INSTITUTO DEL MAR DEL PERU

RESOLUCIÓN DE DIRECCIÓN EJECUTIVA CIENTÍFICA
Nº 159 -2018- IMARPE/DEC

Callao, 30 de julio de 2018

VISTOS:

La Resolución de Dirección Ejecutiva Científica N° 155-2017-IMARPE/DEC de fecha 24 de julio de 2017; el Informe N° 002-2018 de fecha 07 de junio de 2018, del Comité de Gestión de Seguridad de la Información; el Proveído S.G. N° 1433 de fecha 20 de junio de 2018, de la Secretaría General y el Acuerdo de Consejo Directivo N° 063-2018-CD/E de fecha 24 de julio de 2018.

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM de fecha 22 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 del Sistema Nacional de Informática. Precisando que la citada Norma Técnica Peruana, se aplicará a partir del día siguiente de la publicación de la citada Resolución Ministerial, debiendo las Entidades antes mencionadas considerar las actividades necesarias en sus respectivos Planes Operativos Informáticos (POI), para su implantación;

Que, a través del Decreto Supremo N° 081-2013-PCM se aprobó la Política Nacional de Gobierno Electrónico 2013-2017, siendo de alcance nacional y cumplimiento obligatorio por parte de todas las entidades de la Administración Pública a nivel del gobierno nacional, gobiernos regionales y gobiernos locales, las mismas que se implementan en el ámbito de sus funciones y competencias;

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura del Gobierno Electrónico, por considerar a la seguridad de la información, como un

R. GUEVARA
C. CAÑOTE
W. HUERTA
C. MORENO
J. CASTILLO

componente crucial para dicho objetivo; precisando que es responsabilidad del titular de la Entidad la implantación de la referida norma;

Que, a través del Proveído S.G. N° 1433 de fecha 20 de junio de 2018, la Secretaría General remite la propuesta de la Política de Seguridad de la Información elaborada por el Comité de Gestión de Seguridad de la Información conformado mediante Resolución de Dirección Ejecutiva Científica N° 155-2017-IMARPE/DEC de fecha 24 de julio de 2017, y alcanzado mediante N° 002-2018 de fecha 07 de junio de 2018; dicha política tiene por objeto establecer el marco general de gestión para proteger de manera apropiada la información de la entidad con la finalidad de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad de la información y el fortalecimiento de una cultura de seguridad de la información de la entidad;

Que, se debe precisar que la implementación de la referida Política de Seguridad de la Información, es de interés institucional, toda vez que a través de la misma se establecerá, implementará, mantendrá y mejorará continuamente un Sistema de Gestión de Seguridad de la Información, la que guardará armonía con las necesidades y objetivos del IMARPE, con lo que se preservará la confidencialidad, integridad y disponibilidad de la información institucional aplicando un proceso de gestión de riesgo lo cual proporciona confianza organizacional, en el sentido en que los riesgos se manejen adecuadamente;

R. GUEVARA

Que, teniendo en cuenta lo expuesto precedentemente la Oficina General de Asesoría Jurídica mediante Informe N° 248-2018-IMARPE/OGAJ de fecha 02 de julio de 2018, es de la opinión que resulta jurídicamente viable aprobar el documento de gestión denominado: "Política de Seguridad de la Información del Instituto del Mar del Perú", a través del cual se establecen medidas tecnológicas, física y legales necesarias para proteger la información institucional contra el acceso no autorizado, divulgación, aprovechamiento, intromisión de sistemas o mal uso que se pueda producir en forma intencional o accidental, con la finalidad de mitigar las amenazas y el riesgo de exposición de información sensible, asegurando la confidencialidad, integridad, disponibilidad y confiabilidad de la información fortaleciendo la cultura de seguridad en el entidad;

G. CAÑOTE

W. HUERTA

Que, el Consejo Directivo del IMARPE, en su Segunda Sesión Extraordinaria celebrada el 24 de julio de 2018, mediante Acuerdo N° 063-2018-CD/O, aprobó la "Política de Seguridad de la Información del Instituto del Mar del Perú";

C. MORENO

Que, el literal o) del artículo 15° del Reglamento de Organización y Funciones del IMARPE aprobado por Resolución Ministerial N° 345-2012-PRODUCE señala que son funciones de la Dirección Ejecutiva Científica expedir resoluciones que le correspondan en cumplimiento de los acuerdos, de las funciones delegadas por el Consejo Directivo y de otros dispositivos que por norma legal se establezcan;

J. CASTILLO

De acuerdo a las atribuciones conferidas por el Reglamento de Organización y Funciones – ROF del IMARPE, aprobado mediante Resolución Ministerial N° 345-2012-

INSTITUTO DEL MAR DEL PERU

PRODUCE, la Resolución Ministerial N° 246-2007-PCM, Aprueban 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 y la Resolución Ministerial N° 004-2016-PCM, Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Con las visaciones de la Secretaría General, las Oficinas Generales de Planeamiento y Presupuesto y de Asesoría Jurídica;

SE RESUELVE:

Artículo Primero.- Formalizar la aprobación del documento de gestión institucional denominado: "Política de Seguridad de la Información del Instituto del Mar del Perú", cuyo texto forma parte integrante de la presente Resolución.

Artículo Segundo.- Disponer el cumplimiento de la presente Resolución a los órganos involucrados a efectos de tener en cuenta las disposiciones indicadas en la "Política de Seguridad de la Información del Instituto del Mar del Perú".

Regístrese, comuníquese y publíquese

INSTITUTO DEL MAR DEL PERÚ
IMARPE

.....
Blgo. Renato C. Guevara Carrasco
Director Ejecutivo Científico

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Administración
W. HUERTA

INSTITUTO DEL MAR DEL PERU Secretaría General
G. CAÑOTE

Política de Seguridad de la Información

Instituto del Mar del Perú

M. ALMENDOR R.

W. HUERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

PRESENTACION

I. OBJETIVO

II. ALCANCE

III. BASE LEGAL

IV. DISPOSICIONES GENERALES

- **4.1 Propiedad de la Información**
- **4.2 Liderazgo y Compromiso**
- **4.3 Documento fuente del Sistema de Gestión de Seguridad de la Información(SGGI)**

V. LÍNEA BASE DE LA POLÍTICA

- **5.1 Responsabilidad**
- **5.2 Cumplimiento**
- **5.3 Protección de la Información**
- **5.4 Uso apropiado**
- **5.5 Acceso autorizado**
- **5.6 Disponibilidad**
- **5.7 Integridad**
- **5.8 Confidencialidad**
- **5.9 Colaboración**
- **5.10 Administración de las Políticas**
- **5.11 Mejora Continua**
- **5.12 Planificación y control operacional**
- **5.13 Evaluación del Desempeño**
- **5.14 Soporte**
- **5.15 Protección de los recursos tecnológicos**
- **5.16 Autorización de usuarios**
- **5.17 divulgación no autorizada de la información**

VI. LINEAMIENTOS

- **6.1 Política de Seguridad de la Información**
- **6.2 Organización de la Seguridad de la Información**
- **6.3 Seguridad de los Recursos Humanos**
- **6.4 Gestión de Activos de Información**
- **6.5 Control de Acceso**
- **6.6 Criptografía**
- **6.7 Seguridad Física de las instalaciones**
- **6.8 Seguridad de las operaciones**
- **6.9 Respaldo de la información**
- **6.10 Seguridad de las comunicaciones**
- **6.11 Adquisición, desarrollo y mantenimiento de los sistemas**

M. ALMENGOR

W. HUERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

6.12 Relación con los proveedores
6.13 Gestión de incidentes de seguridad de la Información
6.14 Aspectos de Seguridad de la Información en la gestión de continuidad del negocio
6.15 Cumplimiento

VII. ROL Y RESPONSABILIDADES

7.1 Director(a) Ejecutivo(a) Científico(a)
7.2 Comité de Gestión de Seguridad de la Información
7.3 Oficial de Seguridad de la Información
7.4 Responsables de Activos
7.5 Responsables de Riesgos
7.6 Personal de la entidad
7.7 Directores y/o Jefes
7.8 Área Funcional de Recursos Humanos
7.9 Coordinador del Área Funcional de Informática y Estadística
7.10 Oficina General de Asesoría Jurídica

VIII. GLOSARIO DE TERMINOS

M. ALMENGOR R.

W. HUERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

PRESENTACION

En la actualidad las organizaciones están cada vez más interconectadas y requieren compartir información interactuando en un escenario de alta conectividad, esta situación proporciona no solo innumerables oportunidades sino también genera riesgos en el manejo de la información propia por la posibilidad de obtención inadecuada de datos institucionales a través de la filtración en nuestros sistemas informáticos; por esta razón, es necesario que existan políticas de seguridad que minimicen los riesgos derivados de vulnerabilidades informáticas.

En ese sentido el IMARPE ha elaborado su Política de Seguridad de la Información tomando como referencia la Norma Internacional ISO/IEC 27001:2013, y la Resolución Ministerial N° 004-2016-PCM, en la cual se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", dirigidas a todas las entidades integrantes del Sistema Nacional de Informática, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la institución.

La Norma Técnica antes mencionada indica los criterios para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, sin embargo la adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización, la cual está influenciada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos de la organización empleados y el tamaño y estructura de la Institución; sirve para preservar la confidencialidad, integridad y disponibilidad de la información Institucional aplicando un proceso de gestión de riesgos lo cual proporciona confianza organizacional en el sentido en que los riesgos se manejan adecuadamente.

Este documento institucional integra los lineamientos de las políticas de seguridad de la información de las normas antes indicadas e identifican las responsabilidades internas de nuestros funcionarios, estableciendo objetivos orientados a una protección adecuada y consistente de los activos de información del Instituto del Mar del Perú.

Estas políticas de seguridad de la información que se presentan por sí solas no constituyen garantía para la seguridad de la información, sino que dependen fundamentalmente del compromiso y participación del personal para garantizar su cumplimiento.

Es de necesidad del Instituto del Mar del Perú conducir un Sistema de Gestión de Seguridad de la Información, con el fin de establecer, operar, supervisar, revisar, mantener y mejorar la seguridad de la información en concordancia con las

M. ALMENDOR R.

W. HUERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

recomendaciones contenidas en las normas técnicas peruanas, estándares internacionales y mejores prácticas del SGSI y teniendo en consideración las normas establecidas en la Ley de Transparencia y Acceso a la información Pública.

I. OBJETIVO

Establecer las medidas tecnológicas, físicas y legales necesarias para proteger la información institucional contra el acceso no autorizado, divulgación, aprovechamiento, intromisión de sistemas o mal uso que se pueda producir en forma intencional o accidental con la finalidad de mitigar las amenazas y el riesgo de exposición de información sensible, asegurando la confidencialidad, integridad, disponibilidad y confiabilidad de la información fortaleciendo la cultura de seguridad en la entidad.

II. ALCANCE

El presente documento es de aplicación a:

- Personal del Instituto del Mar del Perú – IMARPE, sin distingo de régimen laboral o contractual o de nivel jerárquico.
- Personas naturales o jurídicas que prestan servicios en general y/o que tengan acceso a la información de propiedad del IMARPE.

III. BASE LEGAL

a) Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 13 julio de 2002, modificada por Ley N° 27927
b) Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento aprobado Decreto Supremo Nº 003-2013-JUS.
c) Ley N° 27269 – Ley de Firmas y Certificados Digitales y su reglamento
d) Ley N° 27815 – Ley del Código de Ética de la Función Pública.
e) Ley N° 30096 – Ley de Delitos Informáticos y sus modificatorias efectuadas por Ley N° 30171
f) Resolución Directoral N° 060-2014-JUS-DGPDP que Aprueba Directiva Nº 001-2014-JUS-DGPDP que regula las disposiciones sobre la protección de datos personales.
g) Resolución Ministerial N° 246-2007-PCM del 22 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. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
h) Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática
i) Resolución Directoral N° 155-2017-IMARPE/DEC, que aprueba la conformación del equipo de trabajo denominado "Comité de Gestión de Seguridad de la Información – SGSI" en el Instituto del Mar del Perú.
j) Resolución de Contraloría General N° 320-2006-CG del 30 de octubre de 2006, que aprueba las Normas de Control Interno de aplicación en las entidades del estado.

M. ALMENGOR R.

W. ROBERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

k) Resolución Jefatural N° 386-2002-INEI, Aprueban Directiva "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública"

l) Reglamento interno de trabajo del Instituto del Mar del Perú

IV. DISPOSICIONES GENERALES

Los Lineamientos considerados se encuentran enmarcados de acuerdo a lo dispuesto en la Resolución Ministerial N° 004-2016-PCM, mediante la cual se aprueba el uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", cuyo control deberá ser implementado de acuerdo con las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información".

Siendo la información y los sistemas de información activos importantes para el Instituto del Mar del Perú, La seguridad de la información, en su concepción moderna y técnica, busca fundamentalmente, alcanzar los objetivos de confidencialidad, integridad, disponibilidad y confiabilidad de la información en general.

M. ALMENGOR R.

Mediante la presente Política difundimos los objetivos de seguridad de la información que se esperan alcanzar, los cuales conseguiremos mediante la aplicación de controles de seguridad que permitan gestionar un nivel de riesgo aceptable, determinar y minimizar vulnerabilidades, garantizar la continuidad de los servicios, asegurar el cumplimiento de las obligaciones establecidas en las normas legales vigentes y los requisitos de seguridad destinados a impedir infracciones y violaciones que afecten la seguridad de la información en nuestra Institución.

W. HUERTA

4.1 Propiedad de la Información

Toda la información generada y almacenada en los dispositivos de almacenamiento masivo y de respaldo del Instituto del Mar del Perú - IMARPE, pertenece a la entidad y no puede ser utilizada y/o aprovechada en beneficio personal o de terceros.

J. CASTILLO

La información que es soportada por la infraestructura de tecnología informática del IMARPE pertenece a la entidad a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable del área que genera esa información. Para el control de la información se asignarán responsables quienes deben asegurar proporcionar el acceso a la información que genere su área, con la finalidad de promover un adecuado ambiente de control y separación de funciones.

C. MORENO

4.2 Liderazgo y Compromiso

La Alta Dirección ejecutará las siguientes acciones concretas que garanticen el compromiso Institucional con relación al sistema de gestión de seguridad de la información.

G. CAÑOTE

4.2.1 Verificar que la política de seguridad de la información y los objetivos de seguridad de la información esten alineados y sean compatibles con la dirección estratégica de la organización.

4.2.2 Asegurar que el sistema de gestión de seguridad de la información este incluido en el Mapa de procesos de la organización.

4.2.3 Asignar los recursos económicos necesarios para el adecuado funcionamiento del sistema de gestión de seguridad de la información.

4.2.4 Resaltar la importancia de la seguridad de la información para la Organización.

4.3 Documento fuente del Sistema de Gestión de Seguridad de la Información(SGGI)

Toda Política de Seguridad de la Información debe incluir registros de las decisiones de las unidades orgánicas de la entidad, 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 (SGGI) deberá estar sustentada en lo siguiente:

- Manual del SGSI
- Manual de Funciones y Responsabilidades del SGSI
- Metodología de Análisis de Riesgo
- Inventario de Activos
- Matriz de Riesgos
- Plan de tratamiento del riesgo.
- Declaración de Aplicabilidad
- Políticas del SGSI
- Metodología de Medición del SGSI
- Métricas para el SGSI
- Procedimientos documentados necesarios en la organización para garantizar la planificación efectiva, funcionamiento y control de sus procesos de seguridad de la información

M. ALMENGOR R.

W. HUERTA

J. CASTILLO

V. LÍNEA BASE DE LA POLÍTICA

Los siguientes principios constituyen los fundamentos sobre los que se basará cualquier acción en materia de la seguridad de la información:

5.1 Responsabilidad

Es responsabilidad del Coordinador del Área Funcional de Informática y Estadística hacer uso de la Política de Seguridad de la Información, como parte de sus herramientas de gestión y definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

C. MORENO

Es responsabilidad de los funcionarios del IMARPE realizar las acciones necesarias para una adecuada protección de la información Institucional de las amenazas o vulnerabilidades que pudieran presentarse con la finalidad de minimizar los riesgos.

G. CAÑOTE

5.2 Cumplimiento

La Política de Seguridad de la Información debe ser de conocimiento y obligatorio cumplimiento para todo el personal del IMARPE, siendo considerada como una condición en los contratos de personal. Queda implícito que, si los trabajadores, consultores, contratistas, terceras partes violan o incumplen estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

5.3 Protección de la Información

Los activos de información deben ser protegidos con el nivel de seguridad adecuada, guardando proporción entre el valor y el riesgo de pérdida para la entidad; la protección debe enfocarse en la confidencialidad, integridad y disponibilidad de estos activos.

5.4 Uso apropiado

Los activos de información disponibles en la entidad deben ser utilizados en forma adecuada, eficiente, racional y exclusivamente para el desarrollo de las actividades institucionales.

5.5 Acceso autorizado

Todos los usuarios de los sistemas de información de la entidad deben ser identificados individualmente y sus permisos de acceso deben concederse en forma específica de acuerdo a su rol y nivel de responsabilidades. Los métodos de acceso a los usuarios deben contener obligatoriamente un proceso de autenticación, autorización y auditoria.

5.6 Disponibilidad

Los activos de información deben estar disponibles para su uso por parte de los usuarios autorizados toda vez que lo requieran, garantizando el acceso oportuno a la información y a los recursos relacionados con la misma.

5.7 Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos. Las medidas de validación definidas deben permitir detectar la modificación, adulteración o eliminación de los activos de información.

5.8 Confidencialidad

Los activos de información deben mantenerse protegidos para asegurar la confidencialidad y privacidad asegurando que, solo los que estén autorizados pueden acceder a la información. Se debe considerar que en todo momento deben mantenerse esquemas de seguridad que prevengan la divulgación no autorizada de información.

M. ALMENGOR R.

W. HUERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

5.9 Colaboración

La conservación de la seguridad de la información es un esfuerzo de equipo en el que participan los trabajadores de la entidad y terceros que tengan acceso a los activos de información del Instituto, motivo por el cual estas personas deben desempeñar un papel activo en el cumplimiento y divulgación de las políticas y normas vigentes de seguridad de la información.

5.10 Administración de las Políticas

La Política Institucional de Seguridad de la Información y sus modificatorias serán propuestas por el Comité de Seguridad de Información al Director Ejecutivo Científico para su aprobación; estas políticas deberán ser revisadas como mínimo una vez al año o cuando la modificación de una norma lo amerite.

5.11 Mejora Continua

La organización debe efectuar la revisión periódica de sus procesos para mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la información.

5.12 Planificación y Control Operacional

5.12.1 Planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones para asegurar que el sistema de gestión de seguridad de la información logre los resultados esperados, prevenir o reducir efectos indeseados y lograr la mejora continua.

5.12.2 Mantener información documentada para asegurar que los procesos se han llevado a cabo tal como fueron planificados.

5.12.3 Controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario.

5.12.4 Asegurar que los procesos tercerizados son determinados y controlados.

5.13 Evaluación del Desempeño

Se evaluará el desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información, debiendo determinar

5.13.1 Qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información.

5.13.2 Los métodos para el monitoreo, medición, análisis y evaluación, que permitan asegurar la validez de los resultados.

IMARPE – Área Funcional de Informática y Estadística – M. ALMENGOR R.

IMARPE – Oficina General de Planeamiento y Presupuesto – W. HUERTA

IMARPE – Oficina General de Planeamiento y Presupuesto – J. CASTILLO

IMARPE – Oficina General de Asesoría Jurídica – C. MORENO

Instituto del Mar del Perú – Secretaría General – G. CAÑOTE

5.13.3 Determinar cuándo el monitoreo y medición debe ser realizado y quién debe monitorear y medir

5.13.4 Cuándo los resultados del monitoreo deben ser analizados y evaluados y quién debe analizar y evaluar estos resultados.

5.14 Soporte

Determinar y gestionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

5.15 Protección de los recursos tecnológicos

Los recursos tecnológicos serán protegidos en proporción a su valor y al riesgo de pérdida para la Institución, los mismos que deben ser empleados exclusivamente en el desarrollo de las funciones establecidas para el personal (cualquiera sea su vínculo laboral con la Institución) asegurando que su utilización se hará en forma adecuada, con eficiencia y racionalidad.

5.16 Autorización de usuarios

Cada usuario deberá ser identificado independientemente con un permiso de acceso, asignándosele específicamente e individualmente autorizaciones básicas de operaciones de acuerdo al nivel y tipo de información que necesita para el desarrollo de sus funciones. Los métodos de acceso de usuarios deben exigir un proceso de autenticación, autorización apropiada y auditoría confiable.

M. ALMENGOR R.

5.17 divulgación no autorizada de la información

En caso de detectarse la divulgación no autorizada de información de propiedad del IMARPE, se efectuarán las investigaciones pertinentes para establecer los responsables y determinar las sanciones de ser el caso, situaciones que serán evaluadas por el Jefe inmediato del usuario involucrado y el Comité de Seguridad en concordancia con el informe emitido por el Oficial de Seguridad de la Información sobre el hecho producido y el impacto de su divulgación para la entidad.

W. HUERTA

VI. LINEAMIENTOS

Los lineamientos de las políticas generales de seguridad de la información del Instituto del Mar del Perú - Imarpe son los siguientes:

J. CASTILLO

6.1 Política de Seguridad de la Información

El Instituto del Mar del Perú (IMARPE) es un Organismo Técnico Especializado del Ministerio de la Producción, orientado a la investigación científica, así como al estudio y conocimiento del mar peruano y sus recursos, para asesorar al Estado en la toma de decisiones con respecto al uso racional de los recursos pesqueros y la conservación del ambiente marino, contribuyendo activamente con el desarrollo del país.

C. MORENO

La Política de Seguridad de la Información de la entidad tiene como objetivo establecer el compromiso Institucional en la implementación del

G. CAÑOTE

SGSI. Por lo tanto, el o la Director(a) Ejecutivo(a) Científico(a) de la entidad declara los siguientes lineamientos:

6.1.1 Establecer mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información.

6.1.2 La continua identificación, manejo y tratamiento de los riesgos de seguridad de la información que son relevantes para el IMARPE, según lo definido en la metodología de análisis de riesgos.

6.1.3 La comunicación oportuna de las políticas y procedimientos de seguridad definidos, asegurando que sean comprendidos y se encuentren disponibles para todos los interesados.

6.1.4 El fortalecimiento de los valores y el compromiso de todo el personal de velar por el cumplimiento de la presente política.

6.1.5 Asegurar el aprovisionamiento de los recursos requeridos para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI).

M. ALMENGOR R.

6.2 Organización de la Seguridad de la Información

Se debe mantener una organización interna que le permita prevenir, detectar y responder apropiadamente a eventos que pongan en riesgo la Seguridad de la Información. Para ello, es necesario que se defina en forma clara las responsabilidades del personal en relación con la Seguridad de la Información.

W. HUERTA

6.2.1 Organización Interna

Se debe establecer roles y funciones para la gestión de Seguridad de la Información, las cuales se precisan como:

- Comité de Seguridad de Información
- Oficial de Seguridad de la Información
- Propietarios de la Información
- Propietario de Riesgos
- Personal de la entidad, entre otros

J. CASTILLO

Con la finalidad de:

a. Buscar la protección de los activos de información y para la realización de procesos específicos de seguridad de la información.
b. Proponer acciones para mitigar los riesgos de seguridad de la información y la aceptación de riesgos residuales.

C. MORENO

Las personas con responsabilidades asignadas de seguridad de la información pueden delegar tareas; sin embargo, siguen siendo responsables y deben verificar que las tareas delegadas se hayan realizado correctamente.

G. CAÑOTE

6.2.2 Dispositivos móviles y Teletrabajo

a) Para el caso de los dispositivos móviles proporcionados por la entidad se debe tomar en cuenta lo siguiente:
- Se debe tener un registro de los dispositivos móviles.
- Los locales donde se haga uso de estos dispositivos móviles deben contar con la protección física adecuada.
- Se debe restringir la descarga e instalación de software.
- Se debe aplicar las políticas de controles de acceso para servicios y aplicaciones web.
- Se debe hacer uso de técnicas criptográficas para proteger la información.
- Se debe proteger contra software malicioso (Malware).
- Se debe asegurar la desactivación, eliminación o bloqueo en forma inmediata en caso de hurto o pérdida.
- Se debe realizar respaldos de seguridad de la información sensible o crítica de la entidad.
- Se debe capacitar al personal que utiliza dispositivos móviles de la entidad para concientizarlos sobre los riesgos adicionales derivados de esta forma de trabajo y los controles que se están implantando.

b) Para los casos en que la entidad permita el uso de dispositivos móviles de propiedad privada, se debe considerar lo siguiente:
- La separación del uso privado y de trabajo, incluido el uso de software para apoyar dicha separación y proteger la información de la entidad en un dispositivo privado.
- Facilitar el acceso a la información de la entidad, solo después de que los usuarios hayan firmado un acuerdo de usuario final, reconociendo los derechos de la Institución (protección física, actualización de software, etc.), renunciando a la propiedad de los datos de la institución, lo que permite la eliminación remota de los datos por parte de la entidad en caso de robo o pérdida del dispositivo o cuando ya no se encuentran autorizados a utilizar el servicio.
- Se debe tener en cuenta la legislación sobre privacidad.

c) Se debe indicar las condiciones y las restricciones para proteger la información autorizada para su acceso y/o elaborada en los sitios de teletrabajo.

d) En caso de que la entidad permita actividades de teletrabajo debe considerarse los siguientes aspectos:
- La seguridad física existente en el sitio donde se realiza el teletrabajo.

IMARPE Área Funcional de Informática y Estadística
M. ALMENGOR R.

IMARPE Oficina General de Administración
W. HUERTA

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

Instituto del Mar del Perú Secretaría General
G. CAÑOTE

- El entorno físico de teletrabajo propuesto.
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la entidad, la sensibilidad de la información a ser accesada sobre el enlace de comunicación.
- La provisión de acceso al escritorio virtual que impide el procesamiento y el almacenamiento de información sobre el equipo de propiedad privada.
- Prevenir la amenaza de acceso no autorizado a la información o a los recursos de otras personas que utilizan el alojamiento.
- Las políticas y los procedimientos para evitar conflictos relativos a los derechos de propiedad intelectual desarrollados en los equipos de propiedad privada.

6.3 Seguridad de los Recursos Humanos

A través del Área Funcional de Recursos Humanos del IMARPE se debe promover la cultura de seguridad de la información, para ello se debe considerar los siguientes puntos como acciones preventivas de tal manera que las acciones posteriores del personal no conduzcan a poner en riesgo a la confidencialidad, Integridad y disponibilidad de la información.

M. ALMENEGOR R.

6.3.1 Antes del empleo

Evaluación

La entidad debe realizar la verificación de antecedentes a todos los postulantes a un empleo o servicio en la entidad en concordancia con las leyes, regulaciones y normas éticas y en proporción a los requisitos de las actividades que realizará en la entidad, tales como:

a) Referencias personales, por ejemplo, una de actividades comerciales y una personal.
b) Comprobación (para integridad y exactitud) del currículum vitae del postulante.
c) Confirmación de las calificaciones académicas y profesionales declaradas, entre otros.

W. HUERTA

Términos y condiciones de empleo

a) Se debe precisar las funciones y responsabilidades del personal y de los proveedores, así como los de la entidad en los acuerdos contractuales precisando la política respecto a la seguridad de la información.
b) Que todo el personal que requiera acceso a información sensible debe firmar previamente un acuerdo de confidencialidad o de no-divulgación antes de otorgarle acceso a los sistemas de procesamiento de información.
c) Definir las responsabilidades y derechos legales del personal.

J. CASTILLO

C. MORENO

G. CAÑOTE

d) Definir las responsabilidades para la clasificación y gestión de la información de la entidad, determinar otros activos relacionados con la información, designar las instalaciones de procesamiento de información y los servicios de información a ser manejados por el personal.
e) Determinar las responsabilidades del personal por el manejo de información de otras organizaciones, así como las acciones Institucionales a ser tomadas si el personal incumple los requisitos de seguridad de la entidad.

6.3.2 Durante el empleo

a) Los Directores y/o Jefes de la entidad deben reiterar al personal, cumplir con la política y los procedimientos de seguridad establecidos por la entidad.
b) Todo el personal, debe recibir capacitación, concientización, entrenamiento, formación y actualizaciones periódicas en políticas y procedimientos de seguridad de la información.
c) Se debe establecer en el proceso disciplinario medidas aplicables al personal que ha cometido una falta a la seguridad de la información. Estas medidas servirán como acciones disuasivas para prevenir que el personal incumpla con las políticas y procedimientos de seguridad de la información en la entidad.

M. ALMENGOR

6.3.3 Terminación y/o Cambio de empleo

Al término de la vinculación laboral o contractual, debe asegurarse la devolución de activos asignados y el retiro de los derechos de accesos a los sistemas informáticos de la entidad.

W. HUERTA

6.4 Gestión de Activos de Información

6.4.1 Responsabilidad de los activos

La entidad debe elaborar y mantener un inventario de sus activos de información, asociados a cada proceso, el propietario, responsables y ubicación. El inventario será actualizado una vez al año o ante cualquier modificación de la información registrada o lo que suceda primero.

J. CASTILLO

La responsabilidad de uso de los activos de información recae en el responsable de su elaboración y su custodia, sean estos físicos o electrónicos, cabe señalar que así tenga la autoría de la información, no significa que tenga derechos de propiedad sobre el activo desarrollado en la Institución.

6.4.2 Clasificación de la Información

C. MORENO

a) La entidad debe clasificar la información en función a las disposiciones legales, al valor y la sensibilidad a la divulgación o modificación no autorizada.

G. CAÑOTE

b) El nivel de protección debe evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad y cualquier otro requisito para la información considerada.

c) Debe identificar la información de acuerdo con el esquema de clasificación de la información adoptado por la entidad.

6.5 Control de Acceso

Los responsables de activos de información, incluyendo el contenido de la misma, deben asegurar que estos se encuentren protegidos mediante los controles de acceso necesarios y adecuados.

6.5.1 Gestión de acceso a los usuarios

a) Establecer procedimientos para la gestión de acceso al perfil de usuario a los sistemas y servicios de la entidad.
b) Toda solicitud de acceso debe contar con la autorización del responsable del sistema o servicio.
c) Mantener el registro de todos los usuarios con derecho de acceso a los sistemas de información.
d) Todo cambio de roles o puestos de trabajo deben ser informados por el Jefe de Oficina para ser actualizados de acuerdo a su nuevo nivel de responsabilidad, del mismo modo gestionar la eliminación o bloqueo inmediato de los usuarios que terminen su relación laboral con la entidad.
e) La revisión de los accesos de los usuarios debe ser periódica en coordinación con los responsables de los sistemas de información.

M. ALMENGOR R.

W. HUERTA

6.5.2 Control de acceso al sistema y a las aplicaciones

a) Todo acceso a los sistemas de información y a las funciones del sistema de aplicaciones deben ser restringidas.
b) Todos los derechos de acceso aplicados a sistemas de información deben ser controlados, así como los datos y aplicaciones que son accedidos por el usuario.
c) Los accesos lógicos y físicos deben ser controlados a fin de minimizar los riesgos de aplicaciones y/o sistemas de información; por representar activos sensibles de la entidad.
d) El uso de Internet debe estar orientado exclusivamente a la ejecución de las actividades de la organización y puede ser utilizado por el colaborador para realizar las funciones establecidas para su cargo. Queda prohibido al personal descargar programas que realicen conexiones automáticas, del mismo modo la descarga de música y videos no es una práctica permitida.

J. CASTILLO

C. MORENO

G. CAÑOTE

b) El nivel de protección debe evaluarse mediante el análisis de la confidencialidad, integridad y disponibilidad y cualquier otro requisito para la información considerada.

c) Debe identificar la información de acuerdo con el esquema de clasificación de la información adoptado por la entidad.

6.5 Control de Acceso

Los responsables de activos de información, incluyendo el contenido de la misma, deben asegurar que estos se encuentren protegidos mediante los controles de acceso necesarios y adecuados.

6.5.1 Gestión de acceso a los usuarios

a) Establecer procedimientos para la gestión de acceso al perfil de usuario a los sistemas y servicios de la entidad.
b) Toda solicitud de acceso debe contar con la autorización del responsable del sistema o servicio.
c) Mantener el registro de todos los usuarios con derecho de acceso a los sistemas de información.
d) Todo cambio de roles o puestos de trabajo deben ser informados por el Jefe de Oficina para ser actualizados de acuerdo a su nuevo nivel de responsabilidad, del mismo modo gestionar la eliminación o bloqueo inmediato de los usuarios que terminen su relación laboral con la entidad.
e) La revisión de los accesos de los usuarios debe ser periódica en coordinación con los responsables de los sistemas de información.

IMARPE
M. ALMENGOR R.

IMARPE
W. HUERTA

6.5.2 Control de acceso al sistema y a las aplicaciones

a) Todo acceso a los sistemas de información y a las funciones del sistema de aplicaciones deben ser restringidas.
b) Todos los derechos de acceso aplicados a sistemas de información deben ser controlados, así como los datos y aplicaciones que son accedidos por el usuario.
c) Los accesos lógicos y físicos deben ser controlados ~~afín~~ de minimizar los riesgos de aplicaciones y/o sistemas de información; por representar activos sensibles de la entidad.
d) El uso de Internet debe estar orientado exclusivamente a la ejecución de las actividades de la organización y puede ser utilizado por el colaborador para realizar las funciones establecidas para su cargo. Queda prohibido al personal descargar programas que realicen conexiones automáticas, del mismo modo la descarga de música y videos no es una práctica permitida.

IMARPE
J. CASTILLO

IMARPE
Oficina General de Asesoría Jurídica
C. MORENO

INSTITUTO DEL MAR DEL PERÚ
SECRETARÍA GENERAL
G. CAÑOTE

6.6 Criptografía

6.6.1 Desarrollar e implantar mecanismos para el uso de controles criptográficos para la protección de información con el objetivo de salvaguardar la confidencialidad, integridad/autenticidad, no repudio y autenticación.

6.6.2 toda información a ser transportada en medios magnéticos, dispositivos móviles o removibles y líneas de comunicación tiene que ser cifrada.

6.6.3 Gestionar las claves criptográficas y la recuperación de información cifrada para los casos de claves perdidas, comprometidas o dañadas.

6.6.4 Asignar funciones y responsabilidades de quienes implementan los procedimientos y gestionan las claves.

6.7 Seguridad Física de las instalaciones

La entidad dispondrá las medidas de seguridad física en sus instalaciones que sean necesarias y adecuadas para proteger su información, contra riesgos que atenten contra su confidencialidad, integridad y disponibilidad.

6.7.1 Seguridad asociada a las instalaciones

a) Se debe asegurar el perímetro de seguridad para el ingreso a las instalaciones, así como definir los límites de acceso a las áreas de seguridad de información relevante y las personas encargadas de su custodia y acceso.
b) Contar con dispositivos de seguridad física e informática, así como alarmas contra incendios tanto para las áreas de procesamiento de información como salas de cómputo o cuartos de comunicaciones.
c) Las áreas de procesamiento de información deben estar físicamente en ambientes definidos para el personal autorizado y aparte aquellas áreas gestionadas por personal externo.
d) Se debe restringir el acceso a personas ajenas a la entidad, a mecanismos de información que identifiquen ubicaciones de instalaciones sensibles de procesamiento de la información.
e) Se debe evitar que la información o actividad de carácter confidencial sea de fácil acceso a personas ajenas o no autorizadas.

6.7.2 Seguridad asociada a los equipos de la entidad

Los equipos deben ubicarse o protegerse en lugares adecuados para reducir los riesgos ocasionados por amenazas y accesos no autorizados; y se debe considerar:

a) Todo usuario debe ubicar su equipo de cómputo en un lugar adecuado y seguro que minimice el riesgo de acceso.

IMARPE Oficina Funcional de Informática y Estadística M. ALMENGOR R.

IMARPE Oficina General de Planeamiento y Presupuesto W. HUERTA

IMARPE Oficina General de Planeamiento y Presupuesto J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica C. MORENO

Instituto del Mar del Perú Secretaría General G. CAÑOTE

b) Se debe implementar controles a todo tipo de tratamiento de la información a través de activos físicos para reducir el riesgo de amenazas a la seguridad de la información.
c) Debe estar estrictamente prohibido la ingesta de alimentos en las áreas identificadas para los activos de procesamiento de información.
d) Verificar que las condiciones de temperatura y humedad no afecten negativamente el funcionamiento de todos los activos físicos informáticos.

6.8 Seguridad de las operaciones

Las actividades de gestión sobre los recursos de tecnología de información de la entidad son esenciales para el buen funcionamiento de los servicios de esta Institución, se debe mantener documentados y actualizados los procedimientos operativos informáticos, controlar y documentar los cambios previamente autorizados sobre la plataforma tecnológica y efectuar una separación de tareas y áreas de responsabilidad.

Se deben aplicar medidas efectivas de protección para el software utilizado en los sistemas informáticos de cómputo y la información que estos procesan; de igual forma proteger la información transmitida por sistemas de comunicación de datos en la red interna de la entidad tales como el correo electrónico institucional y en los intercambios de información con otras entidades externas.

M. ALMENGOR R.

6.9 Respaldo de la información (Backups)

6.9.1 Se debe efectuar respaldo de la información, softwares de aplicación, y programar periódicamente su restauración, revisarlos y actualizarlos regularmente.

W. HUERTA

6.9.2 Realizar respaldos de información exacta y completa y realizar un procedimiento de restauración con un grado y frecuencia que se ajuste a los requisitos de la entidad.

6.9.3 Los respaldos deben almacenarse en un lugar que garantice la seguridad de la información, apartado y a distancia, que salvaguarde de daños físicos ante un desastre en su sede principal.

J. CASTILLO

6.9.4 Realizar procedimientos de contingencia y alta disponibilidad de los activos de información a fin de garantizar la continuidad de los servicios.

6.9.5 Realizar pruebas de respaldo y restauración de información para asegurar su confiabilidad y contingencia en casos de emergencia.

C. MORENO

6.9.6 Proteger el respaldo por medios cifrados para garantizar su confidencialidad.

G. CAÑOTE

6.10 Seguridad de las comunicaciones

Para el transporte o remisión de información, la entidad dispondrá las medidas de seguridad en los dispositivos tecnológicos o documentos en forma física de tal manera que solo sea emitida y recibida por las personas o entidades a las cuales se les debe proporcionar la información en el momento y lugar oportunos.

6.10.1 Gestión de la seguridad de la red de datos

a) Tener el Control de las redes protegiendo la información en los sistemas y aplicaciones.
b) Establecer las responsabilidades y procedimientos para la gestión y control de los equipos, de manera remota.
c) Establecer controles para salvaguardar la confidencialidad y la integridad de los datos en las redes, protegiendo los sistemas interconectados.
d) Validar las políticas de seguridad de dominio institucional a fin de asegurar que los controles de seguridad se apliquen en toda la estructura organizacional.
e) Contar con acuerdos de servicios de red relacionados con el proveedor interno y proveedor externo.

IMARPE Área Funcional de Informática y Estadística
M. ALMENGOR R.

6.10.2 Transferencia de Información

Implementar procedimientos y controles para proteger el intercambio de información considerando lo siguiente:

a) Proteger toda transferencia de información de la intercepción, reproducción, modificación, desviación y/o destrucción.
b) Detectar y proteger la red de datos que pueda ser vulnerada por software malicioso (virus, Hackers).
c) Proteger la información que se transmite vía correo electrónico; además de los datos adjuntos.
d) El uso de medios de comunicación electrónica, tales como correo electrónico, repositorios digitales u otros, es de entera responsabilidad del personal que emplea estos medios, a fin de no comprometer a la entidad.
e) Hacer uso de técnicas criptográficas, para proteger la confidencialidad, integridad y autenticidad de la información.
f) Implementar controles y restricciones para detectar los reenvíos de información que puedan afectar la imagen institucional.
g) Aplicar mecanismos que puedan restringir al personal revelar información sensible o confidencial de la entidad.

IMARPE Oficina General de Administración
W. HUERTA

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

6.11 Adquisicion, desarrollo y mantenimiento de los sistemas

Determinar los requisitos de seguridad para todos los sistemas de información de la entidad, los cambios de los sistemas informáticos existentes desarrollados por la entidad o por terceros, estos deben incluir

INSTITUTO DEL MAR DEL PERÚ Secretaría General
G. CAÑOTE

las verificaciones del proceso correcto de las aplicaciones, protección del código fuente y datos en producción.

Los nuevos sistemas a desarrollar y/o actualizar deben cumplir el ciclo de vida de desarrollo de software, desde su requerimiento hasta su validación, así como la aceptación formal por parte de los usuarios solicitantes antes de su puesta en producción. Los cambios en las aplicaciones y en el ambiente de producción deben ser controlados adecuadamente, a fin de minimizar el riesgo en el procesamiento de la información.

6.12 Relación con los proveedores

6.12.1 Seguridad de la información en relación con los proveedores

Debe restringirse el acceso de los proveedores a la información y los activos de la entidad, estos controles también deben incluir:

a) Identificar y evaluar a los proveedores, determinando los niveles a los que permitirá su acceso a la información, monitoreando y controlando periódicamente sus actividades.
b) Definir los requisitos mínimos para el acceso y manipulación de acuerdo a la clasificación de seguridad de la información
c) Efectuar controles de precisión y exhaustividad para garantizar la integridad de la información o del proceso de generación de información proporcionada por cualquiera de las partes.
d) Definir las funciones y obligaciones a los proveedores para proteger la información de la entidad.
e) Determinar acuerdos de recuperación y contingencia que permitan asegurar la disponibilidad de la información proporcionado por cualquiera de las partes.

6.12.2 Gestión de prestación del servicio del proveedor

a) Monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.
b) Supervisar los niveles de desempeño del servicio para comprobar el cumplimiento de los acuerdos.
c) Efectuar auditorías periódicas a los proveedores, efectuando el seguimiento de los posibles problemas identificados.
d) Verificar que el proveedor cuenta con las capacidades y experiencia relacionado con los requerimientos solicitados, a fin de garantizar los niveles de continuidad de servicio.

6.13 Gestión de incidentes de seguridad de la Información

6.13.1 El personal, proveedores de servicios y terceros, deben reportar todo tipo de incidencias que afecten la seguridad de la información a través de los canales de gestión.

IMARPE Área Funcional de Informática
M. ALMENGOR R.

IMARPE Oficina de Secretaría General
W. HUERTA

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

INSTITUTO DEL MAR DEL PERÚ Secretaría General
G. CAÑOTE

6.13.2 Todo el personal independientemente del vínculo laboral con la Institución debe conocer sus funciones y responsabilidades, así como los procedimientos para reportar cualquier evento de seguridad de información.

6.13.3 Concientizar al personal de que cualquier comportamiento anómalo de los sistemas pueden ser señal de un ataque a la seguridad por lo tanto deben ser reportados como una acción de prevención de seguridad de la información y no intentar probar supuestas debilidades que pudieran vulnerar la seguridad Institucional.

6.13.4 Llevar un registro de los resultados de la evaluación de los reportes de incidentes de riesgo de seguridad, así como la acción tomada para futuras referencias y verificaciones para reducir la probabilidad o el impacto de futuros incidentes.

6.13.5 Responder a los incidentes de seguridad de la información de acuerdo con los procedimientos establecidos para cada caso.

6.13.6 Definir y aplicar procedimientos para la identificación, recolección y conservación de la información que pueda servir como evidencia en una acción disciplinaria y/o legal contra alguna persona que cometió faltas contra la seguridad de la información.

6.13.7 El IMARPE tiene derecho a recopilar información como evidencia que involucre acciones por temas legales o de inconductas disciplinarias que afecten la seguridad de la información.

6.14 Aspectos de Seguridad de la Información en la gestión de continuidad del negocio

El Imarpe asegurará que la confidencialidad, integridad y disponibilidad de su información no se vea afectado por un hecho catastrófico de origen natural o por factores humanos.

6.14.1 Continuidad de la seguridad de la información

a) Determinar los requisitos y la continuidad de la gestión de seguridad de la información en situaciones adversas.
b) Establecer el plan de continuidad de la seguridad de la información que esté incluida dentro del proceso de gestión de continuidad del negocio y/o en el proceso de gestión de recuperación ante desastres.
c) En caso de no haber un Plan de Continuidad del Negocio, la gestión de la seguridad de la información debe asumir que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas en comparación a las situaciones normales.

IMARPE Área Funcional de Informática y Estadística
M. ALMENDRA R.

IMARPE Oficina General de Administración
W. HUERTA

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

Instituto del Mar del Perú Notaría General
G. CAÑOTE

d) El Imarpe debe establecer, documentar, implantar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.

e) Establecer una estructura de gestión adecuada para estar preparados para mitigar y responder a un evento disruptivo utilizando personal con la autoridad, experiencia y competencia necesarias.

f) Se debe designar personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para atender un incidente y garantizar la seguridad de la información.

g) Desarrollar y aprobar los planes documentados, los procedimientos de respuesta y recuperación, detallando cómo la entidad va a atender un evento disruptivo y mantener la seguridad de la información en un nivel predeterminado, basado en los objetivos de continuidad de seguridad de la información aprobados.

h) Establecer, documentar, implementar y mantener:
- Los controles de seguridad de la información dentro de los procesos, procedimientos y sistemas de apoyo y herramientas de continuidad del negocio o de recuperación ante desastres.
- Los procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

M. ALMENGOR R.

6.14.2 Redundancias de Datos

Implementar las instalaciones de procesamiento de información con la redundancia necesaria para cumplir con los requisitos de disponibilidad.

W. HUERTA

6.15 Cumplimiento

6.15.1 Cumplimiento de los requisitos legales y contractuales

a) Identificar, documentar y actualizar los requisitos legales, reglamentarios, contractuales relevantes para cada sistema de información de la entidad.

b) Definir, supervisar y actualizar todos los controles y responsabilidades individuales del personal.

c) Definir los derechos de propiedad intelectual y el uso de los productos de software patentados tomando en consideración lo siguiente:
- Asegurar el cumplimiento de los derechos de propiedad
- intelectual y el uso legal de los productos de software e información Institucional.

J. CASTILLO

C. MORENO

G. CAÑOTE

- Adquirir software o licenciamientos en cumplimiento al Decreto Supremo N° 013-2003-PCM y su modificatoria mediante Decreto Supremo N° 076-2010-PCM, que busca garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.
- Mantener un registro apropiado de activos protegidos por el derecho de propiedad intelectual.
- Efectuar revisiones para asegurar que solo serán instalados productos de software autorizados y con licencia.
- No duplicar, ni convertir a otro formato o extraer información de las grabaciones comerciales (video, audio) que contravengan el derecho de autor, con excepción de lo permitido por los derechos de reproducción.
- Prohibido efectuar la reproducción total o parcial de libros, artículos, informes u otros documentos, con excepción de lo permitido por los derechos de reproducción.
- Informar a todo el personal, las consecuencias a la infracción de derechos de Reproducción, las cuales pueden conducir a acciones legales que impliquen procedimientos judiciales.

d) Proteger los registros contra pérdida, destrucción, falsificación, accesos y divulgación de información no autorizada en concordancia con las normas legales establecidas; así como las disposiciones regulatorias y contractuales que la entidad establezca.

e) Emitir directivas que establezcan procedimientos sobre la retención, almacenamiento, tratamiento y eliminación de los registros de información.

f) Garantizar el derecho fundamental de protección de Datos Personales en estricto respeto a la privacidad de las personas dentro del marco legislativo de la Ley N° 29733 "Ley de Protección de Datos personales".

6.15.2 Revisiones de la seguridad de la información

a) El proceso de gestión de seguridad de la información debe revisarse de forma independiente a intervalos planificados, cuando se producen cambios significativos o cuando se sospeche que se haya producido alguna vulnerabilidad.

b) En casos de incidencias en la seguridad de la información, es el oficial de seguridad quien efectuará la evaluación y revisión de las incidencias.

c) Se deben registrar las acciones y resultados de la revisión efectuada, las mismas que serán comunicadas a las áreas auditadas.

M. ALMENGOR R.

W. HUERTA

J. CASTILLO

C. MORENO

G. CAÑOTE

d) Los Directores Generales y Jefes de Oficina deben revisar regularmente el cumplimiento de las normas establecidas para la seguridad y procesamiento de la información dentro de su área de responsabilidad.

e) En caso de detectarse incidencias por incumplimiento o vulnerabilidad de las normas de seguridad de la información, los Directores y/o Jefes de Oficina responsables deben:

- Comunicar al Oficial de Seguridad de la Información
- Identificar la información que ha sido afectada, su importancia e implicancias para la Institución.
- Identificar las causas del incumplimiento de las normas
- Evaluar las acciones necesarias que corrijan las vulnerabilidades y lograr su cumplimiento.
- Implementar las acciones correctivas apropiadas.
- Supervisar la acción correctiva tomada para comprobar su eficacia, efectuar la reevaluación de las acciones implementadas para identificar y evitar posibles nuevas deficiencias y debilidades.

VII. ROLES Y RESPONSABILIDADES

Para el cumplimiento de la presente Política de Seguridad de la Información en el IMARPE, se establecen las siguientes funciones:

7.1 Director(a) Ejecutivo(a) Científico(a)

El o la Director(a) Ejecutivo(a) Científico(a) de la entidad a través del Comité demuestra su compromiso con el Sistema de Gestión de Seguridad de la Información y además debe:

7.1.1 Nombrar al Comité de Gestión de Seguridad de la Información de la entidad y al Oficial de Seguridad de la Información.

7.1.2 Aprobar y Disponer la publicación y distribución de la Política de Seguridad de la Información, aprobar sus modificatorias a propuesta del Comité de Gestión de Seguridad de la Información de la entidad.

7.1.3 Definir las funciones, asignar responsabilidades y la rendición de cuentas y, delegar autoridad y responsabilidad a cada una de las Oficinas para el cumplimiento de la Política.

7.1.4 Asegurar la disponibilidad de los recursos (humanos, de infraestructura, financieros y tecnológicos), mediante la aprobación del presupuesto anual de los proyectos relacionados con el SGSI.

IMARPE Área Funcional de Informática y Estadística
M. ALMENGOR R.

IMARPE Oficina General de Planeamiento, Presupuesto y Modernización
W. [illegible]ATA

IMARPE Oficina General de Planeamiento, Presupuesto y Modernización
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

INSTITUTO DEL MAR DEL PERÚ Secretaría General
G. CAÑOTE

7.2 Comité de Gestión de Seguridad de la Información

El Comité de Gestión de Seguridad de la Información del Instituto del Mar del Perú tiene las siguientes funciones y responsabilidades:

7.2.1 Proponer la política de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y Regulación en el ámbito de seguridad de la información.

7.2.2 Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.

7.2.3 Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información.

7.2.4 Difundir a todo el personal la importancia de una efectiva gestión de seguridad de la información.

7.2.5 Supervisar y evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.

7.2.6 Revisar anualmente la Política de Seguridad de la Información o cuando se realice cambios significativos que impacten en los objetivos de la institución en aspectos técnicos y legales; así como formular proponer las modificaciones que correspondan para su adecuación y aprobación del Director Ejecutivo Científico.

7.2.7 Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

7.3 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información será responsable de:

7.3.1 Elaborar propuestas y gestionar la aprobación de las políticas, normas, procedimientos y estándares relativos a la seguridad de la información de la entidad.

7.3.2 Proponer al Comité de Gestión de Seguridad de la Información, la Directiva de detalle que viabilice la aplicación de las Políticas de Seguridad, así como las acciones, responsabilidades y medidas de seguridad que permitan mantener la integridad, confidencialidad y disponibilidad de la información de la Institución.

7.3.3 Proponer y coordinar con el Comité el análisis y evaluación de riesgos de los activos de información.

7.3.4 Supervisar el cumplimiento e implementación de las políticas.

IMARPE Área Funcional de Informática y Estadística
M. ALMENGOR R.

IMARPE Oficina General de Planeamiento y Presupuesto
W. [illegible]

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

INSTITUTO DEL MAR DEL PERÚ Secretaría General
C. CAÑOTE

7.3.5 Monitorear las incidencias a fin de minimizar los riesgos de los activos de información de la entidad.

7.3.6 Monitorear la efectividad y eficiencia de los controles implementados para la protección de los activos de información.

7.3.7 Solicitar, proponer y efectuar auditorías internas del SGSI.

7.3.8 Efectuar el seguimiento de las acciones correctivas y preventivas realizadas.

7.3.9 Informar al Comité de Seguridad sobre cualquier incidente, vulnerabilidad o exposición de la información que represente un riesgo para la seguridad organizacional.

7.3.10 Programar charlas de concientización y sensibilización sobre la importancia de la Seguridad de la Información.

7.3.11 Otros que considere necesario el Comité de Seguridad de Información.

IMARPE ÁREA FUNCIONAL DE INFORMÁTICA Y ESTADÍSTICA
M. ALMENGOR R.

7.4 Responsables de Activos

La Entidad debe definir a través de la normativa a los responsables de los activos de la Información:

7.4.1 Disponer las medidas adecuadas para la custodia de la información de su responsabilidad.

7.4.2 Participar en los procesos de identificación y clasificación de activos de información.

IMARPE OFICINA DE ADMINISTRACIÓN
W. HUERTA

7.4.3 Mantener actualizado el inventario de activos que se encuentran bajo su responsabilidad.

7.4.4 Autorizar la asignación de accesos sobre la información.

7.5 Responsables de Riesgos

El Comité debe definir a través de la normativa a los responsables de riesgos de la Información:

IMARPE OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO
J. CASTILLO

7.5.1 Decidir el criterio para la aceptación de riesgos de seguridad de la información y los niveles de riesgos aplicables.

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

7.5.2 Identificar los riesgos asociados a la seguridad de la información inherente a su gestión, según los lineamientos y políticas de la entidad, así como solicitar el apoyo de las Direcciones y Oficinas pertinentes para evaluar dichos riesgos y establecer medidas de mitigación.

INSTITUTO DEL MAR DEL PERÚ SECRETARÍA GENERAL
G. CANOTE

7.6 Personal de la entidad

Con respecto al Sistema de Gestión de Seguridad de la Información, es responsable de:

7.6.1 Conocer, comprender y cumplir las políticas y procedimientos de seguridad de la información del IMARPE.

7.6.2 Notificar los incidentes y riesgos a la seguridad de la información a su jefe inmediato superior y/o al Oficial de Seguridad de la Información.

7.6.3 Utilizar la información, sistemas y todos los recursos de la entidad únicamente para los propósitos Institucionales e inherentes a la función asignada.

7.6.4 Mantener la confidencialidad e integridad de la información que se procesa en la entidad.

7.6.5 Reportar incumplimientos o vulnerabilidades del sistema de seguridad de la información.

7.7 Directores y/o Jefes

Con respecto al Sistema de Gestión de Seguridad de la Información, adicionalmente a las funciones que les corresponden como personal, tienen las siguientes responsabilidades:

7.7.1 Fomentar la difusión y el cumplimiento de las políticas y procedimientos de seguridad de la información de la entidad al personal bajo su cargo, para asegurarse que las conozcan y comprendan que los incumplimientos de las mismas podrían resultar en una acción disciplinaria y/o Legal.

7.7.2 Gestionar con el Oficial de Seguridad de la Información las acciones necesarias que permitan asegurar que la información y recursos bajo su responsabilidad se encuentren debidamente protegidos con las medidas de seguridad adecuadas.

7.7.3 Apoyar y facilitar las revisiones periódicas de acciones para la verificación del cumplimiento de las políticas y procedimientos de seguridad de la información.

7.7.4 Determinar los criterios y niveles de acceso a la información bajo su responsabilidad.

7.7.5 Informar al oficial de seguridad el cambio de función/ubicación de cualquier personal de la entidad sea por reasignación o retiro, con la finalidad de modificar o cancelar sus accesos a la información.

7.7.6 Establecer la prioridad de la información y los niveles mínimos de servicio al recuperar información en casos de desastres.

IMARPE Área Funcional de Informática y Estadística
M. ALMENGOR R.

IMARPE Oficina General de Asesoría Jurídica
W. HUERTA

IMARPE Oficina General de Planeamiento y Presupuesto
J. CASTILLO

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

Instituto del Mar del Perú Secretaría General
G. CAÑOTE

7.7.7 Reportar inmediatamente el incumplimiento o infracciones a las políticas y normas de seguridad.

7.8 Área Funcional de Recursos Humanos

Con respecto al Sistema de Gestión de Seguridad de la Información, adicionalmente a las funciones que le corresponden como Área, tienen las siguientes:

7.8.1 Proveer el primer nivel de conocimientos respecto a los temas de seguridad de la información a todo el nuevo personal que se incorpore a la Institución.

7.8.2 Incluir dentro de la inducción a todos los niveles de la entidad charlas sobre la importancia de la seguridad de la información manejada en sus puestos de trabajo.

7.8.3 Coordinar con los Directores Generales, Jefes de Oficina y el Oficial de Seguridad de la Información las acciones necesarias para actualizar la información del personal y los cambios de puestos de trabajo y de funciones del personal.

7.8.4 Las actividades bajo su administración que requieran contratos CAS y con terceros, cuenten con cláusulas que aseguren el cumplimiento de la normatividad para la gestión de riesgos de seguridad de la información.

IMARPE ÁREA FUNCIONAL DE INFORMÁTICA Y ESTADÍSTICA
M. ALMENGOR R.

7.9 Coordinador del Área Funcional de Informática y Estadística

Adicionalmente a las responsabilidades que le corresponden como personal de la entidad, debe tener presente las siguientes funciones y responsabilidades:

IMARPE OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO
W. HUERTA

7.9.1 Definir los niveles de seguridad de la información en coordinación con el Oficial de Seguridad de la Información al inicio de la adquisición, desarrollo y modificación de aplicativos.

IMARPE OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO
J. CASTILLO

7.9.2 Asegurar que los requerimientos y proyectos se realicen usando métodos, técnicas y procedimientos para mantener la seguridad de la información, garantizando de ese modo la confidencialidad, integridad y disponibilidad de los sistemas de información. Esto incluye la ejecución de proyectos relacionados con la mejora de la seguridad de la información.

7.9.3 Efectuar respaldo de la información, así como establecer procesos de recuperación de información.

IMARPE Oficina General de Asesoría Jurídica
C. MORENO

IMARPE SECRETARÍA GENERAL
G. CAÑOTE

7.9.4 Gestionar y monitorear el adecuado mantenimiento de los equipos de procesamiento, almacenamiento y transmisión de información, así

como la conservación de los dispositivos magnéticos utilizados para los respaldos de información.

7.10 Oficina General de Asesoría Jurídica

Adicionalmente a las funciones que le corresponden como Oficina de la entidad, tiene las siguientes responsabilidades:

7.10.1 Mantener informado al Oficial de Seguridad de la Información, las nuevas leyes o las modificaciones a las ya existentes relacionadas a delitos contra el mal uso de la información, delitos informáticos, ley de protección de datos personales y toda aquella regulación relacionada a seguridad de la información a la que esté afecta la entidad.

7.10.2 Establecer un modelo de contrato para los servicios tercerizados y/o la contratación de personal, que incluyan cláusulas que obliguen al proveedor / personal a que sus servicios no afecten la confidencialidad, integridad y disponibilidad de la información de la entidad. En los casos de servicios ya contratados, se deberá definir un modelo de adenda donde se especifiquen las cláusulas anteriormente mencionadas, los cuales deberán ser enviados a los responsables de la contratación.

M. ALMENGOR R.

VIII. GLOSARIO DE TERMINOS

a) **Activo de Información.** - Conocimientos o información que tienen valor para la entidad.

W. HUERTA

b) **Seguridad de la Información.** - Preservación de la confidencialidad, integridad y disponibilidad de la información.

c) **Sistema de Gestión de Seguridad de la Información (SGSI).** - Parte del sistema de gestión global, basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

J. CASTILLO

d) **Riesgo de Seguridad de la Información.** - Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la entidad.

e) **Integridad.** - Propiedad de salvaguardar la exactitud y completitud de los activos.

f) **Sistema de Gestión.** - Marco de políticas, procedimientos, guías y recursos asociados para lograr los objetivos de la entidad.

C. MORENO

g) **Políticas.** - Intenciones globales y orientación expresadas formalmente por la Alta Dirección.

G. CAÑOTE

h) **Acción Preventiva.** - Acción adoptada para eliminar las causas de una no conformidad potencial u otra situación indeseable.

i) **Procedimiento.** - Forma específica de llevar a cabo una actividad o un proceso.

j) **Registro.** - Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas.

k) **Riesgo.** - Es la probabilidad que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.

l) **Aceptación del Riesgo.** - Decisión de aceptar un riesgo.

m) **Análisis del Riesgo.** - Uso sistemático de la información para identificar fuentes y estimar el riesgo.

n) **Gestión del Riesgo.** - Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

o) **Cifrado.** - Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada solo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.

p) **Datos personales.** - Son aquellos que identifican directa o indirectamente a una persona natural (titular de los datos): nombre, fecha de nacimiento, dirección o domicilio y de correo electrónico; número de DNI, RUC, Telefonía fija y celular, seguro social y placa de vehículo; imagen; firma electrónica; y otros datos no sensibles establecidos en los formularios aprobados con Resolución Directoral N° 001-2013-JUS/DGPDP (08 de mayo de 2013).

q) **Datos personales sensibles.**- Son aquellos que pueden ser objeto de tratamiento con el consentimiento expreso y por escrito de la persona natural(titular de los datos) y, por lo tanto, requieren especial protección: datos biométricos (huella dactilar o digital, retina, iris); datos de origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; datos relacionados a la salud o a la vida sexual; y hechos o circunstancias de la vida afectiva o familiar.

r) **Controles criptográficos.** - Son aquellos controles que protegen la confidencialidad e integridad de la información electrónica durante su procesamiento, almacenamiento o transmisión y que comprueban la identidad de quienes acceden a esta.

s) **Usuario Final.** - Son todos los usuarios reconocidos por la entidad y a quienes se le proporciona accesos a la red de información.

IMARPE
M. ALMENGOR R.

IMARPE
W. HUERTA

IMARPE
J. CASTILLO

IMARPE
G. MORENO

IMARPE
G. CAÑOTE

t) **Estaciones de Trabajo.** - Equipo de cómputo asignado a un usuario que se encuentra asociado al dominio institucional.

u) **Teletrabajo.** - Acción de operar la información de modo remoto fuera de la entidad.

v) **Riesgos residuales.** - Es aquel riesgo que subsiste, después de haber implementado controles.

w) **Tratamiento del riesgo.** - Proceso de selección e implementación de medidas para modificar el riesgo.

x) **Evento de seguridad de la Información.** - Es una ocurrencia identificada en un sistema, servicio, o red la cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

y) **Incidente de seguridad de información.** - Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de la entidad y de amenazar la seguridad de la información.

z) **Tratamiento del riesgo.** - Proceso de selección e implementación de medidas para modificar el riesgo.

IMARPE
M. ALMENGOR R.

IMARPE
W. HUERTA

IMARPE
J. CASTILLO

IMARPE
Oficina General de Asesoría Jurídica
C. MORENO

INSTITUTO DEL MAR DEL PERÚ
SECRETARÍA GENERAL
G. CAÑOTE