridad firewall, IDS, IPS, anti-spam/virus/spyware, servicio de wireless y protocolo de autenticación) y generales (energía eléctrica, telefonía iluminación)

- **Personas:** Personal empleado, sus calificaciones, habilidades y experiencia y conocimientos.

- **Intangibles:** Reputación e imagen institucional, secretos comerciales, patentes, registros de marca, confianza de los clientes, ventaja competitiva ética productividad relación de negocios (proveedores, clientes, sociedad) logros e imagen corporativa

ANÁLISIS DEL RIESGO.- Uso sistemático de información para identificar amenazas y estimar el riesgo.

AMBIENTE DE ALMACENAMIENTO.- Espacio acondicionado para resguardar la información, copias de respaldo y documentación.

AMBIENTE DE COMUNICACIÓN.- Espacio acondicionado donde se establece comunicación entre los equipos y los sistemas de información.

AMBIENTE DE DESARROLLO.- Espacio acondicionado donde se elabora y se pone a prueba la herramienta informática.

AMBIENTE DE PROCESAMIENTO.- Espacio acondicionado donde se ingresa, se procesa y se distribuye la información.

AMBIENTE DE PRODUCCIÓN.- Espacio acondicionado donde se despliega la herramienta informática para su uso.

ASIGNACIÓN Y CONTROL DE PRIVILEGIOS.- Consiste en otorgar facultades de acceso a la información a un usuario autorizado, de acuerdo a las funciones delegadas.

AUTENTICACIÓN.- Proceso que permite verificar la identidad de un usuario cuando éste intenta acceder a un sistema de información.

CERTIFICADO.-Documento digital emitido por una entidad independiente que garantiza la identidad de los sistemas y personas en internet. La seguridad del certificado está protegida por técnicas criptográficas.

CIFRADO.-Codificación de datos mediante diversas técnicas matemáticas que garantizan su confidencialidad en la transmisión.

CLASIFICACIÓN DE INFORMACIÓN.- Es un proceso que permite asignar un nivel de protección adecuado a los activos de información, de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.

CLAVE DE ACCESO.- Conjunto de caracteres alfanuméricos, conocidos exclusivamente por el usuario propietario y que le permite el acceso a la información del Ministerio del Ambiente.

CLAVE DE ENCRIPTAMIENTO.- Código que permite acceder a la información de los sistemas encriptados.

CÓDIGO MALICIOSO.- Cualquier programa con una intención molesta, malévola o ilegal. Generalmente están diseñados para ejecutarse sin la intervención del usuario.

COMPONENTE DE RED.- Es todo equipo o medio informático o de comunicación que pertenece a la red del Ministerio del Ambiente.

CONFIDENCIALIDAD.- Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

CONTRASEÑA.- Conjunto de letras, números y símbolos, o incluso frases, utilizadas para autenticar usuarios en un sistema informático. Para que el uso de contraseñas sea efectivo es necesario escogerlas de manera que sean difíciles de adivinar para un atacante.

COOKIE.- Información que, remitida por un servidor de internet al navegador, es devuelta posteriormente en cada nueva conexión. Pueden utilizarse con intenciones legítimas, como la identificación de usuarios, o malévolas, como el almacenamiento no consentido de pautas de navegación.

CORREOS ENCADENADOS.- Son mensajes de correo electrónico donde se solicita que el mensaje sea reenviado a otras personas para que éstas a su vez los reenvíen. Es una de las posibles fuentes de problemas con el correo electrónico, ya que a veces contienen noticias falsas, pueden ser portadores de virus, etc.

CRIPTOGRAFÍA.- Disciplina que se ocupa de la seguridad de la transmisión y el almacenamiento de la información.

CUSTODIO DE LA INFORMACIÓN.- Es el empleado que protege y resguarda la información.

DENEGACIÓN DE SERVICIO.- Ataque informático que, sin afectar a la información contenida en un sistema, lo deja incapacitado para prestar servicio. La denegación puede conseguirse mediante la saturación o el bloqueo de las máquinas.

DECLARACION DE APLICABILIDAD.- Documento que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

DISPONIBILIDAD.- Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados de acuerdo a los niveles establecidos.

ENCRIPTACIÓN.- Medida de seguridad que permite codificar y decodificar la información del Ministerio del Ambiente, de tal manera que no sea legible o fácil de entender por personas no autorizadas. Filtrado de contenidos.- Conjunto de tecnologías que permiten un control de la información transmitida por servicios de

internet. El filtrado de contenidos se utiliza para bloquear virus enviados por correo electrónico, para controlar el acceso a internet de menores, etc.

ESTIMACIÓN DEL RIESGO.- Proceso total de análisis y evaluación del riesgo.

EVENTO DE LA SEGURIDAD DE LA INFORMACIÓN.- Ocurrencia identificada en un sistema servicio o red indicando una posible brecha de la política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.

EVALUACION DEL RIESGO.- Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado del riesgo.

FIREWALL.- Sistema de red que controla a que máquinas y servicios se puede acceder dentro de una red. Puede ser un sistema especializado o un programa instalado (firewall personal). Cuando este control se realiza sobre la información trasmitida y no simplemente sobre la conexión el sistema empleado es un Proxy.

FILTRADO DE CONTENIDOS:

FIREWALL PERSONAL.- Firewall instalado como un programa en una máquina que controla exclusivamente los accesos a ésta. Suele emplearse en ordenadores domésticos con conexión directa a internet.

FIRMA ELECTRÓNICA.- Información digital asociada a una operación en particular realizada en internet que, junto con los certificados, permite garantizar la identidad de los participantes en una transacción.

GENERACIÓN Y ACCESOS A REGISTROS (LOGS).- Consiste en recopilar los datos mínimos necesarios para generar registros a fin de poder reconstruir una acción, transacción u operación para fines de auditoría.

GESTION DEL RIESGO.- Actividades coordinadas para dirigir y controlar el riesgo en una organización.

GUSANO.- Tipo de código malicioso cuya característica principal es que se copia de unos sistemas a otros a través de internet.

INGENIERÍA SOCIAL.- Técnicas que intentan atacar la seguridad de los sistemas informáticos engañando a sus usuarios y administradores. La mayoría de las técnicas de ingeniería social son similares a los timos.

INCIDENTE DE LA SEGURIDAD DE LA INFORMACION.- Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD.- La información no puede ser alterada ni eliminada por cambios no autorizados o accidentales.

INTRUSIÓN.- Intromisión informática en la que el atacante consigue obtener un control completo sobre la máquina. Durante una intrusión el atacante puede obtener y alterar todos los datos de la máquina, modificar su funcionamiento e incluso atacar a nuevas máquinas.

PERFIL DEL USUARIO.- Es el nivel de autorización a la información que se le asigna a un empleado de acuerdo a las funciones encomendadas.

PLAN DE CONTINUIDAD.- Conjunto de procedimientos a seguir en caso se presente una ocurrencia inesperada, permitiendo asegurar la continuidad de los procesos.

PROPIETARIO DE LA INFORMACIÓN.- Es el empleado o dueño de la información que le es asignada para el desempeño de las actividades a su cargo.

PROXY.- Sistema informático cuya misión es hacer de intermediario entre un sistema y otro a través de internet. Entre las misiones de un proxy están acelerar el acceso a internet, filtrar los contenidos a los que se ha accedido y proteger los sistemas evitando su comunicación directa.

RIESGO RESIDUAL.- Riesgo remanente después de un tratamiento del riesgo.

RIESGO INFORMÁTICO.- Es la posibilidad de ocurrencia de alguna situación inesperada que no permita operar normalmente los medios de tecnología de información.

SEGREGACIÓN DE FUNCIONES.- Es la delimitación de funciones que permite controlar y/o reducir el mal uso o modificación no autorizado de los sistemas de información y/o servicios.

SEGURIDAD DE INFORMACIÓN.- Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISMS).- ES la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

SOFTWARE MALICIOSO.- Programas no autorizados que ingresan a la red para causar daño a la institución (virus informáticos, gusanos, caballos de Troya, bombas lógicas, etc.).

SPAM.- Correo comercial no solicitado que se envía a través de internet. El volumen y contenido del SPAM puede dificultar notablemente el uso de servicios de correo electrónico.

TECNOLOGÍA DE INFORMACIÓN.- Es el conjunto de elementos que brindan soporte directo o indirecto a los procesos. Está compuesta por infraestructura (equipos, redes, sistemas base y aplicaciones) e información (bases de datos, procesamiento y transmisión de información).

TERCEROS.- Se considera como terceros a las personas o entidades que brindan servicios al Ministerio del Ambiente bajo diferentes modalidades de contrato.

TRATAMIENTO DEL RIESGO.- Proceso de selección e implementación de controles para minimizar el riesgo.

TROYANO.- Código malicioso camuflado dentro de otro programa aparentemente útil e inofensivo. Los troyanos pueden ir incluidos dentro de programas conocidos, de forma que es necesario controlar la fuente de donde se obtiene el software.

USUARIO DE LA INFORMACIÓN.- Es el Órgano o la persona autorizada que hace uso de la información.

VIRUS.- El tipo más conocido de código malicioso. Programa que se copia dentro de otros programas e intenta reproducirse el mayor número de veces posible. Aunque no siempre es así, la mayoría de las veces el virus, además de copiarse, altera o destruye la información de los sistemas en los que se ejecuta.

APÉNDICE N° 04

Procedimientos vigentes y vinculados a la Directiva de **"Normas y Procedimientos Generales de Seguridad de Información"** del MINAM, y que están contenidos en el Manual de Procedimientos (MAPRO), aprobado mediante Resolución Ministerial Nº 085-2012-MINAM.

CODIGO	NOMBRE DEL PROCESO
1) MP-OGA-051	Atención a pedidos de Soporte Técnico.
2) MP-OGA-052	Creación a cuentas de Usuario, correo electrónico y acceso a sistemas Administrativos.
3) MP-OGA-053	Actualización y Mantenimiento de la Pagina Web Institucional.
4) MP-OGA-054	Administración y Seguridad del Código de Acceso al Servicio de Telefonía fija.
5) MP-OGA-055	Verificación de Uso Legal de Software.
6) MP-OGA-056	Elaboración de Informes de Evaluación de Software.
7) MP-OGA-057	Mantenimiento de Internet.

MINISTERIO DEL AMBIENTE - Oficina de Asesoría Jurídica - C.LÓPEZ - MINAM

MINISTERIO DEL AMBIENTE - Oficina General de Administración - MINAM

MINISTERIO DEL AMBIENTE - PLANEAMIENTO PRESUPUESTO - MINAM