INSTITUTO DEL MAR DEL PERU

Resolución Directoral DE-143-2012

Callao, 25 de Julio de 2012.

VISTO:

La propuesta de las Políticas de Seguridad Informática y de Comunicaciones digitales, elaborado por la Unidad de Informática del IMARPE.

CONSIDERANDO:

Que, la citada propuesta contiene los puntos importantes y acciones necesarias para normar en la prevención y contingencias relacionadas con las tecnologías de información institucional.

Que, el indicado documento ha sido debidamente analizado, revisado y planteado a fin de no contravenir las garantías básicas del individuo, contemplando políticas que reflejan la visión de la actual administración respecto a la problemática de seguridad informática institucional.

Que, mediante Memorándum NºUIE-085-2012 el Jefe de la Unidad de Informática hace de conocimiento a la Dirección Ejecutiva de las Políticas de Seguridad Informática y de Comunicaciones - PSIC, elaborada por la Unidad de Informática del IMARPE.

Que, es necesario definir las Políticas de Seguridad Informática y de Comunicaciones - PSIC en nuestra entidad, a fin de dar estricto cumplimiento a la normativa vigente y facilitar una mejor gestión de la información a la comunidad científica y usuarios internos y externos del sector.

Que, resulta pertinente aprobar las Políticas de Seguridad Informática y de Comunicaciones PSIC del IMARPE, a que se refiere 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".

De conformidad con las facultades conferidas en el Artículo 19º del Reglamento de Organización y Funciones del IMARPE, aprobado por Decreto Supremo Nº009-2001.

- Resolución Ministerial Nº61-2011-PCM; Ley N° 27309 título V capítulo X del Código Penal y que trata sobre los "Delitos Informáticos".

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

- Resolución Ministerial Nº 246-2007-PCM. 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.

- Resolución Ministerial Nº129-2012-PCM. Aprueban 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.

- Resolución Directoral N° DE-225-2009 "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información en el Instituto del Mar del Perú -IMARPE"

Con el visto bueno de las Oficinas de Asesoría Jurídica, de Planificación, Presupuesto y Evaluación de Gestión, de Administración y de la Unidad de Informática y Estadística;

SE RESUELVE:

Artículo 1º.- Aprobar el documento **POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE COMUNICACIONES - PSIC** del Instituto del Mar del Perú- IMARPE, el mismo que en Anexo forma parte de la presente Resolución Directoral.

Artículo 2º.- La Alta Dirección del IMARPE remitirá a la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la Presidencia del Consejo de Ministros, el documento Políticas de Seguridad Informática y de Comunicaciones PSIC.

Artículo 3º.- Disponer que la Unidad de Informática y Estadística publique la presente Resolución en el Portal de Transparencia del IMARPE y difunda a los usuarios internos, a través del correo de dominio institucional.

Regístrese y Comuníquese

Blgo. Marco Antonio Espino Sánchez
Director Ejecutivo
IMARPE

INSTITUTO DEL MAR DEL PERU
UNIDAD DE INFORMÁTICA Y ESTADÍSTICA

POLÍTICAS DE SEGURIDAD INFORMÁTICA Y COMUNICACIÓN (PSIC)

CONTENIDO

POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE COMUNICACIONES - PSIC

1. Introducción

Las políticas de la seguridad informática son un conjunto de lineamientos que establecen el marco de referencia sobre las que se sustentan las normas y/o procedimientos, que son, en este caso, el canal formal de actuación del personal en relación con los recursos y servicios informáticos, enunciando lo que deseamos proteger y el porqué, sin llegar a ser una descripción técnica del mecanismo de seguridad.

Cada política de seguridad informática es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como motor de intercambio y desarrollo en el ámbito de sus funciones. Tal invitación debe concluir en una posición consciente y vigilante del personal respecto al uso y limitaciones de los recursos y servicios informáticos críticos de la Organización.

El presente es una propuesta de las políticas de seguridad informática y de comunicaciones digitales, elaborado por la Unidad de Informática del IMARPE, y contiene los puntos importantes y acciones necesarias para normar en la prevención y contingencias relacionadas con las tecnología de información institucional. Esta ha sido debidamente analizada, revisada y planteada, a fin de no colisionar con los Derechos Humanos y convirtiéndose en una camisa de fuerza, y más bien muestra una buena forma de operar el sistema con seguridad, respetando en todo momento las normas y reglamentos vigentes de la Institución.

Se mencionan algunas acciones que por la naturaleza extraordinaria tuvieron que ser llevadas a la práctica como son: los inventarios de hardware y software, así como todos los aspectos que representan un riesgo o las acciones donde se ve involucrada y que compete a las tecnologías de la información. Se han contemplado también las políticas que reflejan la visión de la actual administración respecto a la problemática de seguridad informática institucional.

2. Finalidad

Afianzar la seguridad de sus sistemas computacionales y evitar su uso indebido, lo cual puede ocasionar serios problemas en sus bienes y servicios informáticos.

El IMARPE considera que las PSIC, por si solas no constituyen una garantía para la seguridad informática, sino que depende principalmente del esfuerzo de todo el personal que labora en la organización el velar por su cumplimiento.

3. Marco Legal

Las normas legales relacionadas con el tema de políticas de Seguridad de la Información y de Comunicaciones que rigen para el sector público, se consideran:

- Ley N° 27309 título V capítulo X del código Penal y que trata sobre los "Delitos Informáticos".
- Ley N° 27815, ley del código de Ética de la Función Pública.
- Resolución Ministerial Nº 246-2007-PCM. 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.
- Resolución Directoral N° DE-225-2009 "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información en el Instituto del Mar del Perú - IMARPE"
- Resolución Ministerial Nº129-2012-PCM. Aprueban 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. Organización de las Políticas de Seguridad Informática

Las PSIC se han organizado en grupos de políticas, según se aprecia a continuación:

- ◊ Políticas Generales
- ◊ Políticas sobre Información Electrónica
- ◊ Políticas sobre Recursos Informáticos
- ◊ Políticas sobre Seguridad Física
- ◊ Políticas sobre Seguridad Lógica
- ◊ Políticas sobre Administración de Recursos.

En la organización de cada política se incluye los siguientes aspectos: *Objetivo, Alcance, Enunciado, y Responsabilidades*

4.1 Políticas Generales

Las políticas consideradas en este grupo son aquellas que están relacionadas con la propiedad, conocimiento, sanciones y responsabilidades de toda política, norma y procedimiento sobre seguridad informática emitida por la organización.

4.1.1 Propiedad de políticas, normas y procedimientos de seguridad informática

Objetivo

El objetivo de esta política, es definir el propietario de las políticas, normas y procedimientos de seguridad informática emitidas por el IMARPE, estableciendo privilegios de acceso y restricciones sobre su divulgación por parte del personal que labora en la organización.

Alcance

El alcance de esta política involucra a todo el personal que labora en el IMARPE, bajo cualquier régimen laboral, así como, por los dispositivos legales que rigen para el Sector Público relacionado a informática.

Política

Toda política, norma o procedimiento de seguridad informática emitida por el IMARPE, es un documento oficial de propiedad de la organización, debiéndosele establecer un grado de confidencialidad que permita asegurar su disponibilidad al personal de la organización, de acuerdo a las funciones que realice.

Toda divulgación de información, políticas, normas o procedimientos de seguridad informática dentro de la organización debe contar con la aprobación de la Alta Dirección o de quien delegue esta facultad.

Responsabilidad

Es responsabilidad de la Alta Dirección o a quien delegue, velar por el cumplimiento de esta política, para lo cual debe dar normas y/o procedimiento que permitan administrar y controlar lo establecido por esta política.

Es responsabilidad de todo el personal que labore en el IMARPE, bajo cualquier régimen el acceder exclusivamente a las políticas, normas y procedimientos que le asigne la organización y el no divulgar a terceras personas cualquier información o documento relacionado con la seguridad informática. Estando obligado a informar a la Alta Dirección o a quien delegue, sobre cualquier evento que afecte a esta política.

4.1.2 *Participación del personal en la seguridad informática*

Objetivo

El objetivo de esta política, es enmarcar la participación del personal que labora en el IMARPE, bajo cualquier modalidad, la seguridad de informática de la organización, relacionado con el conocimiento y aplicación de las políticas, normas y procedimientos.

Alcance

El alcance de esta política involucra a todo el personal que labore en el IMARPE, bajo cualquier modalidad y la aplicación de las políticas, normas o procedimientos sobre la seguridad informática emitidos por la organización.

Política

Todo el personal que labora en el IMARPE, bajo cualquier modalidad es participante activo de los planes y objetivos de la seguridad de la informática de la organización, por lo que deberá conocer y aplicar las políticas establecidas en el presente documento, así como los procedimientos y normas que la regulen. Con la finalidad de asegurar la integridad y confiabilidad de la información y de los recursos informáticos, evitando su uso indebido, lo cual puede ocasionar riesgos que afecten a los bienes y/o servicios informáticos de la organización.

Responsabilidad

Es responsabilidad de la Alta Dirección o de quien esta delegue velar por el cumplimiento de esta política, para lo cual debe establecer normas y/o procedimientos que aseguren su distribución inicial y de toda actualización que se realice, así como establecer los controles necesarios que garanticen el conocimiento de los documentos mencionados por parte del personal de la organización.

Es responsabilidad de todo el personal que labore en el IMARPE bajo cualquier modalidad el conocer y aplicar en forma correcta las políticas, normas y procedimientos de seguridad informática que la organización le otorgue.

4.1.3 *Sanciones al personal por faltas contra la seguridad informática.*

Objetivo

El objetivo de esta política, es establecer la existencia de sanciones al personal de la organización por faltas cometidas contra la seguridad informática, que estén contempladas en el presente documento.

Alcance

Todo el personal que labore en el IMARPE, bajo cualquier modalidad y todo riesgo que afecte la seguridad informática esté o no contemplado en dispositivos legales o en las políticas, normas y/o procedimientos de la organización.

Política

Todo el personal que labore en el IMARPE bajo cualquier modalidad será sancionado ante cualquier infracción contra la Seguridad Informática, conforme lo establece el Código Penal (Decreto Legislativo Nº 635, Libro Segundo, Título V, Capítulo X, Delitos Informáticos, Artículos 207º – A al 207º - C), modificado por la Ley Nº 27309 que incorpora los delitos informáticos al Código Penal; o lo establecido en las políticas, normas y/o procedimientos de la organización; debiendo considerar la gravedad de la infracción por el posible riesgo ocasionando, sin ser atenuante el hecho de no haberse afectado los bienes o servicios informáticos de la organización.

Responsabilidad

Es responsabilidad de la Alta Dirección o de quien esta delegue, en coordinación con la Oficina de Administración (DOA) - Unidad de Personal, establecer el grado de gravedad de las faltas y su correspondiente sanción, los cuales deberán estar indicados en las normas y/o procedimientos establecidos para cada política.

Es responsabilidad de la Alta Dirección o de quien esta delegue, velar por el cumplimiento de esta política, dar normas y/o procedimientos para su regularización y establecer los controles con las herramientas necesarias que le permitan determinar infracciones contra las seguridad de informática.

Es responsabilidad de la Oficina de Administración (DOA) - Unidad de Personal el aplicar, informar y registrar toda infracción cometida con la seguridad informática.

4.1.4 *Actualización de las PSI y de las normas y/o procedimientos que las regulen*

Objetivo
El objetivo de esta política es definir el ente encargado de actualizar las Políticas de Seguridad de Informática (PSI) de la Organización, así como de toda norma y/o procedimiento que regulen a dichas políticas.

Alcance
Toda modificación que se deba realizar a las Políticas de Seguridad Informática y a las normas y/o procedimientos que las regulen. Considerado como modificación las acciones de añadir, cambiar o eliminar parte o totalidad de los documentos.

Política
La función de administrar, controlar y actualizar el presente documento, así como de establecer las normas y/o procedimientos que regulen cada política es de la Alta Dirección o a quien delegue. Siendo de vital importancia el realizar esta función en forma correcta y oportuna, de tal forma que permita garantizar la integridad y confiabilidad de los servicios informáticos.

Responsabilidad
Es responsabilidad de la Alta Dirección o de quien esta delegue el administrar, controlar y actualizar el presente documento, así como establecer las normas y procedimientos que permitan cumplir en forma correcta con lo establecido por esta política.

4.2 Políticas sobre Información Electrónica

Las políticas consideradas en este grupo son aquellas que están relacionadas con la *propiedad, restricciones y protección de la información* electrónica de la organización.

4.2.1 *Propietario de la información electrónica*

Objetivo
El objetivo de esta política, es establecer la propiedad de la información electrónica por parte de la organización, así como las restricciones sobre su utilización o divulgación, de acuerdo a lo dispuesto por la organización, a dispositivos legales aplicables y a las recomendaciones técnicas de ONGEI.

Alcance
De acuerdo con la definición de información electrónica, el alcance de esta política es toda información que se almacene o se procese o se acceda en cualquier activo informático de la organización.

Política
El IMARPE es propietaria único y exclusivo de toda información electrónica de la organización, la cual dependiendo de su tipo de grado de sensibilidad, debe ser identificada, controlada y protegida. Por tal motivo, todo acceso a la información electrónica dentro de la organización debe ser autorizado, identificado y controlado por el área de su custodia.

Toda divulgación de la información electrónica hacia afuera de la organización, debe contar con la aprobación del Director Ejecutivo del IMARPE.

Toda utilización, ingreso o interferencia indebida sobre información electrónica de la organización será considerado "Delitos Informáticos", de acuerdo a los artículos 207°- A, 207°- B y 207°- C del Código Penal.

Las normas y/o procedimientos que regulen esta política deben estar alineadas con lo establecido por el ONGEI según Resolución Jefatural Nº 347-2001-INEI sobre "Normas y Procedimientos Técnicos para Garantizar la Seguridad de la Información Publicadas por las Entidades de la Administración Pública".

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien delegue, administrar y custodiar la información electrónica del IMARPE, estableciendo normas y/o procedimientos que aseguren la integridad, confidencialidad y propiedad de la información, para lo cual debe establecer controles con las herramientas necesarias que garanticen el cumplimiento de esta política.

Es responsabilidad de todo el personal que labore en el IMARPE, el velar por el cumplimiento de esta política, de las normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Alta Dirección o a quien delegue, sobre cualquier divulgación o uso indebido de la información electrónica.

4.2.2 *Información electrónica permitida por el IMARPE*

Objetivo
El objetivo de esta política, es definir la información electrónica a la cual, el IMARPE permite acceder o almacenar en sus recursos informáticos.

Alcance
De acuerdo con la definición de información electrónica, el alcance de esta política es toda información que se almacene o se procese o se acceda en cualquier activo informático de propiedad, en alquiler o que presten servicios al IMARPE.

Política

El personal que labore en el IMARPE, bajo cualquier modalidad solo podrá acceder, procesar o almacenar información electrónica que esté de acuerdo con sus funciones asignadas. Por tal motivo está prohibido que el personal en mención tenga en los recursos informáticos de la organización información de carácter personal o de asuntos ajenos a sus funciones.

La Alta Dirección o a quien delegue con justificación y aprobación debida, puede revisar, monitorear o registrar cualquier información electrónica existentes en los recursos informáticos de la organización, sin necesidad de avisar o solicitar permiso de los usuarios.

Responsabilidad

Es responsabilidad de la Alta Dirección o a quien delegue dar normas y/o procedimientos que regulen esta política y de establecer controles con las herramientas necesarias para verificar que en los recursos informáticos de la organización, solo exista información de corresponda a las funciones del IMARPE, y que corresponda a las labores desempeñadas por cada persona.

Es responsabilidad de todo el personal que labore en el IMARPE el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Alta Dirección o a quien delegue, de toda información que se encuentre en los activos informáticos de la organización y que sea ajena a las funciones del IMARPE.

4.3 Políticas sobre Recursos Informáticos

Las políticas consideradas en este grupo son aquellas que están relacionadas con propiedad de los recursos informáticos y las restricciones sobre su uso. A fin de garantizar su integridad y sus correcto empleo.

4.3.1 Propietario de los recursos informáticos.

Objetivo

El objetivo de esta política es establecer la propiedad de los recursos informáticos adquiridos que presten servicios al IMARPE, así como establecer las restricciones sobre su utilización.

Alcance

De acuerdo con la definición de recursos informáticos, el alcance de esta política es a todo recurso informático que tenga relación con almacenar, procesar o acceder a la información electrónica de la organización y que sea de propiedad del IMARPE. Queda excluida de esta política todo programa o software con uso de licencia legal.

Política

El IMARPE es propietaria única y exclusiva de todos los recursos informáticos adquiridos que le presten servicios a la organización, siempre y cuando no se traten de programas o software con uso de licencia legal.

Tratándose de recursos informáticos alquilados por el IMARPE, para que le presten servicios al IMARPE se reserva todos los derechos derivados de su uso.

Todo recurso informático adquirido por el IMARPE, debe ser asignado, administrado y controlado por la Unidad de Informática, a fin de garantizar su integridad.

Toda asignación de recursos informáticos del IMARPE, al personal que no tiene relación laboral en la organización, deberá estar debidamente autorizada por la Jefatura de la correspondiente Unidad Operativa.

Responsabilidad

Es responsabilidad de la Unidad de Informática, en coordinación con las jefaturas de las Unidades operativas, administrar, asignar y controlar todo recurso informático que exista en la organización, proponer normas y/o procedimientos que regulen y de establecer controles son las herramientas necesarias que garanticen su cumplimiento.

Es responsabilidad de todo el personal que labore en el IMARPE, el custodiar los recursos informáticos que se le asigne, el velar por el cumplimiento de esta política y las normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Unidad de Informática, sobre cualquier evento que ponga en riesgo los recursos informáticos que existan en la organización y del que tenga conocimiento.

4.3.2 *Restricciones de uso de los Recursos Informáticos*

Objetivo

El objetivo de esta política es establecer las restricciones de uso de los recursos informáticos que existan en la organización, a fin de evitar usos indebidos o eventos que pongan en riesgo dichos recursos.

Alcance

De acuerdo con la definición de recursos informáticos, el alcance de esta política es todo medio que tenga relación con el almacenar, procesar o acceder a la información, que sea de propiedad o estén en alquiler en la organización.

Política

El personal que labora en el IMARPE, bajo cualquier régimen o modalidad está prohibido de emplear los recursos informáticos existentes en la organización para fines de negocio o de carácter personal que sean ajenos a las funciones del IMARPE. Por tal motivo la Alta Dirección o a quien esta delegue, puede con justificación, revisar, monitorear o registrar cualquier recurso informático.

Toda utilización, ingreso o interferencia indebida sobre recursos informáticos existentes en la organización será considerado "Delitos Informáticos", de acuerdo a los artículos 207°- A, 207°- B y 207°- C del Código Penal.

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien esta delegue, velar por el cumplimiento de esta política, dar normas y/o procedimientos que la regulen y establecer controles con las herramientas necesarias que le permitan verificar el empleo de los recursos informáticos en funciones propias de la organización.

Es responsabilidad de todo el personal que labore en el IMARPE, el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Alta Dirección o a quien delegue, de todo recurso informático en el que se realicen labores ajenas a las funciones de la organización del que tenga conocimiento.

4.4 Políticas sobre Seguridad Física

Estas políticas buscan proteger los recursos informáticos de riesgos físicos que afecten su correcto funcionamiento. Esta protección está enfocada a prevenir amenazas causadas por lugares inadecuados para su funcionamiento; así como la protección física de los mismos.

4.4.1 Seguridad de las instalaciones donde se ubican los recursos informáticos

Objetivo
El objetivo de esta política es definir las condiciones de seguridad de los lugares en donde se instalen los recursos informáticos.

Alcance
Comprende a los lugares donde se instalen recursos informáticos y al personal encargado de las instalaciones.

Política
Todo lugar donde se instalen o se almacenen recursos informáticos, debe contar con las medidas de seguridad necesarias y cumplir con los requerimientos técnicos especificados y recomendados por el proveedor del recurso, a fin de garantizar su integridad.

Todo lugar donde se instale algún recurso informático deberá ser verificado por la Unidad de Informática. Para lo cual, antes de instalar algún recurso informático en alguna área, se deberá verificar el cumplimiento de los requerimientos necesarios del lugar, tales como: ubicación, condiciones ambientales, suministros de energía, pozos a tierra, elementos de comunicación, requerimientos técnicos especificados por el proveedor del recurso, mantenimiento adecuado (limpieza y orden) y seguridad contra acceso físico, inundaciones e incendios.

Toda instalación de los recursos informáticos es función exclusiva de la Unidad de Informática. Por tal motivo está prohibida la instalación de equipos informáticos por personal no autorizado por dicha Unidad.

Las normas y procedimientos que regulen esta política deben estar concordantes con lo establecido por el ONGEI, según Resolución Jefatural N° 090-95-INEI sobre: "Recomendaciones técnicas para la protección física de los Equipos y medios de Procesamiento de la Información de la Administración Pública".

Responsabilidad

Es responsabilidad de Alta Dirección o a quien esta designe, el velar por el cumplimiento de esta política, dar las normas y/o procedimientos que la regulen y establecer controles con las herramientas necesarias que garanticen la seguridad física de los recursos informáticos.

Es responsabilidad de todo el personal que labore en el IMARPE bajo cualquier régimen o modalidad, el cumplir con esta política, las normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Alta Dirección o a quien delegue, sobre cualquier instalación de equipos informáticos que sea realizada por personal no autorizado y/o en lugares no autorizados.

4.4.2 *Seguridad de los recursos informáticos.*

Objetivo

El objetivo de esta política es establecer las medidas necesarias de seguridad física sobre los recursos informáticos, con relación a manipulaciones por personal no autorizado, cambio, robos totales o parciales de sus partes o cualquier evento que ponga en riesgo su correcto funcionamiento.

Alcance

El alcance de esta política, es a todo recurso informático que sea de propiedad o esté alquilado por la organización, así como a todo personal que este encargado de su manipulación.

Política

Todo recurso informático debe contar con las medidas necesarias de seguridad física a fin de evitar riesgos contra manipulaciones indebidas, cambio de piezas, robos parciales o totales. Tales medidas pueden ser cerraduras contra desembalaje, seguros para computadora portátiles, estabilizadores de fluido eléctrico, cajas con llave para almacenar medios de respaldo, etc.

Todo servicio técnico a los recursos informáticos debe ser realizado únicamente por personal autorizado por la Alta Dirección o a quien esta delegue.

Toda norma y/o procedimiento que regule esta política debe de estar alineada con lo establecido por el ONGEI según Resolución Jefatural N° 090-95-INEI sobre: "Recomendaciones Técnicas para la protección física de los Equipos y medios de Procesamiento de la Información den la Administración Pública".

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien esta delegue, velar por el cumplimiento de esta política, de dar normas y/o procedimientos que regulen y establezcan controles que garanticen su cumplimiento.

Es responsabilidad de todo el personal que labore en el IMARPE, el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Alta Dirección o a quien delegue sobre cualquier evento que pueda afectar a la seguridad física o manipulación inadecuada de los recursos informáticos.

4.5 Políticas sobre Seguridad Lógica

Las políticas sobre seguridad lógica buscan *identificar, establecer, controlar y administrar* los privilegios de acceso a la información electrónica de los usuarios de acuerdo a las funciones que le ha asignado la organización, de forma tal que se garantice que toda información sea accedida y modificada por personal autorizado.

4.5.1 Identificación de recursos informáticos

Objetivo
El objetivo de esta política es identificar en forma electrónica los componentes de la red informática que participan en el intercambio de información, con la finalidad de garantizar el correcto tráfico de la información en la red informática.

Alcance
El alcance de esta política es para todo recurso informático que participe en el intercambio de información en la red informática, tales como servidores, computadoras, equipos de comunicación (concentradores, switch, modem centrales telefónicas, etc.) impresoras, etc.

Política
Todo recurso informático que participe en forma directa en el intercambio de información de la red debe tener una identificación o dirección electrónica única, con la finalidad de garantizar el correcto tráfico de la información en la red.

Toda identificación de los recursos informáticos que estén relacionados con el intercambio de información en la red, debe ser asignada, modificada y controlada por la Alta Dirección o a quien esta delegue. Por tal motivo está prohibido que personal no autorizado realice cualquier asignación o cambio de identificación de los recursos informáticos.

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien esta delegue el velar por el cumplimiento de esta política, proponer normas y/o procedimientos que la regulen

y establecer controles con las herramientas necesarias que le permitan garantizar el correcto intercambio de información entre los recursos informáticos.

Es responsabilidad de todo el personal que labore en el IMARPE, bajo cualquier régimen o modalidad, el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Debiendo informar a la Alta Dirección o a quien esta delegue, de toda modificación de la identificación de los recursos informáticos realizada por personal no autorizado.

4.5.2 Identificación de usuarios

Objetivo

El objetivo de esta política, es identificar en forma univoca a cada usuario que utilice los servicios informáticos, con la finalidad de otorgarle accesos a la información electrónica y a los recursos informáticos de la organización. Esta identificación se relaciona con los privilegios otorgados a cada usuario en función a las labores que desempeña.

Alcance

El alcance de esta política es para todo usuario que acceda a la información electrónica mediante el uso de la red, sistemas, aplicaciones y servidores, en forma interna o externa.

Política

Toda persona que labore en la organización bajo cualquier régimen o modalidad, de acuerdo a sus funciones asignadas en la organización que deberá acceder a la información electrónica, lo hará mediante un identificador de usuario (UserId).

Todo identificador de usuario deberá ser único, de carácter personal, intransferible y de uso obligatorio para los fines otorgados. Dado a que el identificador establece una relación entre las funciones asignadas al usuario y los privilegios de acceso a la información electrónica de propiedad del IMARPE.

Toda administración y control de los identificadores de usuario y de los privilegios otorgado de acceso a la información electrónica de la organización, es función de la Alta Dirección o a quien delegue.

Todo uso indebido de los identificadores de usuario o de los privilegios de acceso otorgados por la organización, son considerados "Delitos Informáticos", conforme lo establece el Decreto Legislativo N° 635, Código Penal, modificado por la Ley Nº 27309, que incorpora los delitos informáticos al Código Penal.

Toda norma y/o procedimiento que regule esta política debe de estar concordante con lo establecido por la ONGEI, según Resolución Jefatural N°076-95-INEI, sobre "Recomendaciones técnicas para la Seguridad e Integridad de la Información que se Procesa en la Administración Pública".

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien esta delegue, velar por el cumplimiento de esta política, de proponer las normas y/o procedimientos que la regulen y establecer controles con las herramientas necesarias que garanticen su cumplimiento.

Es responsabilidad de todo el personal que labora en el IMARPE, el utilizar únicamente la(s) identificación(es) de usuario que le ha(n) sido otorgado(s). Siendo de su total responsabilidad el empleo de ella(s) por terceras personas. Asimismo, es de su obligación, informar a la Alta Dirección o a quien esta delegue, de cualquier empleo indebido de identificación de usuarios, de que tenga conocimiento

4.5.3 *Autenticación de usuarios*

Objetivo
El objetivo de esta política, es definir el derecho de autenticar que el usuario es realmente la persona que argumenta ser, para lo cual el usuario ratifica su identidad suministrando una clave o contraseña que solo él conoce. Teniendo como finalidad el garantizar, que todo acceso a la información electrónica realizada mediante un identificador de usuarios, pertenece a dicho usuario.

Alcance
La autenticación del usuario, está relacionada en forma directa con la identificación del usuario, por tal motivo el alcance de esta política es para toda identificación de usuario otorgada.

Política
Todo personal de la organización, que se le haya asignado una identificación de usuario tiene derecho y la obligación de usar una contraseña personal, exclusiva y confidencial. Por tal motivo, se considera que todo acceso o alteración de información electrónica efectuada con una identificación de usuario es realizado por dicho usuario.

Toda contraseña definida por los usuarios de los servicios informáticos deberá respetar las normas establecidas para su generación. Siendo función de la Alta Dirección o a quien delegue el emitir dichas normas, las cuales deberán estar alineadas con lo establecido por la ONGEI según Resolución Jefatural N° 076-95-INEI sobre "Recomendaciones técnicas para la Seguridad e Integridad de la Información que se Procesa en la Administración Pública".

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien esta delegue establecer normas y/o procedimientos que regulen esta política, así como establecer los controles con las herramientas necesarias para garantizar la confidencialidad de las contraseñas.

Es responsabilidad de todo usuario mantener la confidencialidad de su contraseña, asimismo es de su total responsabilidad los accesos o modificaciones de información realizada con su identificación de usuario salvo que se demuestre lo contrario. También es responsabilidad del usuario el velar por el cumplimiento de esta política, de las normas y/o procedimientos que la regulen, estando obligado a informar a la Alta Dirección o a quien esta delegue de cualquier evento que afecte la confidencialidad de las contraseñas.

4.5.4 Control de accesos internos

Objetivo

El objetivo de esta política es definir la asignación de privilegios para el acceso a la información electrónica, de acuerdo a las funciones del personal que labora en el IMARPE, de igual forma, definir los accesos a recursos informáticos de la organización, con la finalidad de minimizar el riesgo por accesos no autorizados.

Alcance

Toda aplicación o sistemas administrativos y/o comerciales que utilice la organización para el cumplimiento de sus funciones, tales como sistemas para la gestión Financiera, Personal, Logística, etc.

Política

Los directores de las diversas unidades operativas del IMARPE, son los responsables de la información electrónica de los sistemas que están relacionados directamente con la gestión de sus funciones. Por tal motivo son los que establecen los privilegios de acceso a su información y autorizan la asignación de dichos privilegios al personal de la organización, de acuerdo a sus funciones.

La Alta Dirección o a quien delegue en coordinación con la Unidad de Informática, tiene la función de administrar, asignar y custodiar los privilegios de acceso a la información de la organización.

La Unidad de Informática a indicación de la Alta Dirección, es el único ente que puede autorizar y designar el empleo de técnicas y/o herramientas que sirvan para encontrar debilidades de seguridad de acceso a los servicios informáticos de la organización (hacking ético). Por tal motivo sin la autorización debida de esta instancia, está prohibido que el personal que labore en el IMARPE bajo cualquier modalidad utilice o pruebe cualquier técnica y/o herramienta que viole o busque encontrar debilidades en la seguridad de accesos a servicios informáticos desde o hacia la organización.

Todo acceso no autorizado a los servicios informáticos de la organización es considerado "Delito Informático", conforme lo establece el Decreto Legislativo N° 635 Código Penal, modificado por la Ley Nº 27309, que incorpora los delitos informáticos al Código Penal.

Responsabilidad
Es responsabilidad exclusiva de cada jefatura de las diversas dependencias del IMARPE, el definir los privilegios de acceso a la información de su propiedad y autorizar la asignación de dichos privilegios al personal de la organización.

Es responsabilidad de la Alta Dirección o a quien delegue en coordinación con la Unidad de Informática establecer normas y/o procedimientos que regulen esta política, así como de establecer los controles con las herramientas necesarias para verificar el cumplimiento de esta política de sus normas y/o procedimientos que la regulen.

Es responsabilidad de todo el personal que labore en el IMARPE el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Asimismo, es de su obligación, informar a la Alta Dirección o a quien delegue de cualquier empleo de técnicas y/o herramientas que sirvan para encontrar debilidades de seguridad de acceso a los servicios informáticos.

4.5.5. *Control de accesos externos*

Objetivo
El objetivo de esta política es minimizar el riesgo por accesos de terceras personas (intrusos) o virus que provengan de redes externas a la de la organización, mediante el empleo de herramientas de seguridad o restricciones operativas. La finalidad del control de acceso externo es garantizar la integridad de la información electrónica y los recursos informáticos.

Alcance
Todo recurso que permita el acceso externo de intrusos a los servicios informáticos de la organización, así como todo recurso que permita evitarlo.

Políticas
La Alta Dirección o a quien delegue, está encargada de la seguridad sobre el control de accesos externos a los servicios informáticos, por lo cual es la única que puede autorizar, instalar y configurar los equipos que tengan este privilegio.

Todo acceso no autorizado a los servicios informáticos de la organización, es considerado "Delito Informático", de acuerdo al Decreto Legislativo N° 635 Código Penal, modificado por la Ley Nº 27309, que incorpora los delitos informáticos.

Responsabilidad
Es responsabilidad de la Alta Dirección o a quien delegue establecer normas y/o procedimientos que regulen esta política, así como de establecer los controles con las herramientas necesarias para el cumplimiento de esta política y de sus normas y/o procedimientos que la regulen.

Es responsabilidad de todo el personal que labore en el IMARPE, el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen.

Asimismo, es de su obligación, informar a la Alta Dirección o a quien delegue de cualquier evento que afecte la seguridad sobre el control de accesos externos a los servicios informáticos de la organización, del que tenga conocimiento.

4.6 Políticas sobre Administración de Recursos

Las políticas sobre la administración de los recursos informáticos, buscan evitar posibles riegos que afecten la operación de los sistemas informáticos, a causa de manipulaciones indebidas o por desconocimiento.

4.6.1 Administración de hardware

Objetivo

El objetivo de esta política, es dar lineamientos para la administración del hardware o equipos informáticos, con la finalidad de proteger su integridad y garantizar su funcionalidad.

Alcance

Comprende a todos los equipos informáticos, a toda dependencia o personal de la organización que tenga responsabilidad sobre ellos o que de alguna forma tenga relación directa o indirecta.

Política

La Alta Dirección o a quien esta delegue, en coordinación con la Unidad de Logística e Infraestructura, es el ente encargado de administrar los equipos informáticos de propiedad o en alquiler de la organización, para lo cual debe realizar actividades como el registro, traslado, instalación, asignación, mantenimiento, configuración y custodia de los equipos informáticos de propiedad de la organización.

Está prohibido que personal no autorizado por la Alta Dirección o a quien delegue, realice alguna actividad de traslado o instalación o mantenimiento o configuración de equipos informáticos, siendo excepciones a esta prohibición el traslado de los equipos portátiles y la custodia de equipos informáticos que estén asignados a sus usuarios.

Responsabilidad

Es responsabilidad de la Unidad de Logística e Infraestructura, en coordinación con la Unidad de Informática, la administración del equipo informático de la Institución, asimismo participar de todo proceso de adquisición, alquiler o contrato de servicios relacionados a la misma, para lo cual se debe proponer normas y/o procedimientos que regulan y establecen controles que permitan verificar el cumplimiento de esta política.

Es responsabilidad del área de Logística e Infraestructura, informar a la Alta Dirección o a quien delegue, sobre todo proceso de adquisición, alquiler, recepción, evaluación de proveedores de equipos informáticos y de servicios

contratados que tengan relación directa o indirecta con el hardware de la organización.

Es responsabilidad de todo el personal del IMARPE, cumplir con esta política y sus normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Alta Dirección o a quien delegue cualquier evento que afecte la administración de los recursos informáticos de la organización que sean de su conocimiento.

4.6.2 *Administración de software*

Objetivo

El objetivo de esta política, es dar lineamientos para la correcta administración del software, respetando los derechos de autor y propiedad intelectual, con la finalidad de proteger su integridad y garantizar su funcionalidad.

Alcance

Comprende a todo software desarrollado o licenciado en uso por la organización, así como a todas las áreas o personal de la organización que tengan responsabilidad sobre ellos.

Política

La Unidad de Informática, es el ente encargado de la administración de software, para lo cual realiza acciones, de registro, instalación, actualización y configuración del mismo en los equipos informáticos de la organización, respetando los derechos de autor, el número de licencia y la propiedad intelectual del software.

Está prohibido que personal no autorizado por la Unidad de Informática, realice alguna actividad de instalación o actualización o configuración de software, en los equipos informáticos de la organización. En la categoría de software no autorizado por la organización, se incluyen programas tales como: juegos, reproductores de música, protectores de pantalla, aplicativos particulares, aplicativos recibidos por la red o a través de Internet, aplicativos entregados en calidad de prueba (aplicativos en demostración o autorizaciones por un lapso o número de procesos), empaquetadores, etc.

La Unidad de Informática, también está encargada de aprobar los requerimientos, la evaluación de proveedores, la recepción y los servicios, que estén relacionados en forma directa o indirectamente con el software de la organización.

Responsabilidad

Es responsabilidad de la Unidad de Informática, la administración del software de la organización y participar de todo proceso de adquisición o alquiler o contrato de servicios relacionados al software del IMARPE, para lo cual debe emitir normas y/o procedimientos que regulen esta política y establecer controles que le permitan verificar su cumplimiento.

Es responsabilidad de la Oficina de Administración mediante la instancia pertinente, el informar a la Unidad de Informática, sobre todo proceso de adquisición, alquiler, recepción, evaluación de proveedores de software y de servicios contratados que tengan relación directa o indirecta con el software de la organización.

Es responsabilidad de todo usuario, cumplir con esta política, normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Unidad de Informática cualquier evento que afecte la administración del software de la organización, del que tenga conocimiento.

4.6.3 Administración de ambiente de producción

Objetivo

El objetivo de esta política, es aumentar la confiabilidad de los procesos ejecutados en el ambiente de producción, a fin de garantizar la calidad y continuidad del servicio.

Alcance

Comprende a todo recurso centralizado, utilizado para procesos ejecutados en ambiente de producción.

Política

La Unidad de Informática, es el ente organizacional encargado del ambiente de producción, para lo cual debe establecer actividades que garanticen su integridad, funcionamiento y servicio a la organización. Estas actividades están relacionadas con la administración y custodia de los recursos centralizados, tales como: administración de procesos de redes, de correo electrónico, de pases a producción de desarrollos y cambios en los sistemas, planes de respaldo, planes de recuperación y otras actividades asignadas de acuerdo al manual de organización y funciones.

Está prohibido, que personal no autorizado por la Unidad de Informática, realice alguna actividad de operación de los recursos del ambiente de producción.

Responsabilidad

Es responsabilidad de la Unidad de Informática, establecer normas y/o procedimientos que regulen esta política, así como de establecer los controles con las herramientas necesarias para el cumplimiento de esta política y de sus normas y/o procedimientos que la regulen.

Es responsabilidad de todo usuario cumplir con esta política y sus normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Unidad de Informática cualquier evento que afecte la administración del ambiente de producción.

4.6.4 Administración del correo electrónico

Objetivo

El objetivo de esta política es permitir una rápida y eficiente comunicación, basada en la utilización apropiada del servicio de correo electrónico y en propósitos relacionados con las funciones de la organización.

Alcance

Comprende a todo personal que labore en la organización bajo cualquier modalidad, que tenga cuenta de correo electrónico de la organización.

Política

La Unidad de Informática, es el órgano encargado de la administración de correo electrónico, para lo cual debe asegurar su operación continua, mantener actualizadas las cuentas, tomar medidas de seguridad contra virus y controlar el uso debido del correo por parte de los usuarios.

El IMARPE considera los correos electrónicos como información electrónica de su propiedad y que son considerados documentos oficiales para todo uso. Por tal motivo se prohíbe a todo el personal que labora en la organización bajo cualquier régimen o modalidad: el uso de cuentas de correo que no han sido otorgados, el empleo del correo para uso personal o de negocios ajenos a sus funciones, el uso de lenguaje obsceno y abusivo.

Responsabilidad

Es responsabilidad de la Unidad de Informática, administrar el correo electrónico, mediante normas y/o procedimientos que regule esta política y establecer controles con las herramientas necesarias que permitan verificar el cumplimiento de la misma.

Es responsabilidad de todo usuario cumplir con esta política y sus normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Unidad de Informática cualquier evento que afecte la administración del correo electrónico del que tenga conocimiento.

4.6.5 Administración de copia de respaldo

Objetivo

El objetivo de esta política es salvaguardar la integridad de los datos y software en general, mediante el empleo de copias de respaldo, que permitan garantizar la continuidad de las operaciones informáticas ante la eventual presencia de fallas o contingencias.

Alcance

Toda información sensible y necesaria para la continuidad de las operaciones informáticas. Esta información sensible está constituida por la información electrónica de propiedad del IMARPE y de los recursos de software que incluye a: software en general, sistemas operativos, sistemas, aplicaciones, correos y otros.

Política

La Unidad de Informática, es el órgano encargado de la administración de las copias de respaldo, concerniente a la información sensible de la organización y que residan en recursos compartidos de la red. Para el desarrollo de esta función debe realizar estudios sobre la información sensible, tales como: identificación, que tan crítico resulta para la organización, que tanto cambia en el tiempo, volumen de información y otros. Con estas actividades determina la importancia de la información, la periodicidad, tiempo de retención y cantidad de las copias de respaldo.

La Unidad de Informática, debe verificar que las copias de respaldo cumplan su cometido, para lo cual debe realizar pruebas de recuperación de la información sensible, a fin de garantizar que los procesos y los medios de respaldo funcional correctamente.

Todo personal que labore en el IMARPE, bajo cualquier régimen o modalidad no debe almacenar información sensible de la organización en los discos duros de las computadoras personales o portátiles, porque de ocurrir una falla del disco o el robo del equipo significaría pérdidas para la organización.

Toda norma y/o procedimiento que regule esta política debe de estar alineada con lo establecido por el ONGEI según Resolución Jefatural N° 0340-95-INEI sobre "Recomendaciones técnicas para el almacenamiento y Respaldo de la Información que se Procesan en las Entidades del Estado".

Responsabilidad

Es responsabilidad de la Unidad de Informática, administrar las copias de respaldo, buscando minimizar los riesgos ante la presencia de una contingencia, para lo cual debe elaborar normas y/o procedimientos que regulan esta política y establecer controles con las herramientas necesarias que le permitan verificar el cumplimiento de esta política y sus normas y/o procedimientos.

Es responsabilidad de todo usuario el velar por el cumplimiento de esta política y de las normas y/o procedimientos que la regulen. Asimismo, está obligado a comunicar a la Unidad de Informática cualquier información sensible que se encuentre en sus computadoras, a fin de establecer alguna forma de salvaguardar dicha información y evitar perdida de información en la organización ante alguna contingencia.

4.6.6 *Administración de recuperación de contingencias*

Objetivo

El objetivo de esta política, es establecer medidas necesarias que permitan responder eficazmente ante cualquier interrupción de los servicios informáticos. Estas medidas deben responder a un análisis de los posibles riegos a los cuales pueden estar expuestos los recursos informáticos de la organización.

Alcance

Comprende a todos los componentes que conforman la plataforma informática de la organización, inclusive a equipos de respaldo al servicio informático. En cuanto al recurso humano involucra dependiendo de la contingencia a todo el personal de la organización.

Política

La Unidad de Informática es el órgano encargado de elaborar y mantener actualizado el Plan de Contingencia que responda eficazmente a las necesidades de continuidad del servicio informático. Este plan debe considerar: Plan de emergencia que tiene como objetivo el contener el daño causado por un desastre, Plan de Respaldo que tiene como objetivo de mantener los servicios críticos de la operación y el Plan de Recuperación tiene el objetivo de restaurar temporal o permanente la capacidad de los servicios informáticos. Estos planes para garantizar su efectividad deben ser probados.

Responsabilidad

Es responsabilidad de la Unidad de Informática en coordinación con la jefatura usuaria, la administración de recuperación ante la presencia de una contingencia, para lo cual debe elaborar los planes debidos, así como normas y procedimientos que regulen esta política y establecer controles con las herramientas necesarias que le permitan verificar el cumplimiento de esta política y sus normas y/o procedimientos.

4.6.7 *Administración de desarrollo de proyectos informáticos.*

Objetivo

El objetivo de esta política es registrar y controlar los desarrollos de proyectos informáticos, con la finalidad de reducir el riesgo por eventos imprevistos, de tal forma que el proyecto cumpla con las exigencias con que fue concebido.

Alcance

Comprende todo desarrollo de proyectos informáticos realizados por el IMARPE y a todo desarrollo realizado por terceros que brindan el servicio a la organización.

Política

La Unidad de Informática es el órgano encargado de administrar todos los desarrollos de proyectos informáticos de la organización, por lo cual debe registrar desde el requerimiento inicial del usuario hasta el descarte o conclusión de los proyectos.

La Unidad de Informática debe contar con herramientas necesarias para el control de los proyectos y con una metodología para sus propios proyectos y que sirva de base para el desarrollo por servicios de terceros o proveedores que dan servicio a la organización.

Responsabilidad
Es responsabilidad de la Unidad de Informática, velar por el cumplimiento de esta política, dar las normas y/o procedimientos que la regulen y de establecer controles.

4.6.8 *Administración del mantenimiento de aplicaciones.*

Objetivo
El objetivo de esta política es registrar y controlar los mantenimientos de las aplicaciones, con la finalidad de reducir riesgo por eventos imprevistos, de tal forma que el mantenimiento cumpla con las necesidades de los usuarios.

Alcance
Comprende todo mantenimiento a las aplicaciones informáticas que se realizan para el IMARPE, inclusive mantenimientos realizados por terceros para el IMARPE.

Política
La Unidad de Informática es el órgano encargado de administrar todos los mantenimientos a las aplicaciones solicitadas por los usuarios, debiendo empezar desde el requerimiento inicial del usuario hasta el descarte o conclusión del mantenimiento.

La Unidad de Informática debe contar con herramientas necesarias para el control de los mantenimientos de aplicaciones.

Responsabilidad
Es responsabilidad de la Unidad de Informática, velar por el cumplimiento de esta política, dar las normas y/o procedimientos que la regulen y de establecer controles que le permitan verificar el cumplimiento de esta política.

MHCH/RMP/CBR
Julio 2012